Risk-based Verification of Large Offshore Systems

J. Wang, B. Matellini, A. Wall
Liverpool Logistics, Offshore and Marine (LOOM) Research Institute
School of Engineering, Technology & Maritime Operations,
Liverpool John Moores University, Liverpool, UK

J. Phipps
ABS Consulting Ltd, Warrington, UK

Abstract

This paper firstly gives a very brief review on the current status of offshore safety with particular reference to the UK sector. The risk-based verification concept is then described. Following the identification of the research needs, a general risk-based verification framework is proposed with appropriate risk assessment contents incorporated into it. An example is then followed to demonstrate the proposed framework. The THESIS (The Health, Environment and Safety Information System) software package is also used to facilitate the implementation of the framework. In the end both benefits and limitations of risk-based verification in offshore applications are highlighted. The emphasis of the paper is focussed on industrial applications.

Keywords: Offshore installations, offshore safety, risk-based verification, safety-critical elements.

List of Acronyms and Abbreviations

ABS:	American Bureau of Shipping
ALARP:	As Low As Reasonably Practicable
API:	American Petroleum Institute
BOP:	Blow Out Preventor
CR:	Consequence Rating
DCR:	Offshore Installation and Wells (Design and Construction, etc) Regulations
DH:	Duty Holder
DNV:	Det Norske Veritas
ESD:	Emergency Shutdown
GBT:	Gravity Base Tank
HAZID:	Hazard Identification
HMR:	Hazard Management Rating
HSE:	Health Safety Executive
HVAC:	Heating, Ventilation and Air Conditioning
ICP:	Independent Competent Person
L:	Likelihood
LR:	Lloyd's Register
MAE:	Major Accident Event
MAH:	Major Accident Hazard
MODU:	Mobile Offshore Drilling Unit
PA:	Public Announcement
PDQ:	Production and Quarters
PFEER:	Prevention of Fire and Explosion and Emergency Response
PMS:	Preventive Maintenance System
QRA:	Quantitative Risk Assessment

RBV: Risk-based Verification
S: Severity
SCEs: Safety Critical Elements
SCR: Safety Case Regulations
SMS: Safety Management System
SOLAS: International Convention for Safety of Life at Sea
THESIS: The Health, Environment and Safety Information System
TR: Temporary Refuge
VS: Verification Scheme

1. INTRODUCTION

In response to the accepted findings of the *Piper Alpha* enquiry, the Offshore Installations (Safety Case) Regulations (SCR) were introduced in the UK's offshore sector in 1993. An installation cannot legally operate without an accepted operational safety case [Wang, 2006]. The Safety Case Regulations were amended in 1996 to include verification of Safety-Critical Elements (SCEs). The Offshore Installations and Wells (Design and Construction, etc.) Regulations 1996 (DCR 1996) were introduced to deal with various stages of the life cycle of the installation [Health and Safety Executive (HSE), 1996]. The Duty Holder (DH) (i.e. the operator of a fixed installation or the owner of a mobile installation) shall ensure that an installation at all times possesses such integrity as is reasonably practicable [HSE, 1996c]. The DH shall also ensure that the installation is composed of materials which are suitable, and so far as is reasonable practicable, sufficiently proof against or protected from anything liable to prejudice its integrity [HSE, 1996c]. The main feature of the new offshore safety regulations in the UK in particular and worldwide in general is the absence of a prescriptive regime defining specific duties of the operator and specification as regard to what are adequate means [Wang & Kieran, 2000].

Proactive risk assessment processes have been used by the offshore industry in many countries worldwide. Different countries have their own regulatory regimes and often adopt different techniques although the tendency is to use a proatice risk-based approach. Offshore safety regulations in many overseas countries have their characteristics. For example, Brazil's regulations are largely dominated by Petrobras standards while in West Africa such regulations are heavily influenced by deep water developments by British/American/African companies. Terms/definitions are used differently worldwide. For example, UK and many EU countries accept the use of the term "safety case" while the USA may prefer to use the term "risk assessment".

Risk-Based Verification (RBV) plays an important role in maintaining a required level of safety in the life cycle of an offshore installation. It provides a cost-effective solution in facilitating a risk-based regime in the offshore industry. It can be used to help implement offshore safety regulations through minimizing resources and efforts available.

2. FUNDAMENTALS OF VERIFICATION

Verification and validation are often used in a mixed way in engineering design and operation. It is arguable to say that verification ensures the system is designed to deliver all functionality to the user and it typically involves reviewing to evaluate documents, plans, code, requirements and specifications. Verification is usually done with checklists, issues lists, and walkthroughs and inspection meetings. On the other side, validation ensures that the defined functionality is the intended behaviour of the system and it typically involves actual testing and takes place after verifications are completed. However, in this paper verification is used in a general way and is

defined as a continuous and systematic process by which the pre-defined components of an asset are checked and examined to ensure that they conform to the standards which define their operability.

In the context of the offshore environment, verification of SCEs is required to be undertaken by the operator (i.e. a DH), for the life of an installation, from design and construction through to operation and ultimately decommissioning. SCEs are determined through hazard analysis and risk assessment.

Verification aims at providing a systematic and independent examination of the various lifecycle phases of an asset to determine if it satisfies the associated performance specification. It also aims at identifying errors or failures in the work associated with the asset and contributing to reducing the risks to the operation of the asset. It is not used to replace any statutory offshore safety requirements, instead it is complementary to them. It is highly possible that the verification process will duplicate some work that has been carried out previously by other parties involved in the asset or system. Verification is normally undertaken using a suitable written scheme called a Verification Scheme (VS), which is put into effect to ensure that SCEs are suitable and remain in good repair and condition.

The traditional way of verifying the performance of an offshore system is prescriptive in nature. Prescriptive regulations specify rules of action that must be explicitly followed in order to comply with regulation. Possible issues associated with such a prescriptive method are:

1. It is usually difficult to ensure the cost-effectiveness in a way that available resources are rationally allocated to areas with different risk levels.
2. It does not motivate or allow the duty holder to make use of the latest developments in technology to optimise safety in both design and operation. A prescriptive regime tends to encourage a passive attitude among the companies. The authorities become in some sense a guarantor to ensure that safety in the industry is adequate.
3. It usually conveys the minimum requirements for safe design and operation.

A risk-based approach has been used in high technology industries such as the aviation sector for many years. It has been increasingly used in the offshore industry in order to justify any decisions to be made in design and operation. A risk-based approach can [Wang, 2006]:

1. Improve the performance of the system and ensure that new design/operation strategies are efficient ones.
2. Ensure that experience obtained can be used in the current system and new systems.
3. Provide a mechanism for predicting and controlling the high risk scenarios with the available resources in a cost-effective way.

2.1 Definitions

Independent Competent Person (ICP): This is a person (or body) appointed by the DH to act for a particular asset. The responsibilities of the ICP may include:

- Reviewing and commenting on the SCEs.
- Reviewing the Verification Scheme to ensure that all mandatory elements required by the legislation have been included within the scheme.
- Providing comment on the Performance Standards established for the SCEs.

- Undertaking activities offshore and onshore as required by the Verification Scheme.
- Careful and critical scrutiny to determine compliance with the Performance Standards.
- Issuing all relevant reports and remedial action recommendations.
- Keeping the Verification Scheme under review.

The ICP will:

- Be recognized as an organization providing this type of service.
- Have adequate resources to ensure that the requirements will be delivered on time and to the right quality.
- Have systems in place to manage the delivery of the Verification Scheme requirements.

Individuals employed as ICPs to performing activities under the scheme will be required to have:

- Recognized qualifications and relevant experience relating to the SCE discipline.
- Demonstrable knowledge of the goal-setting legislative regime, major hazard management and appreciation of risk assessment techniques.
- Independence from the management system governing responsibility for carrying out actions of survey, inspection or test of items covered by the Verification Scheme.
- No current or previous responsibility for any items that might compromise their objectivity in carrying out verification activities.

Performance Standard: This defines the standards and measures of how something/someone must perform, typically in terms of functionality, availability, reliability, etc.. It can be qualitative, quantitative, or both in terms of the performance required of a system, an item of equipment, a person or a procedure. It could have been set for almost everything in the design. It can be used as the basis for managing hazards through the life cycle of the installation.

Performance Standards are generated for all SCEs identified and shall provide assurance that SCEs are, and remain suitable for their intended purpose. The standards must enable the SCEs to be verified as suitable and remaining in good repair and condition and thereby provide assurance that the level of safety set out in the Safety Case (i.e. risk assessment) will exist throughout the life cycle of the asset.

One or more key parameters are identified which, together, ensure that the individual goal of a SCE is achieved. Some are verified in design while others are verified by actual measurements. These actual measurements are the performance measures. Performance Standards are initially established in the design phase of the development by competent persons within design. Subsequently to ensure that the Performance Standards are maintained through the operations, a scheme of testing and inspection is developed to and implemented to demonstrate that such Standards would be achieved. The nature of such Performance Standards means that they will form part of the installation maintenance and inspection procedures for the systems concerned.

*Safety Critical Elements (*SCEs): These are defined as the systems, equipment and structural items that could result in, control, or mitigate the effects of a major hazard. A definition of SCEs as given in the UK Safety Case Regulations (SCR) states:

“Safety Critical Elements means such parts of the installation and such of its plant including programs, or any part thereof:

- the failure of which could cause or contribute substantially to; or

- a purpose of which is to prevent, or limit the effect of, a major accident."

SCEs are normally defined at a system level. Within the Performance Standards a further breakdown into specific sub-systems is applied when considered necessary. SCEs relate to structure, plant, equipment, systems etc., but they should exclude procedures or management systems.

In verification, the SCEs are checked and examined to ensure that they conform to the Performance Standards which define their operability. The Verification Scheme produced would have to, in order to be regarded as a suitable written scheme, give assurance that the SCEs:

- Are suitable and fit for purpose.
- Remain in good repair and condition.

In this context, "suitable" includes being appropriate for the intended use, dependable and effective when required, and able to perform as intended. The Verification Scheme should provide independent checks to confirm continuing suitability throughout the installation's life cycle. It should take account of maintenance work, repairs and operating practices. The scheme is complementary to, but not a substitute for, routine maintenance programs. A Verification Scheme would be expected to identify errors or failures in areas such as specification, selection of appropriate Performance Standards, design, construction or maintenance of elements which have been identified as safety-critical, so that appropriate preventive or remedial action can be taken.

2.2 RBV developments

The topic of RBV has recently attracted much attention from both the academic community and the industrial sector. For example, a method has been formulated by Henningsson & Wohlin [2005] to address how to select a suitable verification and validation process depending on the functionality being developed. The method describes how a suitable process is created and selected where the appropriate process is identified based on functionality and coupling between the system entities being developed. Vik et al. [1998] have developed another model to analyze the environmental hazard and risk of offshore chemicals used and discharged to the marine environment. BP and Landmark have identified desired improvements in testing, core competencies, and independent verification [Sawaryn, 2006]. Details of the audit process are included to enable other parties to conduct similar audits for themselves. The risks and potential loss imply that critical applications should be managed formally as safety-critical systems. Overall the concept of RBV has its wide application to the areas of real time systems and software design. It has comparatively limited application in offshore design and operations. However, the concept of RBV has attracted much attention in the offshore industry. Det Norske Veritas (DNV) has developed an offshore service specification DNV-OSS-300 on risk-based verification [DNV, 2004]. In DNV's verification scheme, principles of risk-based verification are described with the possible benefit highlighted. Lloyd's Register (LR) has developed a verification methodology for management SCEs for offshore installations under the1996 amendments to the safety case regulations 1992 [LR, 2002]. The methodology describes verification scheme, SCEs, performance standards and verification scheme format. Safety-critical software verification is also included. American Bureau of Shipping (ABS) is also in the process of developing its own verification scheme. Many industrial offshore operators have developed their own RBV schemes with applications. For example, Pride North Sea UK Ltd has developed a MODU (Mobile Offshore Drilling Unit) verification scheme and applied it to those installations in the Pride North Atlantic [Pride, 2001]. Four Elements Ltd has developed a

verification scheme with demonstration examples [Four Elements Ltd, 1997]. Transocean has developed a verification scheme for SEDCO installations [Transocean, 2003].

The literature review indicates that there are similarities between all the verifications schemes available. Some emphasise one specific technical issue with more depth than the others. In general, it seems that the RBV concept has not been formalized in a way that information flow in the scheme is based on risk assessment. In particular, the role of SCEs in RBV has been interpreted differently in SCE criticality assessment. The operational aspects have been put more emphasis compared to the design aspects. Furthermore, very limited software has been used to facilitate RBV. This paper addresses the above issues by providing a general RBV framework with the following specific new features:

1. A hierarchical asset definition proposed to allow hazard identification.
2. A step-by-step way of identifying major accident hazards for an offshore asset.
3. A progressive way of identifying SCEs and estimating their criticality.
4. Definition of performance standards, identification of means of performance assurance and identification of means of verification with illustrative examples.
5. Demonstration of the RBV framework's implementation through the use of a widely used software package.

3. RISK-BASED VERIFICATION SCHEME

To improve the efficiency of Verification Scheme, a risk-based process can be employed in which the outcome may result in resources and attention being focused towards the high risk areas. The risk associated with an asset or a system can be assessed in relation to different levels and the Verification Process can be used to manage such risk. Through a RBV process, work effort and resources can be optimized thus leading to improvements in effectiveness. Clearly a risk assessment is the key in conducting a RBV while the findings from the examination of quality management systems, documents and production activities are important. The major steps in a RBV scheme [Wang et al., 2010] are shown in Figure 1 which will be described in detail below. The involvement of the ICP in a RBV is shown in Figure 2 [Transocean, 2003] which is self-explanatory.

3.1 Step 1: Definition of Asset Hierarchy

An asset may be a large system or a small component/feature. It can be an offshore installation, a system, a process or a development phase such as feasibility, design, construction, commissioning, operation and decommissioning. In RBV of offshore installations, the first step is to define the asset hierarchy in which asset specification is made. This includes:

- Detailed description of asset in terms of functionality, capacity, operational requirements etc. Such a description may need to be given at different indenture levels (i.e. system level, subsystem level etc.).
- Identification of verification philosophy.
- Identification of codes and technical specifications to be used.

An asset hierarchy represents increased detail in describing the asset being studied for RBV. It shows how the systems and their associated subsystems work together in operations to provide the

intended working function. It is worth stressing that an asset hierarchy should include both hardware and software systems, together with the management system in RBV. In particular it should reflect both the structural and process flow characteristics of the asset.

In general, an asset hierarchy has multiple hierarchical layers. At the top level, process flow diagrams need to be developed where typical systems include wells, process plant, Emergency Escape and Rescue (EER) systems, etc. in an offshore installation. At the lower levels of the hierarchy, the breakdown of each system becomes more detailed. Eventually the breakdown stops at a required level of resolution where each system is reduced to a set of items that are interrelated to formulate a working system.

An appropriate verification philosophy is defined in a way that the main features of the Verification Scheme are determined and the process for hazard management is organized. Various stages in the life cycle of the asset may need to be dealt with. Typical stages may include design, construction, operations and abandonment.

Appropriate national/international codes and technical specifications to be used in RBV need to be identified and complied with. Appropriate guides produced by the regulatory bodies may also need to be identified.

Insert Figure 1 here.

Insert Figure 2 here.

3.2 Step 2: Major Accident Hazard Identification and Screening

The approach to system selection and setting of Performance Standards is to establish a clear link between hazard, risk and the appropriate risk reducing measures. The risk reducing measures can be control of release of a hazard as well as control of consequence. This structured approach will make it easier to audit and review Performance Standards in the light of any future modifications or changes in circumstances or legislation.

The risk-based approach requires an initial risk ranking exercise of hazards identified in suitable studies. Using this approach allows hazards considered comparatively trivial to be separated from major hazards so that attention can be focused on the most significant hazards hence achieving optimization of effectiveness of the related verification activities.

A hazard in the form of a Major Accident Hazard (MAH) or Major Accident Event (MAE) is typically considered as:

- Fire, explosion or release of a dangerous substance involving death or serious personal injury to persons onboard or engaged in an activity on board or in connection with it.
- Any event involving major damage to the structure of a vessel/installation, plant, or loss of vessel stability.
- The collision of a helicopter or a vessel with an installation.
- Any other event arising from a work activity involving death or serious personal injury to five or more persons on the vessel or engaged in an activity in connection with it.

Additionally such hazards or events can be considered from an environmental and health perspective such as pollution. Table 1 below illustrates a typical listing of MAHs/MAEs.

Insert Table 1 here.

The derivation of MAHs of an offshore installation is conducted through the following processes:

1. System breakdown.
2. Hazard identification.
3. Hazard screening.
4. Determination of major accident hazards.

A large offshore installation can be broken down into platform, export system, etc. which can be further broken down, if necessary, in order to identify possible hazards. The level of breakdown is dependent on the level at which SCEs are identified. Considering that SCEs are usually identified at the system level, the system breakdown for hazard identification is also kept at this level (i.e. Temporary Refuge, marine riser, etc.).

Through Hazard Identification (HAZID), a selected list of hazards specific to the problem under review is produced at an already defined level of system breakdown. Hazard Identification uses brainstorming technique involving a small group of experienced and suitably qualified personnel from various disciplines to determine the hazards.

3.2.1 Hazard Screening

Figure 3 shows the development of a hazard and a series of consequences in the form of a Bow Tie. From Figure 3, it can be seen that an identified hazard can have several associated consequences. Such consequences are then studied to determine the initial risk profile of the hazard. The purpose of the hazard screening process is to eliminate those hazards which have a low risk profile. Then it is possible to focus on those hazards with medium or high risks which would be developed further.

The concept of initial risk profile illustrates that likelihood categories are considered irrespective of any particular controls or barriers that may be in place. Figure 4 illustrates a typical risk assessment matrix from the THESIS (The Health, Environment and Safety Information System) Bow Tie software in which a 5×6 risk matrix is shown. The matrix is applicable for people, assets, environment, and reputation as defined on the left half of the figure.

THESIS assists companies/operators in the analysis and management of the (major) hazards and risks to which their business is exposed, and graphically displays the relationship between hazards, controls, risk reduction measures and a business's HSE activities. The software has been developed based on the Bow Tie concept to visually display how hazards are controlled, and how the risk associated with them are reduced to be ALARP. As part of the process Performance Standards can also be defined and managed.

Insert Figure 3 here.

Insert Figure 4 here.

The consequence severity of each identified consequence of a hazard can be classified as one of the following six severity categories:

1. '0' (No Injury/No Asset Damage/No Environmental Pollution).
2. '1' (Slight Injury/Component Damage/Minor Environmental Pollution).
3. '2' (Minor Injury/Intermediate Asset Damage/Intermediate Environmental Damage).

4. ‘3’ (Major Injury/Major Asset Damage/Major Environmental Pollution).
5. ‘4’ (Single Fatality or Multiple Major Injuries/Severe Asset Damage/Severe Environmental Pollution).
6. ‘5’ (Multiple Fatalities/Loss of Asset/Catastrophic Environmental Pollution).

The occurrence likelihood of each identified consequence of a hazard can be described using one of the following six levels:

1. ‘A’ (Incident never occurred in industry).
2. ‘B’ (Incident has occurred in industry).
3. ‘C’ (Incident has occurred within operation).
4. ‘D’ (Happens several times per year with operator).
5. ‘E’ (Happens several times per year at location).
6. ‘F’ (Happens every month).

Engineering judgment and past experience as well as the information in the risk assessment are required to carry out hazard identification and screening. Figure 4 forms the basis of determining the risk levels of each consequence of an identified hazard based on the combined consequence severity and occurrence likelihood. It can be seen from Figure 4 that the risk associated with a consequence of a hazard could fall within one of the following three risk categories:

1. Low.
2. Medium.
3. High.

The risk associated with a consequence of a hazard is determined by synthesizing the sub-risks with respect to the people, asset and environment categories. The highest of such sub-risks is assigned to the risk associated with the consequence of a hazard. For example, if the sub-risks of a consequence of a risk are estimated as “Low”, “Medium” and “High” with respect to the people, asset and environment categories respectively, then the risk associated with such a consequence is given as “High”.

Once the risk associated with each consequence of a hazard is obtained, it is possible to determine the risk profile of the hazard. The rule to use is to assign the highest risk estimation of the constituent consequences to the risk associated with the hazard. For example, if a hazard has four identified consequences with their risks judged as “Low”, “Low”, “Medium” and “Medium” respectively, then the risk profile of the hazard is obtained as “Medium”.

There are many other existing methods such as cause-consequence analysis that can be used for determining risk levels of each consequence. Such methods may provide more detailed estimates of risks. However, a comparatively simple matrix method is sufficient for use in selecting Major Accident Hazards.

3.2.2 Determination of Major Accident Hazards

Hazards classified as “Medium” or “High” are identified as MAHs. Hazard identification and screening can be conducted at any required level of detail within the asset hierarchy.

It is worth noting that the user can have the flexibility in defining categories for estimating the occurrence likelihood or consequence severity of a hazard, depending on the situation in hand.

As a result, the risk assessment matrix could be 3×3, 4×4 or 5×5 in terms of possible combinations of both occurrence likelihood and consequence severity.

As will be seen, when estimating the Safety Criticality rating of SCEs within Section 3.6, only three categories ('High', 'Medium' and 'Low') are used. 'High' corresponds to '4' and '5' used in Figure 4; 'Medium' to '2' and '3'; and 'Low' to '0' and '1'.

3.3 Step 3: Identify Safety Critical Elements

In general, all the SCEs can be classified as follows in terms of their role in offshore operations:

- Preventive SCE.
- Mitigating SCE.

Preventive SCEs are defined as those items of equipment or structures whose failure could lead to MAH(s) while the purpose of mitigating SCEs is to prevent or limit the consequences of MAH(s). In regard of safety management, SCEs are only associated with installation hardware and equipment related software/logic systems and do not include safety related management systems, processes and procedures.

To identify SCEs, each individual system is studied to see if its failure will directly lead or contribute substantially to the occurrence of MAHs. The term "contribute substantially to the occurrence of a major accident" is intended to include within the category of SCE those systems whose failure would not directly initiate a major accident but would make a significant contribution to a chain of events which could result in a MAH. If the purpose of a system is to prevent or limit the effort of a MAH, then it is also identified as a SCE. For example, failure of the lifting facility could result in dropped object/load which is a MAH. As a result, the lifting facility is identified as a SCE. The evacuation system aims at preventing or limiting possible effects of a fire which is a MAH and therefore it is also identified as a SCE. It is usual to tag SCEs with unique identifying codes which can be recognized, for example, by maintenance management systems.

3.4 Step 4: Definition of Performance Standards

For each of the SCEs identified, performance of the element or sub-elements will be considered and a Performance Standard will be set. When Performance Standards are qualitative, descriptive words for each element can be used. Where sufficient information is available for a quantitative Performance Standard to be set, then it can be readily incorporated. Where there is insufficient information to set a standard, draft Performance Standards should be proposed and reviewed with the ICP at an early stage, as soon as information becomes available following completion of any studies which may prove necessary.

The key to being able to set meaningful Performance Standards for a system/element is to have a clear and concise statement of the role of the system, based on an understanding of the suitability of the system for use in managing the specific hazard and knowledge of the range of applicability of the system concerned. These functional statements will be used as the foundation for defining the elements of the Performance Standards for the system.

It is essential that the engineer responsible for the development of the Performance Standards of SCEs is with necessary experience on the operations of the offshore installation or production unit being investigated in the RBV. Appropriate references may be needed to produce such Performance Standards. Those include:

- Quantitative Risk Assessment (QRA) of the installation or process system.
- Safety case (i.e. risk assessment).
- Relevant industrial guidance.
- Accident/incident reports in the public domain.
- SOLAS (International Convention for Safety of Life at Sea).
- MODU Code.
- Class rules.
- Industry standards such as API (American Petroleum Institute) Specification and recommended practice.
- National/international standards.

The SCE's functionality, reliability and availability, survivability and interaction/dependency on other systems established shall comply with standards referenced within the safety case or equivalent. However, performance requirements in terms of infrequent failure probabilities (for example, less than 1×10^{-6}/yr) shall usually be avoided, instead being replaced by a requirement for testing or inspection that will verify that such a performance can be expected.

1. Functionality.

   The Performance Standard regarding functionality is developed in terms of functional requirements and performance criteria of a SCE. Both functional requirements and performance criteria are produced with respect to the risk assessment, safety justification and other guidance, Classification rules etc. Functional requirements define key functions to be carried out by the system in order to meet system goals. For example, the function requirements of the Temporary Refuge (TR) system are provision of basic life-support conditions in respect of breathable air and ambient temperature conditions; provision of sufficient access/egress points and routes to provide safe transfer of personnel to and from the TR; and provision of suitable systems during major incidents to enable emergency response personnel to communicate internally with the workforce and externally with outside bodies.

   Performance criteria are those which must be met by the function in order to achieve system goals. Such criteria must be measurable in terms of hazard characteristics to be responded to, area to be covered, speed of response, duration, etc. For example, the performance criteria regarding functionality for the TR system could be:

   - AO steel construction, A60 fire walls facing the well/drill floor areas.
   - Internal conditions (maximum temperature 50°C, maximum CO_2 – 20000ppm, maximum CO – 1200ppm, maximum H_2S – 20ppm, maximum flammable gas – 50% LEL, thermal radiation from interior surfaces – $2kW/m^2$).
   - Adequate thermal protection for personnel to muster safely at evacuation points ($<2kW/m^2$).
   - Suitable communication systems for internal use (Public Announcement/radio links with fire team etc and communications with relevant external bodies.

2. Reliability and availability

   The performance criteria for reliability and availability of a SCE are required to have availability to function on demand and to ensure that system goals are achieved. They can be

either descriptive or quantitative. Such criteria are again produced with respect to the risk assessment, safety justification and other guidance (for example, SOLAS), Classification rules etc. The performance criteria for availability and reliability of the TR system are, for example, that the HVAC (Heating, Ventilation and Air Conditioning) system closes on demand verified through monthly tests.

3. Survivability

   Survivability defines the fire/explosion/accident event characteristics which each SCE must survive to ensure performance of essential system functions. As appropriate, the time duration over which a SCE must survive may need to be defined. The hazardous event/performance criteria for survivability of a SCE can be defined using risk assessment, safety justification and other guidance. For example, the hazardous event/performance criteria for survivability of the TR system are to maintain integrity of all systems for duration of incident or until the evacuation of personnel takes place and to have minimum TR endurance of 1 hour.

4. Interaction/dependency on other systems

   In an offshore installation, a SCE may interact with other systems which provide essential support in ensuring the achievements of the SCE. The Performance Standard for interaction/dependency on other systems of a SCE is defined in terms of the supporting or interactive systems and their interaction/dependency on the SCE. For example, the systems that interact with the TR system include: HVAC system, communications system, well control system, fire and gas system, ballast system, mooring system, propulsion system, evacuation system, escape system, lifesaving equipment and emergency power systems.

   In terms of their interaction/dependency with the TR system, the HVAC system prevents ingress of smoke or gas into TR; the communications system is required for use by emergency response team and for communication with outside bodies; the well control system provides control of well closure operations to prevent loss of containment from well/reservoir; the fire and gas system provides detection of smoke/gas ingress to TR and initiates shutdown of HVAC to prevent loss of TR integrity, etc.

   The information given in the interaction/dependency category of the Performance Standards provides an overview of how other systems influence the SCE. It is usually the case that such other systems are also SCEs for which Performance Standards have to be developed. There are no verification activities associated with interaction usually. Only if an identified interaction of a SCE changes, would any review be required. In the event that the change in interaction is adverse then review by the management is required.

3.5 Step 5: Identification of Means of Performance Assurance

The means of assuring performance includes consideration of activities contained in the systems used to manage risks i.e. the Safety Management System (SMS) and the Preventive Maintenance System (PMS). These systems contain activities that contribute to assuring performance of SCEs such as:

- Inspection, maintenance, testing routines, failure reports and operations procedures.
- Audits.
- Risk assessment studies.

As discussed previously, the Bow Tie methodology is able to capture activities and tasks critical to the performance and maintenance of barriers. These tasks are considered as Critical Tasks and

reflect activities which support the Performance Standards and Verification Scheme. Key aspects of the Performance Standards and Verification Activities documents are:

- The documents show the visual examination, testing, review and audit requirements for action by the ICP to verify that the requirements of the Performance Standards are being met.
- Actions relating to Class and to Flag State requirements, together with other requirements of the Verification Scheme are indicated in the Mode column of the document, as follows:
    - C – Class requirement.
    - F – Flag State requirement.
    - V – Other verification requirement.
- The Performance Standards reference column links the activities to requirements in the Performance Standards for:
    - P – Performance criteria (including functional requirements if necessary).
    - F – Functionality.
    - RA – Reliability and availability.
    - S – Survivability.

The means of performance assurance of a SCE is based on the Performance Standards produced. It is produced through visual examination, testing and review. All the three methods are described in columns of task reference number, task details, performance reference mode, frequency of examination/test/review, and Performance Standard reference.

1. Visual examination.

   Visual examination for assuring performance standards is produced through review of Class requirement, Flag State requirement and other possible verification requirement. Possible tasks can be determined together with the frequency of each task. For example, for the TR system of an offshore installation, there could be three visual examination tasks:

   - Confirm that suitable communication systems exist for internal PA (public address)/radio links with fire team, etc. and communication with relevant external bodies.
   - Confirm that the following equipment and facilities have been provided to monitor and control incidents: fire & gas panel, HVAC, emergency shutdown of Emergency Shutdown (ESD), Blow Out Preventor (BOP), winch controls, and propulsion & ballast controls (main & secondary).
   - Confirm that sufficient access/egress points and routes are provided to allow safe transfer of personnel to and from the TR system.

   All the three tasks should correspond to the operational requirements in the safety documentation. They address some elements of the Performance Standard relating to functionality of the TR system and they should be conducted on a yearly basis.

2. Test.

   Testing is usually undertaken during the design phase. During the operational phase, it is unusual to use testing to determine the means of performance assurance of the SCE.

3. Review.

   Review for assuring Performance Standards regarding functionality, reliability and availability, and survivability is produced through review of the Class requirement, Flag State requirement and other possible verification requirements. Possible tasks can be determined together with the frequency of each task. Review could involve the study of design proposal, study of a design

management system, study of a maintenance system and review of system testing. For example, for the TR system of an offshore installation, there could be six visual examination tasks:

1) Review HVAC system testing to ensure that system closes down automatically on smoke or gas detection at the inlets.
2) Review TR system information for confirmation of structure/fire protection to ensure integrity against fire and blast consequences shown in the safety statement.
3) Confirm that the TR is constructed in suitable materials, with suitable protection facing the well/drill floor areas.
4) Confirm that adequate thermal protection has been provided to allow personnel to muster safely at evacuation points.
5) Design review to confirm that the minimum endurance of the TR.
6) Review the planned maintenance system and the previous records to ensure that the level of maintenance is acceptable. It is necessary to have 100% review of maintenance and inspection records over 2 year period – nominally 50%/year.

All the six tasks correspond to the operational requirement in the safety statements/case. They address the remaining elements of the Performance Standard relating to functionality, reliability and availability, and survivability of the TR system.

Where required, the ICP will issue Remedial Action recommendations which will be referenced on the log sheet.

3.6 Step 6: Assessment of Criticality

The definition of a SCE is based on the severity of possible consequences and the role it plays in hazard management should there be a failure of that element. Therefore, to provide a RBV scheme, the concept of Safety Criticality is introduced. This recognizes that all elements defined as safety critical will not necessarily be equally critical. The more severe the possible consequences and the more important the role the SCE plays in hazard management, the greater the Safety Criticality of that element.

SCEs can thus be ranked according to the degree of Safety Criticality associated with them.

The purpose of estimating Safety Criticality is to provide an input to the asset's Verification Scheme to ensure that the Means of Verification applied through maintenance and inspection are based on the significance of the MAHs and the role of the SCEs in contributing to risk reduction.

These verification arrangements include:

- The means of performance assurance and re-assurance.
- The frequency of verification tasks and methods used for verification.
- Appropriate allocation of resources is given to SCEs with different Safety Criticality ratings.
- The extent of demonstration that the level of verification is adequate.

Based on the role a SCE fulfils and the severity of possible consequences caused by the occurrence of the SCE, the Safety Criticality of an individual SCE can be established. This is then applied to develop the requirement for verification. The process for assessing the Safety Criticality of a SCE is described as follows:

3.6.1 Identify Hazard Management Rating

Hazard Management Rating is used to measure the role SCEs play in hazard management. An example for a Hazard Management Rating (HMR) system based on the role of the SCE, is shown in Table 2.

Insert Table 2 here.

3.6.2 Identify Consequence Rating

Consequence Rating is used to measure the severity of possible consequences should a SCE fail. The method used to identify Consequence Rating is a three-tier system based on the contribution of each MAH to the consequence severity levels, as shown in Table 3. The Consequence Rating (CR) of possible consequences of a SCE is described in terms of its contribution to the injuries/fatalities, asset damage or environmental damage.

Insert Table 3 here.

3.6.3 Identify Safety Criticality Rating

With the Consequence Rating and Hazard Management Rating identified, the Safety Criticality of the identified SCEs is then established using the criticality matrix as shown in Table 4.

Insert Table 4 here.

When determining the Safety Criticality of a SCE using Table 4, it is necessary to investigate all the possible combinations of CR and HMR ratings. It is possible that more than one Safety Criticality value for a SCE would be generated. In such a case the highest Safety Criticality value is chosen for the SCE. For example, a particular SCE with 'M' for HMR and with CR values of 'H', 'M' and 'L' for Personnel, Asset and Environment, respectively, will have three Safety Criticality values 'High', 'Medium' and 'Low'. A Safety Criticality rating of 'High' should be assigned to this SCE.

Those SCEs with an identical overall Safety Criticality rating may also be further differentiated. For example, suppose:

- SCE 1 has a Safety Criticality rating of 'High' across all the three consequence categories.
- SCE 2 has Safety Criticality ratings 'High', 'High' and 'Low' across the three consequence categories.
- SCE 3 has Safety Criticality ratings 'High', 'Medium' and 'Low' across the three consequence categories.

In this instance SCE 1 is regarded as the most critical SCE.

3.6.3 Risk Assessment of Performance Standards

As a further iteration of risk analysis an option is available to carry out risk assessment of Performance Standards. This option would depend on the need for detailed analysis and also the availability of data in hand for use in such an assessment.

The Performance Standards of a SCE in terms of the functionality, reliability and availability, and survivability can be documented. Each Performance Standard of the SCE on the functionality, reliability and availability, or survivability can be modelled in terms of their risk levels using the following two parameters:

- The Likelihood (L) of the Performance Standard being violated.
- The Severity (S) of possible consequences given the violation of the Performance Standard.

Engineering judgment and past experience, as well as the information from the risk assessment may be required to estimate the above two parameters of a SCE. Then risk levels associated with each Performance Standard of the SCE can be estimated. Suppose the following information is obtained for the Performance Standards of a SCE in terms of the functionality, reliability and availability, and survivability:

- Functionality: S = '5', L = 'E', thus Risk Level = "High"
- Reliability and Availability: S = '3', L = 'D', thus Risk Level = "Medium"
- Survivability: S = '2', L = '2', thus Risk Level = "Low"

From the above it can be seen that the risk associated with the Performance Standard of the SCE in terms of functionality is the highest. As a result the Performance Standard of the SCE on functionality is considered as the most important among the Performance Standards of a SCE in terms of the functionality, reliability and availability, and survivability.

Through such a risk assessment, the Risk-based Performance Standards can be produced. Effort paid in the development of performance verification activities should be proportionate to the level of risk estimated. For example, within a SCE, a Performance Standard with a "High" risk would need to have more carefully designed verification activities as compared to a Performance Standard with a "Low" risk.

3.7 Step 7: Identification of Means of Verification

3.7.1 Means of Verification in Design and Construction

Guidance on how the means of verification may be implemented in design and construction is illustrated in Table 5 subject to:

- Review and agreement with the appointed ICP.
- Review based on the previous performance of similar SCEs.

Insert Table 5 here.

3.7.2 Means of Verification for Operations

Guidance on how the means of verification may be implemented in operations is illustrated in Table 6 subject to:

- Review and agreement with the appointed ICP.

- Review based on the SCE's previous performance.

Insert Table 6 here.

3.8 Step 8: Documentation of the Verification Arrangements

The SCEs, Performance Standards, Means of Performance Assurance and Arrangement for Verification are to be documented in an individual Verification Scheme for the asset. The Verification Scheme is reviewed by the appointed ICP, in accordance with the Coastal State Regulations. The purpose of this review is for the ICP to identify any shortfalls or omissions in the list of SCEs and assess the suitability of the Verification Scheme and associated documentation. On the basis of the Performance Standards set for each SCE, written schemes of Verification are prepared. These written schemes will be drafted with the necessary scheme detail and examination details (for initial and periodic examinations), to provide the DH with a practical set of written schemes.

3.9 Step 9: Execution of Verification Scheme

The DH is responsible for appointing the ICP to operate and review the Verification Scheme and to carry out verification tasks under the scheme, and where necessary to revise the scheme.

4. AN ILLUSTRATIVE EXAMPLE

To be able to demonstrate the described RBV procedure, a simplified example is used. Considering the large number of SCEs associated with an offshore installation, it is not feasible to demonstrate the described RBV procedure using a whole platform. In order not to lose generality, a generic jack-up offshore installation is used in which the functions, features, characteristics and attributes common to all installations of different types are described. For demonstration purposes, a relatively higher level of breakdown is utilized. This example is presented in parallel with the described RBV scheme in Section 3.

4.1 Definition of Asset Hierarchy

The example used is a large, heavy duty jack-up platform. The platform is a self-elevating fully integrated drilling, production and quarters (PDQ) platform. The main elements of the structure are a triangular hull. The connections between the hull and the legs are by jacking and locking systems located in jack houses and locking rooms at the corners. Internally it is divided into two levels. The machinery deck is the bottom level, immediately above the double bottom. The platform control room and offices are on the main deck level. This entire level of the accommodation block is the platform TR with its own integral HVAC system. The topside structure sits on the Gravity Base Tank (GBT), a reinforced concrete structure which provides the foundation.

Verification philosophy of the asset can be identified. In this case study, the Verification Scheme is organized for the operational stage only. The facilities and means of operation relating to this installation were developed to comply fully with the DCR regulations and Prevention of Fire and Explosion and Emergency Response (PFEER) Regulations. The means of establishing and maintaining all aspects of the installation critical to safety is achieved through a formalized,

auditable process of safety integrity. The integrity of the installation's Safety Critical Elements is maintained on a "live" basis by a formal, rigorous integrity assurance process to ensure that the risks to personnel, asset and the environment are maintained to As Low As Reasonably Practicable (ALARP) throughout the operating life of the installation.

4.2 Major Accident Hazards and Screening

Through a structured, auditable approach, MAHs on the offshore installation can be placed in one of the categories described in Table 1. Possible consequences of such MAHs include human deaths/injuries, asset damage and environmental damage.

At the defined system breakdown level, each individual system (i.e. crane lifting equipment) is investigated through a HAZID session.

Each identified hazard can be estimated with respect to the associated consequences in terms of consequence severity and occurrence likelihood shown in Figure 4. Then those judged with a low risk profile can be screened out for further analysis although they should be kept within the low risk region throughout offshore operations.

4.3 Identification of Safety Critical Elements

The identification of SCEs is here conducted at the defined level of system breakdown. Possible MAHs can be found in Table 1. Then the SCEs of the offshore installation can be identified through investigating possible links between the constituent systems and the identified MAHs. Table 7 shows examples of some registered SCEs of this offshore installation at the system level. Alternatively SCEs can also be identified through the Design and Operations Safety Cases (i.e. risk assessment) of the installation.

Insert Table 7 here.

4.4 Definition of Performance Standards

For demonstration purposes, only the HVAC System (No. 3, General SCE) is for detailed study. Its Performance Standards are defined as shown in Tables 8.

Insert Table 8 here.

4.5 Identification of Means of Performance Assurance

The Means of Performance Assurance for the HVAC System is shown in Table 9.

Insert Table 9 here.

4.6 Assessment of Criticality

For the HVAC System, the following ratings are obtained:

- Hazard Management Rating = M (Medium)
- Consequence Rating = H (High) for Personnel
- Consequence Rating = H (High) for Asset
- Consequence Rating = L (Low) for Environment

This yields the following Safety Criticalities

- Safety Criticality Rating = H (High) for Personnel
- Safety Criticality Rating = H (High) for Asset
- Safety Criticality Rating = L (Low) for Environment

The highest rating, "High", is then chosen as the overall Safety Criticality Rating of the HVAC System.

4.7 Identification of Means of Verification

From the obtained Criticality Rating of the HVAC system and also from the guidance in Table 9, the Means of Verification can be given below:

- For the ICP, it is necessary to have 100% witnessing of inspections and testing, as appropriate over 4 year period – nominally 25%/year. For equipment with single unit test, testing would be witnessed annually.
- For document review, it is necessary to have 100% review of maintenance and inspection records over 1-2 year period – nominally 100% or 50%/year depending on extent of records.

4.8 Documentation of the Verification Results

The HVAC system, its Performance Standards, Means of Performance Assurance and Arrangement for Verification can then be documented. A review of them can be conducted by the appointed ICP.

4.9 Execution of Verification Scheme

The Verification Scheme can be executed for the other identified SCEs by following the analysis described in Sections 4.4-4.8 above. The Verification Scheme will then be reviewed utilizing the experience gained.

5. IMPLEMENTATION OF RBV USING THESIS

The hazard modelling and safety information management features of THESIS can be used for implementing the proposed RBV scheme of offshore installations. In the following, THESIS is used to facilitate the RBV of the example presented in Section 4.

Step 1: Definition of Asset Hierarchy

From Figure A.1 in Appendix A, it can be seen that the offshore installation is broken down into platform, GBT and export system. It is also possible to further break down the hierarchy to allow

effective hazard identification if necessary. The case information can be given using the window shown in Figure A.1.

Step 2 Major accident hazard identification and screening

Under each of those categories of platform, GBT and export system, hazard identification can be conducted using HAZID and the identified hazards are recorded using THESIS. Figure A.2 shows how the identified hazards are recorded. In the left side of Figure A.2, it can be seen that all the identified hazards are listed where their associated consequences, threats and barriers can also be recorded. The right side of Figure A.2 gives a Bow Tie diagram of a highlighted hazard. For example, the selected hazard "minor leak of the sea water system in the utility systems" shown in Figure A.2 has two possible consequences: "Reducing Operation Efficiency (ROE)" and "causing discomfort in the working environment". There are also two threats leading to the identified hazard. These are "not tight sealing in pipe connections" and "minor leakage of pumps".

Each identified consequence associated with the hazard can be assessed using the risk matrix approach shown in Figure 5. Figure A.3 gives an example of risk assessment of hazard "Reducing Operation Efficiency (ROE)" associated with "minor leak of the sea water system in the utility systems". Through such an analysis, the risk profile associated with each identified hazard is produced. For example, from Figure A.4 it can be seen that the sub-risks associated with "Reducing Operation Efficiency" with respect to the people, asset and environment categories are "Low" (C×1), "Low" (C×2) and "Low" (C×1). The risk record of hazard "minor leak of the sea water system in the utility systems" is also shown in Figure A.4 (i.e. in the "Ranking" box). Both the operator and the ICP can then sign off the identified hazard and its assessment using the "Sign Off" window shown in Figure A.4. Those hazards classified as "High" or "Medium" are identified as MAHs.

Step 3: Identification of SCEs

Each individual system in the categories of platform, GBT and export system is then investigated to see if its failure would result in the occurrence of any identified MAHs or if its purpose is to prevent or limit the consequences of any identified MAHs. Figure A.5 lists up some typical SCEs of the offshore installation being investigated. Such associated MAHs and possible consequences caused by the failure of each SCE can be presented in a form of a Bow Tie. An example is shown in Figure A.6 where the associated MAHs and possible consequences of SCE 3 (i.e. the HVAC system) are given. It is necessary to redefine appropriate terms in THESIS when using it for implementing the RBV of offshore installations. The flexibility of redefining technical terms in THESIS allows the user to use its own preferred terminology in the RBV of offshore installations.

Step 4: Performance Standards

The Performance Standards of each identified SCE are defined in terms of functionality, reliability and availability, survivability and interaction/dependency on other systems. Such Performance Standards can be presented using THESIS. The Performance Standards of the HVAC system in terms of functionality, reliability and availability, survivability and interaction/dependency on other systems are shown in Figures A7-A10.

Step 5: Means of Performance Assurance

The Means of Performance Assurance for each SCE can be described using THESIS. Figure A.11 gives a THESIS window for describing the Means of Performance Assurance of each SCE. Figure A.12 demonstrates how the Means of Performance Assurance for the HVAC system is presented in a THESIS window in terms of visual examination.

Step 6: Criticality of SCEs

The Criticality Rating of each SCE can be estimated using the approach described in Section 4.6. Then it can be inputted into the THESIS-based RBV system. The Criticality Rating of the HVAC system is shown in Figure A.13 (i.e. in the “Ranking” box).

Step 7: Means of Verification

The Means of Verification of each SCE can be appropriately identified using the obtained Criticality Rating and the information in Table 5. It can then be managed using THESIS. For example, the Means of Verification of the HVAC system with respect to visual examination is shown in Figure A.12.

Step 8: Documentation of Verification Arrangements

The information of the identified SCEs, their Performance Standards, Means of Performance Assurance and Arrangements for Verification can be documented in THESIS as shown above. As soon as the RBV is completed for a selected SCE, the SCE can be in an “Assigned” status as shown in Figure A.14.

Step 9: Execution of Verification Scheme

The RBV of any offshore installation can be executed by following the above steps. Any feedbacks from the experience can be fed into the THESIS-based RBV system. The RBV record incorporating THESIS is a “live” management system that any necessary changes can be made during the offshore design/operation and any record of change can be kept.

6. CONCLUSIONS

RBV can appropriately ensure using available resources on a balanced way to control risks throughout the life cycle of an asset. In principle, through focusing on high-risk elements and prioritizing verification efforts it should provide both time and cost savings compared with the traditional prescriptive verification or certification regime.

Through use of formal hazard identification and risk assessment methods, RBV may give substantial cost benefit while keeping the overall risk within an acceptable level during the verification process. This may be particularly true for systems with a high level of complexity, new technologies, and new design/operation features. This possible benefit can be mutual to both verification bodies and customers from reduced or controlled risks.

A possible limitation could be that all parties involved in the verification process need to put effort and time to get familiar with the scheme. Another limitation may be that high level of uncertainty in data or lack of data could make it difficult for risk assessment to be conducted where appropriate subjective judgments are often necessary. This certainly requires the ICP to be knowledgeable in the areas of verification.

Nevertheless, it is widely accepted that any developed risk-based scheme should preferably be introduced into a commercially stable environment in order that the application has the chance to become established to prove feasible, otherwise it is more likely that its full potential will not be realized.

Acknowledgements

Thanks are given to the Royal Academy of Engineering for providing the financial support of Professor J. Wang's industrial secondment of 6 months at ABS Consulting Ltd. This research is partially funded by the UK Engineering and Physical Sciences Research Council (EPSRC) under grant reference EP/F041993/1. This paper is the opinion of the authors and does not necessarily represent the belief and policy of their employers.

REFERENCES

1. ABS Consulting, The Health, Environment, Safety Information System (THESIS) Software, 2007, Warrington, UK.
2. DNV, Offshore Service Specification DNV-0SS-300 - Risk-based Verification, Norway, April 2004.
3. Four Elements Ltd, HeereMac Verification Scheme – Methodology, 1997, London, UK.
4. HSE. The offshore installations and wells (design and construction, etc.) regulations 1996, ISBN 0-11-054451-X, No. 913, HSE Books, Suffolk, UK, 1996.
5. LR, Verification methodology for management safety-critical elements for offshore installations under the1996 amendments to the safety case regulations 1992, Aberdeen, UK, 2002.
6. Pride North Sea UK Ltd, MODU verification scheme for Pride North Atlantic, 2001, Aberdeen, UK.
7. Sawaryn S.J., Sanstrom B., McColpin G., "The management of drilling-engineering and well-services software as safety-critical systems", SPE Drilling & Completion, Vol.21 (2), 2006, 141-147.
8. Transocean, SEDCO 704 verification scheme, 2003, Aberdeen, UK.

9. Vik E.A., Bakke S., Bansal K.M., “Partitioning of chemicals - important factors in exposure assessment of offshore discharges”, Environmental Modelling & Software, Vol.13 (5-6), 1998, 529-537.
10. Wang J and Kieran O. Offshore safety assessment and safety based decision making – the current status and future aspects, Journal of Offshore Mechanics and Arctic Engineering, Vol.122, No. 2, 2000, 63-69.
11. Wang J., “A review of marine and offshore safety assessment”, Quality and Reliability Engineering International, Vol.22, No.1, 2006, 3-19.
12. Wang J., Phipps J., Matellini D.B., “A study of risk-based verification for offshore engineering systems”, Proceeding of the 10th International Probabilistic Safety Assessment & Management Conference, 7-11 June 2010, Seattle, Washington, USA, paper 10, 13 pages.

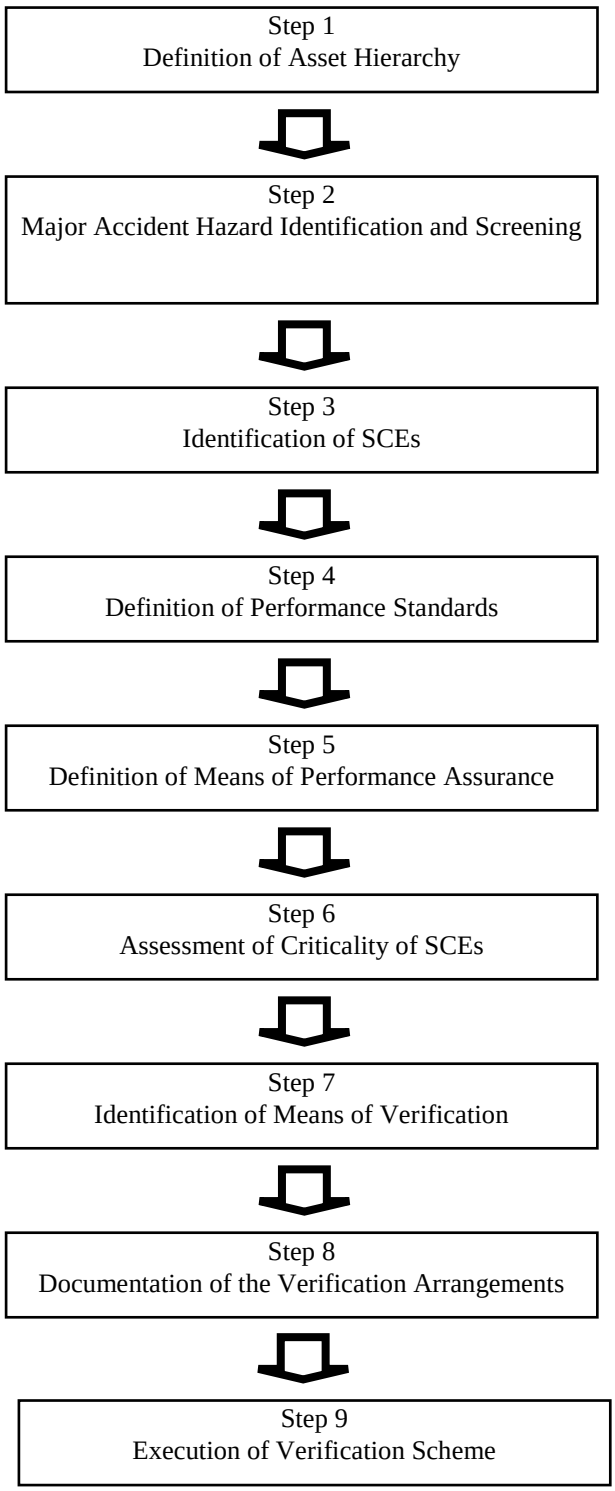

Figure 1 – Major steps in RBV

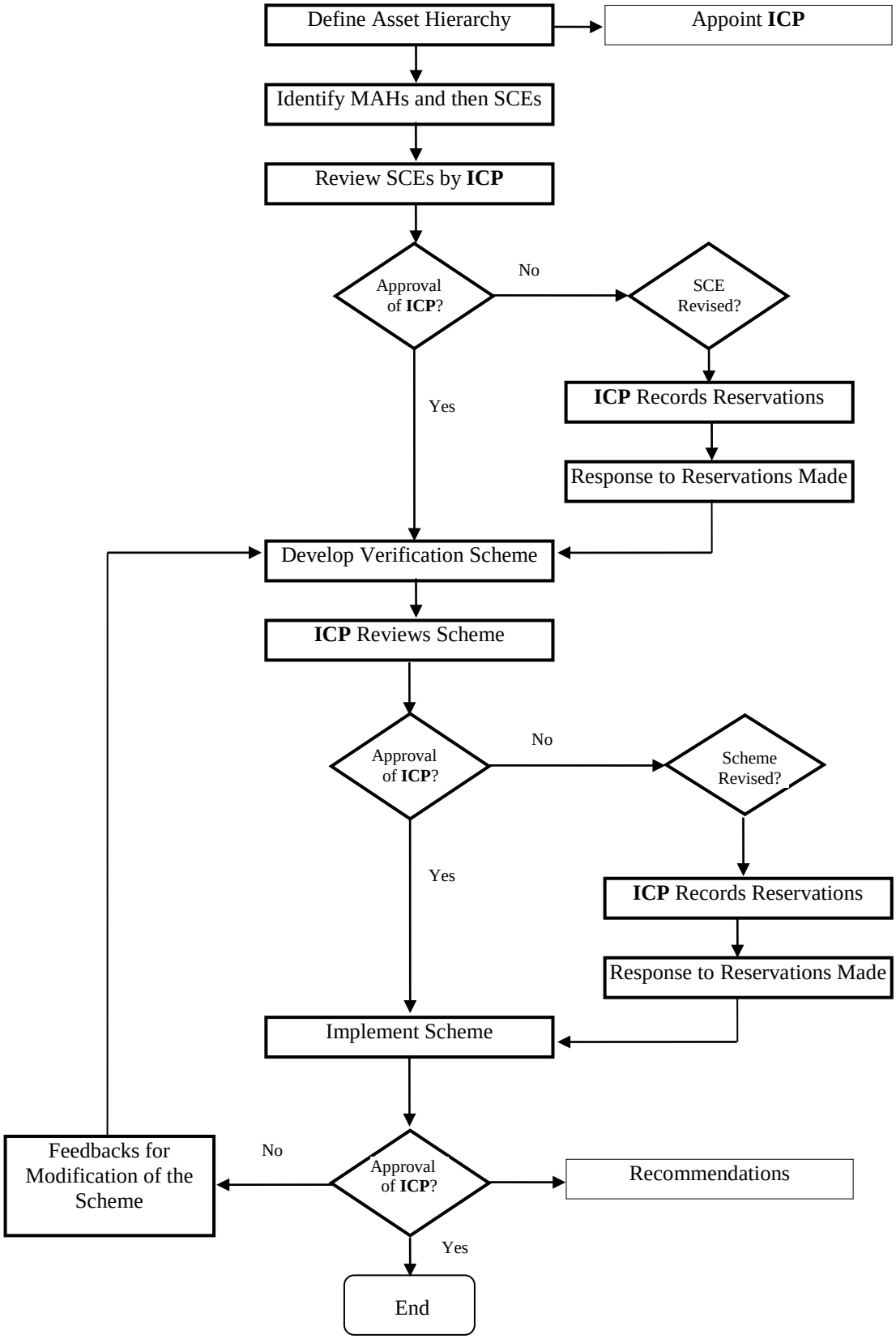

Figure 2 – Involvement of the ICP in a RBV

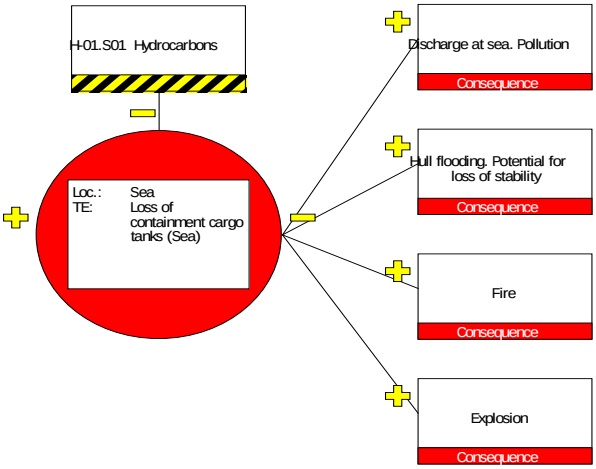

Figure 3 – Developed Consequences

	Consequence				Likelihood				
					A	B	C	D	E
Rating	People	Assets	Environment	Reputation	Never heard of in the world	Heard of incident in industry	Incident has occurred in our Co.	Happened several times per year in Co.	Occurs several times per year at location
0	No health effect/injury	No damage	No impact	No impact					
1	Slight health effect/injury	Slight damage	Slight impact	Slight impact					
2	Minor health effect/injury	Minor damage	Minor impact	Limited impact					
3	Major health effect/injury	Local damage	Localized impact	Considerable impact					
4	Single fatality / multiple injuries	Major damage	Major impact	Major national					
5	Multiple fatalities	Extensive damage	Massive impact	Major international					

Manage for continuous improvement

Incorporate risk reduction measures

Intolerable

Figure 4 – Typical Risk Assessment Matrix

Appendix A: THESIS DIAGRAM

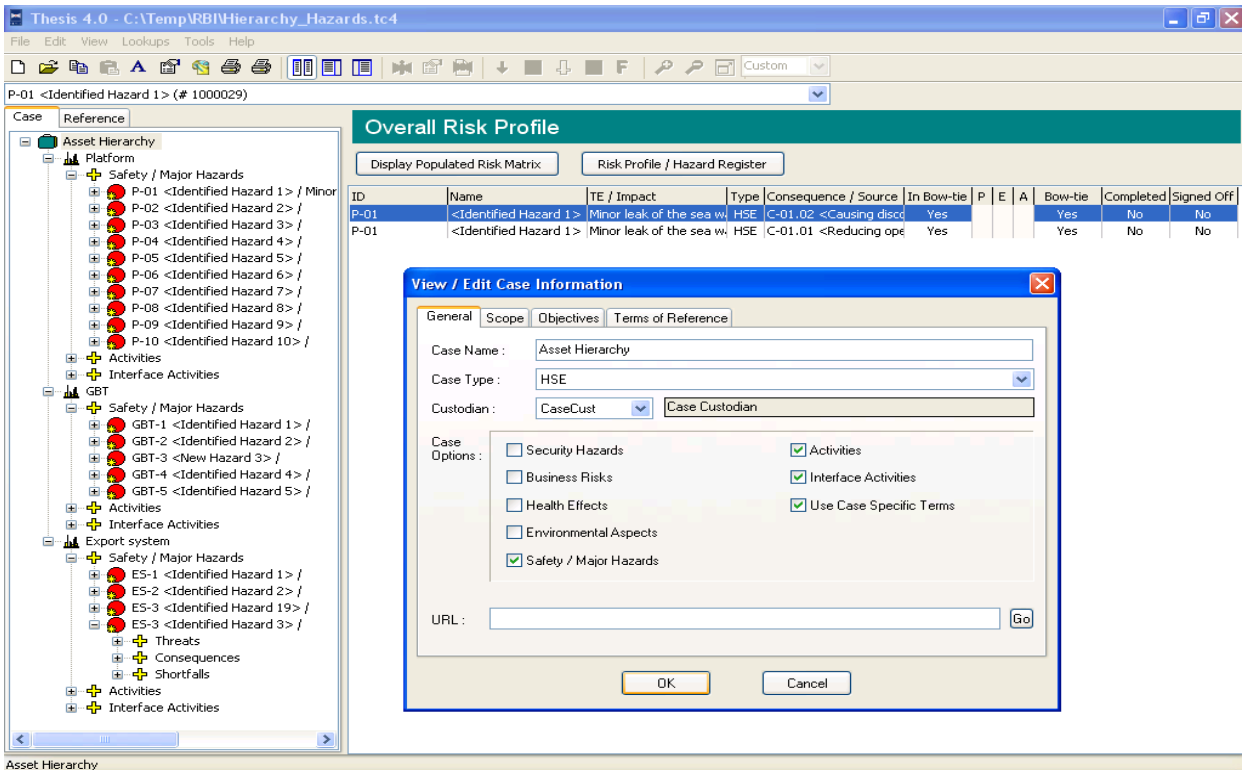

Figure A.1 – Definition of Asset Hierarchy

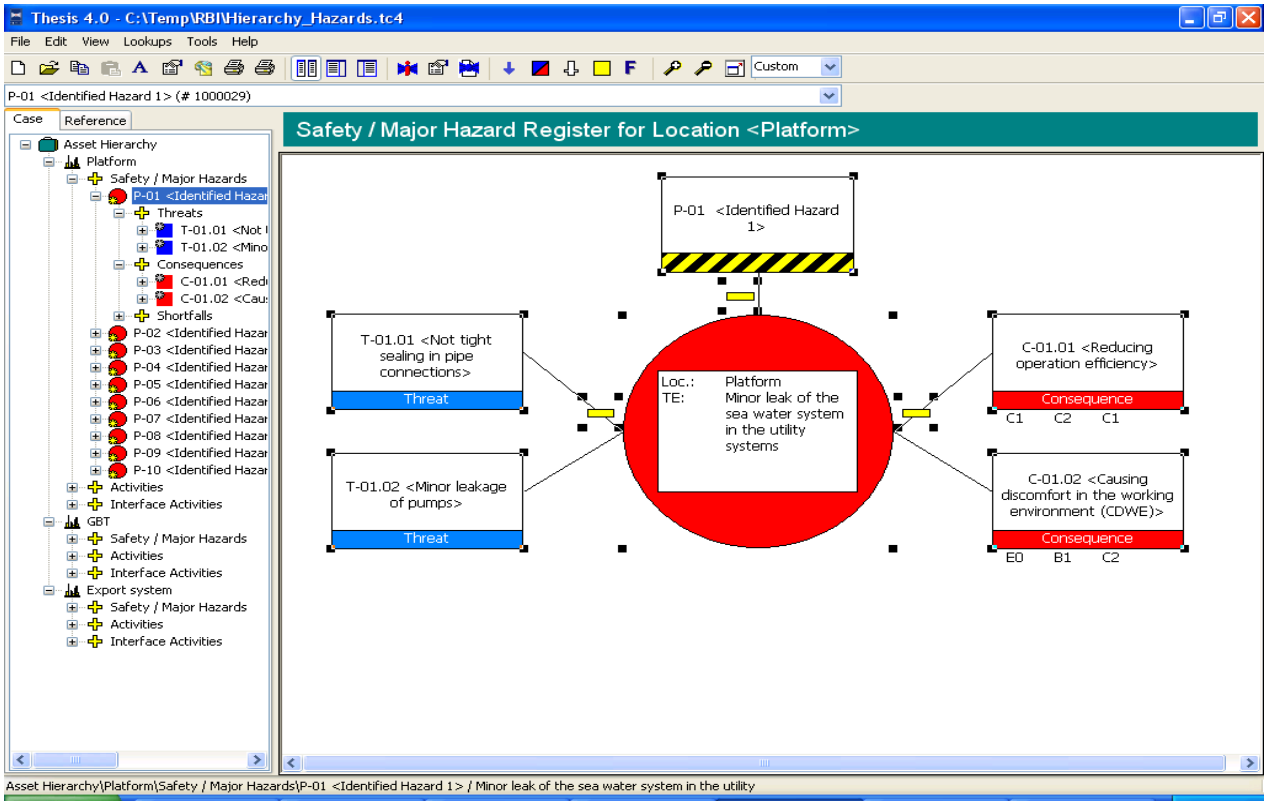

Figure A.2 – Definition of Asset Hierarchy

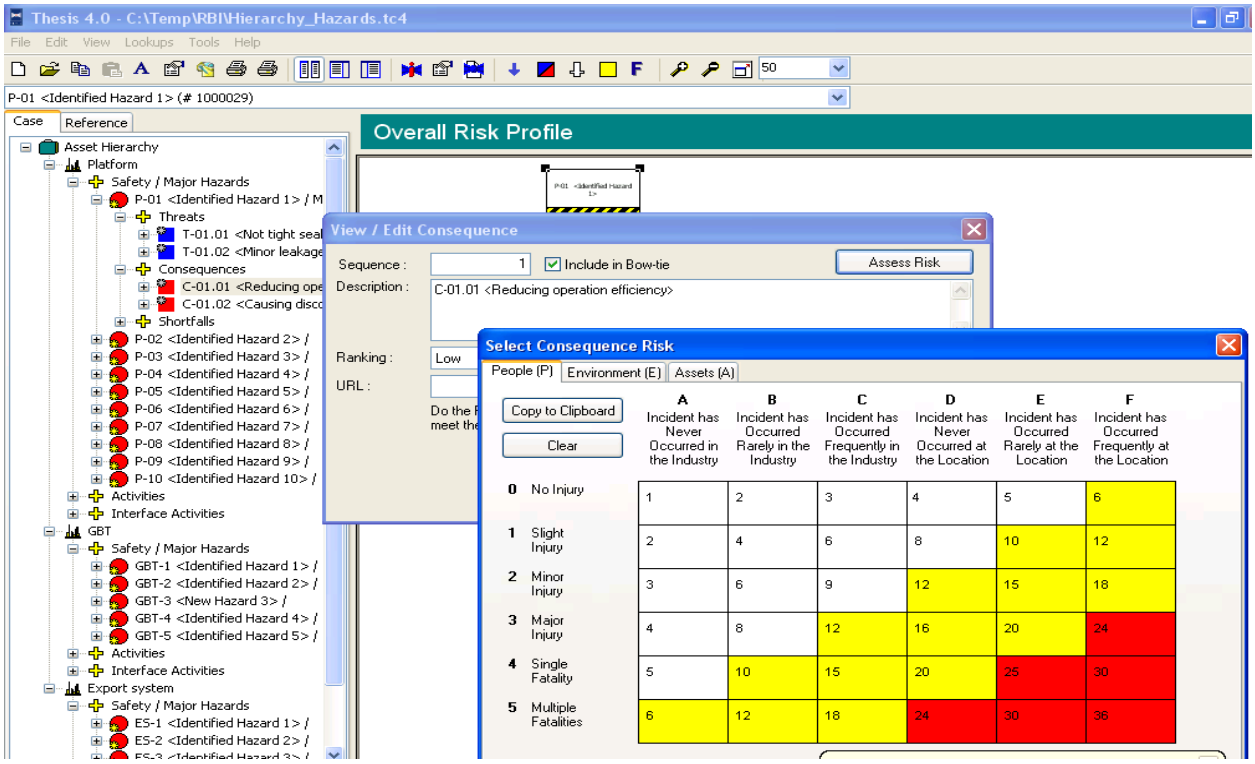

Figure A3 – Risk Assessment of a Consequence Associated with a Hazard

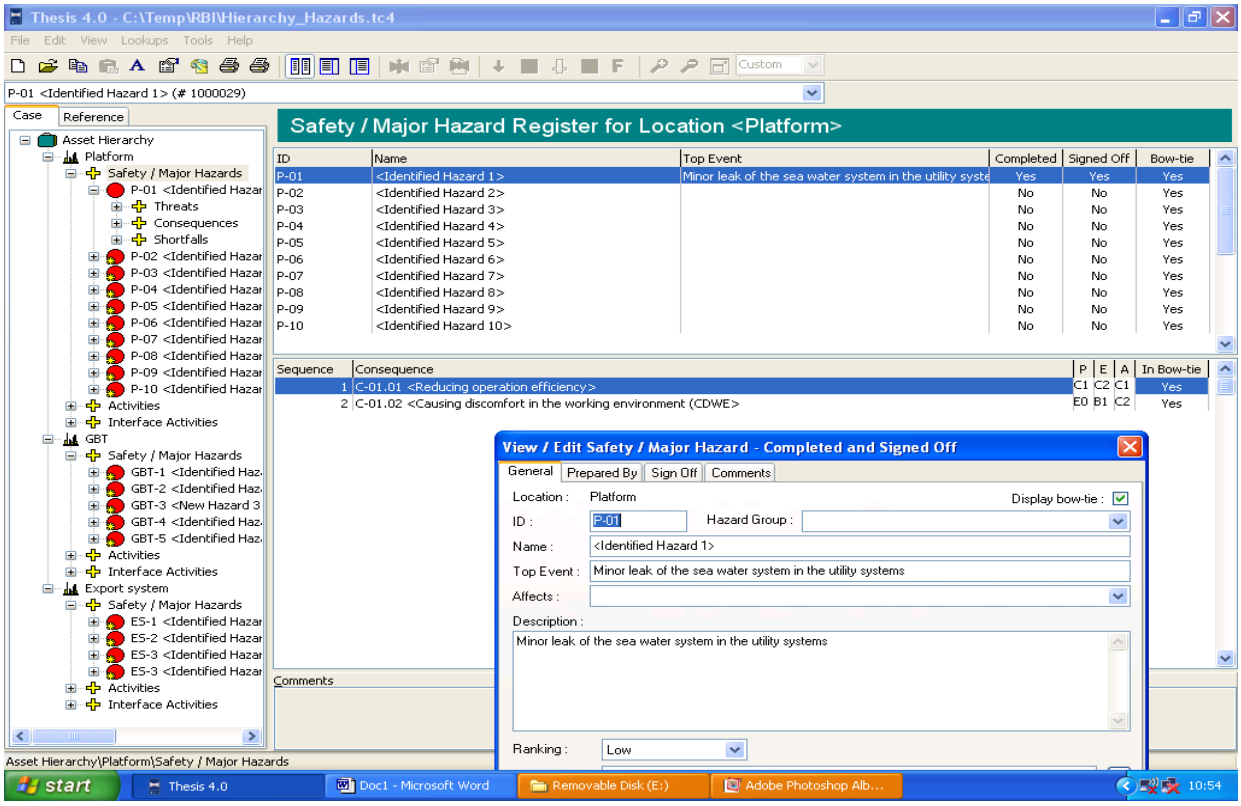

Figure A.4 – Risk Record of an Identified Hazard

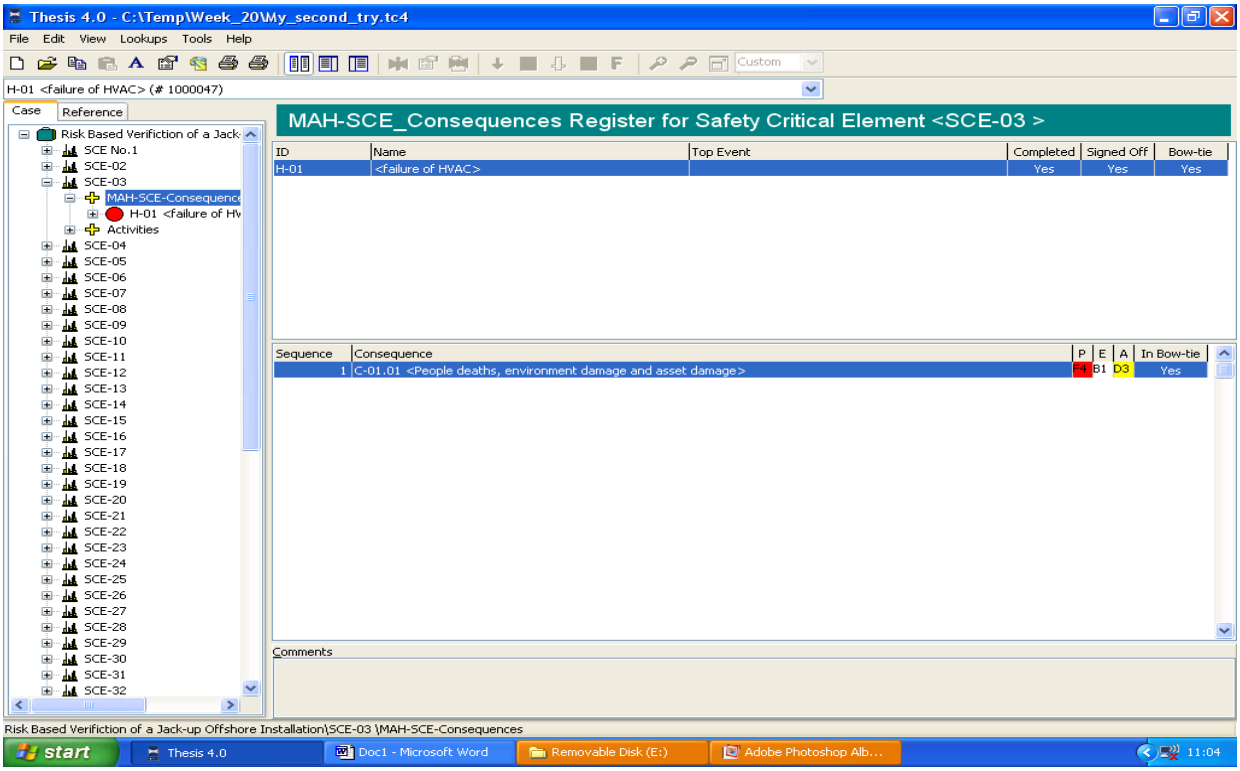

Figure A.5 – A Register of SCEs in THESIS

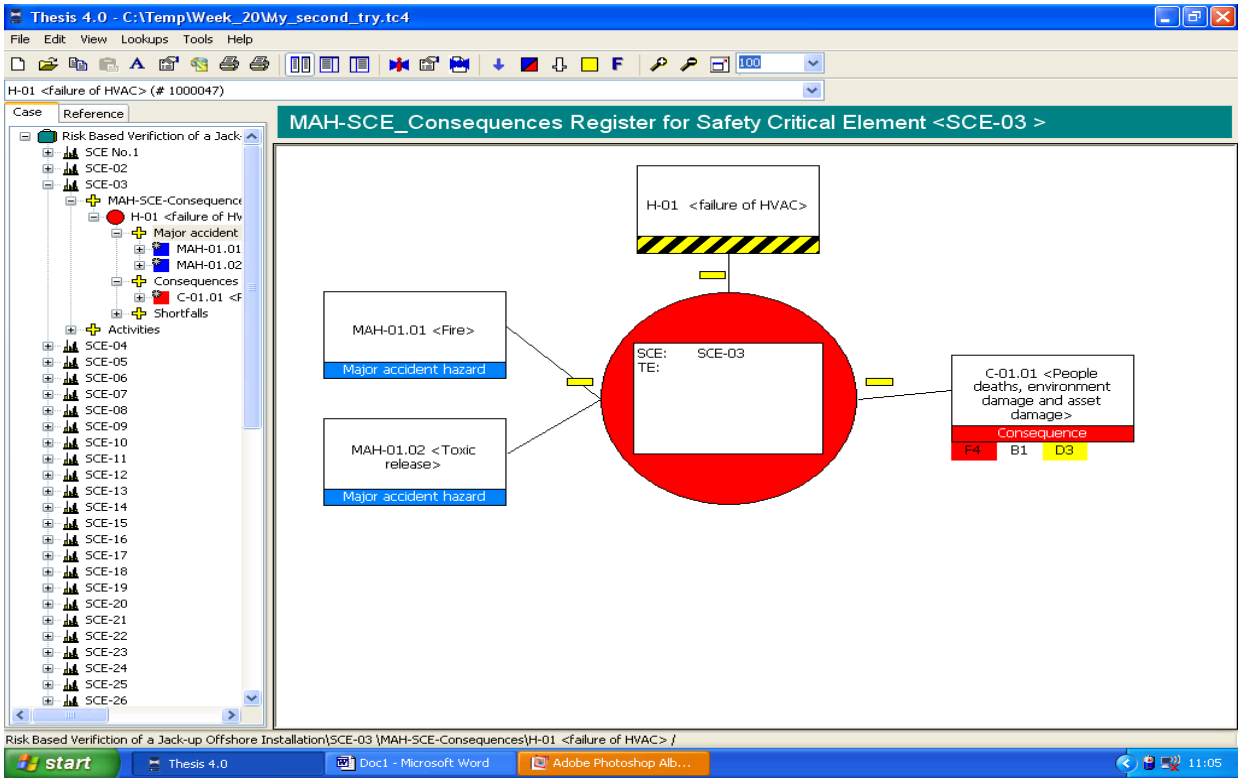

Figure A.6 – A Bow Tie Diagram of a SCE

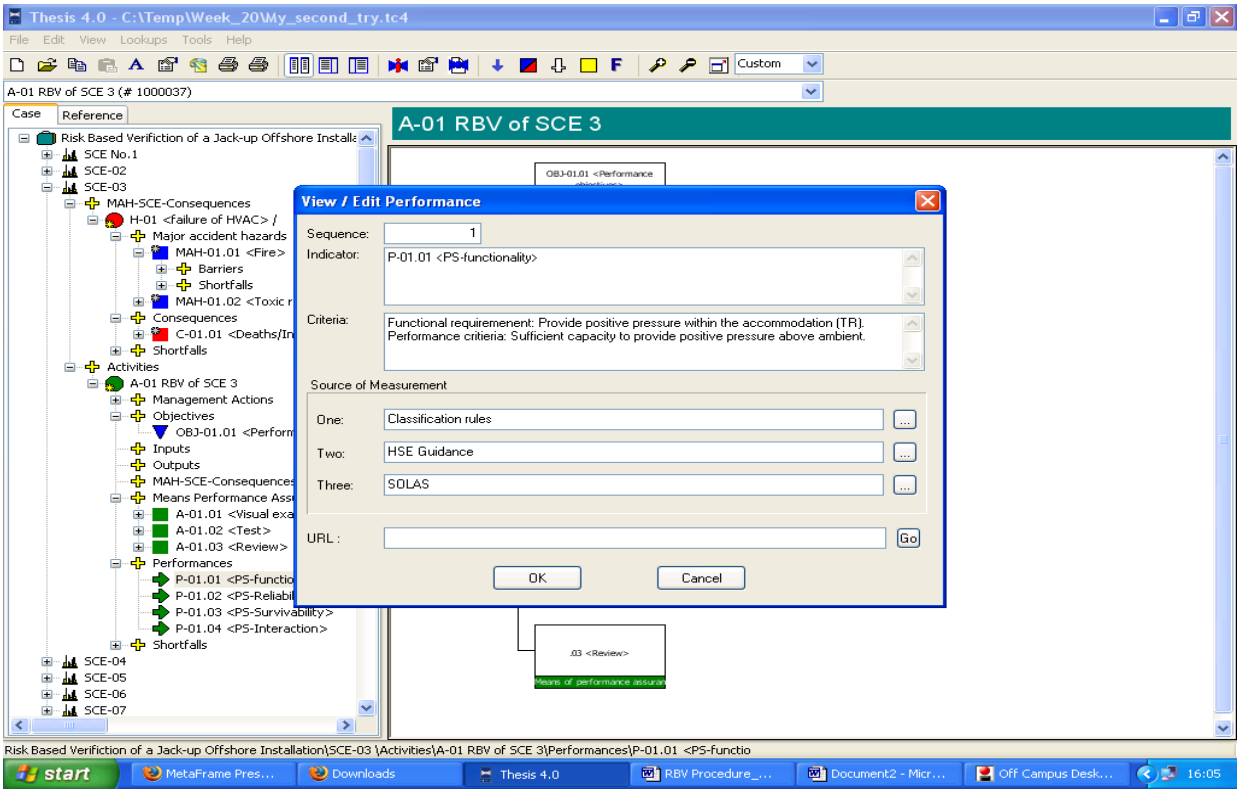

Figure A.7 – Performance Standard of the HVAC System in Terms of Functionality

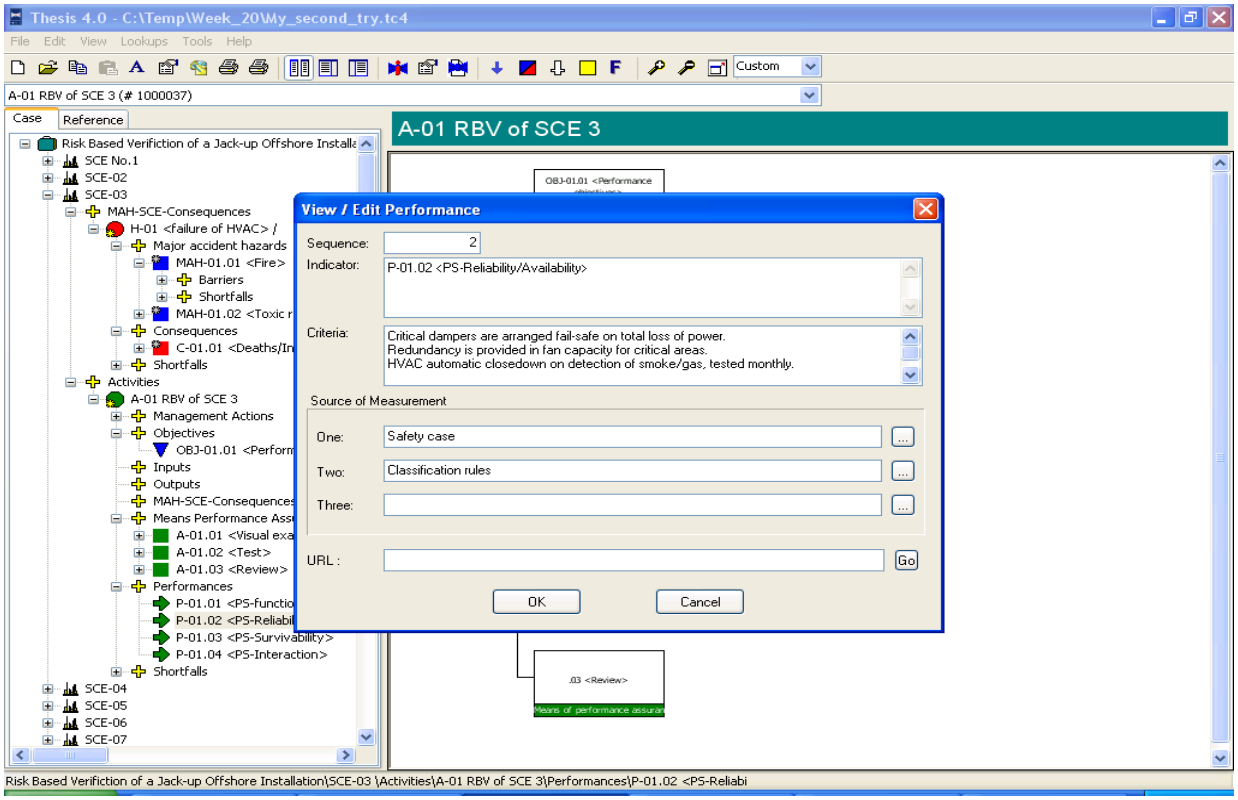

Figure A.8 – Performance Standard of the HVAC System in Terms of Reliability/Availability

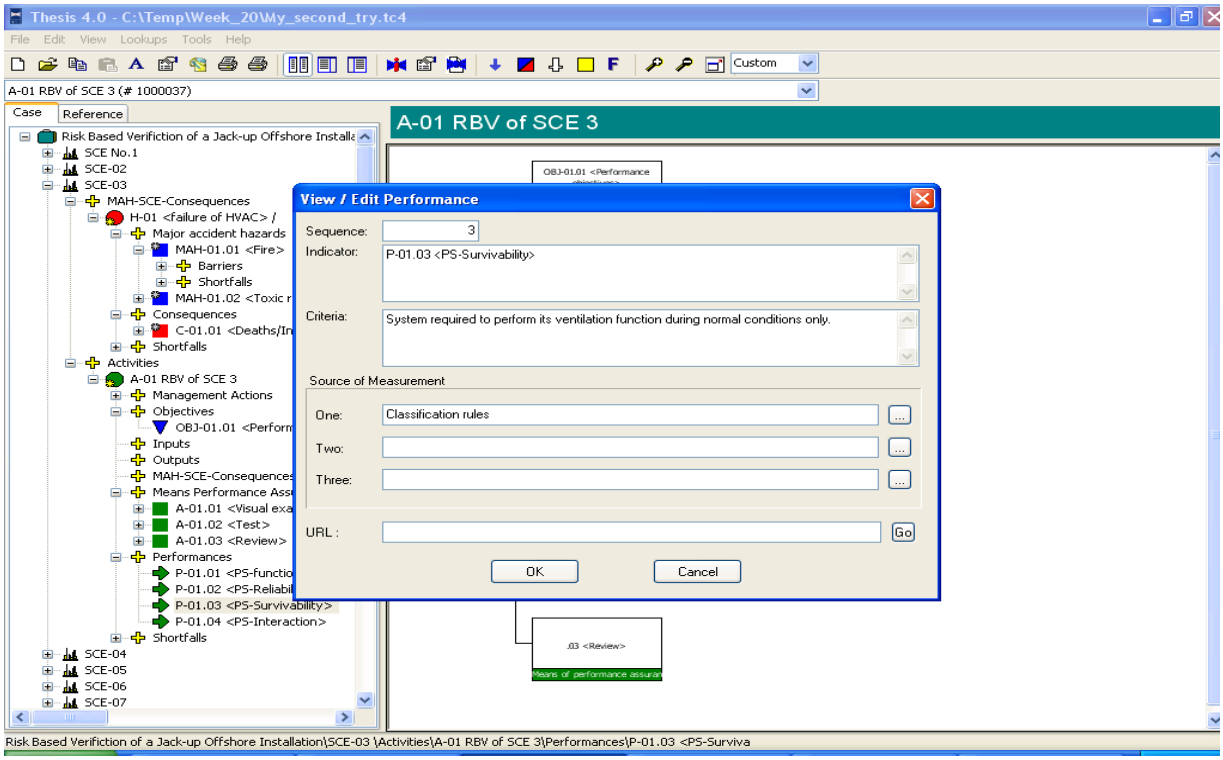

Figure A.9 – Performance Standard of the HVAC System in Terms of Survivability

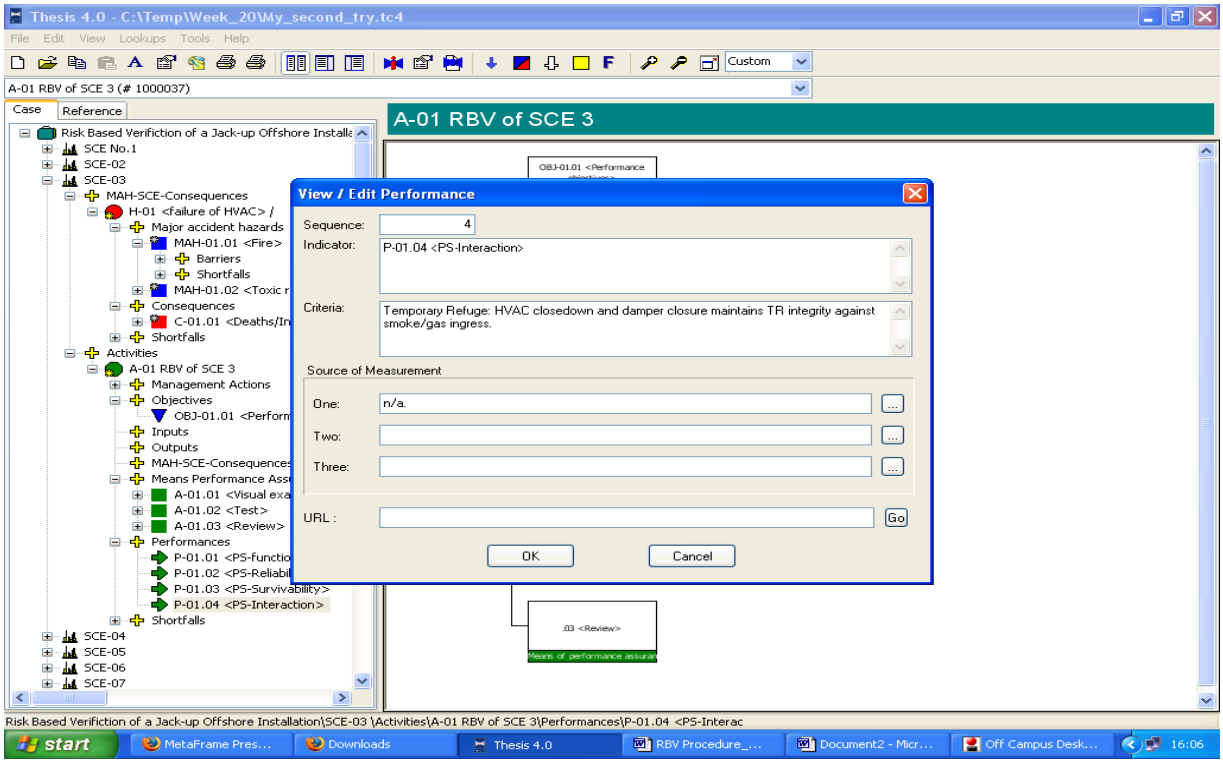

Figure A.10 – Performance Standard of the HVAC System in Terms of Interaction/Dependency on Other Systems

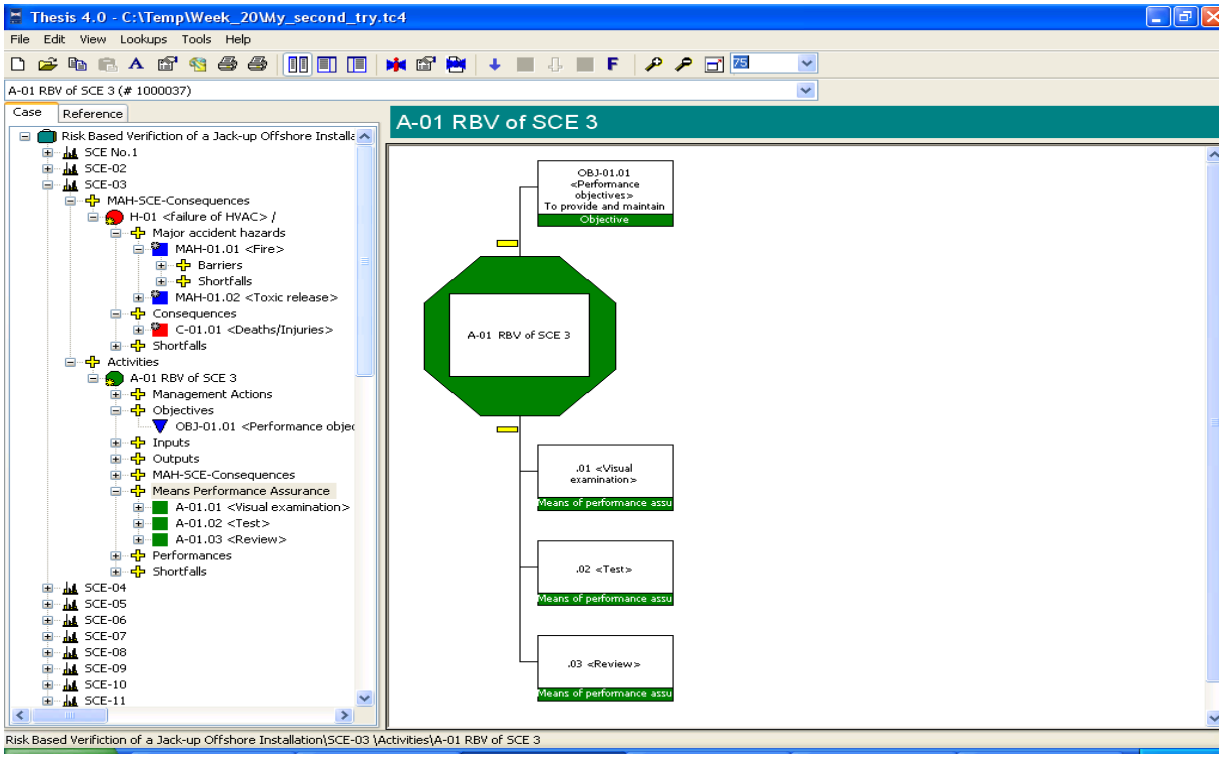

Figure A.11 – Means of Performance Assurance of the HVAC system

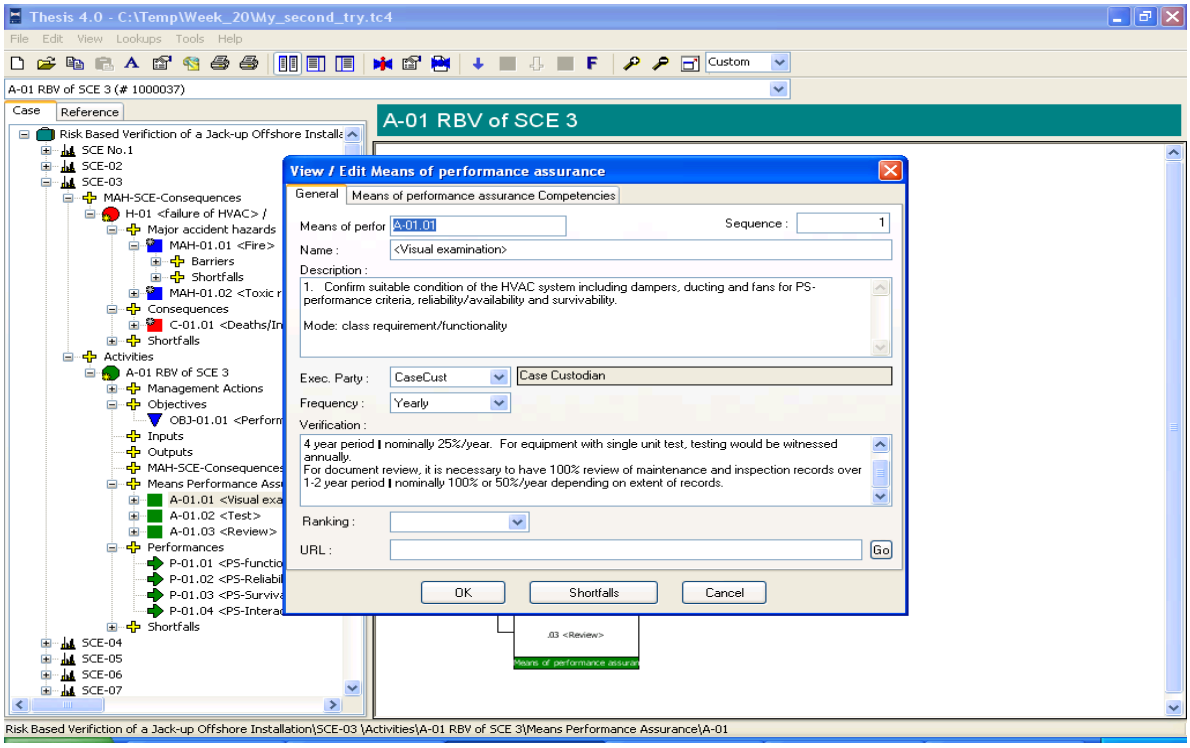

Figure A.12 – Means of Performance Assurance of the HVAC System in Terms of Visual Examination

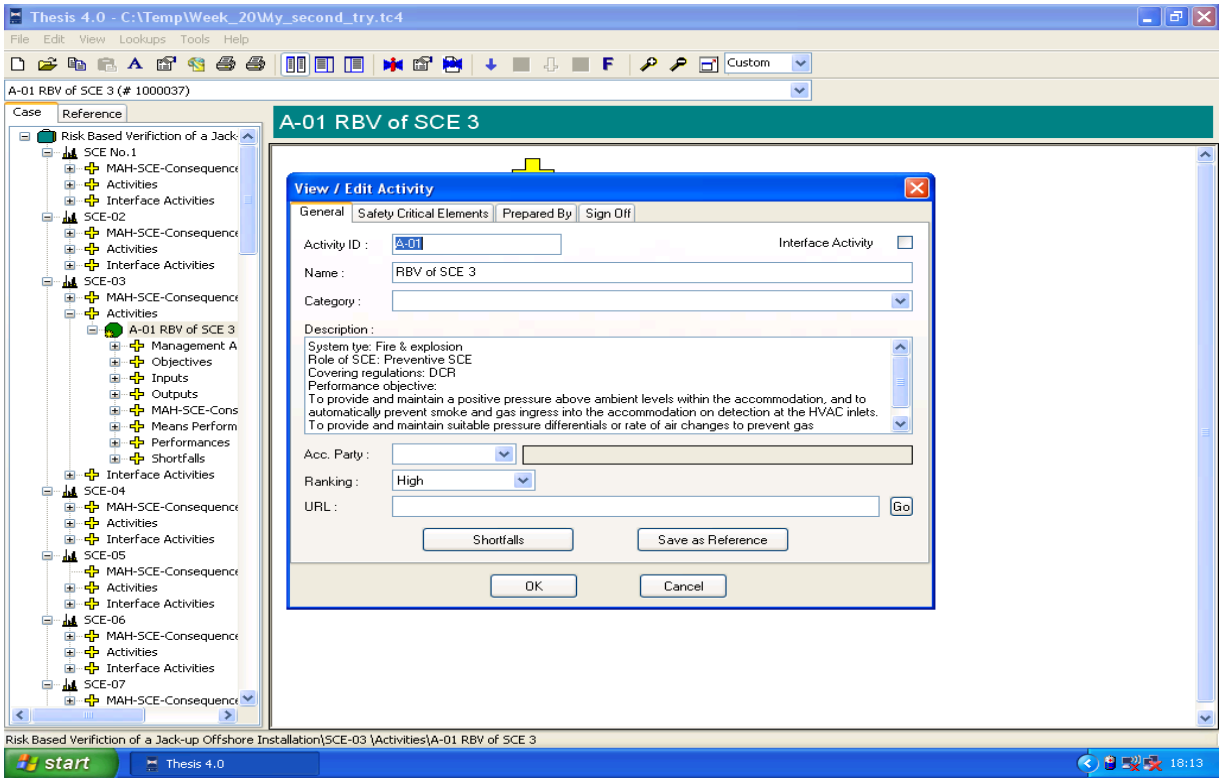

Figure A.13 – Criticality Rating of HVAC

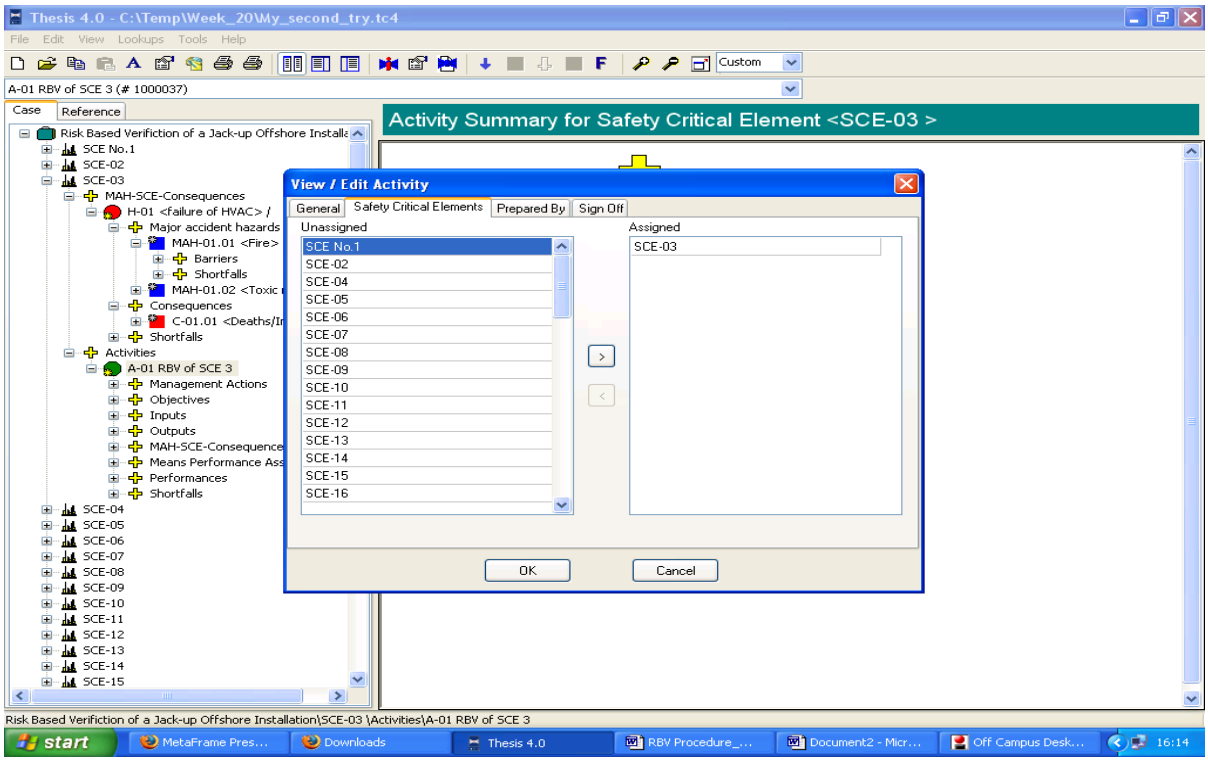

Figure A.14 – The Assignment of SCEs