Risk Assessing the Risk Identification Process

James Turner, Senior Consultant, Xodus Group Ltd. Cheapside House, 138 Cheapside, London, EC2V 6BJ, UK

Risk identification is the first step of a chain of processes of risk management. Risk identification happens at multiple stages through the life of a design from concept through development and into operation. Where risk identification fails, the potential exists for unidentified hazards to bypass the rest of the risk management process with all its safeguards, mitigations and systems. These can become major events and are colloquially known as "black swans" or characterised as "unknown unknowns". It is acknowledged that safety input to projects is most powerful (and cheapest) early in design; combining these statements, it is both efficient and impactful to overall safety of designs to focus on delivering the best possible risk identification processes.

This paper explores the ways that risk identification can fail and discusses ways to focus on improving risk identification processes and their delivery. A generic model for common risk identification techniques (such as HAZID and HAZOP, which are found to have common features in their iterative structure and the use of guidewords) has been developed using Hierarchical task Analysis (HTA). This model has then been subjected to a Human Failure Analysis (HFA). In so doing, a form of "meta-analysis" is provided, using risk assessing tools applied to the risk assessment process itself. The resultant model and failure modes discovered are presented and discussed.

Keywords: HAZOP, HAZID, Risk Assessments, Process Improvement

Introduction

There is a famous quote from Donald Rumsfeld, then US Secretary of Defence, which makes a seemingly garbled statement about knowns and unknowns. It was largely ridiculed at the time as being an example of obfuscating political verbiage, but on later analysis has gained some praise as a basic explanation of an important heuristic (decision making) principle.

> *"as we know, there are known knowns; there are things we know we know. We also know there are known unknowns; that is to say we know there are some things we do not know. But there are also unknown unknowns -- the ones we don't know we don't know." – Donald Rumsfeld, 2002*

In the context of risk identification, unknown unknowns should definitely concern us, for they are the unidentified, unaddressed risks to which we may be vulnerable. A term used regarding accidents is a 'black swan' event. This analogy relates to the experience of European explorers first encountering black swans in Western Australia in the 1690's, which overturned a commonly held belief, dating back to Roman times, that there were no such things as black swans. A black swan incident is one which blindsides an organisation and has the potential, because it has not been foreseen or planned for, to be of significant negative consequence.

Speaking at a very high level, there are two fundamental approaches which can mitigate risk from unknown unknowns. The first is to build a system which is as robust as possible in every way through its features and implementation, such that it will be capable in the face of both expected and unexpected challenges. This may mean different things in different contexts, but could include inherent safety, defence in depth through layered, independent barriers, monitoring / feedback systems and continual improvement - essentially, all aspects of modern best-practice risk management. The second is to seek to make risk identification as good as possible, and by doing so to reduce the potential number of black swans.

Any identified risk which is addressed by risk management cannot become a black swan to challenge the robustness of systems. The process of improving risk identification is therefore aligned with the inherent safety imperative, that it is better to remove a source of risk than build up controls and systems against it.

In addition, the nature of risk identification type activities is that they occur early in the design process. It is a truism that safety is cheapest when applied early in a design process, hence effort applied to improving risk identification will efficiently improve overall safety performance. This will be true up to a point of diminishing returns in further improvement; it is not being suggested that the goal should be no black swans, rather to make every effort to minimise the potential for them through improved risk identification.

These arguments make the case to focus on improvement of risk identification. It is incumbent on all process safety professionals to strive for excellence in risk identification, because to not do so is to lose an opportunity to better manage and control risks.

To provide structure to this goal of improving risk identification, a series of steps are proposed:

- characterise risk identification methods;
- develop a general model;
- apply rigorous failure mode analysis;
- consider revealed failure modes and ways to improve risk identification in the light of these.

Characterising Risk Identification Processes

The generic process of "risk identification" is one which can have many forms. Risk identification, as an activity, can span a vast array of processes from simple to complex. At the most basic level, all animal life engages in risk identification as they interact with their environment, taking in information from their senses, and using an array of heuristics (decision-making rules) to process this and adopt appropriate responses to any perceived threat.

Human behaviour follows a similar pattern, but the nature of our environment and the mental faculties with which we process information about it, allow much more complex risk identification and processing to occur, considering such factors as past events, predictions, team-based consensus assessment and advanced sensors and modelling. The apex of these processes is found in high hazard industries, where extensive and detailed risk identification processes seek to use the best tools available to identify unlikely, complex, potentially high consequence hazards as part of project and design processes.

Whilst a wide range of techniques have been developed [Gould, 2000], it can be stated that many fall into a closely comparable family, demonstrating a consistent set of identifying features. As a term of convenience, 'Facilitated Safety Hazard / Risk' review (FSHR) has been adopted [Turner, 2017]. The identifying features of methodology which characterise this group are:

1. FSHR studies are run as facilitated discussion and brainstorming workshops with a small, normally multidisciplinary, team of engineers and other specialists.
2. FSHR studies are concerned with the identification of hazards or risks and the associated safeguards and mitigations. They also identify recommendations or actions in consideration of the improvement of control of identified risks.
3. FSHR studies are iterative in their structure in that they repeatedly apply looping processes of assessment to different aspects of a scope. In some cases, these iterative loops are nested.
4. FSHR studies are recorded, often by a dedicated scribe, in a formal, structured "line item" style using some form of worksheet, usually on a computer.

A tabulation of some of the most popular techniques which fulfil these criteria is shown below. This listing is not exhaustive. They can be broken down into three sub-groups: Hazard & Operability (HAZOP) style, Hazard Identification (HAZID) style and Failure Mode & Effects Analysis (FMEA) style.

Table 1 – Types of Facilitated Hazard / Risk Review (FSHR)

Sub Group	Technique	Notes
HAZOP	HAZOP	Hazard & Operability study, using nodes, guidewords, parameters and deviations to guide brainstorming in consideration of detailed process schematics
	CHAZOP	HAZOP applied to computerised systems
	SAFOP / EHAZOP	HAZOP applied to electrical power systems
HAZID	HAZID	Hazard identification using nodes and guidewords to lead brainstorming of general project or design potential hazards
	ENVID	HAZID applied with environmental focus
	CHA	Keyword led concept phase study
	PHA	HAZID style concept assessment of process related hazards
FMEA	FMEA	Failure mode identification using a bottom up component level failure assessment.
	FMECA	FMEA adding consideration of criticality of failure.

Between them, these techniques account for a very large proportion of the structured risk identification used within high hazard industry design and project processes.

Developing a General Model for FSHR

Several existing models for FSHR-type hazard identification techniques have been put forward at varying levels of detail and scope. [Whitty, 2009 and IEC, 2016] These vary from detailed mechanical models which focus on the iterative structure, to more broad-brush views which provide context of all activities between scoping up a study and closing out actions. Each model is a suitable tool for its chosen purpose, be that education on the way the process works or a guide to implementation of procedure, however, for the purposes of this paper, a model was required which would allow forensic examination of potential failure modes. To this end, a Hierarchical Task Analysis (HTA) has been used to break down the process.

HTA is a process for the development of a structured, goal-oriented step-wise breakdown of any task operation. HTA proceeds by the following process:

- Define overall goal of the HTA in terms of the level of detail required, and the total scope which will be covered;
- Define the top-level task goal which will form the top level of the hierarchy;

- Define sub-tasks required to achieve the goal;
- In parallel, develop plan statements which indicate the logical sequence of operations, any loops or optional steps;
- Define further sub-sub-tasks and associated plan statements, using as many layers of nesting / sub-division as necessary to achieve the level of detail established by the overall goal.

In this case the developmental goal of the model is to:

- Provide a comprehensive scope which also represents the characteristic iterative style of FSHR;
- Deliver a level of detail of sub-task breakdown sufficient to allow a subsequent assessment of failure modes.

The HTA has been developed in software tool Human Factors Risk Manager v. 4.12.13.0 by HRA [Embrey, undated]. The resultant hierarchy is shown in Appendix A in tabular form, followed by diagrammatic outputs. The HTA identifies tasks and plans describing how the tasks will be completed and the agents, i.e. the persons responsible for carrying out the task. The resultant model is an abstract view of the process, but by stripping out the iterative looping into the plan statements, provides a suitable basis on which to base the subsequent Human Failure Analysis (HFA).

FSHR Failure Mode Analysis

To conduct a rigorous failure mode assessment of the risk assessment process itself, a "meta-risk identification", a desktop Human Failure Analysis (HFA) has been completed. The results of the study are shown in Appendix B.

HFA is a systematic process for failure mode identification, similar to FMEA, which dovetails with HTA by taking the bottom level tasks and seeking to develop failure mode scenarios for each in turn. Tasks are categorised, and guideword failure types are provided to facilitate scenario development. Table 2 below shows these activity types, and a breakdown of the analysis completed arraying these categories against the four top-level activities within the HTA. Table 3 details the totals of each individual failure mode.

Table 2 – Task Types

	Definition	Preparation	Examination	Documentation
Information Entry	0	0	2	0
Information retrieval	3	2	3	0
Information Communication	0	2	2	0
Diagnosis	1	0	7	0
Planning	1	3	0	0
Actions	0	2	4	4
Checking	0	0	0	2
Monitoring	0	0	3	0
Supervision	0	0	2	0

Table 3 – Failure Modes

ACT5 Action too fast/slow	1	COM1 information not communicated	2
ACT9 Action omitted	5	COM4 Ambiguous/unclear information communicated	2
ACT8 Wrong action on right object	2	DIAG1 Diagnosis not carried out	1
ACT10 Action incomplete	1	DIAG3 Diagnosis incorrect	6
ACT11 Action too early/late	1	PL1 No plan	1
INFR1 Information not obtained	2	PL2 Inaccurate plan	3
INFR3 Information retrieval incomplete	1	MON1 Monitoring omitted	3
INFR4 Information incorrectly interpreted	2	SUP2 Supervision inadequate	2
INFR2 Wrong information obtained	3	CH1 Check omitted	1
INFE1 Information entered into wrong place/field	1	CH4 Wrong check	1
INFE2 Wrong information entered	1		

Improving FSHR Practice

The analysis completed has used a generic model to generate a set of potential failure modes. From this it can be seen that failure modes are most common in the preparation and execution phases, and that the single most common failure mode is incorrect diagnosis, while there are a large spread of failure modes associated with the incorrect treatment or communication of information. No value judgements have been made however, to the severity or likelihood of each of these failure modes, as these values will be determined to a large extent by situation-specific factors.

The process followed, of the development of HTA and a subsequent HFA, could be applied by a company or practitioner in a manner related to an individual study type, or to a specific facility or series of studies, to yield a bespoke failure mode profile which could be taken further in analysing failures and developing improvements in risk identification practice.

In seeking to improve risk identification practice, a number of approaches are available [Health & Safety Laboratory, 2003], and the following sections are provided as examples of potential routes to achieve this goal, in terms of strategy, tactics and implementation.

Marginal Gains – An example strategy for improvement

The fundamental potential consequence identified throughout the HFA which has a direct safety implication is that of failure to identify, or to propagate forward through the study a potential hazard for consideration. By failing to carry this hazard beyond the identification stage, none of the later safeguards, mitigations or hazard management processes can address it. (This is the "black swan" condition referred to earlier.)

As seen from the model created, the process of conducting a FSHR study is one with a very large number of steps. The model, which strips out the iteration inherent to the process, identifies twenty-five discrete steps, but over the course of an entire study as it is executed, iteration will result in many of these steps (primarily steps 3.1 – 3.4) being iterated hundreds, perhaps even thousands of times. Where a step is repeated so many times, even a small percentage chance of failure will have a large effect on the overall quality of the study.

The concept of "Marginal Gains" is a sporting strategy made famous by GB Olympic cycling performance director, Dave Brailsford in 2003. The principle is to attack individual failure modes of each step of a process for small gains to improve the overall process additively. This is directly applicable given that risk identification is a many-stepped process, with failure modes in each step that can be individually attacked.

Marginal gains strategy can be seen as merely an exhortation to, "do everything better", but successful implementation of the strategy involves a more considered process of identifying failure modes within the process and sequentially addressing them through minor changes and improvements (such as the example tactic and implementation following) to achieve the end goal of an overall better process.

Purity of Study – An example tactical decision for improvement

The tactical decisions made in setting up a study will be strongly correlated with the eventual quality of the risk identification completed; one such decision is how "pure" to make a study. What is meant by this is, to what extent the study will be focussed only on risk identification, or if it will also provide aspects of risk assessment or other elements of the surrounding engineering process.

A hypothetical 100% pure risk identification study would be one which ceased consideration of an issue as soon as the potential risk scenario had been detailed. In practice, as a bare minimum, a filter is placed over this level of output regarding whether the assessing team consider it to be credible. Non-credible hazards are not recorded, credible hazards are recorded.

Many studies proceed further in moving from identification into an assessment mode of operation. This may include risk assessment against a matrix, identification of safeguards and mitigations, and generation of recommendations. Risk assessment matrices (three by three, five by five or other such grids, which set likelihood against severity to characterise risk) are a powerful tool in rapidly pseudo-quantifying risk. They can be applied both before and after the consideration of safeguards and mitigations if the study identifies such features. These safeguards and mitigations may be implemented already or possibly suggested for implementation by raised recommendations. A further step away from "pure" risk identification is the appending of other processes to the review, such as Safety Integrity Level (SIL) assessment.

These additional elements are the natural follow on steps as part of the overall risk management process. It is not wrong to incorporate them, but it should be done consciously, with awareness of what effect this will have, in terms of time taken, and level of focus provided to the core risk identification task. In particular, the decision must be made of whether to include these add-ons within the iterative structure i.e. to complete all tasks (risk identification, risk assessment, SIL assessment) for one line-item at a time before moving onto the next, or to block them at the end of a node, a day or the whole study.

Scope Stitching – An example best practice implementation for improvement

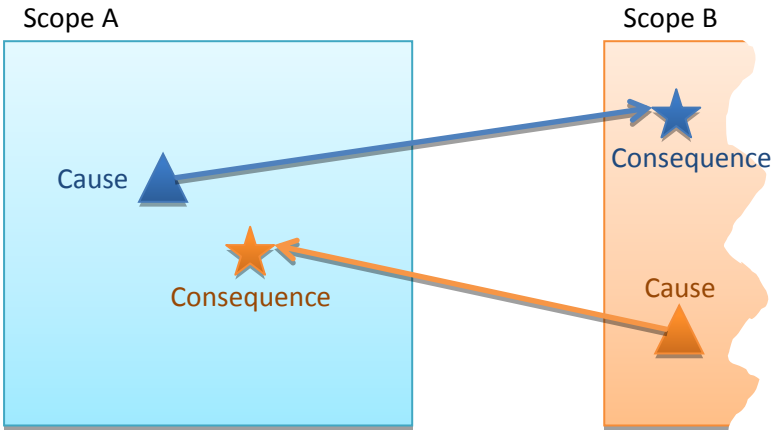
One of the error types identified within the HFA (Line item 1.1, "Elements of scope omitted from study") is concerned with the definition of boundaries, and what can happen if incomplete coverage is provided either by the study as a whole or in a gap between two nodes of a study. The following best practice addresses this failure mode.

The purpose of this treatment is to ensure complete coverage of potential hazards for the scope whilst minimising wasteful consideration of items outside of scope. The approach is to: during review of Scope A, consider the consequences on Scope

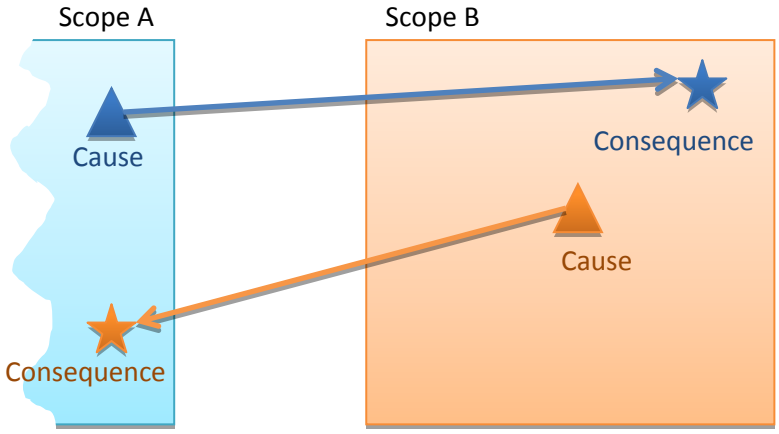
B of all causes within Scope A and consider causes from adjacent Scope B (so far as they are apparent) with impact anywhere on Scope A.

Then when reviewing Scope B, invert that process: consider the consequences on Scope A of all causes within Scope B and consider causes / risk sources within Scope A with impact on Scope B. This means reviewing this boundary region twice effectively, but by covering it while "standing on both sides of the divide" good confidence can be achieved of fully overlapping the join, "stitching together" the two pieces of scope and not missing anything. This is illustrated in Figure 1 below.

View during review of Scope A



View during Review of Scope B



Total produced seamless coverage

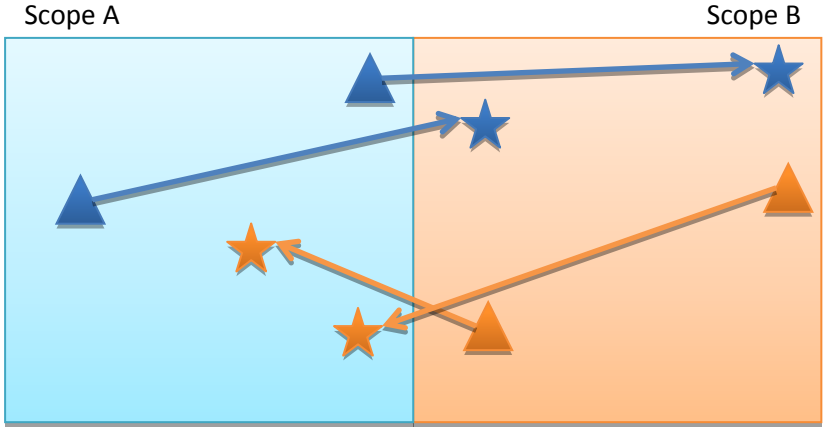


Figure 1 – Illustration of Scope Stitching Approach

Conclusion

This paper seeks to draw together a number of threads in regard to the development of best practice in the field of risk identification. The existence as a concept of "unknown unknown", "black swan" events is posited, and the threat that they can pose to any system of risk management. Defence against potential black swans can be achieved through minimisation of these potential unrevealed risks, by focussing on best practice excellence in the field of risk identification.

As a systematic methodology to drive a repeatable, scientific process of improvement, a model is proposed, to genericise the risk assessment methodology process itself, using Hierarchical Task Analysis to break down these complex workshop-based activities into intelligible steps, which can be further subjected to Human Failure Analysis. These two steps may be repeated, and made situation specific, in any high hazard industry which makes use of similar risk identification tools conforming to the familiar facilitated workshop style.

In possession of such an assessment of risk identification methodology failure modes, practitioners are well placed to seek the required improvements, using whatever methodologies (of which some examples are explored) in terms of high-level improvement strategies, situation-specific tactics, or detail-focussed implementation improvements are found most appropriate and relevant.

Acknowledgements

The author wishes to thank the staff of the University of Sheffield Process Safety & Loss Prevention course, his supporting colleagues at Xodus Group and cooperating client organisations of projects on which this paper bases its findings.

References

Embrey, D, Zaed, S, "A Set of Computer Based Tools Identifying and Preventing Human Error in Plant Operations", www.humanreliability.com/software, undated

Gould, J, Glossop, M, Loannides, A, "Review of Hazard Identification Techniques", Health and Safety Laboratory, HSL/2005/58, 2000

Health & Safety Laboratory, "Good Practice and Pitfalls in Risk Assessment", Research Report 151, 2003

International Electrotechnical Commission (IEC), "Hazard and Operability Studies (HAZOP Studies) Application Guide", IEC 61882:2016 Edition 2.0, 2016

Turner, J, "Investigating the Quantification and Analysis of Facilitated Safety Hazard / Risk Review Processes", University of Sheffield, 2017

Whitty, S, Foord, T, "Is HAZOP worth the effort it takes?", Hazards21 Paper 91, 2009

Appendix A – HTA

ID	Description	Agent/Person
Plan 0	Do in sequence	
1	Definition	
Plan 1	Do in sequence	
1.1	Define scope & objectives	Study Customer
1.2	Define FSHR Study type	Study Customer & Facilitator
1.3	Define Responsibilities & select team	Study Customer & Facilitator
2	Preparation	
Plan 2	2.1 - 2.4 can be completed in parallel / any sequence, then do 2.5 & 2.6 in sequence	
2.1	Plan study	Facilitator & Scribe
2.2	Collect Data	Facilitator, Scribe & Team
2.3	Develop template / recording tool	Scribe & Facilitator
2.4	Estimate timing & develop schedule	Facilitator, Scribe & Team
2.5	Arrange meetings	Scribe & Facilitator
2.6	Publish Terms of Reference	Scribe & Facilitator
3	Examination	
Plan 3	[Note 3.3 & 3.4 occur continuously during all phases of 3] Complete 3.1 then 3.2, iterating these two steps for all sections of primary scope division (commonly nodes)	
3.1	Define intent of section of primary scope division	Facilitator, Scribe & Team
3.2	Assess section of primary scope division	
Plan 3.2	Complete 3.2.1, iterating this step for all instances of secondary level scope division (commonly guidewords, or parameters if tertiary iteration is applicable)	
3.2.1	Assess section of secondary scope division	Facilitator, Scribe & Team
Plan 3.2.1	If applicable, iterate 3.2.1.1 for all instances of tertiary level scope division (commonly guidewords)	
3.2.1.1	Assess section of secondary / tertiary scope division	
Plan 3.2.1.1	Complete 3.2.1.1.1 - 3.2.1.1.4, iterating these steps for all credible hazards	
3.2.1.1.1	Identify deviation from design intent	Facilitator, Scribe & Team
3.2.1.1.2	Identify causes and potential consequences	Facilitator, Scribe & Team
3.2.1.1.3	Identify safeguards and mitigators	Facilitator, Scribe & Team
3.2.1.1.4	Identify appropriate additional recommendations where required	Facilitator, Scribe & Team
3.3	Manage Study	
Plan 3.3	Complete as required during study	
3.3.1	Manage study progress and duration, taking breaks appropriately	Facilitator
3.3.2	Manage team, maintaining focus and attention	Facilitator
3.3.3	Manage scribe, ensuring accurate understanding and recording	Facilitator
3.4	Record FSHR study	Scribe
4	Documentation	
Plan 4	Complete 4.1 - 4.3 in sequence	
4.1	Check records	Scribe & Facilitator
4.2	Produce & issue report	Scribe & Facilitator
4.3	Distribute recommendations to actionees	Scribe

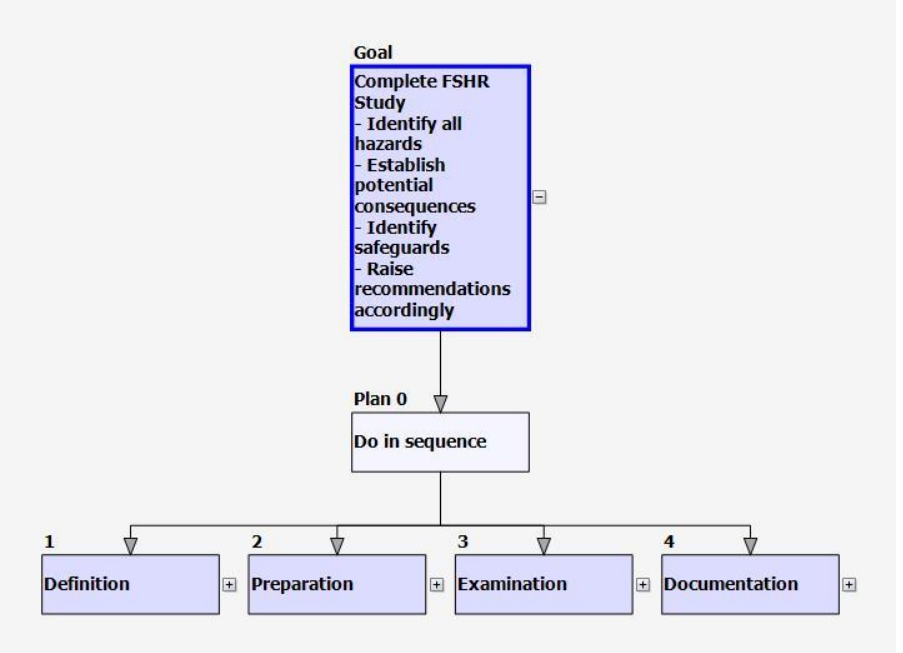


Figure A1 - Top level Structure, FSHR HTA

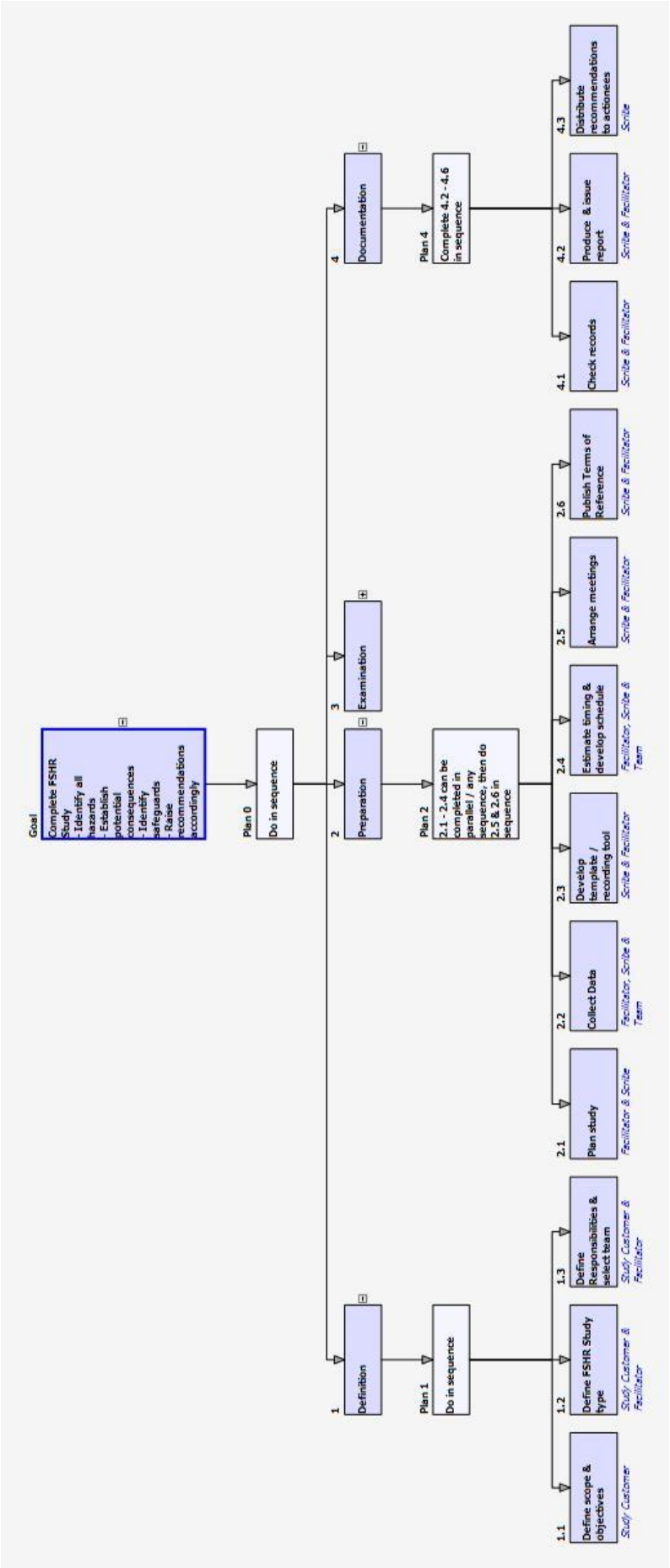


Figure A2 - 1st & 2nd Level Structure (Examination branch minimised), FSHR HTA

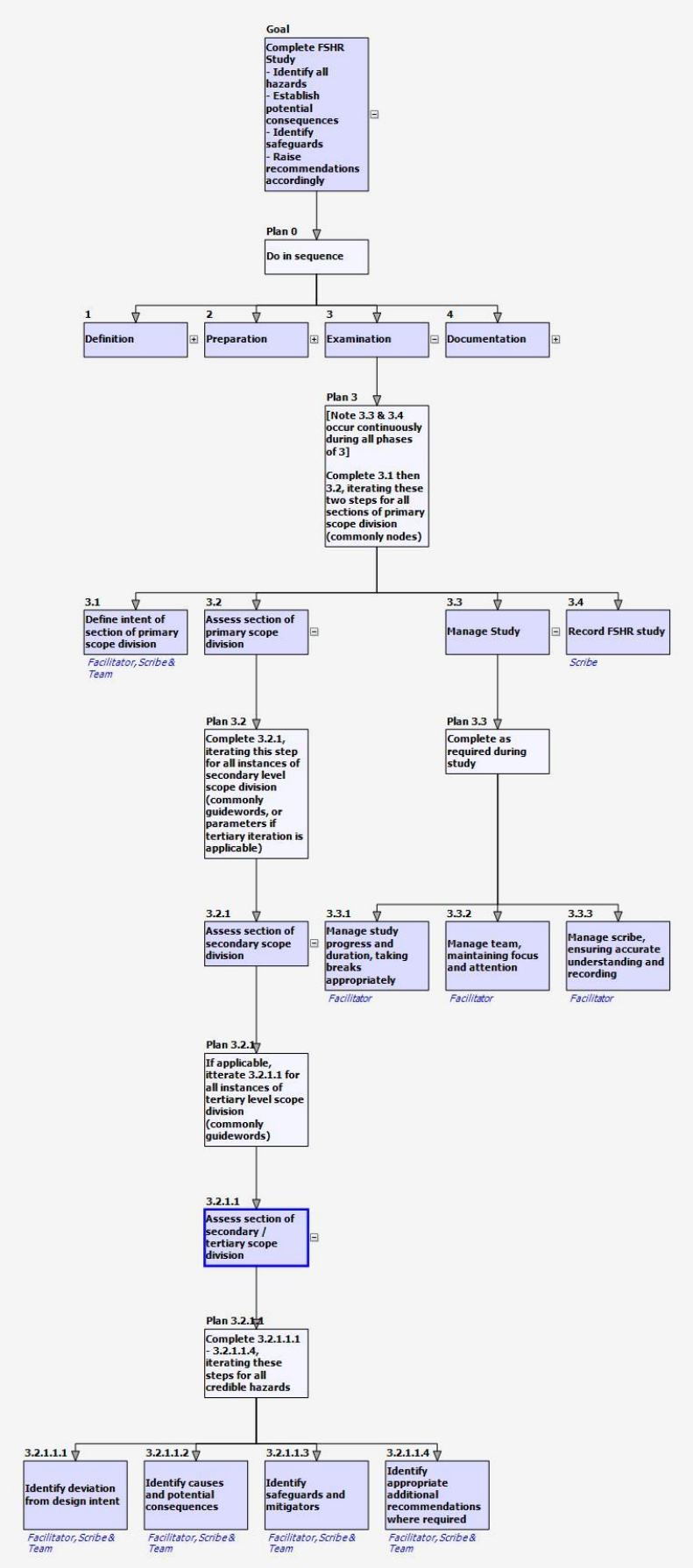


Figure A3 - Examination branch structure, FSHR HTA

Appendix B – HFA

ID	Description	Agent/Person	Activity Type	Failure Mode	Error Description	Consequences	Existing Risk Control Measures
Plan 0	Do in sequence						
1	Definition						
Plan 1	Do in sequence						
1.1	Define scope & objectives	Study Customer	Information Retrieval	INFR3 Information retrieval incomplete	Insufficient data available to successfully carry out study	Study postponed or not completed, or attempted without suitable information.	Project management processes, technical authority checks
1.1	Define scope & objectives	Study Customer	Information Retrieval	INFR4 Information incorrectly interpreted	Elements of scope omitted from study	Study incomplete. Element of design not subjected to hazard identification leading to unknown hazards propagating through design	Technical authority checks
1.2	Define FSHR Study type	Study Customer & Facilitator	Diagnosis	DIAG3 Diagnosis incorrect	Incorrect study type selected	Study not fit for purpose, either presenting insufficient level of detail or being overly onerous and time consuming	Engineering procedures, technical authority checks
1.3	Define Responsibilities & select team	Study Customer & Facilitator	Planning	PL1 No plan	Inappropriate facilitator, scribe or team member selected	Reduced likelihood of successful study completion, or reduced overall quality of study	Engineering procedures, technical authority checks
1.3	Define Responsibilities & select team	Study Customer & Facilitator	Information Retrieval	INFR1 Information not obtained	Selected team members unavailable or too busy to dedicate time to study	Inability to start or complete study, potential for elements of study to be completed without relevant discipline input	Project management processes, facilitator enforcement of need for quorate team at all times
2	Preparation						
Plan 2	2.1 - 2.4 can be completed in parallel / any sequence, then do 2.5 & 2.6 in sequence						
2.1	Plan study	Facilitator & Scribe	Planning	PL2 Inaccurate plan	Insufficient time allowed for study	Reduced quality of study due to rushing or inability to finish review of scope	Formal estimation process
2.2	Collect Data	Facilitator, Scribe & Team	Information Retrieval	INFR2 Wrong information obtained	Incorrect drawings or revisions of drawings used	Scope reviewed not reflecting design, leading to incorrect hazards being identified or missed	Engineering procedures, technical authority checks
2.2	Collect Data	Facilitator, Scribe & Team	Information Retrieval	INFR1 Information not obtained	Drawings not available or not acquired / not ready in time	Inability to start study or attempting to proceed without drawings leading to inability to successfully complete study	Project management processes, technical authority checks
2.3	Develop template / recording tool	Scribe & Facilitator	Actions	ACT9 Action omitted	Template not developed ahead of study	Inability to start study	Engineering procedures, technical authority checks
2.3	Develop template / recording tool	Scribe & Facilitator	Actions	ACT8 Wrong action on right object	Unfamiliarity with recording software	Inability of scribe to keep up with study	Training and selection of scribe
2.4	Estimate timing & develop schedule	Facilitator, Scribe & Team	Planning	PL2 Inaccurate plan	Insufficient time allowed for study	Reduced quality of study due to rushing or inability to finish review of scope	Formal estimation process
2.4	Estimate timing & develop schedule	Facilitator, Scribe & Team	Planning	PL2 Inaccurate plan	Study setup in wrong order	Reduced efficiency of study process	Facilitator and scribe experience, technical authority checks
2.5	Arrange meetings	Scribe & Facilitator	Information Communication	COM1 Information not communicated	FSHR study not communicated to team, room not booked etc.	Inability to start study, double booking may reduce attendance	Engineering procedures
2.6	Publish Terms of Reference	Scribe & Facilitator	Information Communication	COM1 Information not communicated	FSHR team not provided with information ahead of study	Reduced efficiency at start of study due to need for more alignment process	Engineering procedures
3	Examination						

ID	Description	Agent/Person	Activity Type	Failure Mode	Error Description	Consequences	Existing Risk Control Measures
Plan 3	[Note 3.3 & 3.4 occur continuously during all phases of 3] Complete 3.1 then 3.2, iterating these two steps for all sections of primary scope division (commonly nodes)						
3.1	Define intent of section of primary scope division	Facilitator, Scribe & Team	Actions	ACT9 Action omitted	Attempting to start FSHR without first describing system and system intent	Misalignment of team understanding, inability to efficiently proceed with study	FSHR procedures
3.1	Define intent of section of primary scope division	Facilitator, Scribe & Team	Actions	ACT10 Action incomplete	Insufficient discussion of primary scope division	Misalignment of team understanding, inability to efficiently proceed with study	FSHR procedures, facilitator checks on team alignment prior to commencing study
3.2	Assess section of primary scope division						
Plan 3.2	Complete 3.2.1, iterating this step for all instances of secondary level scope division (commonly guidewords, or parameters if tertiary iteration is applicable)						
3.2.1	Assess section of secondary scope division						
Plan 3.2.1	If applicable, iterate 3.2.1.1 for all instances of tertiary level scope division (commonly parameters)						
3.2.1.1	Assess section of secondary / tertiary scope division						
Plan 3.2.1.1	Complete 3.2.1.1.1 - 3.2.1.1.4, iterating these steps for all credible hazards						
3.2.1.1.1	Identify deviation from design intent	Facilitator, Scribe & Team	Diagnosis	DIAG3 Diagnosis incorrect	Inability of team to brainstorm credible hazards	Gap in coverage of study review leading to unrevealed hazards	FSHR procedures often including guidewords, selection of appropriately experienced and trained facilitator
3.2.1.1.1	Identify deviation from design intent	Facilitator, Scribe & Team	Diagnosis	DIAG3 Diagnosis incorrect	Team developing a hazard scenario which is not real	Potential for development of unneeded safeguards or recommendations	FSHR procedures, selection of appropriately experienced and trained facilitator, team knowledge of scope and understanding of process
3.2.1.1.1	Identify deviation from design intent	Facilitator, Scribe & Team	Information Retrieval	INFR4 Information incorrectly interpreted	Misunderstanding of scope or intent leading to incorrect hazards identified	Incorrect or unrevealed hazards	FSHR procedures, selection of appropriately experienced and trained facilitator
3.2.1.1.1	Identify deviation from design intent	Facilitator, Scribe & Team	Information Communication	COM4 Ambiguous/unclear information communicated	Different team members misunderstanding each other's' perspectives on scope or intent leading to incorrect hazards identified	Incorrect or unrevealed hazards	FSHR procedures, selection of appropriately experienced and trained facilitator
3.2.1.1.1	Identify deviation from design intent	Facilitator, Scribe & Team	Actions	ACT9 Action omitted	Deviation identified but not recorded or not recorded correctly	Incorrect or unrevealed hazards	FSHR procedures, selection of appropriately experienced and trained facilitator and scribe
3.2.1.1.2	Identify causes and potential consequences	Facilitator, Scribe & Team	Information Retrieval	INFR2 Wrong information obtained	Cause not identified, leading to discounting of a real hazard	Gap in coverage of study review leading to unrevealed hazards	FSHR procedures, selection of appropriately experienced and trained facilitator, team knowledge of scope and understanding of process

ID	Description	Agent/Person	Activity Type	Failure Mode	Error Description	Consequences	Existing Risk Control Measures
3.2.1.1.2	Identify causes and potential consequences	Facilitator, Scribe & Team	Diagnosis	DIAG3 Diagnosis incorrect	Incorrect cause identified leading to misunderstanding of hazard potential	Incorrect or unrevealed hazards	FSHR procedures, selection of appropriately experienced and trained facilitator, team knowledge of scope and understanding of process
3.2.1.1.2	Identify causes and potential consequences	Facilitator, Scribe & Team	Diagnosis	DIAG3 Diagnosis incorrect	Consequence underestimated or overestimated	incorrect severity of hazard recorded leading to insufficient or unnecessary safeguards and recommendations	FSHR procedures, selection of appropriately experienced and trained facilitator, team knowledge of scope and understanding of process
3.2.1.1.2	Identify causes and potential consequences	Facilitator, Scribe & Team	Diagnosis	DIAG1 Diagnosis not carried out	Category of consequence (e.g. environmental) not considered	Unrevealed consequences	FSHR procedures, selection of appropriately experienced and trained facilitator, team knowledge of scope and understanding of process
3.2.1.1.3	Identify safeguards and mitigators	Facilitator, Scribe & Team	Diagnosis	DIAG3 Diagnosis incorrect	Incorrect safeguards and mitigators identified	Potential for hazard to be insufficiently controlled	FSHR procedures, selection of appropriately experienced and trained facilitator, team knowledge of scope and understanding of process
3.2.1.1.4	Identify appropriate additional recommendations where required	Facilitator, Scribe & Team	Diagnosis	DIAG3 Diagnosis incorrect	Required recommendations not raised	Potential for hazard to be insufficiently controlled	FSHR procedures, selection of appropriately experienced and trained facilitator, team knowledge of scope and understanding of process
3.2.1.1.4	Identify appropriate additional recommendations where required	Facilitator, Scribe & Team	Information Communication	COM4 Ambiguous/unclear information communicated	Recommendations insufficiently detailed to allow later comprehension / completion	Potential for inability to achieve recommendation intent leading to uncontrolled hazards	FSHR procedures, selection of appropriately experienced and trained facilitator
3.3	Manage Study						
Plan 3.3	Complete as required during study						
3.3.1	Manage study progress and duration, taking breaks appropriately	Facilitator	Monitoring	MON1 Monitoring omitted	Failure to maintain planned schedule	Inability to complete study to time, or rushing of later stages of study	FSHR procedures, selection of appropriately experienced and trained facilitator
3.3.1	Manage study progress and duration, taking breaks appropriately	Facilitator	Monitoring	MON1 Monitoring omitted	Sessions running too long, not taking regular breaks	Fatigue of study team leading to reduced quality of output and efficiency of working	FSHR procedures, selection of appropriately experienced and trained facilitator
3.3.2	Manage team, maintaining focus and attention	Facilitator	Supervision	SUP2 Supervision inadequate	Failure to prevent team digressing from scope or process	Reduced efficiency of FSHR process	FSHR procedures, selection of appropriately experienced and trained facilitator
3.3.2	Manage team, maintaining focus and attention	Facilitator	Monitoring	MON1 Monitoring omitted	Failure to retain attention of team members on focus of study	Reduced participation and engagement in study, resulting in lower quality of output, potential to not identify all appropriate hazards	FSHR procedures, selection of appropriately experienced and trained facilitator
3.3.3	Manage scribe, ensuring accurate understanding and recording	Facilitator	Supervision	SUP2 Supervision inadequate	Failure to provide support to scribe, clarifying and checking	Potential for errors in records, scribe excessively stressed	FSHR procedures, selection of appropriately experienced and trained facilitator
3.4	Record FSHR study	Scribe	Information Retrieval	INFR2 Wrong information obtained	Scribe mishearing or misunderstanding information	Errors in meeting record leading to loss of information	Facilitator checks, selection of appropriately experienced and knowledgeable scribe

ID	Description	Agent/Person	Activity Type	Failure Mode	Error Description	Consequences	Existing Risk Control Measures
3.4	Record FSHR study	Scribe	Information Entry	INFE1 Information entered into wrong place/field	Scribe misplacing information within worksheets	Errors in meeting record leading to loss of information	Facilitator checks, selection of appropriately experienced and knowledgeable scribe
3.4	Record FSHR study	Scribe	Information Entry	INFE2 Wrong information entered	Typographic errors (especially of alphanumeric detail e.g. equipment tag numbers)	Errors in meeting record leading to loss of information	Facilitator checks, selection of appropriately experienced and knowledgeable scribe
3.4	Record FSHR study	Scribe	Actions	ACT5 Action too fast/slow	Scribe unable to keep up with pace of study	Reduced efficiency of study	Software shortcuts and aids, selection of appropriately experienced and capable scribe
4	Documentation						
Plan 4	Complete 4.1 - 4.3 in sequence						
4.1	Check records	Scribe & Facilitator	Checking	CH1 Check omitted	Inaccuracies in meeting records unrevealed	Report developed with errors, potential for inaccurate hazard information to be transmitted	Technical authority checks
4.1	Check records	Scribe & Facilitator	Checking	CH4 Wrong check	Post-meeting changes made to study without agreement of study team	Potential for workshop based decisions to be altered by checkers opinions, invalidating the results	Technical authority checks
4.2	Produce & issue report	Scribe & Facilitator	Actions	ACT11 Action too early/late	Excessive delay in producing report	Delay in hazard information being communicated to project, may reduce time available to solve issues raised	Engineering procedures, technical authority checks
4.2	Produce & issue report	Scribe & Facilitator	Actions	ACT9 Action omitted	Formal report not issued	Information not communicated to project, or reliance on uncontrolled, unofficial study output records	Engineering procedures, technical authority checks
4.3	Distribute recommendations to actionees	Scribe	Actions	ACT9 Action omitted	Recommendations not distributed to actionees	Inability to address issues raised by study leading to uncontrolled or insufficiently controlled hazards	Engineering procedures, technical authority checks
4.3	Distribute recommendations to actionees	Scribe	Actions	ACT8 Wrong action on right object	Recommendations distributed to incorrect / inappropriate people	Inability to address issues raised by study leading to uncontrolled or insufficiently controlled hazards	Engineering procedures, technical authority checks