Guidance on human factors safety critical task analysis

Second edition

energy institute

GUIDANCE ON HUMAN FACTORS SAFETY CRITICAL TASK ANALYSIS

Second edition

January 2020

Published by
Energy Institute, London
The Energy Institute is a professional membership body incorporated by Royal Charter 2003
Registered charity number 1097899

The Energy Institute (EI) is the chartered professional membership body for the energy industry, supporting over 20 000 individuals working in or studying energy and 200 energy companies worldwide. The EI provides learning and networking opportunities to support professional development, as well as professional recognition and technical and scientific knowledge resources on energy in all its forms and applications.

The EI's purpose is to develop and disseminate knowledge, skills and good practice towards a safe, secure and sustainable energy system. In fulfilling this mission, the EI addresses the depth and breadth of the energy sector, from fuels and fuels distribution to health and safety, sustainability and the environment. It also informs policy by providing a platform for debate and scientifically-sound information on energy issues.

The EI is licensed by:
– the Engineering Council to award Chartered, Incorporated and Engineering Technician status, and
– the Society for the Environment to award Chartered Environmentalist status.

It also offers its own Chartered Energy Engineer, Chartered Petroleum Engineer, and Chartered Energy Manager titles.

A registered charity, the EI serves society with independence, professionalism and a wealth of expertise in all energy matters.

This publication has been produced as a result of work carried out within the Technical Team of the EI, funded by the EI's Technical Partners. The EI's Technical Work Programme provides industry with cost-effective, value-adding knowledge on key current and future issues affecting those operating in the energy sector, both in the UK and internationally.

For further information, please visit **http://www.energyinst.org**

The EI gratefully acknowledges the financial contributions towards the scientific and technical programme from the following companies:

BP Exploration Operating Co Ltd
BP Oil UK Ltd
Centrica
Chevron North Sea Ltd
Chevron Products Company
Chrysaor
CLH
ConocoPhillips Ltd
DCC Energy
EDF Energy
ENI
E. ON UK
Equinor
ExxonMobil International Ltd
Innogy
Kuwait Petroleum International Ltd
Nexen CNOOC
Ørsted
Perenco
Phillips 66
Qatar Petroleum
Repsol Sinopec
RWE npower
Saudi Aramco
Scottish Power
SGS
Shell UK Oil Products Limited
Shell U.K. Exploration and Production Ltd
SSE
TAQA Bratani
Total E&P UK Limited
Total UK Limited
Tullow Oil
Uniper
Valero
Vattenfall
Vitol Energy
Woodside
World Fuel Services

However, it should be noted that the above organisations have not all been directly involved in the development of this publication, nor do they necessarily endorse its content.

ISBN 978 1 78725 165 6

Published by the Energy Institute

Hard copy and electronic access to EI and IP publications is available via our website, **https://publishing.energyinst.org**.
Documents can be purchased online as downloadable pdfs or on an annual subscription for single users and companies.
For more information, contact the EI Publications Team.
e: **pubs@energyinst.org**

CONTENTS

Contents continued

Page

LIST OF FIGURES AND TABLES

Page

Figures

Tables

FOREWORD

The human contribution to major accident hazard (MAH) risk in the energy and allied industries is well-known. In recent years, the sector has made significant inroads in both the management of human failure, and in optimising human performance. In part this can be attributed to application of the first edition of the Energy Institute's (EI) document *Guidance on human factors safety critical task analysis* (SCTA). Originally published in 2011, the first edition filled a gap by enabling companies and human factors (HF) non-specialists to conduct quality HF analyses in a structured and consistent format. The document raised awareness of the value of investing in HF studies to better manage the risk of human failure, leading to reported improvements in safety and reductions in losses. Regulators also recognise that its correct application will help satisfy requirements for safety critical tasks to be comprehensively analysed and their risk appropriately assessed.

This second edition of the guidance has been updated, focusing on the identification of safety critical tasks (SCT). Feedback to EI's Human and Organisational Factors Committee (HOFCOM), as custodian of the guidance, confirms that users would benefit from learning more about the range of methods for SCT identification that has been developed, and how to avoid pitfalls. New case studies are included in section 4 to show how companies have identified SCTs.

This publication has drawn on many existing sources from the public domain, and has supplemented these with input from practitioners and case study material. It is aimed at those who: participate in SCTA; incorporate SCTA into a wider risk assessment; commission SCTA, and those that are required to read, understand and act upon SCTA. Thus, the target audience includes designers, operations personnel, assessors and managers.

The EI welcomes feedback on its publications. Feedback or suggested revisions should be submitted to:

Technical Department
Energy Institute
61 New Cavendish Street
London, W1G 7AR
e: technical@energyinst.org

ACKNOWLEDGEMENTS

Guidance on human factors safety critical task analysis (second edition) was developed by Dr. Ed Smith and Richard Roels (DNV-GL) under direction of the EI HOFCOM. During this project, HOFCOM members included:

Tony Atkinson	ABB
Jonathan Bohm	HSE
Roger Bresden	Saudi Aramco
Ed Corbett	HSL
Alix Davies	EDF
Bill Gall	Kingsley Management Ltd.
Peter Jefferies	Phillips 66
Stuart King	EI (Secretary)
Simon Monnington	BP plc
Eryl Marsh	HSE
Richard Marshall	Essar Oil UK (Vice-Chair)
Rob Miles	Hu-Tech Risk Management Services Ltd.
Helen Rycraft	IAEA
Caroline Myers	ExxonMobil Corporation
Rob Saunders	Shell International
Gillian Vaughan	EDF Energy (Chair)
Frank Verschueren	FOD WASO
Phil Spence	ConocoPhillips

Project management and technical editing were carried out by Stuart King (EI).

The EI would also like to acknowledge the following individuals and organisations who commented on, provided resources, or otherwise made significant contributions to the second edition:

Phil Basildon	RWE
Gillian Hockin	BP
David Jamieson	Shell
Ed Jamieson	RWE
Vitor Monteiro	BP

Furthermore, the EI would also like to acknowledge the following individuals and organisations who commented on, provided resources, or otherwise made significant contributions to the first edition:

Wayne Barratt	Rhodia
Andy Brazier	AB Risk Ltd.
Allan Greensmith	Total Lindsey Oil Refinery
Jamie Henderson	Human Reliability Associates
Chris Venn	Chevron

BP LPG
BP Chemicals Limited Hull Site
ConocoPhillips Humber Refinery
Human Reliability Associates

Affiliations are correct at the time of contribution.

1 INTRODUCTION

1.1 BACKGROUND

There is widespread awareness in the energy industry that human failures whilst performing SCTs have contributed to major accidents, such as Macondo, Piper Alpha, Chernobyl and Texas City. The proactive identification and analysis of such SCTs has improved in recent years reflecting increased awareness and acceptance of the value of looking at such activities in detail, using the SCTA process. This growth is due to: significant uptake of the first edition of this guidance; the recognition that purely technical approaches to safety have their limitations, and through ongoing regulatory support.

1.2 WHAT IS SAFETY CRITICAL TASK ANALYSIS?

Task analysis can be simply defined as the study of what a person is required to do, in terms of actions and mental processes, to achieve a goal (Kirwan and Ainsworth, *A guide to task analysis*). It involves describing how a task is done, often through a series of smaller sub-tasks. SCTA focuses on how tasks that are critical to major accident risk are performed. The following is a definition of an SCT:

- An SCT is a task where human factors could cause, or contribute to, a major accident[1], or fail to reduce the effect of one, including during:
  - operational tasks;
  - prevention and detection;
  - control and mitigation, and
  - emergency response.

Using these headings, the following show illustrative SCTs identified by practitioners:

- Operational tasks:
  - loading liquid petroleum gas (LPG) from bulk storage to road tanker;
  - sampling of hazardous substances, and
  - blinding/de-blinding of piping and equipment.
- Prevention and detection:
  - test level trips, and
  - override or suppress safety function (e.g. inhibit fire or gas detectors).
- Control and mitigation:
  - pressure safety valve (PSV) inspection and testing, and
  - firewater pump inspection and testing.
- Emergency response:
  - deploy active firefighting equipment (to fight fire), and
  - launching a lifeboat.

1 Control of Major Accident Hazards (COMAH) Regulations: 'major accident' means an occurrence such as a major emission, fire, or explosion resulting from uncontrolled developments in the course of the operation of any establishment to which these regulations apply, and leading to serious danger to human health or the environment (whether immediate or delayed) inside or outside the establishment, and involving one or more dangerous substances (COMAH Regulations 2015)

SCTs, like the ones listed, will have several critical sub-tasks that require analysis. More information about identifying SCTs is given in 2.3.1.

The process of SCTA includes:

– determining which tasks are safety critical;
– prioritising SCTs for analysis;
– understanding which human action or inaction might make a failure more likely or more serious, and
– guiding the user in how to identify and install adequate layers of protection for these SCTs, in order to reduce the likelihood or consequences of human failure.

SCTA normally links to the type of MAH safety analysis that would be conducted at a project design stage or for safety report/safety case updates[2] and is often done with the assistance of SCTA experts. However, as operations are dynamic, and tasks and equipment change, some companies are embedding SCTA as an ongoing activity, applied when changes occur. For widely distributed operations, it may not be practical to get specialist input in all locations and times, for these reasons it makes sense for operators to build company SCTA capability close to the front line in operations management and supervision. Having this SCTA knowledge in the workforce also exerts a positive influence on the quality of risk assessment and incident investigations and also the quality of improvement suggestions (see 3.3.5 which outlines an example approach).

SCTA can also be an extremely useful and powerful tool in the context of operations, maintenance and safety culture. It provides a structured format for personnel to explore their procedures and gain an enhanced awareness of the critical elements and steps in an SCT. Given adequate resources in terms of the make-up of the participants and the time made available, it can be transformative in assisting operations in identifying and addressing assumptions, and in developing their mental model of what are actually key barriers, and what are the safeguards (activities that support the barrier, but in themselves will not prevent MAHs). In assessing a critical element of the SCTA – performance influencing factors (PIFs) – personnel also gain a deeper insight into how these safeguards:

– have the potential to turn into degradation factors, reducing or negating the effectiveness of actual barriers, and
– how both barriers and safeguards are critically dependent on human performance and actions.

Clearly, having that in-house capability allows sites to deploy the tool in a sustained and effective manner, building it into their safety management system (SMS).

Focus on process safety and catastrophic risk

The focus for this publication is on tasks with the potential for a catastrophic event, such as explosion, fire, release of toxic substance, loss of containment etc. and **not** occupational or personal safety risks. When performing an SCT, there will be occupational dangers such as: a finger getting caught when tensioning a bolt, or falling when accessing a valve. However, these risks are not the target for SCTA (such issues should be managed through alternative means). Attempting to analyse SCTs and their associated personal safety risks in a combined SCTA process is not advised.

2 In the UK, terms such as 'COMAH critical tasks' and 'MAH critical tasks' are sometimes used, reflecting the terminology used by the UK regulator; the present guidance is applicable to these terms.

1.3 BENEFITS

Unlike learning from incidents, SCTA is a proactive way to manage risk. It helps ensure better risk control by identifying improvements in, amongst others, plant and equipment design, task design, the operational environment, procedures and training. Many high-hazard companies have positively embraced SCTA as the established industry approach to review and demonstrate that the human component of MAH risk is being managed.

Some companies are now extending the application of SCTA to critical production and quality tasks, resulting in business benefits too. Scheduling SCTA at appropriate points in the design phase of a project will potentially also achieve cost savings, as have been achieved by using hazard and operability (HAZOP) studies for better process and engineering risk control.

A comprehensive SCTA programme of work should result in:

– improved MAH safety performance;
– fewer environmental incidents;
– reduced production downtime;
– quality benefits, and
– cost reduction in major projects.

Although not the core purpose for SCTA, it may also lead to improvements in general health and safety performance, fewer reportable incidents and reduced lost-time-accidents, through better designed work.

1.4 PURPOSE

The main purposes of this publication are:

– to raise awareness of SCTA particularly amongst HF non-specialists, to encourage its use, and
– to assist organisations in determining and demonstrating adequate safety measures (e.g. within offshore safety cases and COMAH safety reports).

In terms of expected users, it is aimed at those who:

– participate in SCTA, such as someone who is asked to provide discipline or supervisor/operator expertise in a group identification session;
– incorporate SCTA into a wider risk assessment as part of a safety report/case;
– commission SCTA and desire help with preparing a specification, and
– are required to read, understand and act upon SCTA.

Thus, the target audience includes designers, operations personnel, assessors and managers.

Those who actually conduct SCTA will also benefit from consulting some of the references listed in Annex B and should obtain prior experience through participation in SCTA projects. For relatively simple SCTAs, someone with experience in traditional safety studies such as HAZOP studies may have most of the relevant competences (see case study 5, section 4). However, for more complicated SCTAs, specialised HF support may be required (see case study 6, section 4).

1.5 SCOPE

1.5.1 Focus on qualitative approaches

The publication covers: analysis of tasks; human failure assessment (qualitative[3]), and risk reduction/control. It does not describe the quantification of human failures. In some circumstances, quantification offers some benefits. For example:

– where the SCTA is part of a wider risk assessment that is using quantitative risk criteria, and
– where the SCTA is helping to decide whether a manual or an automated system is safer, and where relative failure rates are an important part of that comparison.

However, experience of human failure quantification has shown that it can: use up large amounts of resource effort; struggle to factor in non-compliance (violations), and there are also often very large uncertainties in human failure quantification, due in part to lack of pertinent data. Thus considerable care should be exercised in selecting which projects would benefit from quantification. Specialists should be involved in this selection and in the execution of human failure quantification. There are references in 3.3 to available quantification techniques. EI also publishes a guide on this subject: *Guidance on quantified human reliability analysis (QHRA).*

1.5.2 Other approaches to task analysis

It should be noted that this publication does not cover all possible task analysis techniques. Task analysis can be done in many different ways, for example, assessing staffing levels, determining the optimum balance of automation and human involvement, improving training regimes, etc. These are well covered in specialist publications (including Kirwan and Ainsworth, *A guide to task analysis*, and Shepherd, *Hierarchical task analysis*). It should also be noted that SCTA is only one tool available for identifying and helping to address HF issues, and whilst it can be used for many applications, it should be complemented with other tools and techniques.

1.5.3 SCTA and routine task risk assessment

Some companies perform task risk assessments ahead of a planned job that has MAH potential. Like SCTA, the focus is on identifying and avoiding risk from human failure. However, task risk assessments are often performed for a specific event (e.g. with a specified time, date and work crew) and tend to assume the plant design and operation is fixed. SCTA has a broader scope, often covering a whole site and considering all types of mitigations and controls.

3 Note that the HSE states that its expectation is for a qualitative analysis of human performance. However, particular risk assessment tools may drive analysts towards quantification (e.g. layers of protection analysis (LOPA)) (HSE core topic 3: *Identifying human failures*).

2 SAFETY CRITICAL TASK ANALYSIS PROCESS

This section provides a step-by-step framework for SCTA that allows flexibility to address a wide variety of projects and situations. In addressing the main steps, a variety of tools can be used depending on circumstances, examples of which are detailed in section 3.

2.1 OVERVIEW

Previous publications have proposed processes for conducting SCTAs and human failure analysis. As part of its HF toolkit, the UK Health and Safety Executive (HSE) produced *Identifying human failures* (HSE Core Topic 3), a paper for its inspectors that outlines a seven-step process for SCTA. This seven-step process overlaps considerably with two other processes from Shorrock and Hughes, *Let's get real*, and HSE Offshore Technology Report, OTO 1999/092.

Based on these three sources, the process in Figure 1 has been developed, the steps from which are described in 2.2 to 2.8.

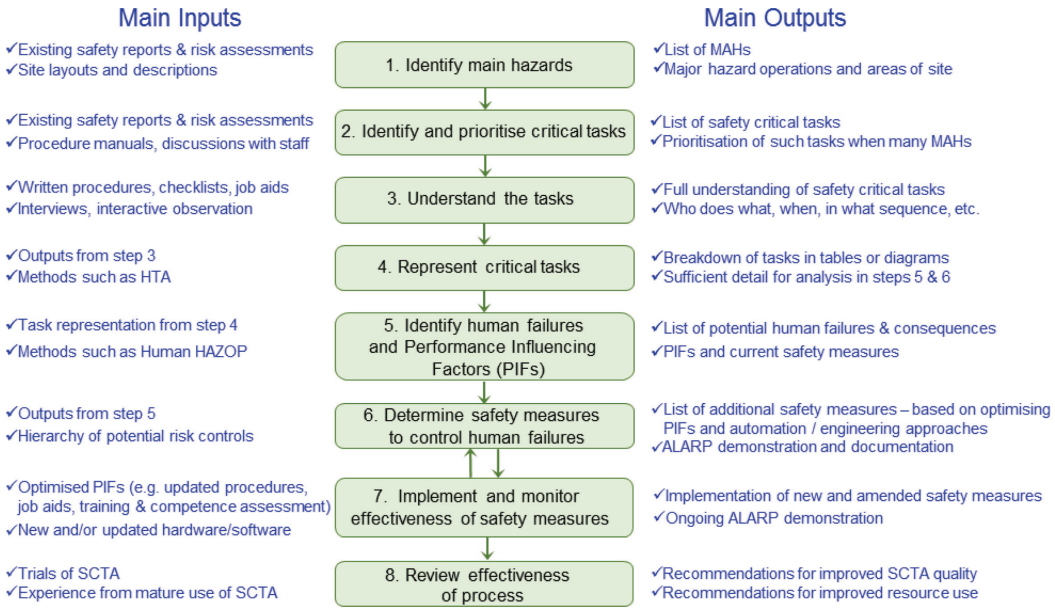

Figure 1: Summary of SCTA process

This second edition of the guidance has added step 7 'Implement and monitor effectiveness of safety measures' in order to highlight that SCTA is not a stand-alone activity. Rather it links to the development of procedure updates, training material, competence assessments and HF integration more widely. This additional step is consistent with HSE's HF roadmaps.

2.2 STEP 1 – IDENTIFY MAIN SITE HAZARDS

In order to recognise their SCTs, a site should first identify their MAHs. This could be a relatively straightforward process of extracting them from existing safety reports/safety cases or relevant risk assessments. However, in the case of a new facility where such documents do not yet exist, the SCTA should be scheduled to start once the main site hazards become clear, Otherwise considerable effort may be wasted analysing tasks that have little influence on overall site risks.

This step is likely to involve consultation with process safety specialists, site personnel and authors of the risk assessments, to ensure that all correct and most up-to-date documentation has been reviewed and that the MAH identification is comprehensive.

If an organisation is conducting SCTA for the first time at a major site where there are many MAHs, it may be necessary to prioritise and start with the highest risk units as revealed in the safety reports/safety cases and/or through the use of risk assessment tools. From this prioritisation a realistic (i.e. achievable) programme of SCTA can be organised.

The resulting list of higher risk units should be the starting point to identify SCTs (see step 2).

Example MAH scenarios from an LPG bulk storage/distribution site include:

– roadcar gantry: pipework or hose failure;
– transfer pipework failure;
– storage vessels: pipework/vessel failure;
– storage vessel overfill;
– roadcar overfill, and
– dropped load.

2.3 STEP 2 – IDENTIFY AND PRIORITISE SAFETY CRITICAL TASKS

Having a prioritised list of SCTs helps ensure that subsequent analysis effort is directed appropriately. Task identification and prioritisation is often different for each site, depending on the hazards and information available about the tasks. It should be performed by someone that has a commensurate level of experience and competence to judge the best mix of approaches. Fairly extensive guidance is provided for this step, reflecting the need to develop a justifiable and manageable set of SCTs.

This step covers:

– capturing SCTs at the right level;
– identifying tasks;
– screening and prioritising tasks;
– what types of task are of interest;
– defining required actions, and
– common pitfalls, misunderstandings and misapplications, and their solutions.

2.3.1 Capturing SCTs at the right level

Experience has shown that it can be difficult to specify an SCT at the right level. Several problems exist:

– Focus is too narrow: e.g. focusing on the final critical step before an incident results, and overlooking important preceding steps that led to the event. For example, 'open valve' could be the last critical step before an MAH release, but this is too specific to be an SCT itself. What is the overall task? (For example, it could be 'draining an LPG tank'.) There may be several other critical sub-tasks – such as 'go to correct tank', 'determine tank level', 'identify correct valve', etc. Focusing on just the last step ('open valve') will miss all these other sub-tasks.

– Focus is too wide: likewise, if the focus is too general (e.g. 'draining operation') then this will make the SCT hard to analyse. What is being drained (e.g. is it an LPG tank or something else)? Do all 'draining operations' contain the same sub-tasks? (This is unlikely.)

– Wrong focus: some organisations might consider any task that can result in injury to be an SCT. This is unhelpful. SCTA is intended to be used for MAHs, not personal safety risks (which can be addressed by other means). Likewise, some organisations might consider all procedures to be safety critical. Again, this is unhelpful because a) not all SCTs will have a procedure (although they all should have one); b) not all procedures are related to MAHs and c) there isn't necessarily a 1:1 ratio between procedures and SCTs – i.e. an SCT may be covered by several procedures.

The following list shows some example SCTs and illustrative sub-tasks to help the reader be clear about what to look for when identifying SCTs. Case study 2 shows a complete set of SCTs identified for a large complex refinery (see 4.2).

SCT: **Unload LPG from road tanker to bulk storage (i.e. import LPG)**, example sub-tasks:

- Go to storage vessel unloading point.
- Determine ullage (capacity) in storage vessel.
- Connect earth lead.
- Carefully open tanker valve.

SCT: **Test level trips (on production separator)**, example sub-tasks:

- Go to separator.
- Confirm set point to test.
- Isolate signal.
- Insert transmitter.
- Note result.
- Remove bypass.

SCT: **Assemble small bore tubing**, example sub-tasks:

- Form/bend tubing.
- Fit tube support bracket.
- Insert ferrule on pipe.
- Tension nut.

2.3.2 Identifying tasks

There are various approaches to identifying tasks that may be safety critical. These include using:

– previously published SCT lists;
– outputs from existing risk tools (e.g. HAZOP, fault trees etc.);
– procedures and existing task information;
– active and involving approaches (focus groups and walk-throughs), and
– incident investigation reports.

These are described in 2.3.2.1–5, and illustrated in case studies 1–3 in section 4. When doing this it can help to group similar tasks together, starting with the higher risk units identified from step 1, for example:

– operational;
– maintenance, inspection and testing;
– process upsets and
– emergency.

This makes it clear what is under consideration, and should ensure the right people are involved. Task grouping (considering similar tasks together on the basis they are similar in nature, and so the group assembled to analyse them would have the appropriate expertise) will also help demonstrate coverage of the different types of SCT.

2.3.2.1 Using previously published SCT lists

Some companies have very similar hazards and equipment performing identical functions. For example, LPG bulk storage/distribution sites may share similar inventory, loading and unloading equipment and bottling facilities. If a good SCT register exists, it follows that the same SCTs apply at other equivalent sites. However, unless the systems under review are identical, it is advisable to perform a fresh SCT identification process and then use existing SCT lists as a check.

2.3.2.2 Using outputs from existing risk tools

MAH safety reports/safety cases and risk assessments may provide:

– HAZOP tables identifying operational and maintenance task failures as causal factors of MAHs (e.g. 'operator mis-sets flow control valve', or 'any manual valve left open in error on the import gas system').
– Fault trees showing task failures as contributors to MAH top events (see Figure 6).
– Safety integrity level (SIL) assessments of emergency shutdown and safety control systems. These are required by the relevant standards (IEC 61508 and IEC 61511) to include the contribution of human failure. SIL determination may be based on quantitative or semi-quantitative methods such as fault tree analysis (FTA) or LOPA (see 3.3.4). Underlying such methods will be the identification of relevant SCTs. Ideally, analyses will highlight how a human helps to deliver the required function, for example responding to an alarm, or maintaining a critical instrument. If not, it will be necessary to infer SCTs.
– Bow tie diagrams showing HF contributions to hazard initiation and escalation (see Figure 8).

– Safety and environmental critical elements (SECEs) and their associated performance standards can be used to identify supporting assurance routines as SCTs.

If these risk tools have already made the links between tasks and MAHs in a comprehensive manner, an inventory of SCTs can be readily assembled. To achieve this efficiently will require good knowledge of safety assessment techniques, such as the ability to understand and interpret fault trees, and the ability to identify relevant human tasks from potentially extensive HAZOP tables through experience of relevant guidewords.

Working with bow ties

Well-structured bow ties are essential if they are to be used to identify SCTs. Checking that bow ties conform with recognised good practice will help the user understand any potential issues before progressing. Using a poorly structured bow tie can lead to missed SCTs and inappropriately defined tasks being progressed (see case study 1 and 2 in section 4 for examples of good practice).

If bow ties focus on hardware barriers (e.g. fire and gas detection, deluge systems), it can be difficult to identify operational SCTs; therefore, some practitioners indicate such bow ties are better-suited to identifying maintenance SCTs (see case study 3, in section 4).

3.3.3 provides an overview of the bow tie approach and how it can be used to identify SCTs.

2.3.2.3 Using procedures and existing task information

The following can help identify SCTs:

– operating manuals and procedures;
– previously risk-assessed procedures;
– planned maintenance routines, and
– safety critical equipment registers.

Operating manuals and procedures

The aim here is to identify SCTs from procedural information, rather than to determine which procedures are SCTs. A common trap is to conclude that 'all' procedures are safety critical, which leads to many procedural steps being unnecessarily subjected to detailed analysis. SCTs and procedures are different things. Some SCTs will draw on aspects of several procedures;others will be a part of a single procedure. Being clear about the start and end point of an SCT will help define what procedural information is relevant. Case study 3, section 4, provides an example of how to identify critical tasks from procedures. Relevant steps are to:

– Gather procedures of the relevant MAH units from available manuals.
– Identify which procedures involve human tasks that link to MAH initiating events, detection, control, mitigation and emergency response (see Table 1).
– Focus on those tasks that involve extensive human interactions with equipment or with other personnel.
– Consult with and check the resulting SCT identification with site personnel. This is critical to identify the full range of SCTs and to pick up key ones not covered by formalised procedures. If it is found that an SCT is not covered by a procedure, then this should ideally be remedied before carrying on with the SCTA. Non-routine tasks which may not be covered by written procedures at some sites are discussed in 2.3.3.

Table 1: Example procedure screening matrix for an LPG bulk storage/distribution site

Hazardous events: operating procedures	Roadcar gantry: pipework or hose failure	Transfer pipework failure	Storage vessels: pipework/ vessel failure	Storage vessel overfill	Roadcar overfill	Dropped load
1. Propane road tanker loading direct from depot import line	✓				✓	✓
2. Butane road tanker loading direct from depot import line	✓				✓	✓
3. Propane import to site storage vessels				✓		

Previously risk assessed procedures

Outside of the SCTA process, some companies have reviewed their procedures to prioritise a set for risk assessment. The outputs of this process can be useful to identify SCTs, especially if it focuses on MAH risk, and takes into account topics such as task consequence, task complexity and level of human involvement. If procedures have not been prioritised, but have been risk assessed, the findings can be reviewed to create a list of SCTs.

Planned maintenance routines

Database records of planned maintenance routines can be interrogated to provide a list of tasks and associated equipment. This is useful to identify maintenance, inspection and testing (MIT) tasks. Sometimes it is possible to select only those routines that support achievement of performance standards (which can help to confirm the task may provide a safety critical function). Making sense of the list may benefit from input from maintenance leaders and system owners (e.g. relevant technical authorities). The resulting list can then be subject to screening and prioritisation.

Safety critical equipment registers

Some regulations require companies to hold lists of safety critical equipment. These can provide a very useful starting point, especially for MIT task identification.

Practitioner experience: maintenance, inspection and testing (MIT)

Practitioners highlight that MIT tasks tend to be overlooked, often because they do not have accompanying procedures. Referring to safety critical equipment registers and maintenance routines may not pick out all the associated tasks, especially those undertaken by specialist contractors. It can help to explicitly ask what the MIT activities are for each system, and then record these as tasks for screening and prioritisation. Tasks performed by contractors should be identified and subject to screening and prioritisation in the same way.

2.3.2.4 Active and involving approaches

Some sites have opted to take an active approach to SCT identification, involving the workforce, either to complement other techniques, or because there is limited information about the site. Examples include:

– Area/plant walk-throughs with operators/maintainers; the setting provides the cues for participants to recall and report difficult tasks.
– Focus groups and brainstorming for simple sites (e.g. warehousing, basic blending and non-toxic inventories). This works by allowing participants to 'bounce ideas off one another', and reflect their experience of doing the work. Using a facilitator, taking one area of a plant at a time, and ensuring the right disciplines attend, will help ensure a useful identification process.

2.3.2.5 Incident investigation reports

Incident investigation and near miss/close-call reports may highlight SCTs and can therefore provide useful checks on task lists. Incidents at other similar sites can also be reviewed.

2.3.3 Screening and prioritising tasks

Once a list of potential SCTs has been prepared, the next step is to prioritise the tasks for detailed analysis. The techniques used are:

– criticality/prioritisation table and matrix, and
– task criticality ratings.

Analysis or risk ratings from the existing risk tools listed in 2.3.2.2 might be used to feed into these techniques.

2.3.3.1 Using criticality/prioritisation table and matrix

One of the simplest ways to prioritise tasks is to assess the consequences of task failure and the degree of human involvement. An example matrix approach is shown in Figure 2 with relevant guidance tables. A more sophisticated approach is shown in Figure A.1. It should be noted, however, that some organisations prioritise by only focusing on high consequence failures. Case study 1 shows an example of this approach (see section 4).

Consequences of human failure	Example guidance
High (H)	A human failure could result directly in realisation of an MAH
Medium (M)	A human failure could escalate to an MAH if other barriers are judged to be at risk of failure
Low (L)	A human failure should not lead directly or indirectly to an MAH

Level of human involvement	Example guidance
High (H)	Task involves extensive or complex human interactions with safety critical equipment or processes
Medium (M)	Task involves limited or simple human interactions with safety critical equipment or processes
Low (L)	Task involves minimal human interactions with safety critical equipment or processes

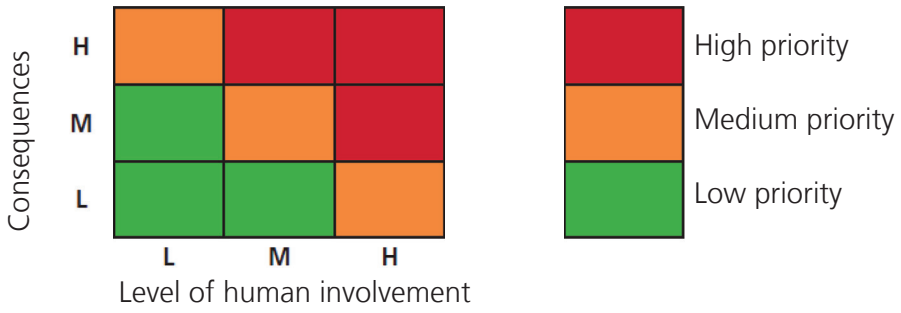

Figure 2: Example simple criticality/prioritisation tables and matrix

Some practitioners have amended the 'level of human involvement' scale to include more detail. Table 2 was developed for use at a UK onshore oil and gas processing terminal.

Table 2: Example simple criticality/prioritisation table

Human performance demands	Guidance
High (3)	The task involves high cognitive load, high memory demands, multiple concurrent activities, frequent interruptions at critical steps etc
Medium (2)	The task involves moderate cognitive load, requires some recollection of critical data; there may be some overlap between activities, interruptions sometimes occur
Low (1)	The task is simple, straightforward, requires little recall of critical data; steps are sequential, interruptions are rare

2.3.3.2 Using task criticality ratings

For larger and more complex sites, it can be necessary to get a wider spread of scores than the criticality/prioritisation matrix permits, and to understand the task in slightly more detail. The approach described in HSE OTO 1999/092 could be considered. It prioritises tasks based on a scoring to five questions:

1. How hazardous is the system involved?
2. To what extent are ignition sources introduced into the task when it is performed?
3. To what extent does the task involve change to the operating configuration?
4. To what extent could incorrect performance of the task cause damage?
5. To what extent does the task involve defeating protection devices?

Based on the scores to these questions, criticality ratings are produced. Originally developed around generic offshore production tasks, it has been used and adapted across a range of other task types, including tasks derived from bow ties and procedures.

Alternative questions to HSE OTO 1999/092

SCTA practitioners emphasise that it may be necessary to adapt the five questions specified, or develop new ones, to suit the hazards and tasks that are of interest. Otherwise, there is a chance that tasks will not be scored properly. It is good practice to trial any amended questions prior to formal use (e.g. ahead of a screening workshop).

An example: a producer of high quality effect chemicals did not have a hydrocarbon inventory, but loss of containment was potentially a major environmental issue for them. Therefore, they replaced the second question on ignition sources with one focused on the environmental aspects: 'To what extent is the operator directly manipulating materials potentially hazardous to the environment?'. The answer options focus on the volume of materials and the task location (response options are reproduced in Annex A, Table A.3).

An example of another scoring system is shown in Table A.4. It is based on scores for the hazard (based on the substance involved and the quantity) and an HF score based on likelihood of recovery, task complexity, etc. The HF score questions have themselves proved applicable to screening maintenance tasks (at gas processing facilities).

2.3.4 What types of task are of interest?

The identification of SCTs should consider routine and non-routine tasks. For example, operational tasks (such as filling a storage tank) and maintenance tasks (such as breaking into a pipeline) could have the potential for initiating a major accident such as loss of containment. In addition, tasks relating to event escalation and emergency response should be considered. Tables 5 to 8 show example SCTAs of all these types of task. It is possible (or even probable) that past risk assessments have identified SCTs.

It may be difficult to link human actions to MAH events, as units may have many risk control systems (RCSs) – for example, alarms, trips and relief valves – designed to prevent consequences of failures being realised. It may help to think about tasks where:

– The system is opened up, such as maintenance preparation tasks.
– RCSs are maintained; for example trips are tested. For such tasks there is the possibility that they may not be reinstated or reinstated incorrectly, leaving the site without a key risk control.
– The conditions that RCSs are designed to protect against may be created (for example, over-pressurisation whilst starting up or shutting down a piece of equipment).

Note that a task can be a physical action, such as opening/closing a valve, a checking- or a communications- activity, or it can be a mental action such as a diagnosis or decision-making activity. All of these tasks should be covered in the approaches outlined in 2.3.2.

As well as considering direct interactions between humans and equipment, this step should also review tasks involving human-human interactions that influence MAH risk (for example, shift handovers or communications between supplier and recipient of product).

Some organisations have found it difficult to specify tasks related to emergency response as this phase may involve so many different scenarios. It is recommended that emergency response exercises are used to input and update SCT lists.

2.3.5 Defining required actions

A register of SCTs should be produced that lists tasks and their associated prioritisation. This can include the relevant MAH(s) and who performs the task. To progress the list of SCTs to Step 3 'Understand the task', some practitioners simply start with the most critical tasks and then work down the list of SCTs. If there are many, or different, types of SCT, it can help to create an action plan for the remaining SCTA steps. Considerations for the plan include:

- Other planned work at site; a planned shutdown, or specific operation (e.g. pipeline pigging) may provide an opportunity to analyse relevant SCTs in time to act on findings. Reviewing upcoming permits against the SCT list can identify opportunities to understand the task.
- Practical constraints such as site access, access to personnel and system demonstrations etc. when trying to understand the task, especially offshore. However, some companies have overcome this by video recording SCTs (see: Hopwood, Maguire and Adams, 2015)
- Novel and untested systems may be prioritised over well-established activities. Similarly, sub-optimal systems, such as where interlocks are known to have failed, or where an operational risk assessment is in place, may also warrant a higher priority.
- How the task is best understood, represented and analysed for human failure (steps 3–5). Developing a full hierarchical task analysis and then reviewing it in a workshop setting will require much more planning and resource compared to some alternatives such as a plant walkabout, where it may only be necessary to consider environmental issues (e.g. if the task and error types are already well understood).
- Where near identical tasks are performed, such as instrument testing, it is advisable to do one full SCTA process on a representative task, and then review the others to find differences.

2.3.6 Common pitfalls, misunderstandings and misapplications – and their solutions

Table 3 presents what experienced practitioners report as the most significant blockers to SCT identification, along with potential enablers.

Table 3: Blockers to SCT identification and potential enablers

Blocker/issue	Enabler
Incorrectly identifying critical support activities such as audit, inspection, and management of change as SCTs. Whilst some SCTA thinking (e.g. error analysis and identification of PIFs) can be used for analysis of critical support activities, experience shows that SCT techniques should be amended to work properly for such activities. Some practitioners see this as diverting effort from frontline tasks which SCTA should focus on	If a site is new to SCTA, the focus should be on applying SCTA to active 'sharp end' tasks which, if not carried out correctly, would have serious consequences. The supporting processes and procedures should be checked to ensure they are consistent with relevant good practice. As a programme of SCTA work develops, it may be appropriate to use SCTA thinking to assess supporting critical activities
Tasks are poorly defined, or defined in a generic manner, making it unclear what the task is. Examples include: – 'Supervision' is an important activity, but difficult to analyse as an SCT – 'Housekeeping' and 'vehicle checks' are not specific enough – 'Confined space entry': it is not clear what type of space is being analysed. – Some have attempted SCTA on a hazardous event – e.g. 'overpressurisation of a vessel'; however, this is not a task, and does not work well	Tasks should be defined according to: – specific human actions or decisions; – identifiable/specific equipment, and – a clear link to MAH risk (e.g. in the case of 'supervision' a supervisor check that an isolation is correct)
Some companies have adopted the approach of defining an SCT as the final critical step that is taken just before an incident occurs. This risks overlooking the critical steps leading up to that point. For example, when repairing a leaking gas main, defining the SCT as 'clamp main' overlooks key preceding critical steps such as: – identify source(s) of leak; – determine volume of escaping gas; – decide on isolation; – decide to work in same excavation as escaping gas; – don fire equipment and – perform ongoing atmosphere monitoring	It is necessary to understand the preceding tasks leading up to the critical step, therefore a broader definition of the SCT should be used. In this case 'repair gas escape' would be an appropriate SCT (see case study 4, section 4)
Tasks that are genuinely safety critical are not progressed for analysis because they do not attract a sufficiently high rating	All tasks that could be contenders for being SCTs should receive sufficient effort to determine if they are SCTs. The form and depth should reflect the risks involved

Table 3: Blockers to SCT identification and potential enablers (continued)

Blocker/issue	Enabler
Some maintenance tasks identified as 'safety critical' can be so substantial that they would be run as a standalone capital expenditure (CapEx) project by the company, making it redundant to analyse in isolation	During maintenance task screening, consider if the task would be performed as a capital project; if 'yes', note it and do not progress Check that procedures governing CapEx projects have adequate coverage of HF issues
Some companies have incorporated both MAH related tasks and personal safety risks when identifying SCTs. However, it is not clear how to prioritise personal safety along with MAH tasks	It is best to keep SCTA conducted on MAH risks separate from methods covering personal safety risk
Sites state that all procedures are 'safety critical tasks' which can undermine prioritisation and lead to too many tasks being progressed for detailed analysis	Procedures and SCTs should be understood as two different things. Clear start and end points for SCTs will frame the SCT under consideration and avoid equating an SCT with a procedure. A proper screening and prioritisation process will identify where analysis effort is best spent
Task prioritisation/screening techniques have their limitations. If scores are interpreted too rigidly, some lower scoring tasks that would benefit from thorough SCTA may not be progressed for detailed analysis	Experienced practitioners emphasise screening is simply trying to prioritise which tasks are progressed for more detailed analysis. If there is good reason to progress different tasks (regardless of the score received), record the reasons and progress accordingly; practitioners emphasise not to manipulate the scores to achieve this, but to be transparent
Some sites have found that task screening and full SCTA can take some considerable time	The structured analysis of HF around MAH risk represents a worthwhile investment, even if it is perceived to take time. For established assets, full SCTA may only be needed once, with less onerous updates happening periodically and as part of changes. Therefore the findings should be valid for a very long time Focusing in on only the critical sub-tasks in an SCT (see step 4), and grouping similar tasks together for analysis can help Having a realistic and properly resourced plan (see 2.3.4) and schedule for analysing SCTs will help ensure work is delivered in a timely manner Test-running the SCT identification process is recommended to ensure it works efficiently, before convening any workshops
Only using one source of information when identifying SCTs can mean some SCTs are missed (because no single approach will be a complete source of SCTs)	Some practitioners emphasise using a combination of 'top-down' (i.e. outputs from risk tools) and 'bottom-up' approaches (i.e. identifying SCTs from procedures) to help ensure SCTs are not missed

2.4 STEP 3 – UNDERSTAND THE TASKS

The aim of this step is to establish, in simple terms, a short but comprehensive description of the identified SCT(s). This includes:

– what is done by whom;
– in which sequence;
– what tools and information are required;
– what interactions with other people are required, and
– if there is a need for multi-tasking.

Factors with the potential to affect human performance should also be identified, such as work conditions (noise, lighting, etc.), time pressure, interface design, lack of stimulation during monotonous supervisory tasks, etc. These are known as performance influencing factors (PIFs) or performance shaping factors (PSFs), with more examples listed in Tables A.1 and A.2.

There are three main data collection techniques (Figure 3) that are widely used when gathering information about the identified SCTs (Shorrock and Hughes, *Let's get real*):
a. interactive observation;
b. interviews with personnel, and
c. examination of documents.

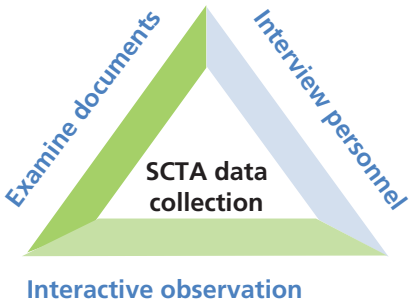

Figure 3: Data collection techniques

Experience has shown that interactive observation is a key technique, as it can identify PIFs that would probably be missed if just interviews and document reviews were relied on. For example, difficulties opening a 'pig trap' or lighting issues are harder to identify away from the site. PIF identification can be supported with use of a checklist (see Table A.1). Some practitioners emphasise that a 'walk-through-talk-through' approach has advantages over watching a task being performed for real, as you witness what is happening and why, without risking interruption at a key point.

Using the mixture of techniques from a, b and c ensures that the SCTA is analysing how tasks are actually carried out in practice, not only how they should be carried out according to written procedures. There are also some additional data collection techniques such as questionnaires, analysis of simulations and interface surveys that are suitable for some specific SCTs (Kirwan and Ainsworth, *A guide to task analysis*).

Importantly, when employing data collection methods in the design phase of a plant or before a major change project, operations and design personnel should work closely together to

describe the interactions between the operator and the system. This enables operations staff to identify how this system differs from those they are used to working with, and gives the design engineer an insight into how this system is truly likely to be operated.

a. Interactive observation

To ensure consideration is given to aspects of the SCTs that the operators might not be consciously aware of (such as habits developed over a long time), interactive observation should complement document examination and interviews. This is best done by walking through the task, with a commentary by the operator of what is being done, why it is being done, and key factors influencing decision making, etc. Such a walk-through observation will highlight the workability of the task and should enable the analyst to see if procedures are an accurate reflection of how things are really done. The employees to be observed should always be made familiar with the observer in advance and should receive a thorough explanation of the method and its objective. Directly after the observation the involved person(s) should have an opportunity to explain why they carried out the task the way they did.

b. Interviewing personnel

Interviewing personnel is often the most important part of the data collection. Interviews can be carried out with individuals or with small groups. If it is not practical to hold the interview on-site (for example due to noise or work distractions), personnel can be asked to talk through the SCT in a room appointed for the interview. However, whenever possible, the interview should take place where the task is usually carried out (or at least using a mock-up of the task) so that the employees can talk the interviewer through the task while performing it.

Relevant background information should be gathered, such as if tasks are conducted as per the written procedures, or in the same way by all personnel, etc. Employees may be reluctant to reveal such information if it involves admitting breaking company rules, and so the interviewer should aim at creating a trusting atmosphere; undertakings of confidentiality may be helpful, although should be agreed in advance with all parties.

Even a small number of interviews can usually reveal a surprisingly large amount of information, although if a larger number can be scheduled this will help the interviewer to obtain a more balanced impression of critical tasks (however, there is often limited availability of interviewees).

c. Examination of documents

The examination of documents is often carried out as a first step. Some of these documents can be reviewed remote from a site if the SCTA is being supported or led by non-site personnel. This can help prepare analysts for the interviews and observations to follow. However, the availability of procedures and their use should be checked on site. A comprehensive search and analysis of documents such as existing written procedures, checklists, job aids, training material, and diagrams of plant layouts and equipment, can save a lot of subsequent effort during data collection. The review should include checking for accessibility, clarity, accuracy, workability and currency. Additional documents to review may include any relevant safety studies, accident/incident reports, log books and shift pattern descriptions.

It should be noted that this can potentially be a lengthy process, especially if documentation requires major updates. It should be stressed that SCTA is not a paperwork exercise and hence the following stages are very important.

Contribution of third parties

Some SCTs depend on the contribution of third parties, such as emergency services. Their participation in the SCTA process is valuable to confirm understanding of the shared responsibility and to check that potential errors have been identified and can be managed effectively.

Creating an open and confidential atmosphere to collect information

SCTA depends on understanding where things can go wrong. This may mean those participating in the process talking about where they may not follow procedures, or where they made a mistake. Building a good rapport with contributors is important and can be helped by:

- Site management conveying they want contributors to say how things can, and have, gone wrong, and that there will be no repercussions.
- SCTA facilitator highlighting outputs will not be attributed to individuals.
- De-personalising conversations, so it is not about how someone has 'failed' but how the system can be defeated, or has failed to support them doing their work.

Be positive when someone hints that a task is difficult, or can go wrong; ask more about it.

Streamlining data collection

Some practitioners emphasise that it is possible to streamline Step 3 ('Understand the task') and Step 4 ('Represent SCTs'). Mature sites that have procedures that genuinely reflect how the job is done in reality can provide the task steps, leaving the identification of PIFs as the main activity for Step 3. If the procedure has been validated with techniques described here, such as interactive observation etc, there will be greater confidence that the procedure can be used in this way. If a procedure has been subject to only a desktop review, for example, it will be difficult to confirm that it genuinely reflects how the job is done, in which case streamlining the process is not the approach to take.

2.5 STEP 4 – REPRESENT THE SAFETY CRITICAL TASKS

The SCTs can now be represented in such a way that they can be systematically analysed and sub-tasks identified. However, if the subsequent steps of the SCTA are carried out on every single sub-task of an SCT, many of which may not be safety critical, there will be wasted effort and less attention paid to the safety critical aspects of the tasks. It is therefore important to identify the sub-tasks within overall tasks that are safety critical and require further, structured human failure analysis.

At the simplest level this can involve listing the steps in a task (for example, see 1.2 which defines SCTs, 2.3.1 which shows SCTs and sub-tasks, and the first column of Table 5). Descriptions of tasks should always start with a verb; this rule helps the analysis to focus on tasks rather than vaguer concepts such as a person's job or work. It is customary to record the roles involved in performing the task. For well understood, relatively straightforward tasks, this may be sufficient to proceed to step 5 (see 2.6) of the SCTA. For more complex tasks, such as those involving variable sequences of sub-tasks conditional on previous sub-tasks, or to help obtain an overview of all the steps in a task, it may be helpful to employ

additional techniques. Some practitioners have applied the prioritisation tools described in 2.3.3 to identify sub-tasks (e.g. Case study 4, see 4.4).

A popular technique is hierarchical task analysis (HTA). HTA represents tasks in terms of top-down hierarchies, that can be shown as a tree diagram (good for visualisation, see Figure 4) or as a table, a so-called tabular task analysis (TTA). TTA is better for detailed description, and by adding further columns for errors, consequences, PIFs, risk controls etc., the rest of the SCTA process can be completed in a straightforward manner.

The HTA diagram in Figure 4 shows how the task of manually activating blowdown is completed. The first box specifies the overall task, 'manually activate blowdown'; this is sometimes referred to as a 'goal'. The next layer of boxes describes the complete task in four sub-tasks. The first three tasks are mainly cognitive processes; the last (activate blowdown), is principally a physical task. The 4 sub-tasks are described in more detail in the next layer of boxes. To work out when to stop describing a task/sub-task, it can help to keep in mind the MAH events involved, and whether or not it is worth looking at human failures for the sub-task. Task analyses often have a numeric structure that corresponds to the different task levels. Sometimes 'plans' are included which describe the order that sub-tasks are completed in and the conditions that need to be met before a task can be completed.

Task vs sub-task

It is difficult to create a 'foolproof' terminology for describing tasks. For the purposes of this guide, a 'task' means the single safety critical task being considered. Sub-tasks are the key activities undertaken as part of that task. The next layer down breaks the sub-task into further sub-tasks. Really, this is just breaking the task down into smaller components for analysis.

A key issue in this step is determining how much detail is required. In HTA it is possible to describe some sub-tasks in detail (if they are themselves safety critical) and represent others much more briefly. If everything is broken down in great detail a mass of information is generated, potentially of little practical value. Although 'rules of thumb' for this have been sought, generally the level of detail is a subjective judgement based on the experience of the SCTA analyst or team. It is not unusual to find that more detail is required to be added at a later stage following steps 5 and 6 of the SCTA when these have shown that a particular sub-task is more safety critical than first thought. In addition, extra detail can be useful in Step 7 in terms of procedure reviews and updates following the STCA. However, step 4 provides an opportunity to simplify the analysis and remove those sub-tasks which clearly are not safety critical. The role for HTA in this step is further described in section 3.

Regardless of the technique chosen, this stage of the SCTA should have represented each SCT in such a way that it can be analysed for potential human failures, with a good understanding of current working conditions and the safety measures already in place.

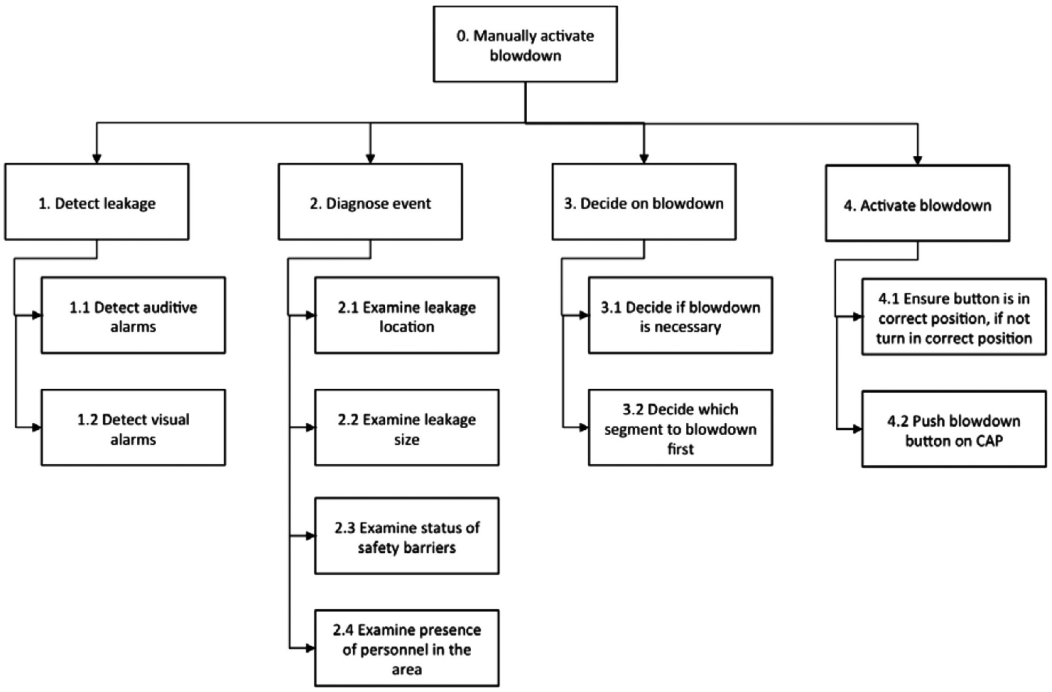

Figure 4: Example HTA diagram[4]

Practitioner experience – non-linear SCTs

SCTA often involves breaking down a task into sub-steps, which are presented in a hierarchical manner. However, some SCTs and critical sub-tasks are not conducted in a linear, stepwise fashion; some are complex activities or decisions and may be performed in an exploratory and iterative manner. This can affect how the task is represented and analysed. Conventional hierarchical approaches can still work by identifying the cognitive tasks/decisions that will be taken and then breaking these down into sub-tasks. An example of this is given in Case Study 4 (see 4.4) which looked at repairs to leaking gas mains. Here the importance of early 'site assessment' and 'repair planning' were emphasised as each shaped how the physical repair would be performed and the risk controls that would be deployed. Each of these was broken down into sub-steps for error analysis.

Various methods for representing SCTs are described in section 3. Some examples of 'non-linear' tasks might potentially include:

– Emergency response: activities of emergency response team, firefighting, evacuation etc.
– Respond to critical alarm (e.g. gas release).
– Breaking a joint in a hydrocarbon line.
– Berthing a vessel.

In general, SCTs associated with mitigating an incident tend not to be performed as sequential steps.

4 Reproduced from IFE/HR/E-2017/001, *The petro-HRA guideline*

2.6 STEP 5 – IDENTIFY HUMAN FAILURES AND PERFORMANCE INFLUENCING FACTORS

For each of the key sub-tasks represented by step 4, potential human failures should be identified. There is a variety of techniques to do this, including group based methods and techniques typically used by single analysts. Two common group approaches have developed:

– apply a set of failure guidewords or prompts for each step of the task, or;

– use the list of guidewords at the beginning of a session to introduce the types of errors that are of interest, but then let attendees think through how a task can go wrong based on their experience, rather than applying guidewords at each step. This also permits recording of the specific error(s) using language of those that do the job, rather than simply just the guideword.

Process safety or technical safety people may prefer the first approach, whilst job operators/ maintainers' experience is more suited to the second approach. Sometimes it is possible to work both approaches in parallel (i.e. some think through the guidewords, others thinking though how they do the job), but this is heavily dependent on the preferences of those involved.

A set of common guidewords is given in Table 4; a larger set of guidewords with examples of their use is provided in Table A.5. The application of these guidewords to the SCTs produces a list of potential human failures as illustrated in Tables 5 to 8 (see 2.9).

Table 4: Example human failure identification guidewords[5]

Action failures		**Checking failures**	
A1	Operation too long/short	C1	Check omitted
A2	Operation mistimed	C2	Check incomplete
A3	Operation in wrong direction	C3	Right check on wrong object
A4	Operation too little/too much	C4	Wrong check on right object
A5	Operation too fast/too slow	C5	Check too early/late
A6	Misalign		
A7	Right operation on wrong object	**Selection failures**	
A8	Wrong operation on right object	S1	Selection omitted
A9	Operation omitted	S2	Wrong selection made
A10	Operation incomplete		
A11	Operation too early/late		
A12	Operation in wrong order		
A13	Misplacement		
Information retrieval failures		**Planning failures**	
R1	Information not obtained	P1	Plan omitted
R2	Wrong information obtained	P2	Plan omitted

5 Adapted from HSE Core Topic 3: *Identifying human failures.*

Table 4: Example human failure identification guidewords (continued)

R3	Information retrieval incomplete	
R4	Information incorrectly interpreted	
Information communication failures		**Violations**
I1	Information not communicated	V1 Deliberate actions
I2	Wrong information communicated	
I3	Information communication incomplete	
I4	Information retrieval unclear	

A key practicality with guidewords concerns how many guidewords to use at each sub-task of an actual SCTA. Applying each guideword for each sub-task would usually be too resource intensive. The list in Table 4 is good as a thought process; however, there is a trade-off between thoroughness and practicality that should be managed. Usually a workshop chair (in the case of groups) or the SCT analyst will select an appropriate subset that covers most of the frequent and/or serious failures; however, a full list can be used for initial test studies and then optimised based on experience; some organisations also use the full list for a new process where there is little local experience.

Associated with the identification of failures, it is usual to include:

– The existing safety measures in place including the current potential for recovery from that particular failure.
– The potential consequences of the failure if recovery is not achieved. If there are no MAH safety related consequences then further analysis is not needed for this failure in terms of SCTA. However, if there are significant environmental or business related consequences this may be fed into parallel or future studies.
– The PIFs relevant to the failure. These are not shown in Table 5 but have been included in Tables 7 to 9. Typically, they include ambient environment, training, tools, human/machine interface (HMI), supervision, work patterns, team and social issues, etc. These should be included as part of the data collection in step 3 (see 2.4) and analysed in more detail in step 5. Typically, a subset of the most relevant PIFs from the lists shown in Annex A is associated with each potential failure. This will then help guide the analysts in determining whether effective safety measures are already in place or whether additional measures are needed.

In order to help understand the causes for the failures in Table 4, it can be helpful to use the taxonomy of slips, lapses, mistakes and non-compliances (violations) (see *Human failure types*). Some analysts find that this helps determine what the relevant safety measures that address these causes are, and whether additional measures are needed.

Having completed this step the SCTA will have analysed the current situation at the site with respect to SCTs and be ready to determine if further risk reduction is required.

2.6.1 Group-based approaches

For a group-based approach, the group composition should include the disciplines relevant to the system being analysed. This should include a technical expert who understands how the plant should work and why, and an expert who knows how the job is done in practice;

both roles could be filled by the same person. While aiming to include experienced people in the group for their accumulated knowledge, it is also valuable to have less experienced employees to reduce the potential for assumptions and well established habits, custom and practice to influence the SCTA. The group will be led by a facilitator and the discussions and outputs documented by a recorder. Key points to consider in order for group sessions to be most successful include the following:

2.6.1.1 Planning

- Briefing material should be supplied in advance to participants, explaining the workshop objectives, format, tasks to be analysed, background and relevant material generated in steps 1–4.
- Ensure the correct mix of disciplines and experience.
- Have diagrams, photographs, details of any procedures ready to hand at the meeting, together with any relevant historical data.

2.6.1.2 Facilitation

- Prior to analysing an SCT, some practitioners start with a description of the task and context, covering: how frequently is the task done; the history of the task; how it is initiated; the 'physicality' of the task; could it be done under emergency conditions? how long does it take? etc.
- Henderson and Hunter (2018) discuss several useful measures for a successful workshop:
  - Outlining why the task is being analysed (especially if there are reasons beyond it being linked to an MAH, e.g. recent near misses etc.).
  - Prior to getting into the detailed task steps, it can help to list the known task hazards and associated control measures. When human failures are identified, it can speed up the process by referring back to the list of hazards and controls, rather than repeating the text.
  - Sketching out a simple process diagram illustrating key activities can help if participants are not familiar with the task.
  - To help hone in on the critical sub-tasks within an SCT, the authors explore the possibility of scoring the sub-tasks to determine criticality. An example of this is described in case study 4 (see 4.4).
- The chair/facilitator should know what format will be used to achieve the desired level of detail across all tasks; for example, what tabular templates to use (tested in advance), what subset of guidewords from Table 3 and PIFs from Annex A will be favoured?
- Consider a mixture of techniques. As well as systematically working through guidewords, 'out of the box thinking' should be encouraged via freeform brainstorming to capture more unusual failures and to keep the group fresh.

2.6.1.3 Recording

- Documentation of group sessions should be sufficient for future follow-up of actions and recommendations, and should include any assumptions made for future validation.
- Further guidance on obtaining the best from such group sessions is available, for example, in CIA *HAZOP: Guide to best practice*.

2.7 STEP 6 – DETERMINE SAFETY MEASURES TO CONTROL RISK OF HUMAN FAILURES

Once potential human failures have been identified, the following hierarchy of additional risk controls (HSE Core Topic 3) should be considered:

- Can the hazard be removed?
- Can the human contribution be removed, e.g. by a more reliable automated system?
- Can the consequences of the human failure be prevented (or mitigated), e.g. by additional barriers in the system?
- Can human performance be assured by mechanical or electrical means? For example, the correct order of valve operation can be assured through physical key interlock systems or the sequential operation of switches on a control panel can be assured through programmable logic controllers. Actions of individuals alone should not be relied upon to control a major hazard.
- Can the PIFs be optimised, (e.g. improve access to equipment, increase lighting, provide more time available for the task, improve supervision, revise procedures or address training needs)?

When identifying extra safety measures it should be recognised that introducing new risk controls can also introduce unintended negative safety impacts. For example, a new, hypothetically more reliable, automated system may introduce important new maintenance failures. An analysis of new failure modes and their risks should be part of this step.

In determining what additional safety measures would be effective it should be understood how the human failures identified in step 5 fit within the classification of slips, lapses, mistakes, and non-compliances. For example, with respect to Table 5, improving training is unlikely to have a big impact on reducing slips and lapses, whereas it could potentially have an impact on mistakes and violations. In contrast, reducing distractions, through a less cluttered workplace or by the removal of extraneous activities, could have a significant effect on slips and lapses, but is unlikely to be so relevant to violation reduction. Table 5 maps failure types against safety measures, representing strong improvement potential with a tick (✓) and possible improvement potential with an asterisk (*).

Table 5: Mapping effective safety measures against human failure classification[6]

Safety measures – improvements in:	Slips	Lapses	Mistakes	Non-compliances (violations)
Control/display design	✓	✓	✓	✓
Equipment/tool design	✓			✓
Memory aids		✓		
Training			✓	✓
Work design	✓	✓		✓
Procedures	*	✓	✓	✓
Supervision	*	*	✓	✓
Reducing distractions	✓	✓	✓	
Environment	✓	✓	✓	✓
Communications	*	*	✓	✓
Decision aids			✓	
Behavioural safety			✓	✓

6 Adapted from Shorrock and Hughes, *Let's get real*.

Matching additional safety measures to failure types and PIFs is probably the element of SCTA that will be most unfamiliar for a non-HF specialist. Many of the other steps in the SCTA process are very similar in broad terms to traditional risk assessment steps.

Workforce involvement, though important during the whole process of SCTA, is crucial in this step. Operators and design personnel are more likely to understand, accept and act according to the resulting safety measures when they have had input to the development of these measures (see *Guidance on effective workforce involvement in health and safety*). Very often, skilled and experienced employees have sensible and practical suggestions for failure prevention, reduction and mitigation ready to be harvested by the SCTA facilitator.

Very often workshops are used to review the task, identify errors, consequences and PIFs and determine the current and additional risk controls. Identifying good risk controls can be difficult in this way as the focus tends to be on the error and its consequences. Often it is just a set of proposals that are identified, which then require further analysis to determine suitability, or for extra measures to be identified.

Tables 5 to 8 show examples of potential additional safety measures to address human failures. It is often convenient to split these into those that prevent or reduce the chance of the failure, and those that mitigate the consequences, including through improving the chance of failure recovery. The documenting of potential additional measures is a key stage in demonstrating that risks have been reduced to a defined level, such as the 'as low as reasonably practicable' (ALARP) criterion used in the UK. If SCTA tables similar to Tables 6 to 9 show very few entries in the columns for potential additional measures, the effectiveness of this step in the process may need to be reviewed.

The determination of what is 'reasonably practicable' is usually based on the collective subjective judgement of the team. Precedents from other sites can be used to support such judgements. In some cases, cost benefit assessment may be used, but this is usually restricted to instances where the potential risk reducing measure is very expensive but the risk reduction may be significant; in such rare cases subjective judgement may not be sufficient. Table 10 shows an illustrative ALARP demonstration table.

In order to ensure that the recommendations (illustrated in Tables 6 to 9) are followed up, they should be allocated timescales and persons responsible as per normal HAZOP or hazard analysis (HAZAN) processes. In addition, SCTA outputs should be regularly audited and the number of outstanding recommendations monitored.

There should be cross-referencing between the safety reports/cases and the SCTA document. A summary of SCTA recommendations should be considered for the safety report/ case, together with a demonstration that these have been actioned. If the main causes of MAHs relate to tasks analysed in the SCTA report, it may be necessary to include larger sections of the SCTA in the safety report/case.

A special note should be made concerning non-compliances (violations). If there are significant non-compliances occurring, then an SCTA will be an insufficient tool to ensure that risks are adequately managed. There may be a need for a specialist review of safety culture and an organisation's SMS. PIFs in an SCTA may indicate why non-compliances are occurring (for example, procedures too difficult, not enough time available, etc.), but this process is unlikely to mitigate the risk from non-compliances on its own.

2.8 STEP 7 – IMPLEMENT AND MONITOR EFFECTIVENESS OF SAFETY MEASURES

The output from step 6 will be a set of additional safety measures. Implementation should follow the systems and processes the organisation has in place to implement change. This may include aspects such as procedure updates, briefings for new equipment, training, etc. It should be possible to track all additional safety measures through to implementation.

Once implemented, it is important to check that the measures are having the intended effect. Information from this can come from existing safety management activities such as audit, inspections, reviewing near-misses and even incident investigations. However, getting feedback from personnel implementing the safety measures directly provides additional relevant information. Post-task debriefs/wash-up sessions can be used to understand whether equipment changes, or procedural updates are working as intended. Supervisory feedback from their observations and discussions can also provide good insights.

Where feedback suggests that safety measures need amending, checking against the SCTA output should help clarify how the measure was intended to work. There may need to be some iterations between steps 6 and 7.

2.9 STEP 8 – REVIEW THE EFFECTIVENESS OF THE PROCESS

The process described in steps 1 to 6 is deliberately high level. It should be adapted to fit within a site's SMS, and in particular matched and integrated into the site's process for safety risk assessment.

For a site that has done little or no SCTA of the sort described in this publication, it would be worthwhile developing a process based on initial trials (as per case study 5 in section 4) as follows:

– Choose a task(s) that clearly does link to MAHs or that clearly is high priority due to past incidents. Use this for the initial trial.
– Conduct SCTA as per steps 3 to 6. Get personnel involved, informed, trained and committed.
– Review the trial for lessons learned.
– Adapt the process so that it is suited to the site and leads to outputs that are beneficial and practical. Use the trial as a case study to help sell the benefits of wider use of SCTA.
– Obtain management commitment to conduct comprehensive SCTA for all MAHs.

As the process becomes established, regular reviews should be carried out to check that the SCTAs are producing good quality outputs and that the benefits obtained (such as reduced incidents, reduced costly redesign, etc.) justify the resources used. It is likely that various optimisations will be possible as experience is built up, and it may be possible to develop a library of generic SCTAs that could be reused for different MAHs around the site or between an organisation's multiple sites. For example, the task of isolating sections of plant prior to maintenance (see Table 8) may have both generic aspects associated with potential human failures and risk controls as well as local specific aspects, such as those associated with its location.

2.10 SCTA TECHNIQUES AND OUTPUT SUMMARY

Figure 5 illustrates which SCTA steps the more popular techniques support. Many of these techniques are also used in safety reports/cases and can help to integrate SCTA into these documents. They provide key inputs to step 2 of the SCTA (see 2.3) and can help transfer the outputs from steps 5 and 6 (2.6 and 2.7 respectively) of the SCTA into safety reports/cases to improve risk management of a site.

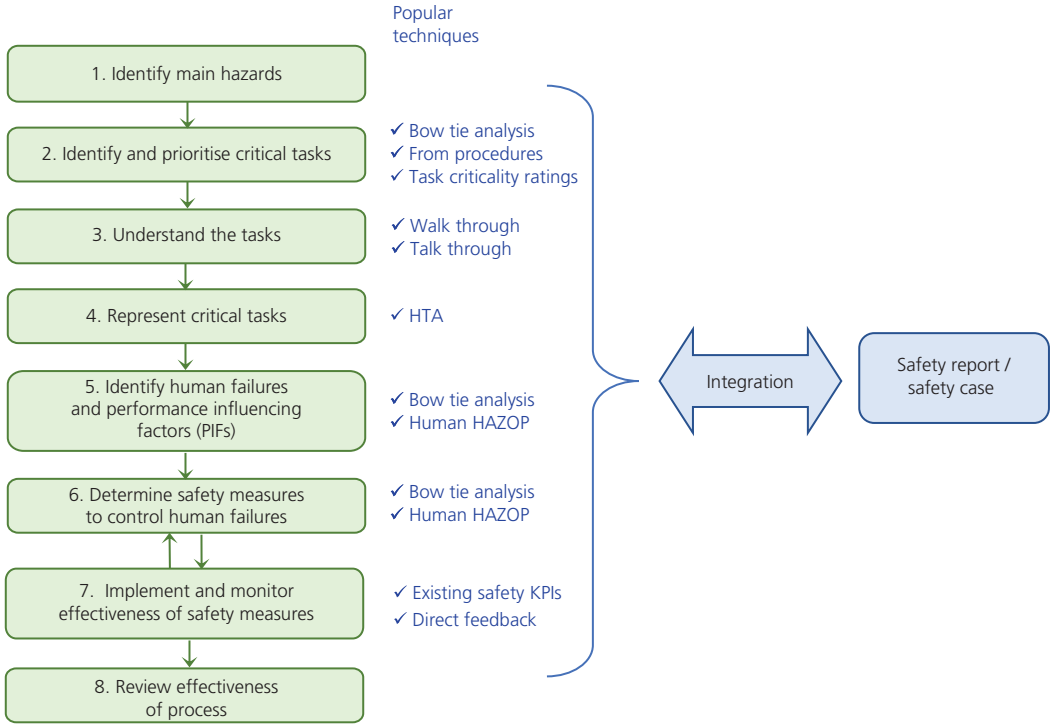

Figure 5: Mapping techniques to SCTA steps

2.11 ILLUSTRATIVE EXAMPLES OF OUTPUTS

Tables 6 to 9 show examples of the analysis undertaken in steps 4-6 of the SCTA. Table 6 shows tasks related to emergency response, using the HSE proforma from HSE Core Topic 3. The subsequent tables adapt the HSE proforma slightly and provide examples covering operational and maintenance tasks that could lead to major accident initiation and tasks associated with detection, control and mitigation of a major accident. It should be noted that Table 6 does not include PIFs, whilst the subsequent examples do illustrate how PIFs can be incorporated into the analysis.

The exact format should be adapted to best suit an organisation's SMS and existing safety risk assessment process. For example, some organisations include columns that evaluate explicitly the likelihood of failure occurrence (sometimes with and without additional safety measures) and link this to risk matrices as an output. However, it should be noted that the SCTA outputs should not be made so complex that they cannot then be understood by those who need to be aware.

Table 6: Example of emergency response task analysis[7]

Human factors analysis of current situation				**Additional measures to deal with human factor issues**		**Notes**
Task or task step description (Note 1)	**Likely human failures** (Note 2)	**Potential to recover** from the failure before consequences occur (Note 3)	**Potential consequences** if the failure is not recovered (Note 4)	Measures to **prevent the failure** from occurring (Note 5)	Measures to **reduce the consequences** or **improve recovery potential** (Note 6)	**Comments,** references, questions (Note 7)
Task step 1.2 – Control room operator (CRO) initiates emergency response (within 20 minutes of detection)	Action too late: Task step performed too late, emergency response not initiated in time	Control room (CR) supervisor initiates emergency response	Emergency shutdown not initiated, plant in highly unstable state, potential for scenario to escalate	Optimise CR interface so that operator is alerted rapidly and provided with information required to make decision; training; practise emergency response	Recovery potential would be improved by ensuring that the central control room (CCR) is staffed at all times and by clear definition of responsibilities	
Task step 1.3 – CRO checks that emergency response successfully shuts down the plant	Check omitted: Verification not performed	Supervisor may detect that shutdown not completed	Emergency shutdown not initiated, or only partially complete, as above	Improve feedback from CR interface	Ensure that training covers the possibility that shutdown may only be partially completed. Ensure that the supervisor performs check	
Task step 1.4.1 – CRO informs field operator of actions to take if partial shutdown occurs	Wrong information communicated: CRO sends operator to wrong location	Outside operator provides feedback to CRO before taking action	Delay in performing required actions to complete the shutdown	Provide standard communication procedures to ensure comprehension. Provide shutdown checklist for CRO	Correct labelling of plant and equipment would assist field operator in recovering CRO's error	

Notes:

1. Task steps taken from procedures, walkthrough of operation and from discussion with operators.
2. This column records the types of human failure that are considered possible for this task. It also includes a brief description of the specific error. Note that more than one type of failure may arise from each identified difference or issue.
3. Not all human failures will lead to undesirable consequences. There may be opportunities for recovery before reaching the consequences detailed in the following column. Recovery from errors should be taken into account in the assessment; otherwise the human contribution to risk will be overestimated. A recovery process generally follows three phases: detection of the error, diagnosis of what went wrong and how, and correction of the problem.
4. This column records the consequences that may occur as a result of the human failure described in the previous columns.
5. Practical suggestions as to how to prevent the failure from occurring are detailed in this column, which may include changes to rules and procedures, training, plant identification or engineering modifications.
6. This column details suggestions as to how the consequences of an incident may be reduced or the recovery potential increased should a failure occur.
7. This column provides the facility to insert additional notes or comments not included in the previous columns and may include general remarks, or references to other tasks, task steps, scenarios or detailed documentation. Areas where clarification is necessary may also be documented here.

7 Adapted from HSE Core Topic 3: *Identifying human failures*.

Table 7: Example of task analysis relating to accident initiation – operations – road tanker loading at fuel terminal

SCTA of current situation					**Additional measures to deal with HF issues**		**Notes**
Task or task step description	**Potential human failures**	**PIFs**	**Safety measures and recovery mechanisms**	**Consequences (if failure not recovered)**	**Measures to prevent or further reduce chance of failure**	**Measures to reduce consequences or improve recovery potential**	**Comments/ recommendations/ open issues**
Driver to carry out preparatory checks before tanker loading	**Check omitted:** Driver fails to check product indicators on vehicle before loading commences	Procedures	Manual action to initiate emergency shutdown (ESD) included in procedures. However, procedures not reviewed for several years.	Overfill protection activated on each product compartment Unknown product quantity remaining could lead to potential overfill if overfill protection fails	1. Review design of procedure and loading bay to reduce potential for distractions or loss of place in procedure		Additional measure 1 has been closed out. Additional measures 2, 3 and 4 to be taken forward as recommendations from SCTA. Review experience from other sites to determine frequency of such events
		Competence	Training programme for tanker drivers covers this task		2. Introduce programme of behavioural observations of drivers	3. Observation of bays on CCTV	
		System/ equipment interface				4. Introduce ESD buttons at either end of the loading bay	

Table 8: Example of task analysis relating to accident initiation – maintenance – pipeline interventions

SCTA of current situation					**Additional measures to deal with HF issues**		**Notes**
Task or task step description	**Potential human failures**	**PIFs**	**Safety measures and recovery mechanisms**	**Consequences (if failure not recovered)**	**Measures to prevent or further reduce chance of failure**	**Measures to reduce consequences or improve recovery potential**	**Comments/ recommendations/ open issues**
Isolate relevant section of pipeline	**Right operation on wrong object:** Isolate wrong pipeline	Procedures	Job controlled under permit-to-work (PTW)	Potential for loss of containment	1. Introduce a task risk assessment before such interventions		Additional measures 2 and 3 have been closed out. Additional measures 1, 4 and 5 to be taken forward as recommendations from SCTA.
		Communications	Interface with pipeline operators established		2. Review communication flows between relevant parties		
		Clarity of signs	Pipelines on site clearly labelled (but are they consistent across site?)		3. Check consistency of pipeline labelling across site		
		Competence	Approved training programme for maintenance technicians		4. Review contractor training	5. Enhance supervision of contractors by site staff – should notice failure	

Table 9: Examples of task analysis relating to accident escalation – detection, control and mitigation of events

SCTA of current situation					**Additional measures to deal with HF issues**		**Notes**
Task or task step description	**Potential human failures**	**PIFs**	**Safety measures and recovery mechanisms**	**Consequences (if failure not recovered)**	**Measures to prevent or further reduce chance of failure**	**Measures to reduce consequences or improve recovery potential**	**Comments/ recommendations/ open issues**
Test fire pumps	**Operation omitted:** Failure to replenish fuel supply to diesel pump	Procedures	Fuel replenished after each test as part of procedure	Activation of low level alarm fitted to pump fuel tank Running time of pump reduced or fails to start		2. Include random checks on fuel levels as part of monthly safety surveys	Additional measure 1 has been closed out. Additional measures 2 and 3 to be taken forward as recommendations from SCTA.
		Staffing Levels			1. Check adequacy of staffing level to conduct tests and replenish fuel		
		System/ equipment interface				3. Improve visibility of alarm indicator on CR panel	
Detect and interpret alarm	Information not communicated: Alarm not detected or interpreted correctly	Staffing Levels	CR staffing sufficient	Escalation of event			Consider cost-benefit analysis of upgrade to alarm system and shutdown system to determine practicability of measures 4 and 5
		System/ equipment interface	Well-designed HMI		4. Improve reliability of alarm system so that CROs react more promptly	5. Consider additional automated shutdown equipment	
		Competence	CR staff trained in diagnostic techniques				

Table 10: Illustrative ALARP demonstration

Example measures	Safety benefits	Analysis of practicability (cost, operational impact)	Decision	Comment
Enhance supervision of contractors by site staff (measure 5, Table 8)	Judged to have significant benefits given recent incidents at site. Would not just benefit this task but other tasks analysed in SCTA Would reduce frequency of relevant MAH significantly	Measure would be in line with practices at other company sites Could be introduced with a low impact on operations and staffing	Implement measure	Monitor impact of this measure and obtain feedback from supervisors after six months
Improve visibility of alarm indicator on CR panel (measure 3, Table 8)	Although visibility could be improved, CROs judge it to be adequate already. Small safety benefits are anticipated	Rearrangement of indicators is not straightforward for this particular CR. Significant costs	Do not implement now	Revisit this decision if an upgrade of CR is planned in the future

2.12 FREQUENTLY ASKED QUESTIONS

2.2 to 2.9 describe the SCTA process and provide some practical guidance relevant to individual steps. However, the following questions are commonly asked concerning practical aspects of the overall process.

How many tasks might I expect to identify at my type of facility?

This will depend on the nature of a facility but the following examples are given as illustrations:

– At a company running 60 process units, 1 400 safety critical tasks were identified. Note that this number followed a rationalisation from an initial list of 14 000. This highlights the necessity to create a manageable set of SCTs.
– For an LPG bulk storage and distribution site, 12 safety critical tasks were identified.
– An inspector from a regulatory body estimated 20–30 SCTs approximately per safety report.

How long should each analysis take?

The length of time spent analysing each SCT will vary widely. As a rough estimate it would be typical to spend a few days analysing a task which is either complicated with many interfaces or where an organisation is conducting a SCTA for the first time. For a simpler task, or when a company is more experienced, half a day per task would be more realistic.

In the latter case it is assumed that much of steps 1-4 have been carried out in advance and steps 5-6 are being applied to a logically arranged group of SCTs.

What resources should be involved?

Some companies have trained up operations specialists to undertake these analyses and they conduct them largely on their own, bringing in other specialists as needed. Other organisations make more use of groups and workshops.

The group/workshop approach has advantages when there are many organisational and discipline interfaces and also when an organisation is starting SCTA, as it is an effective way to spread learning quickly. However, the use of large groups within workshops may not always be practicable or could be inefficient if tasks are well understood from previous analyses.

In terms of requisite skills and experience:

– Steps 1 and 2 will require knowledge of safety assessment and contents of safety reports/cases, site operations and requirements of SCTs.
– For steps 3 and 4, if there is a need for complex HF analysis an HF specialist may be required. However, some organisations carry out the whole SCTA process, including these steps, with specially trained operational staff or those with a safety engineering background.
– As noted, steps 5 and 6 can be performed with facilitated multidisciplinary groups or by suitably trained individuals supported by specialists as required.
– For steps 6 and 7, in terms of following up SCTA outputs and reviewing the process effectiveness, this will involve primarily project and safety managers.

Do people need any training before participating?

If an organisation decides to conduct all the SCTAs using operational staff, then they will probably require special training. If experienced safety engineers or HF specialists conduct most of this work, and site personnel participate in workshops, training should be minimal; a briefing for workshop participants should be sufficient.

How long are SCTA findings valid for?

The main reason for needing to repeat SCTA is because of a change to plant, product, procedure, or workforce that means the original analyses require updating and in line with the site's ongoing ALARP demonstration.

3 SUPPORTING METHODS AND TECHNIQUES

A number of techniques can be used to provide practical support to SCTA. HTA and Human HAZOP are seen as core techniques for SCTA; other techniques may be used to support SCTA, but are not considered core.

In some safety reports/cases, an SCT analyst may find HAZOP tables, fault trees, event trees and bow ties as described in this section. In others, there may only be summary tables or text. Where this information is readily available from existing safety documentation the analyst should take advantage of this and feed this information into the list of SCTs. If it is not readily available, the SCT identification methods in 2.3 should be used.

3.1 HIERARCHICAL TASK ANALYSIS

3.1.1 Brief description

HTA represents tasks in terms of hierarchies of 'goals' and 'operations', using 'plans' to show when these should be carried out. This produces a hierarchy of tasks, usually represented in a top-down tree diagram format (see Figure 4). Since the task analysis is hierarchical, the analysis can be developed as much or as little as necessary. The HTA is usually numbered for easy and reliable reference to the various tasks/operations and levels in the task analysis representation. HTA can be used as a general method for representing a range of tasks, including those with significant cognitive (or mental) aspects, and has been described as the HF equivalent of the piping and instrumentation diagram (P&ID).

The general HTA steps are:

1. Identify the main task goal.
2. Describe the main goal as a set of sub-operations, with a plan specifying under what conditions, and in what order, the operations are performed. Descriptions may be graphical and/or textual. Remember to use verbs.
3. Decide whether further breakdown of operations is needed: if so go to 2, otherwise proceed to 4.
4. Analyse for inefficiencies of task operations to achieve goal.
5. Recommend changes to task operations and plans to improve system performance. Look at redesign of the task, interactions, tools, products or the system.

3.1.2 Applicability

HTA is best suited for analysing relatively simple cognitive and physical tasks where a clear goal, tasks and sub-tasks required to accomplish the goal can be determined. HTA is well suited to providing the basis for human failure identification. HTA can be applied in all life cycle stages to help designers describe how tasks should be carried out.

3.1.3 Pros and cons

Potential strengths include:

– HTA is relatively easy to learn and to use.
– It is easy within an HTA to assimilate a large amount of information relatively quickly.

– It can be used as a basis for addressing a large range of problems.
– HTA is an economical method of gathering and organising information, since the analyst needs only to develop the parts of the hierarchy where it is justified.
– HTA is best developed collaboratively between the task analyst and people involved in operations. This increases the chance that the outputs will be understood and used.

Potential disadvantages are:

– That a standalone HTA tends to focus on 'what' a task or sub-task involves, rather than 'why' it is being done that way. As part of the process described in section 2, however, the 'why' should be addressed in steps 5 and 6 of the SCTA, when potential alternatives to the current way of doing tasks are considered.
– The analyst should develop a measure of skill in order to analyse a task effectively – the technique is not a simple procedure that can be applied immediately. However, the necessary skills can be acquired reasonably quickly through practice.
– As noted, HTA should be carried out with a measure of collaboration from managers, engineers and other operating staff. While this collaboration is in most respects a strength, it entails commitment of time and effort from busy people.

3.1.4 Examples and further reading

A number of relevant examples are provided in Shepherd (2001), *Hierarchical task analysis*, covering batch and continuous process control tasks, mechanical maintenance and staff supervision. More examples and additional description of HTA are provided in Kirwan and Ainsworth, *A guide to task analysis*, and EI *Human factors briefing note no. 11 – Task analysis*.

3.2 HUMAN HAZOP AND TEAM/GUIDEWORD BASED VARIANTS

3.2.1 Brief description

HAZOP was initially developed as a systematic critical review method for process plant design (CIA, *HAZOP: Guide to best practice*; IChemE, *HAZOP and HAZAN*). An HAZOP involves a mixed skill set team of people who have experience of operating the plant or knowledge of the design that is under review. Review sessions are guided by an HAZOP leader and their conclusions are recorded so that follow-up actions can be pursued. The HAZOP approach involves considering each sub-system of the process in turn and subjectively evaluating the consequences of deviations from the way the design is intended to work. This examination of deviations is structured around a specific set of guidewords, which ensure complete coverage of all possible problems whilst allowing sufficient flexibility for an imaginative approach. Thus the potential hazards and operating problems can be identified, and recommendations made to remedy the problem or clarify the issue where the team is uncertain.

Human or procedural HAZOPs began to be developed in the 1980s and adapted the traditional format as follows:

– The system description in terms of connected nodes takes the form of a task analysis (for example, an HTA diagram), a set of procedures, a decision flow diagram, or an HMI diagram as examples.
– Guidewords are used which help the group identify typical human failures, for example, related to action failures, checking failures, information retrieval failures, communication failures, etc.

3.2.2 Applicability

Human HAZOP has been used widely in the energy industry to study, amongst others, offshore drilling (drillers' HAZOP, see Comer et al., *A driller's HAZOP method*), evacuation systems and SCTs at onshore oil and gas facilities. It can be applied in all life cycle stages commensurate with information available, i.e. conceptual HAZOP early in design and full HAZOP later when more details are available.

3.2.3 Pros and cons

Potential strengths include:

– It is a systematic method that should cover the main potential failures.
– Traditional HAZOP is already well established in many parts of the energy industry and hence extending it to address HF issues should be a natural development.
– The team approach involves a range of personnel (including operators/supervisors) so that they can understand recommendations and any actions that come out of the process.

Potential disadvantages are that:

– It is resource intensive.
– Its success heavily depends on the facilitation of the leader and the knowledge, experience, degree of cooperation and commitment of the team.
– The extensive documentation that may be produced can be a challenge to communicate to all affected personnel.

3.2.4 Examples and further reading

A full example of a human HAZOP for a COMAH site SCT is included in section 4 as case study 5 (which is based on Ellis and Holt, *A practical application of 'Human HAZOP' for critical procedures*). An example of a drillers' HAZOP is given in Comer et al, *A driller's HAZOP method,* and an offshore evacuation HAZOP in Boyle and Smith, *Emergency planning using the HSE's Evacuation, Escape and Rescue (EER) HAZOP technique*. A fuller description of the method is provided in Kirwan and Ainsworth, *A guide to task analysis,* and HSE Core Topic 3.

3.3 OTHER TECHNIQUES

3.3.1 Fault tree analysis

FTA is a logical representation of the many events and failures that may combine to cause one safety critical event, such as a system failure or an MAH. It uses logic gates (mainly AND or OR gates) to show how 'basic events' may combine to cause the critical 'top event'.

In the context of step 2 in 2.3 (the identification of SCTs), fault trees often identify human failures in combination with technical failures. Figure 6 shows a simplified tanker unloading example with an associated fault tree to study the hazard of storage tank overfilling. Potential human operator failures are highlighted in the tree, i.e. the operator might fail to check that there is enough space in the tank and the operator might fail to respond to an alarm when a high level has been reached.

Fault trees can also be used to analyse the human failures in more detail, showing causal events singly or in combination.

Another important use can be to illustrate common cause failures and dependencies in a system. For example, Figure 7 shows the human operator, failures connected through an AND gate. If these failures involve the same operator the two inputs to the AND gate are not independent. If AND gate inputs are assumed incorrectly to be independent this can lead to a significant underestimate of risk. Thus, each AND gate should be systematically analysed to determine HF influence and such dependencies. A simple way to do this is to identify where different human failures that appear in the tree could be made by:

– the same person;
– people from the same team (including co-located persons), and
– people working to common procedures, with common tools, who have experienced the same training, etc.

Based on this analysis, the risk prioritisation for certain tasks may increase and the need to analyse them in more depth may be increased. In terms of implications for SCTA, it may be more effective to analyse dependent tasks as a group in order that common PIFs can be identified and mitigated.

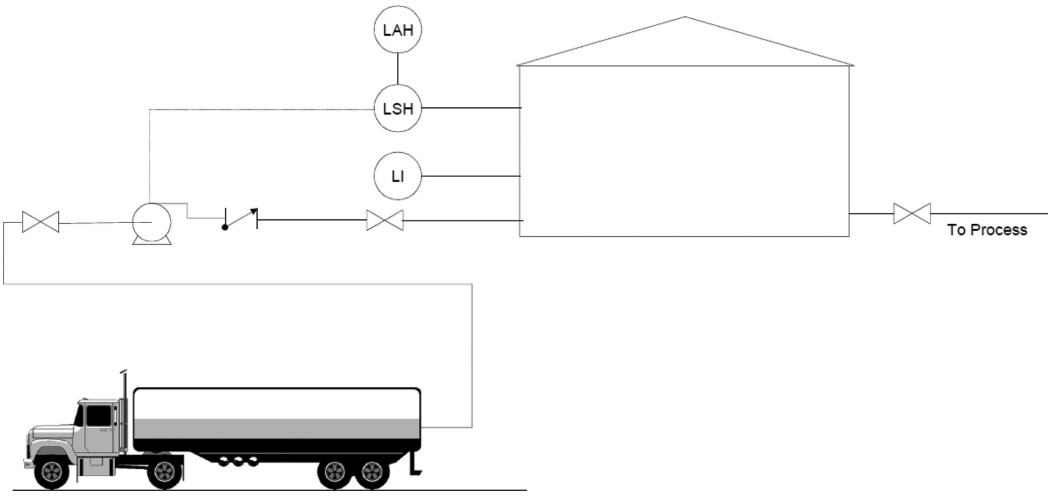

Figure 6: Simplified tanker unloading example

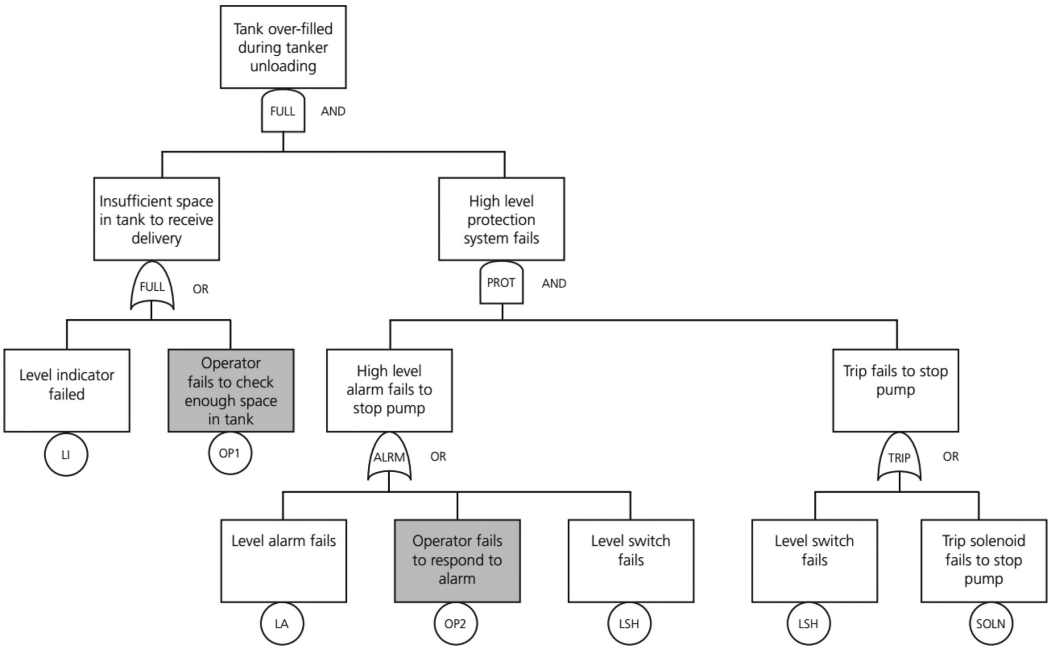

Figure 7: Associated fault tree

For more details on FTA see CMPT *Guide to quantitative risk assessment for offshore installations*. For a more complex method for addressing dependencies in human tasks see the technique for human error rate prediction (THERP) method described in Kirwan, *A guide to practical human reliability assessment*.

3.3.2 Event tree analysis

Event tree analysis (ETA) is a logical representation of the various events that may follow from an initiating event. It uses branches to show the various possibilities that may arise at each step. It is often used to show consequences of an initiating hazard.

Figure 8 shows an example event tree looking at potential escalation from a fire at an MAH unit. Again, important human tasks can be highlighted and fed into the list of SCTs (step 2 in 2.3). Event trees can help to identify those tasks or failures which are most safety critical and which have the greatest impact upon MAH risk. For more details on ETA see CMPT, *Guide to quantitative risk assessment for offshore installations*.

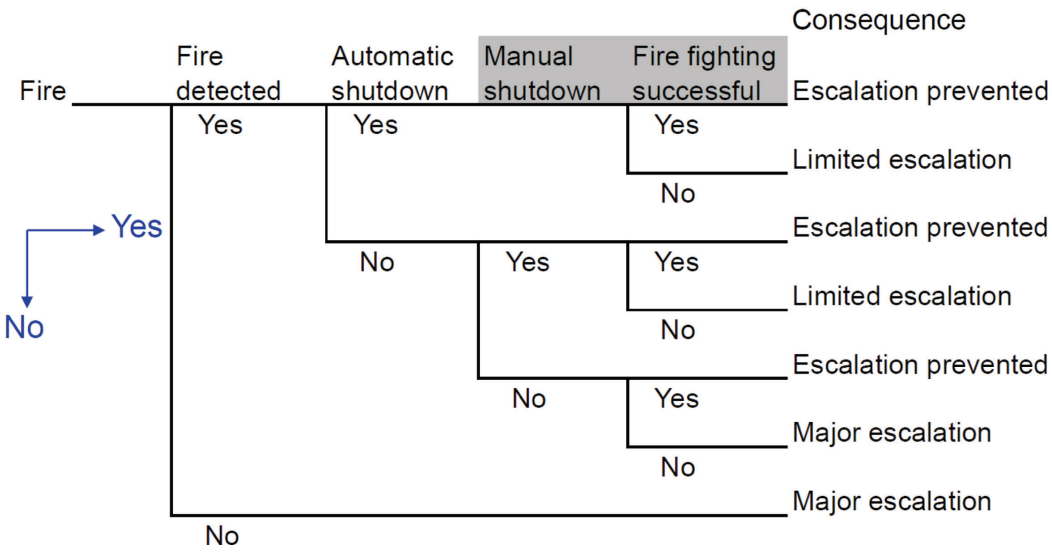

Figure 8: Example event tree analysing MAH escalation

3.3.3 Bow tie analysis

Bow tie diagrams have become a popular way to show how major incidents can occur. Bow ties show the threats that can lead to a loss of control of a hazard and the various consequences that may follow. Overlaid on the threats and consequences are the barriers designed to prevent or mitigate an event. Often bow tie diagrams are contained on one sheet of paper for ease of understanding and effective communication. Figure 9 shows a partially developed bow tie which illustrates the basic structure.

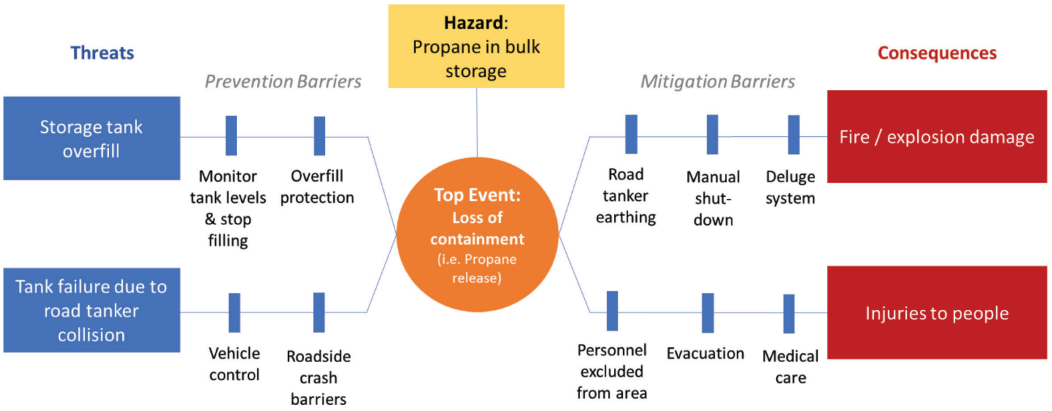

Figure 9: Partially developed bow tie

Various publications have been produced on how to develop bow ties, with accompanying rules for how they should be constructed, including an IEHF *White paper on human factors in barrier management*, and EI/CCPS *Bow ties in risk management: A concept book for process safety.* In terms of SCTA, bow ties can be helpful to identify SCTs. Tasks that are barriers themselves, or that directly support barrier effectiveness can be regarded as SCTs. The following could be identified as SCTs (or safety critical sub-tasks) from Figure 9:

– checking storage tank capacity and taking appropriate action;
– inspection and maintenance of crash barriers;
– on-site driving;
– maintenance, inspection and testing of the overfill protection;
– earthing road tanker;
– manual activation of shutdown and associated alarms;
– maintenance, inspection and testing of deluge system;
– escape and evacuation, and
– providing medical care (may include rescue of injured personnel).

Figure 10 shows an extension to a bow tie which introduces 'degradation factors' which can degrade barrier effectiveness; in this case, 'start-up procedure not followed'. It also shows a series of 'degradation controls' (e.g. regular review of procedure etc.). The diagram leads to the conclusion that 'start-up' is an SCT for this system. The degradation controls would not generally themselves be SCTs, although 'active supervision' might be a critical sub-task of 'start-up', especially if it includes supervisor sign-off.

The degradation controls allow identification of those specific organisational factors which support human related barriers and SCTs. These could be regarded as important PIFs to be included in the SCTA.

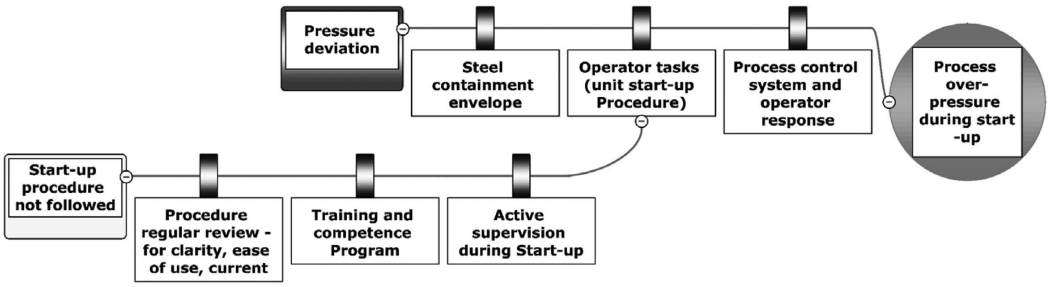

Figure 10: Human error as a degradation factor, highlighting 'start-up' as an SCT

3.3.4 Layer of protection analysis (LOPA)

If a site has performed LOPA analyses, these can be useful to help identify SCTs. An HSE research report (HSE RR716) provides several examples of LOPA outputs; key elements of one of these is summarised here to show how SCTs can be identified.

The HSE report describes an LOPA looking at the risk of a vapour cloud explosion resulting from tank overfill:

> *'Tank gauging and overfill protection are provided by an Automatic Tank Gauging (ATG) system and operator response to alarms for each tank. Additionally, a partially independent High Level (HL) alarm and operator response for pipeline fed transfer. This system comprises a separate sensor for each tank, a common Programmable Logic Controller (PLC) and alarms with manual initiation of shut-down. The manual action is that the pipeline vendor, either by means of a signal from the independent*

high level alarm or by means of a telephone call from the site operator, stops the transfer pump and informs the site so that they can then close the tank import valve.'

This description identifies the layers of protection, some of which are clearly human tasks. The overall SCT might be identified as 'keep tank levels within specified limits', and some identifiable sub tasks could be:

– respond to ATG alarm(s);
– respond to HL alarm(s), and
– manually initiate shutdown.

Initiating events are also reported:

– incorrectly calculating the ullage;
– supervisor fails to divert;
– supervisor transfers to wrong tank;
– supervisor diverts to wrong tank;
– exporter fails to close their export valve, and
– failure of ATG.

The first five of these are clearly errors in critical steps, which could be used to identify further sub-tasks. The description of the technical system and the layers of protection could also be used to identify MIT tasks associated with some of the hardware as potentially critical tasks.

3.3.5 Integrating SCTA into daily operations

Some companies have opted to integrate some SCTA steps into the regular work of the site, rather than running SCTA as an entirely separate activity. One company did this through a task improvement process[8] (TIP) mirroring the SCTA approach. The company wanted to implement a technique with the rigour of SCTA in a way that was integrated into the existing activities of a site. Experience had shown that more value was created when operators' input was provided in an operational setting, rather than 'the HAZOP room'. TIP also enabled 'human performance' on a specific job to be considered, something which can be difficult to address through the task risk assessment process. TIP was developed as a method for identifying stages in a task where a mistake might result in incidents with significant consequences. It aims to facilitate a conversation around error through a field 'walk and talk through', done locally. Personnel need to be skilled in the approach for it to be effective; equipping personnel to perform TIP requires an investment to ensure that they have the required skills.

The process is outlined in Table 11.

8 Courtesy of BP, UK.

Table 11: TIP outline

TIP stages	Activities and considerations
1. Identify the task	Critical activities in support of risk barriers Use local processes to decide which tasks to apply TIP to
2. Understand the task	Ask the operators or technicians Refer to procedure Compare 'what is done' with 'what is documented' (i.e. work as done vs. work as imagined)
3. Break task into stages for field evaluation	Consider different locations involved Consider different equipment, people, information etc Consider any change in what is being done Consider interdependencies and check assumptions Note stages and key steps on TIP fieldwork sheet
4. Walk through task stages in field with operators	Understand the purpose of each stage Consider the potential consequence of mistakes Identify 'flag conditions' (PIFs) that might increase the potential for mistakes Work on the hypothetical basis that mistakes will happen
5. Identify opportunities to improve	Fix defects Improve or remove things noted using flag conditions Identify additional safeguards Eliminate activity or task if preferable Explore in the field with the operators

TIP is supported with templates, guides and a short webinar. It is necessary to collate complete TIPs to monitor implementation and to identify longer-term improvements for implementation.

Pros and cons

Potential strengths include:

– Efficient approach to SCTA, especially if conducted offshore as it may avoid visits by SCTA specialists. It may help to alleviate the resource effort required to run an SCTA programme.
– Equipping personnel with the ability to conduct SCTA will have spin-off benefits when they perform other tasks – e.g. identifying potential errors, etc.
– Can reinvigorate initiatives around operational and procedure reviews.
– SCTA done in the field is within the comfort zone of operations personnel.

Potential disadvantages are:

– It might be harder for frontline personnel to 'take a step-back' and consider the full range of risk controls if they are looking at a specific job, e.g. the potential contribution

of improved hardware/software may go undetected as it is not considered feasible for the job at hand.

– Monitoring and retaining control of the SCTA process may be more difficult as it falls to operations personnel to implement.

3.3.6 Additional techniques

There are many other HF and safety assessment techniques that could provide support to SCTA. Kirwan and Ainsworth, *A guide to task analysis*, provides descriptions of many additional qualitative techniques associated with task analysis including:

– observation;
– questionnaires;
– simulators/mock-ups;
– table top analysis;
– walk-throughs and talk-throughs, and
– interface surveys.

For an overview of additional safety assessment techniques that could support SCTA, CMPT, *Guide to quantitative risk assessment for offshore installations*, CCPS, *Guidelines for chemical process quantitative risk analysis,* and Lees, *Loss prevention in the process industries,* describe the use of hazard checklists, what-if analysis, and failure modes effects and criticality analysis (FMECA) amongst many others.

Note that EI *Guidance on quantified human reliability analysis (QHRA)*, Kirwan, *A guide to practical human reliability assessment,* HSE RR679*, Review of human reliability assessment methods* and IOGP 434-5, *Human factors in QRA* have full descriptions of quantitative human reliability methods, including absolute probability judgement (APJ), paired comparisons (PC), THERP and human error assessment and reduction technique (HEART).

4 CASE STUDIES

4.1 CASE STUDY 1 – IDENTIFYING SCTS AT A REFINERY

A UK refinery decided to focus its SCT identification by looking at its COMAH safety reports and associated bow ties. The company did the following:

– Created a list of COMAH critical scenarios (around 100) from 19 COMAH safety reports.
– Identified related risk controls/layers of protection/safeguards based on COMAH report bow ties and process hazard analysis.
– Identified the relevant COMAH critical tasks by reviewing the risk controls/layers of protection/safeguards using relevant disciplines, including operations, process engineering, rotating equipment, instrumentation, etc.
– Ensured there were tasks in each of the categories of: normal operations; start-up; shutdown; upsets; emergencies; MIT and emergency response.
– Identified COMAH critical task lists for each business team and/or area which has a reference back to the safety report.

For operations tasks, the operating procedures and task instructions were risk-ranked, using the criticality/prioritisation table and matrix method described in 2.3.3.1.

4.2 CASE STUDY 2 – IDENTIFYING SCTS AT ANOTHER REFINERY

A large complex refinery in the UK (Tier 1 site operating under UK COMAH regulations) implemented a programme of SCTA. The site reviewed its main production activities to identify SCTs which, if carried out incorrectly, could result in an MAH scenario; for example the start-up of equipment such as process heaters where a purge must be carried out before ignition of pilots to prevent explosion. In addition, unit HAZOPs were reviewed to identify the main barriers to various MAH scenarios. Where barriers were identified, the site considered how a human was involved in ensuring its availability; for example if a barrier was an HL trip, someone was involved in its design, maintenance, testing and operation.

The site identified 44 representative SCTs which were a selection of:

– operational tasks (Table 12);
– MIT tasks (Table 13), and
– emergency response tasks (Table 14).

Many of the 44 tasks were replicated across several different production units; as such, the absolute number of SCTs was much higher. When the site moved onto analysing SCTs, they focused analysis on the critical steps identified within each task, rather than every single step in the task. Owing to similarities between units, it was possible to transpose task and error analysis findings between some units. However, the site still planned to review each unit to pickup individual PIFs (e.g. access or lighting differences). Tables 12 to 14 show the SCTs identified.

Table 12: Operational SCTs

Category	SCT (COMAH critical task)
Breaking containment	Changing a pressure gauge
	Clearing blocked drain/vent pipework
	Connecting/disconnecting berth loading arms
	Draining to sewer
	Sampling of hazardous substances (LPG, Benzene, hydrogen sulfide (H_2S))
	Tank/sphere water drawing
Control of overrides	Override or suppression of basic process control system (BPCS)/alarm
	Override or suppression of safety functions
Feed/product movement	Import of feed to storage tank
	Rundown/blending of product to tank
	Road tanker filling, e.g. LPG
	Road tanker unloading e.g. caustic or hydrofluoric acid
MIT of critical equipment	Testing of critical check valves
	Testing of emergency valves
Marine activities	Berthing of vessels
Prepare equipment for maintenance	Pressure safety valve (PSV)/thermal safety valve (TSV) removal/(re) installation for testing
	Prepare exchanger, pump, compressors
	Prepare vessels or tanks for atmospheric entry
	Prepare vessels or tanks for inert entry
Routine operator duties	BPCS – Placing a control valve on bypass control
	Gas testing
	Light individual burners as necessary
Start-up unit/ equipment	Air freeing and leak testing
	Line-up and start compressor
	Line-up and start pump
	Furnace/heater start-up
Shutdown unit/ equipment	Process unit shutdown
	Furnace/heater shutdown

Table 13: Maintenance, inspection or testing tasks

Category	SCT (COMAH critical task)
Live line working	Grit blasting
	Hot tapping
	Leak sealing
	Lifting over live lines/equipment
	Quill insertion/removal
MIT of critical equipment	PSV and TSV inspection and testing
	Critical instrument inspection and testing
	Trip function inspection and testing
	Inspection and testing of critical equipment (mechanical)
Safe isolation of plant for maintenance	Blinding/de-blinding of piping and equipment

Table 14: Emergency response tasks

Category	SCT (COMAH critical task)
Response to MAH	Response to flammable release
	Fire emergency response plan
	Response to toxic release
MIT of critical equipment	Isolation of fire main for maintenance
	Inspection and testing of fire protection water systems and fire water pumps
	Maintenance of emergency response vehicles and equipment

The site also identified what it described as 'communication related critical tasks' which are key operational safeguards that rely on accuracy of communications. These were:

– shift to shift handover;
– prepare and issue permits to control work;
– lock out tag 'out for maintenance'.

The site initially identified management of change and equipment inspection as SCTs; however, following a review, it was decided that such activities are not, strictly speaking, 'tasks' but rather processes that are often multidisciplinary with a large number of participants. Whilst such activities may be subject to human failure the controls to eliminate or reduce error are related to competence, training and approval by subject matter experts. These activities will be reviewed to identify the potential for human failure, but not using the full SCTA methodology.

4.3 CASE STUDY 3 – IDENTIFYING SCTS FOR A SERIES OF MATURE OFFSHORE PRODUCTION PLATFORMS

A UK North Sea operator embarked on a programme of SCTA for its offshore production platforms. Different approaches for SCT identification were found to be suited to each of the following: operations; maintenance; process upsets; emergency response and decommissioning. These are described as follows:

4.3.1 Operations

Looking at the safety case and bow ties helped the operator identify the MAHs and barriers, but these were not expressed in terms of operations tasks and so were not useful for SCTA. The company's HF specialist used the operating procedures in the hydrocarbon system manuals (e.g. covering oil, condensate, gas, flaring, drains etc.) as the basis of a list to be screened – i.e. each procedure was considered to be a task. This led to a list of around 80 procedures per facility, covering topics such as start-up and shutdown of plant, sampling and testing, and isolation for maintenance. The list of procedures was then subject to the standard HSE five-item questions (see 2.3.3.2) which was done with experienced operations staff. The company found that some of the questions and rating scale descriptions did not help to discriminate between tasks and so these had to be modified slightly. Experience showed that a sense check with operations was required when interpreting the scores; some procedures received high scores, such as compressor start-up; however, these were considered to be highly automated and well understood. Some less frequently performed tasks, with lower scores, were still progressed for detailed task and error analysis. For each platform, approximately 10 SCTs were progressed for detailed analysis. Experience showed that it is necessary to use a different set of criteria for scoring isolation or maintenance tasks as the original HSE five-item questions were not designed for these tasks.

4.3.2 Maintenance

The starting point for identifying critical maintenance tasks were the bow-ties found in the safety case. These represent MAH risk and the barriers which are in place. Some of the barriers refer to safety critical element groups that must be maintained as barriers against the MAH. The list of safety critical element groups was used as the starting point for identifying safety critical maintenance e.g. of pressure vessels, heat exchangers, rotating equipment, fire and gas detection, firewater pumps. Representative examples of maintenance tasks in each group were developed and these were then screened in a similar way to the operations tasks, but using a different set of criteria (again, the original HSE five-item questions were not designed for maintenance tasks).

Preparation for maintenance and reinstatement following maintenance was screened under operations (as this work is largely done by operations personnel). This meant that the maintenance screening focused on the very specific maintenance tasks (e.g. overhaul of fire pump). The maintenance team's interface with operations was also covered as part of maintenance SCTA. The company found that maintenance SCTs could be easily replicated across different assets (owing to similar equipment, SCEs, and therefore similar tasks). Experience has shown that a one-off exercise to look at safety critical maintenance routines is beneficial, but to embed this work it is beneficial to screen for safety critical maintenance in line with the yearly facility maintenance plans and assess as required.

4.3.3 Process upsets

Two approaches to identify critical tasks have been used:

– **Using HAZOPs** – The main source of information on process upsets is from facility HAZOP assessments. It was first necessary to identify process upsets with MAH risk, which often were already available from the HAZOP. It was then necessary to screen the process upsets with MAH risk to identify those in which operator action is required, i.e. where the operator is the final barrier in relation to the MAH. Simple guidance was developed to allow this assessment, which categorises the criticality of the operator in the response and therefore the extent of HF assessment that may be required. Although this approach was found to be useful, it is very time-consuming to identify MAH risk in an HAZOP if this has not already been done, and further time is then needed to determine the criticality of the human response.

– **Alarms assessment** – Another source for identifying where the operator is critical in a process upset is from the alarms rationalisation process. Where this process had identified and categorised SRAs then this could be used to inform where HF input may be required. Safety-related alarms are those where failure of the operator to respond will escalate to an MAH scenario. In other words, the operator is the final barrier against the MAH and there is no automatic protection e.g. trip systems or pressure relief systems. Where SRAs were identified, consideration was given to the operator actions that are required, and an HF assessment was carried out on these tasks. This approach was effective for identifying situations where the risk of relying on operator response should be engineered out. The overall process is likely to be managed by process control engineers with HF input.

4.3.4 Emergency response

Emergency response scenarios which require HF input can be identified through HAZOP studies and directly from the MAH risks identified in the safety case. The HF interest is typically in decision making during emergency response and where operator action is required, for example, manual activation of a deluge system. HF assessments can be carried out against emergency response plans/procedures in relation to MAH scenarios which have been identified.

4.3.5 Decommissioning

In terms of screening for safety critical decommissioning activities, a list of the key decommissioning activities was taken from project work packs. The activities of interest were those relating to decommissioning of hydrocarbon systems and those which may affect structural integrity. These tended to be stand-alone project activities with specific procedures written for them and so HF input should have been provided at the time of developing these procedures i.e. at the planning stage. It has been found that a customised set of criteria are needed to screen decommissioning tasks: one set for residual hydrocarbon risks and another for structural risks.

4.4 CASE STUDY 4 – USING TASK SCREENING TO IDENTIFY SAFETY CRITICAL SUB-TASKS

The company elected to use SCTA to review its arrangements for repairing so-called high-volume gas escapes. These are escapes from gas mains typically buried under the public highway or pavement. This was self-evidently an SCT, owing to hazardous escaping gas and the amount of human involvement in making the repair. The approach followed the eight-step process, but an extra step was added to assess how critical each individual **sub-task** was to the repair. This was done using a modified version of the HF questions (described in Table A.5). As well as honing in on the critical sub-tasks, the approach helped to appraise different methods for repair. By looking at the number and extent of critical sub-tasks for each repair option, the company could take an objective view of how it wanted to proceed. Full detailed SCTA was also performed for all repair options, with results recorded in a tabular format.

A workforce questionnaire was used to gain a wider view of the sub-tasks, and the beliefs and attitudes involved. Following a pilot, it was completed by 530 personnel, and covered the following themes:

– risk perception;
– risk reduction measures;
– contingency planning and recovery options;
– site monitoring;
– awareness of what a high-volume escape is;
– ignition control;
– role of personal protective equipment (PPE), and
– working arrangements.

The study:

– gave focus to SCTs which may not have been previously considered as such, e.g. understanding the importance and relevance of routine tasks such as atmosphere testing;
– represented an opportunity to define in a structured manner how repairs were performed;
– underlined the importance of the early site assessment and repair planning activities as these directly influence the subsequent risk of the job;
– provided input to support the training the company would deliver, and
– supported changes to how the company would execute repairs.

4.5 CASE STUDY 5 – CHEMICAL OFFLOADING OPERATION

This case study is from outside the energy industry but readily applicable to the industry. It is representative of many recent unpublished SCTAs that have been based on the HSE HF toolkit (HSE Core Topic 3). It is based on Ellis and Holt, *Practical use of human-HAZOP* and involved an SCTA at a chemical manufacturing site, which is a 'top tier' site under the COMAH regulations. The company wished to assess the reliability and robustness of the safety critical procedures identified in the COMAH and SIL studies. The assessment method they developed was trialled on one of the safety critical procedures associated with an MAH.

The COMAH scenario selected from the site safety report involved the offloading of organic peroxide from 200 litre drums from a dedicated unloading bay into storage tanks. This operation has the potential for ignition of an explosive atmosphere within the drums. A serious explosion and fire had occurred on the facility a few years earlier and the design of the unloading process had been improved in light of this experience. Nevertheless, this scenario was judged to present a risk at the upper end of the ALARP band during the COMAH risk assessment.

The basis of safety for this operation is to purge the drums with nitrogen prior to inserting a dip-pipe into the drum and starting the pump-out stage. A key step is the operator connecting a flexible nitrogen hose to the drum vent facility. Interlocks have been installed to prevent the dip-pipe being removed from its mount or the offloading pump running before the nitrogen purge flow and purge time are completed. It was realised prior to the HF SCTA that failures could still be made by the operator that would cause the basis of safety to be compromised.

The assessment approach was based on HSE guidance (HSE Core Topic 3), hence it being similar to the steps in section 2, and it is summarised in Table 15 with respect to the seven steps. It should be noted that it used a team-based HAZOP approach involving the workforce and that it was conducted by HF non-specialists. Ellis and Holt conclude that the assessment produced effective recommendations. An example output is shown in Table 16.

Table 15: Summary of case study 5[9]

Steps	Key issues
Step 1 – Identify main site hazards	Identified from COMAH report 2000, updated 2005
Step 2 – Identify safety critical tasks	Identified from COMAH and SIL studies. Focused on task where HFs known to be significant. Previous risk assessment had judged offloading operation to be at higher end of ALARP band
Step 3 – Understand the tasks	Written procedure was reviewed Observation of drum unloading activity. Confusion observed due to use of both plastic and metal drums – this distracted from proper performance of safety critical steps
Step 4 – Represent the safety critical tasks	Procedure broken down into key steps using HTA. Key steps are ones that could either prevent or mitigate the effects of a drum explosion or fire. Steps of no relevance to the hazardous event were discarded
Step 5 – Identify human failures and PIFs	Team-based HAZOP approach Nodes of HAZOP formed by key task steps Guidewords and standard PIF lists used

9 Presented in accordance with section 2 eight-step process

Table 15: Summary of case study 5 (continued)

Steps	Key issues
Step 6 – Determine safety measures to control risk of human failures	Recovery mechanisms considered Risk reduction measures assessed – engineering controls and HF improvements Human-HAZOP recorded
Step 7 – Implement and monitor effectiveness of safety measures	Not covered in reference source
Step 8 – Review the effectiveness of the process	Trial appeared effective. Suitable for wider application to other tasks on site

Table 16: Example output from human HAZOP[10]

Step	Human failure	Consequences/ severity	Potential to recover/ likelihood	Risk reduction measures	Recommendations
Screw nitrogen hose into drum hand tight	Hose not fitted to drum or fitted to wrong drum (note that plastic and metal drums have different connection sizes requiring adaptor to be changed)	Failure to purge air from drum, risk of ignition when dip pipe put into drum causing explosion and fire	Operator signs checklist to confirm that hose has been fitted to drum	No reliable means of detecting that hose has been fitted to drum can be devised	Ensure that adaptors for different bung sizes are readily available to the operator, e.g. shadow board in area.

4.6 CASE STUDY 6 – POWER PLANT CONTROL ROOM OPERATION

This case study is an older example from a power station safety assessment which also fits into the framework described in section 2.

This case study description is based on a chapter from Kirwan and Ainsworth, *A guide to task analysis*, and involved an SCTA at the design stage of a nuclear power station. The

10 Adapted from Ellis and Holt, *Practical use of human-HAZOP*.

pre-construction safety report (PCSR) identified 50 safety critical operator actions, and this case study is based on an analysis of one of these.

Following a reactor trip, if the main feedwater is unavailable, the auxiliary feedwater system should automatically start to provide decay heat removal. This feedwater would normally be returned to the condensate storage tanks via the main condensers, but if for any reason the condensers are unavailable, the condensate storage tanks will become depleted. If it is not possible to use the residual heat removal system (RHRS) to remove the remaining decay heat, the operator must obtain additional supplies of auxiliary feedwater from the town's water reservoir, by realigning valves at the reservoir and on plant.

The overall approach to the analysis of this task is summarised in Table 17 with respect to the eight steps in section 2. The SCTA was primarily the work of an HF specialist supported by other disciplines. More advanced techniques such as use of CR mock-ups were justified on the basis of the catastrophic potential of task failure.

The analysis was based on breaking the task down into:

– initiating cues;
– control actions;
– decisions;
– communications;
– sustaining cues (feedback), and
– termination cues.

This structure facilitated identification of potential failures, PIFs and recommended safety measures as shown in Table 18. The assessors put considerable effort into then communicating this information, with the underlying rationale, to the various discipline engineers ('interface area' column in Table 18) to ensure that the outputs were acted upon during the design.

Table 17: Summary of case study 6[11]

Steps	Key issues
Step 1 – Identify main site hazards	From probabilistic safety assessment supporting PCSR
Step 2 – Identify safety critical tasks	From probabilistic safety assessment supporting PCSR – over 50 operator actions to ensure that plant could be safely operated or could be safely shut down following a fault
Step 3 – Understand the tasks	Description of operator actions derived from PCSR and supplemented with control panel drawings, drawings of proposed video display units (VDU) formats, system diagrams, etc Informal discussions with technical specialists

11 Presented in accordance with section 2 eight-step process

Table 17: Summary of case study 6 (continued)

Steps	Key issues
Step 4 – Represent the safety critical tasks	Draft set of main steps identified by analyst 'talk through' of these proposed steps was then undertaken by operations specialist using control panel drawings to check for completeness and correct sequences Each of the steps then redescribed to appropriate level of detail which indicated how each step would be carried out and what equipment was necessary These task descriptions were then checked by the analyst in an accurate CR mock-up
Step 5 – Identify human failures and performance influencing factors	Tasks decomposed into: – initiating cues; – control actions; – decisions; – communications; – sustaining cues (feedback), and – termination cues Mismatches identified between the information/control which was currently available in the design and that which was required to successfully undertake each step
Step 6 – Determine safety measures to control risk of human failures	Mismatches which were highly likely to result in a failure to fulfil a safety action were given highest priority. Behavioural mechanisms were identified and potential remedies recommended Reports produced clearly identifying systems affected so that relevant system owners could understand and act on outputs
Step 7 – Implement and monitor effectiveness of safety measures	Not covered in reference source
Step 8 – Review the effectiveness of the process	Because analysis was undertaken early on in the project, the recommendations could be implemented at little cost The reports were sent to the licensing authorities so that they had confidence that each of the operator actions had been adequately safety assessed

Table 18: Example output from nuclear power station SCTA[12]

Task decomposition	Failure	PIFs	Recommendation	Interface area
Initiating cues	Operator fails to initiate realignment of feed water based on monitoring on-site storage tank levels	Monitoring has to be sustained for several hours while other tasks are undertaken (potential distraction)	A VDU system alert alarm when the on-site storage tank levels fall below 45 minutes' supply	Alarms
Control actions	Failure to open feed water valves in time	Town's water reservoir valves located offsite. Might need to be found in bad weather or darkness	All the valves must be prominently labelled so that it is easy to locate and distinguish them. The relevant plant operating instructions should provide guidance to personnel to assist them to locate all of the valves	External to main CR procedures
Termination cues	Failure to check that appropriate feedwater valves have been opened	No flow meters in the town's water lines. Therefore no independent check	Valve positions to be shown on VDU display. (Valve positions should indicate 'actual positions' and not 'directed to go to positions' which was a key contributor in the Three Mile Island nuclear incident in 1979.) Procedures and training to ensure that valve positions are checked by operator	VDU procedures Training

12 Adapted from Kirwan and Ainsworth, *A guide to task analysis*.

5 HIGH- VERSUS LOW- QUALITY SCTA

This section provides a concise listing of points which can be used by readers to benchmark their work and ensure that they do not fall into common traps. It will also help organisations specify what they want from an SCTA and what questions to ask during a SCTA.

5.1 HOW TO RECOGNISE A HIGH QUALITY SCTA

The following are judged indicators of a high quality SCTA:

- A clear rationale for the selection of SCTs (e.g. linkage to MAHs or past incidents).
- Signs that the appropriate amount of effort has gone into data collection (e.g. evidence of interviews and task observation to back up document review).
- SCTs clearly represented visually and/or in tables so that the reader can understand the tasks.
- Demonstration in the SCTA that the human failure identification is as comprehensive as possible (e.g. systematic use of guidewords for all tasks plus some creative brainstorming to think 'outside the box').
- If a team is used, evidence that the team has the appropriate mix of experience/ knowledge.
- Clear tabular outputs and recommendations brought together in a way that can be easily communicated to affected stakeholders.
- Evidence of workforce involvement in all steps.
- SCTA process matched and integrated to the rest of the site SMS and risk assessment process (for example, cross-references to existing risk assessment procedures, safety case documents, etc.).
- SCTA recommendations are regularly audited and reported as a site key performance indicator (KPI).

5.2 HOW TO RECOGNISE A LOW QUALITY SCTA

The following are judged indicators of a low quality SCTA:

- The study looks like a theoretical exercise with little sign of personnel involvement.
- It gets over-involved in details of procedures with little relevance to MAHs.
- There are obvious missing tasks (e.g. a focus on operational tasks, but nothing on maintenance and non-routine tasks).
- Failure to take account of past incidents with an HF component (either at the site or well-known in industry).
- Failure to identify non-compliances (violations) in SCT steps.
- PIFs not identified, or if they are identified, not mapped across to actions/ recommendations to demonstrate that they are being optimised.
- Evidence of gaps in the team knowledge (for example, plenty of offshore major hazard experience but a lack of marine experience in a floating production, storage and off-loading (FPSO) SCTA).

- Inappropriate use of risk control hierarchy (for example, consistently asking if certain PIFs can be improved (such as training), without considering if the hazard could be removed completely).
- Not matching additional safety measures to HF failure types (see step 6 in 2.7).
- Resulting documentation unusable as a decision-making or communication tool.
- Over-complex method with little chance of being used in a widespread manner (i.e. only a niche tool).
- Lots of quantitative analysis without a solid underlying qualitative analysis.
- No ALARP demonstration, i.e. a failure to identify a reasonable set of potential additional measures and no clear rationale as to why some were implemented and others rejected.
- No clear management or auditing of SCTA recommendations.

ANNEX A
EXAMPLES OF SUPPORTING MATERIAL

Table A.1: Performance influencing factors

Job factors
– Clarity of signs, signals, instructions and other information – System/equipment interface (labelling, alarms, error avoidance/tolerance) – Difficulty/complexity of task – Routine or unusual task – Divided attention – Procedures inadequate, inappropriate or unavailable – Preparation for task (e.g. PTW, risk assessments, checking) – Time available/required – Tools appropriate for task – Communication, with colleagues, supervision, contractor, other – Working environment (noise, heat, space, lighting, ventilation)
Person factors
– Physical capability and condition – Fatigue (acute from temporary situation, or chronic) – Stress/morale – Work overload/underload – Competence to deal with circumstances – Motivation vs. other priorities
Organisation factors
– Work pressures e.g. production vs. safety – Level and nature of supervision/leadership – Communication – Staffing levels – Peer pressure – Clarity of roles and responsibilities – Consequences of failure to follow rules/procedures – Effectiveness of organisational learning (learning from experiences) – Organisational or safety culture, e.g. everyone breaks the rules – Change management

Table A.2: Alternative checklist of performance influencing factors

PIF	Notes
Premises	
Workplace maintenance	Workplace maintenance/housekeeping issues that make the task harder (e.g. lighting not repaired, cluttered environment)
Workplace access	Any aspects of the workplace design that make it harder to carry out the task (e.g. access, confined spaces)
Physical environment	Issues relating to temperature, task lighting, noise levels, ventilation or weather that make the task more difficult
Plant and equipment	
Availability of equipment	Issues relating to availability of necessary equipment that make the task more difficult (e.g. equipment stored in a location distant from where the task is carried out)
Choice of equipment	Whether employees always use the specified equipment for the task
Equipment design	Whether the design of the equipment causes any problems when carrying out the task (e.g. is it possible to manipulate controls when wearing PPE?) and whether signs and labels are clear
Equipment installation	Issues relating to the location and positioning of equipment that make the task more difficult (e.g. valves that have been installed upside down)
Equipment maintenance	Whether the maintenance of equipment makes the task more difficult (e.g. poorly maintained valves that are difficult to open or close in an emergency)
Procedures and systems of work	
Choice of method	Whether there is much variation in the way employees carry out tasks, or whether they routinely deviate from the existing procedure
Suitability of accepted method	Whether the accepted task method is the best way to carry out the task (e.g. have employees worked out more efficient informal practices?)
Availability of procedures	Where procedures are necessary, are there any issues relating to their availability (e.g. is it easy for employees to refer to the procedure)?
Accuracy of procedures	Where procedures are necessary, are they up-to-date, accurate, unambiguous and workable?
Adequacy of supervision	Where a task requires supervision, is it provided?
Quality of training	Whether the task training provides employees with sufficient knowledge and skill to carry out the task. Are training programmes in need of evaluation and review?
Training updates	If changes have taken place in the way the task has been carried out, whether employees have been adequately trained in the changes
Refresher training	Whether employees receive task refresher training at appropriate intervals

Table A.2: Alternative checklist of performance influencing factors (continued)

PIF	Notes
Procedures and systems of work (continued)	
Task employee experience	Do all staff who might be required to carry out the task have the necessary recent experience?
Competency	Do staff meet defined competency requirements to carry out the task? Is an employee's initial and continuous competency assessed by regular and formalised observation/assessment programmes (quantitative and qualitative assessments)?
Communication	Issues relating to the communication of information between employees, supervisors, departments or organisations that make the task more difficult to carry out
Information from equipment	Whether employees obtain all of the information they require to carry out the task (e.g. from gauges, sensors, instruments)
Clarity of responsibility	Whether it is clear what the roles are when a task is being carried out (e.g. in an emergency who is expected to take an overview of the situation?)
Change management	Whether changes to the task or system have been adequately managed (e.g. have changes to operating configuration been passed on to operators?)
People	
Fatigue	Whether there are any issues relating to fatigue that might make a task more difficult to complete
Distractions	Whether the task is prone to distractions (e.g. if it is carried out in, or close to, a communal area)
Multi-tasking	Whether employees are typically required to carry out other tasks whilst completing this one and whether this presents any risks (e.g. operators leaving a charging process to do other activities)
Time pressure	Whether the task is ever carried out under time pressure and if this makes it more difficult to complete successfully
Capabilities	Whether this is the type of task that inexperienced or unqualified employees might be tempted to undertake unaided (e.g. when faced with production deadlines)

Table A.3: Example adaptation of the HSE's 5-item task criticality scheme – covering environmental hazards, posed by loss of containment

New diagnostic question	Definition	Rating guide and score			
		0	1	2	3
To what extent is the operator directly manipulating materials potentially hazardous to the environment?	Task moves/ manipulation of substances potentially hazardous to the environment	None	Movement or manipulation of small quantities of hazardous materials.	Movement or manipulation of large quantities of hazardous materials inside controlled locations (e.g. vessels, pipework, bunded areas).	Movement of large quantities of hazardous materials outside of controlled locations (e.g. vessels, pipework, bunded areas).

Table A.4: Example task criticality scoring for tasks involving handling or use of hazardous substances

Task description	Plant area	Links to MAH	Hazard score			Human factors score					Sum of HF scores	Overall criticality rating (Sum of HF x hazard score)	Notes
			Substance score	Quantity score[13]	Mean hazard score[14]	Likelihood of recovery	Task complexity	Task familiarity	Removal of safety systems	Impact of human actions			
			High (3) – toxic, extremely flammable	High (3) – e.g. full storage tank content	3	High (3) – the task can continue if failures are made and there are no warnings or planned checks to capture the failures	High (3) – the task involves numerous and/or complex steps	High (3) – the task is carried out less than once a month by the operator	High (3) – the task requires trip systems to be overridden and/or safety valves to be isolated and/or changes to the configuration	High (3) – there is a significant possibility that actions can result in hazard release	15	45	
			Medium (2) – highly flammable	Medium (2) – e.g. part storage tank content	2	Medium (2) – the task can continue if errors are made but there is planned opportunity (e.g. through a check) to recognise the failure	Medium (2) – the task involves several steps	Medium (2) – the task is carried out between once a week and once a month by the operator	Medium (2) – the task requires alarms to be defeated	Medium (2) – there is a possibility that actions can result in the hazard release	10	20	

13 Could be based on pressure and size of line equipment, or storage tank contents or flow per hour from ship/road/rail tankers.

14 Extremely flammable includes flammable and highly flammable liquid substances maintained at a temperature above their boiling point.

15 Mean of 'substance' and 'quantity' score. Could include an extra column for location (e.g. populated areas (high score) and remote locations like jetty head (low score)).

Table A.4: Example task criticality scoring for tasks involving handling or use of hazardous substances (continued)

Task description	Plant area	Links to MAH	Hazard score			Human factors score					Sum of HF scores	Overall criticality rating (Sum of HF x hazard score)	Notes
			Substance score	Quantity score[13]	Mean hazard score[14]	Likelihood of recovery	Task complexity	Task familiarity	Removal of safety systems	Impact of human actions			
			Low (1) – flammable, corrosive, dangerous to the environment	Low (1) – e.g. line content	1	Low (1) – the task can continue if failures are made but there is notification of the failure (e.g. by an alarm)	Low (1) – the task involves a few simple steps	Low (1) – the task is carried out once a week, or more frequently, by the operator	Low (1) – the task requires gauges, meters or displays to be defeated	Low (1) – there is a small possibility of actions resulting in hazard release	5	5	
						Zero (0) – the task cannot continue if failures are made (e.g. there are interlock systems or trips that prevent the consequence being realised)			Zero (0) – the task does not require safeguards/ equipment to be defeated	Zero (0) – there is no possibility of actions resulting in the hazard release	0	0	

Table A.5: Example human HAZOP guidewords

Code	Classification	Description	Examples/comments
	Action	**Practical 'hands on' task**	
A1	Operation too long or too short	Action took too long or not long enough	Not flushing pump long enough or flushing too long and overfills slop drum or overcools column
A2	Operation mistimed	Action carried out at wrong time – out of sequence (procedure)	Draining or venting equipment before isolation – out of sequence
A3	Operation in wrong direction	Action carried out in wrong direction	Operator turned left instead of right (associated with other codes, e.g. right act on wrong object)
A4	Operation too little or too much	Action not sufficient or too much	Applying too little or too much heat, pressure or cooling to a reactor
A5	Operation too fast or too slow	Action too slow or too fast	Flushing hot residue pump too fast (thermal shock), or too slow (solidifies residue)
A6	Misalign	Incorrect line-up of process valves/ pipework	Wrong alignment of product rundowns causing contamination, vessel overfill or loss of containment
A7	Right operation on wrong object	Action correct but on wrong equipment	Correctly opening valve, but choosing wrong valve. Carry out correct maintenance on wrong equipment
A8	Wrong operation on right object	Incorrect action but on correct equipment	Fitting incorrect part on correct equipment. Selecting right switch but operating it in wrong direction
A9	Operation omitted	Required action not carried out	Failing to close/open a valve or start/stop a pump. Missing a step in a procedure or rule
A10	Operation not completed	Required action not completed	Pump prepared for maintenance is not fully depressurised or drained
A11	Operation too early or too late	Required action performed too early or late	Breaking flanges before pipework is completely drained/ depressurised – (not out of sequence) Planned testing schedule on ESD systems inadequate

Table A.5: Example human HAZOP guidewords (continued)

Code	Classification	Description	Examples/comments
	Checking	**Observing/confirming equipment status**	
C1	Check omitted	Required check not carried out	Failing to reconcile instrument with gauge or failing to check equipment has been depressurised
C2	Check not completed	Required check not completed	Failing to complete pre-start-up checks. Checks instrument but not local gauge
C3	Right check on wrong object	Check correct but on wrong equipment	Checks drain valve is closed but on wrong pump. Right ESD test but on wrong system
C4	Wrong check on right object	Check incorrect but on right equipment	Incorrect application of procedure or test but on correct device/equipment
C5	Check too early or too late	Required check performed too early or late	Pressure test plant before all maintenance complete. Only 'service testing' high pressure system when hydrocarbon full and up to temperature and pressure. (No inert testing or hydro-test carried out prior)
	Information retrieval	**Document, machine, or instrument information**	
R1	Information not obtained	Procedure/permit/task analysis, gauge etc. information not read	Failing to acquire and read critical information (not reading procedure or critical lab result)
R2	Wrong information obtained	Procedure/permit/task analysis, gauge etc. information wrong/outdated	Inaccurate, ambiguous or outdated procedure, faulty gauge or instrumentation
R3	Information retrieval not complete	Procedure/permit/task analysis, gauge etc. information not fully gathered	Reads PTW, but fails to read the associated risk assessment
R4	Information wrongly interpreted	Procedure/permit/task analysis, gauge etc. ambiguous	Acquires all relevant data but misinterprets requirements (often associated with competency issues)
R5	Information not available/accessible	No information available or accessible for use in task	No procedure exists or is unobtainable. Not enough instrumentation in place

Table A.5: Example human HAZOP guidewords (continued)

Code	Classification	Description	Examples/comments
	Communication	**Human to human communications (written or verbal)**	
I1	Information not communicated	No information communicated verbally/ written	Failing to log or pass on information at shift handover or to/ from CCR
I2	Wrong information communicated	Incorrect information communicated	Inaccurate logs/turnovers, inaccurate verbal directives
I3	Information communications incomplete	Not enough information communicated	Unfinished or inadequate turnover, lacking receiver feedback. Fail to communicate the 'big picture'
I4	Information communications unclear	Communication takes place but is ineffective.	Ambiguity of language/text. Noisy environments, lacking receiver feedback
	Selection/decision	**Decision making**	
S1	Selection/decision omitted	Selection/decision not made	Failure to react under pressure. Unaware of the need. (Unaware of event, lacks enough knowledge)
S2	Wrong selection/ decision made	Making wrong choice	Lacks rule based experience and/or knowledge based detail
	Planning	**Devising methodology for carrying out task**	
P1	Plan omitted	Plan/strategy not made	Working on 'critical' system with no clear strategy or procedure
P2	Plan incorrect	Wrong plan/strategy made	Flaw in plan due to lack of knowledge or misperception of a situation

Table A.5: Example human HAZOP guidewords (continued)

Code	Classification	Description	Examples/comments
P3	Plan not completed	Plan does not cover all possible eventualities	Inadequate risk assessment, task analysis. (Similar to P2 above)
	Diagnosis/decision making	**Misinterpretation of symptoms/causes**	
D1	Diagnosis not made	Symptoms not recognised (e.g. new or unique event)	No diagnosis made due to no symptoms evident or lacking knowledge of symptoms that are evident (new problem or symptoms, no previous experience)
D2	Diagnosis not correct	Symptoms mimic other problems; same problem but causations different	Diagnosis based on experience of similar problem. Diagnosis not recognised as that previously experienced due to differing evolution of symptoms
D3	Diagnosis too early or too late	Decision made too early or too late	Early yet wrong diagnosis based on initial symptoms evident or late diagnosis due to slow evolution or recognition of symptoms
	Non-compliances	**Breaking rules etc. knowingly and with intent**	
V1	Deliberate actions (best intentions, optimising, situational, exceptional violations)	Wrong perception of organisational requirements or culture.	Works outside procedure with an incorrect perception of company support for their action (e.g. to improve productivity, to mitigate an evolving adverse situation)
V2	Deliberate actions (personal benefits, reckless or malevolent act)	Intended action, shortcut to benefit self, easier, less time (does not consider consequences or gambles against them happening)	Works outside of procedure only to benefit self (time or energy saving). Horseplay. Sabotage

Table A.5: Example human HAZOP guidewords (continued)

Task complexity		Low			Moderate			High		
Task frequency (taking into account how often each individual performs task)		Frequent	Infrequent	Rare	Frequent	Infrequent	Rare	Frequent	Infrequent	Rare
Consequence	Low									
	Moderate									
	Severe									

Nothing required	No instruction required beyond basic operator training
Work instruction	Typically produced for an operating routine (low/moderate complexity task) taking less than a shift. Sampling etc.
Reference procedure	Review of procedure required before executing task. (Can be guideline or detailed step-by-step but does not need sign off).
Critical procedure	Step-by-step instruction required – In hand use of procedure and sign off at each step required. Sign off required.

Figure A.1: Example risk-based operating task classification guide[16]

16 Courtesy of ConocoPhillips, Humber Refinery

ANNEX B
REFERENCES AND BIBLIOGRAPHY

B.1 REFERENCES

American Institute of Chemical Engineers (AICHE) / Center for Chemical Process Safety (CCPS)
https://www.aiche.org/ccps

Guidelines for chemical process quantitative risk analysis, second edition

Ceter for Chemical Process Safety (CCPS) / Energy Institute (EI)

Bow ties in risk management, A concept book for process safety, EI and Center for Chemical Process Safety (CCPS)

Chemical Industries Association (CIA)/ European Process Safety Centre / Institution of Chemical Engineers (IChemE)
https://www.cia.org.uk / https://epsc.be / https://www.icheme.org

HAZOP: guide to best practice, second edition, European Process Safety Centre

The Centre for Marine and Petroleum Technology (CMPT)

Guide to quantitative risk assessment for offshore installations, first edition, available from EI

Energy Institute (EI)
https://publishing.energyinst.org/

Guidance on effective workforce involvement in health and safety, first edition

Guidance on quantified human reliability analysis (QHRA)

Human factors briefing note no. 11 – Task analysis

Human failure types

Health and Safety Executive (HSE)
http://www.hse.gov.uk

Assessment principles for offshore safety cases (APOSC)

A human factors roadmap for the management of major accident hazards

HSE Core Topic 3: *Identifying human failures*

Inspecting human factors at COMAH establishments (operational delivery guide)

HSG48, *Reducing error and influencing behaviour*

RR 033, *Evaluation report on OTO 1999/092 Human factors assessment of safety critical tasks*

RR716, *A review of Layers of Protection Analysis (LOPA) analyses of overfill of fuel storage tanks*

RR679, *Review of human reliability assessment methods*

Offshore Technology Report OTO 1999/092, *Human factors assessment of safety critical tasks*

Safety report assessment guide: Human factors, Version 1.2

International Association of Oil and Gas Producers (IOGP)
https://www.iogp.org

Report No. 434 – 5, *Human factors in QRA*

International Electrotechnical Commission (IEC)
https://www.iec.ch

IEC 61508 *Functional safety of electrical/electronic/programmable electronic safety-related systems*

IEC 61511 *Functional safety-Safety instrumented systems for the process industry sector*

Institute for Energy Technology (IFE)
https://www.ife.no

IFE/HR/E-2017/001, *The Petro-HRA guideline*

Institution of Chemical Engineers (IChemE)
https://www.icheme.org

Kletz, T. *HAZOP and HAZAN*, third edition

Various authors

Boyle, P. and Smith, E.J. *Emergency planning using the HSE's evacuation, escape and rescue (EER) HAZOP technique*, Hazards XV, Symposium Series No.147, Institution of Chemical Engineers, Rugby

Comer, P., Fitt, J.S. and Ostebo, R. *A driller's HAZOP method*, Paper at Eurospec '86, Soc. Petroleum Eng., London

Ellis, G.R. and Holt, A. *A practical application of 'Human HAZOP' for critical procedures*, Hazards XXI, 2009 IChemE, Symposium Series No. 155

Ellis, G.R. and Holt, A. *Practical use of human-HAZOP*, presentation given at IChemE Hazard XXI conference, session 12

Henderson, J., and Hunter, N. *Developments in human factors critical task reviews (HFCTR)*, paper at Hazards 28.

Hopwood, M., Maguire, C., and Adams, L. *Use of visual media for offshore task analysis*.

Kirwan, B. *A guide to practical human reliability assessment*, Taylor and Francis

Kirwan, B. and Ainsworth, L.K. *A guide to task analysis*, Taylor and Francis

Lees, F.P. *Loss prevention in the process industries*, 2nd edition, Butterworth-Heinemann

Lucas, D *Human error predictions and controls: Demonstrations made in COMAH safety cases*, Paper presented at an IBC conference on Human Error, London

Shepherd, A. *Hierarchical task analysis*, Taylor and Francis

Shorrock, S.T. and Hughes, G. *Let's get real: How to assess human error in practice*, IBC Human Error Techniques Seminar

B.2 BIBLIOGRAPHY

Chartered Institute of Ergonomics and Human Factors (CHIEHF) – https://www.ergonomics.org.uk

Human factors in barrier management, *white paper*

Energy Institute (EI)

https://www.energyinst.org

Human factors briefing notes (20 individual briefing notes covering a cariety of HF topics)

ANNEX C
ABBREVIATIONS AND ACCRONYMNS

AICHE	American Institute of Chemical Engineers
ALARP	as low as reasonably practicable
APJ	absolute probability judgement
APOSC	assessment principles for offshore safety cases
ATG	automatic tank gauging
BPCS	basic process control system
CapEx	capital expenditure
CCPS	Center for Chemical Process Safety
CCR	central control room
CCTV	closed circuit television
CHIEF	Chartered Institute of Ergonomics and Human Factors
CIA	Chemical Industries Association
CMPT	Centre for Marine and Petroleum Technology
COMAH	Control of Major Accident Hazards
CR	control room
CRO	control room operator
CTA	critical task analysis
EER	evacuation, escape and rescue
EI	Energy Institute
ESD	emergency shutdown
ETA	event tree analysis
FMECA	failure modes, effects and criticality analysis
FPSO	floating production, storage and off-loading [unit]
FTA	fault tree analysis
H2S	hydrogen sulfide
HAZAN	hazard analysis
HAZOP	hazard and operability study
HEART	human error assessment and reduction technique
HF	human factors
HL	high level
HMI	human/machine interface
HOFCOM	Human and Organisational Factors Committee
HSE	Health and Safety Executive
HTA	hierarchical task analysis
IChemE	Institution of Chemical Engineers
IEC	International Electrotechnical Commission
IFE	Institute for Energy Technology

KPI	key performance indicator
LAH	level of alarm high
LI	level indication
LOPA	layers of protection analysis
LPG	liquid petroleum gas
LSH	level set high
MAH	major accident hazards
MIT	maintenance, inspection and testing
P&ID	piping and instrumentation diagram
PC	paired comparisons
PCSR	pre-construction safety report
PIF	performance influencing factor
PLC	programmable logic controller
PPE	personal protective equipment
PSF	performance shaping factor
PSV	pressure safety valve
PTW	permit-to-work
RCS	risk control system
RHRS	residual heat removal system
SCT	safety critical task
SECE	safety and environmental critical elements
SCTA	safety critical task analysis
SIL	safety integrity level
SMS	safety management system
SRA	safety related alarm
THERP	technique for human error rate prediction
TIP	task improvement process
TSV	thermal safety valve
VDU	video display unit

This publication has been produced as a result of work carried out within the Technical Team of the Energy Institute (EI), funded by the EI's Technical Partners and other stakeholders. The EI's Technical Work Programme provides industry with cost effective, value adding knowledge on key current and future issues affecting those operating in the energy industry.

Energy Institute
61 New Cavendish Street
London W1G 7AR, UK

t: +44 (0) 20 7467 7100
e: pubs@energyinst.org
www.energyinst.org

9781787251656

ISBN 978 1 78725 165 6
Registered Charity Number: 1097899