Safety Critical Tasks and Management of Human Error

Rocio Miguez, Principal Engineer, DNV GL, Cromarty House, 67-72 Regent Quay, Aberdeen AB11 5AR

Richard Roels, Principal Consultant, DNV GL, Vivo Building, 30 Stamford St, South Bank, London SE1 9LQ

Jim Cameron, Technical Authority Manager, CNOOC Petroleum Europe Ltd., Discovery House, Prime Four Business Park, Kingswells Causeway, Aberdeen, AB15 8PU

Human failures have contributed to major accidents such as Piper Alpha, Chernobyl and Texas City. Attributing incidents to 'human error' has often been seen as a sufficient explanation in itself and something which is beyond the control of managers, but this view is not acceptable to regulators. Duty holders must consider Human Factors (HF) as an explicit part of barrier management, protecting against major accident hazards (MAHs). HF must be recognised, assessed and managed effectively to control MAH risks.

There is a clear regulatory requirement that duty holders of offshore installations in UK waters must take account of human and organisational factors when assessing and managing MAHs. Guidance from the UK Health and Safety Executive (HSE) on 'Human factors in the management of major accident hazards' expands on the regulator's expectations in this respect, which include carrying out qualitative human reliability assessment on tasks where human failure could impact on MAH management.

DNV GL has developed a process to help duty holders apply Safety Critical Task Analysis (SCTA), and build in-house company capability, to ensure that human error risks are managed to a level which is as low as reasonably possible. This process is aligned with the updated Energy Institute guidance on safety critical task analysis and has successfully been trialled with one of the UK major operators.

This paper provides details of an application of the SCTA process, the iterative approach used to developing it, and the lessons learned during the process.

Keywords: Safety critical tasks, human error analysis

Challenge

CNOOC Petroleum Europe Ltd. (CNOOC) is committed to help their people achieve their potential through effective performance management. This requires business processes and supporting organisational structures to improve individual performance. CNOOC collaborated with DNV GL to define an overall approach to human factors in the management of the company's major accident hazards. The approach needed to meet the regulator's requirements and CNOOC's expectations, and be pragmatic, i.e. making the best use of the existing major accident hazard (MAH) bowties and learnings from incident and accident investigations. Moreover, the assessment of HFs had to be incorporated into other processes, e.g. operational risk assessments, management of change, management of deviations, etc.

Background

Human failures have contributed to major accidents, such as Piper Alpha, Chernobyl and Texas City. People play a vital role in the management of MAHs. It is therefore necessary that human activities that could affect MAH management are scrutinised to help ensure that people do what they need to do, without error. Guidance from the Health and Safety Executive (HSE) on HF [3] expands on the regulator's expectations in this respect, which include carrying out qualitative human reliability assessment on tasks where human failure could impact on MAH management.

The Energy Institute has developed a safety critical task analysis (SCTA) process [1] following the HSE's guidance to operators and its Inspectors [3]. DNV GL and CNOOC have adopted this process to define a pragmatic approach to SCTA and human error analysis (HEA).

SCTA methodology

A project was set up to adapt the Energy Institute process to the operator's needs. The team included Technical Safety Engineers and a HF specialist from DNV GL and CNOOC, and Technical Authorities with process safety knowledge and experience.

The project defined safety critical tasks (SCTs) as those involving significant levels of human interaction with safety critical equipment or processes, with the potential to influence a MAH. SCTA looks at tasks and activities involving significant levels of human involvement which, if performed incorrectly, have the potential to initiate, mitigate or prevent a major accident sequence.

The main steps in the SCTA process are shown in Figure 1, together with the purposes of each step. The scope of the work described in this paper was to identify SCTs and to prepare a ranked inventory of tasks, prioritised for HEA.

The ultimate aim of the analysis was to identify the critical tasks that support the availability of barriers needed in order to prevent or further reduce major accident hazard risks.

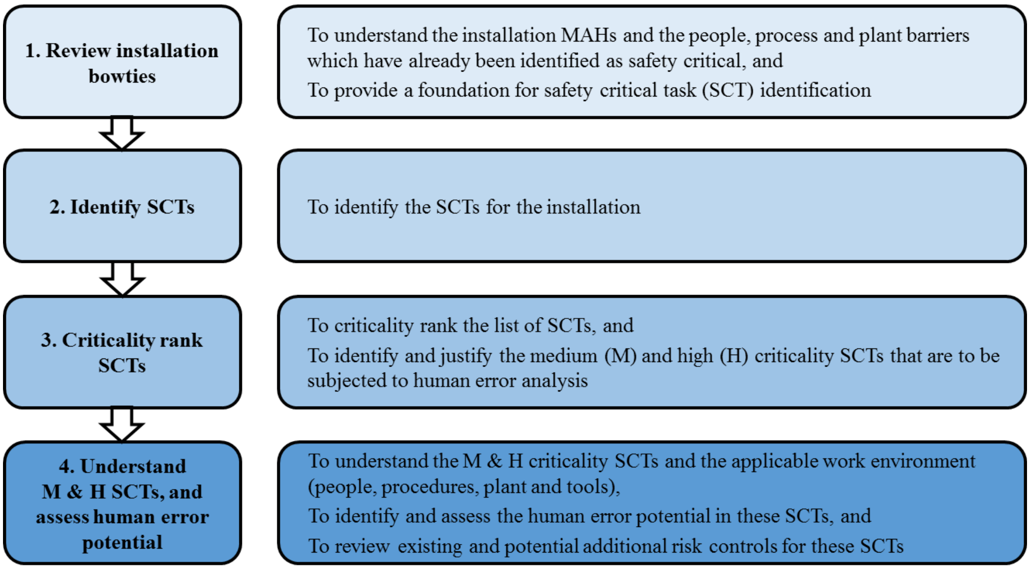

Figure 1 – SCTA main steps

Review of the installation's bowties

The starting point for identifying tasks and activities with major accident potential is the existing MAH assessment studies and bowties supporting the safety case. The review generated a list of:

- Safety and Environmental Critical Elements (SECEs) with
- Details of their main component parts, and
- Process barriers

SCT Identification

SCT identification is an iterative process comprising document review, experienced judgement and brainstorming sessions with Technical Authorities. The sub-steps are presented in Figure 2.

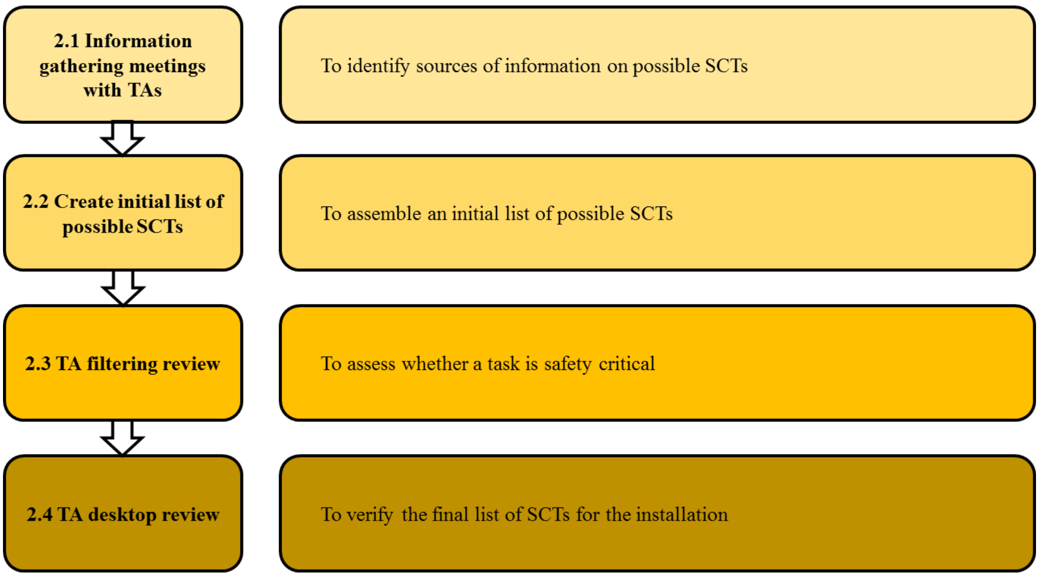

Figure 2 – SCT identification process

The information sources identified in Step 2.1 were interrogated to identify and create an initial list of SCTs. This involved document review (e.g. for operating procedures) and extraction of data from computerised systems (e.g. for maintenance routines). SECEs, along with their performance standards and assurance routines, and the generic SCT list provided in [2] were discussed.

The list of possible SCTs was reviewed by the Technical Authorities, to ensure that it was comprehensive. Technical Authorities also supported filtering reviews, based on their experienced judgement, and the application of a Screening Tool (3x3 matrix) developed to assess whether a task is safety critical, based on an assessment of:

- The consequence of human error, i.e. the MAH potential and whether there are other barriers in place, and
- The level of human involvement, i.e. interactions with safety critical equipment and the complexity or error potential.

The Screening Tool filters the initial list of possible SCTs and proposes whether the activity is, or is not, a SCT. The possible SCTs assessed as “no” were not considered further in the SCTA process, but they still need to be managed.

Tasks which were thought of as safety critical but 'back office' (and carried out offshore or onshore) were identified at this point, e.g. annual pipeline and structural integrity reviews, or helideck certification. This step also prompted the identification of safety critical processes, which govern the SCTs, but were out of the SCTA scope. Safety critical processes typically fall within the scope of the following management system elements:

- Operations and maintenance procedures
- Management of change
- Safe systems of work
- Operational readiness.

SCT criticality ranking

The list of installation SCTs was criticality ranked to understand which SCTs are more (or less) critical to MAH management and identify and justify the medium (M) and high (H) criticality SCTs, to which HEA would then be applied. This was carried out in a workshop attended by Technical Authorities, representatives of the offshore workforce (with knowledge of the possible SCTs), a workshop leader and a scribe.

For operations and maintenance tasks, the criticality ranking was carried out by scoring the responses to the following five questions for each SCT (adapted from the HSE OTO report [2]):

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 isolations or the operating configuration?
4. To what extent could incorrect performance of the task cause release of a hazardous substance, escalate an event, or cause damage?
5. To what extent does the task involve defeating or overriding isolation or protection devices?

The response to each of these questions is a score of 0 to 3, using the assessment scales given in Attachment 1. The sum of these scores is a number from 0 to 15. Table 1 shows the categorisation of SCTs based on the scores (adapted from the HSE OTO report [2]).

Table 1– SCT criticality ranking based on the 5-questions scoring

Sum of Scores	Criticality ranking
10 or greater	High
8-9	Medium
7 or less	Low

For well operations tasks, the screening process adopted was the same, but the questions, assessment scales and categorisation of L, M and H criticality SCTs are different. These are given in Attachment 2.

The output of this assessment was a criticality ranked list of SCTs, including the identification and justification of M & H criticality SCTs.

Understanding of M & H SCTs and assessment of human error potential

The core of this step is gathering information from worksite observation of the SCTs being done (or simulated) and from Technicians who are experienced in carrying out the tasks. This step must therefore be done offshore, but also requires some preparatory and follow-up work onshore. The sub-steps are presented in Figure 3.

An important objective is to identify and understand the key steps (those that are critical to MAH management), so that they can be assessed in the subsequent HEA and effort is not wasted carrying out HEA on non-key steps.

Key steps from the SCT description are transferred to the HEA form (Attachment 3). These were scrutinised to identify the potential for human error or failure in those steps. This requires a combination of:

- Discussion with a Technician who carries out the task;
- 'Walking and talking' through the task at the worksite, with the Technician; and
- Observation and/or questioning of the Technician.

Experience with extensive HAZOP style guidewords used to identify human error potential shows that they can be difficult to apply, and so the following list was adapted from [3]. It asks how could the step:

- Not be completed at all? (e.g. non-communication).
- Be partially completed? (e.g. too little or too short).
- Be completed at the wrong time? (e.g. too early or too late).
- Be inappropriately completed? (e.g. too much, too long, on the wrong object, in the wrong direction, too fast/slow).
- Be completed in the wrong order?

Or:

- Could the wrong task or procedure be selected and completed?
- How could a deliberate deviation from a rule or procedure (a 'procedural violation') occur?

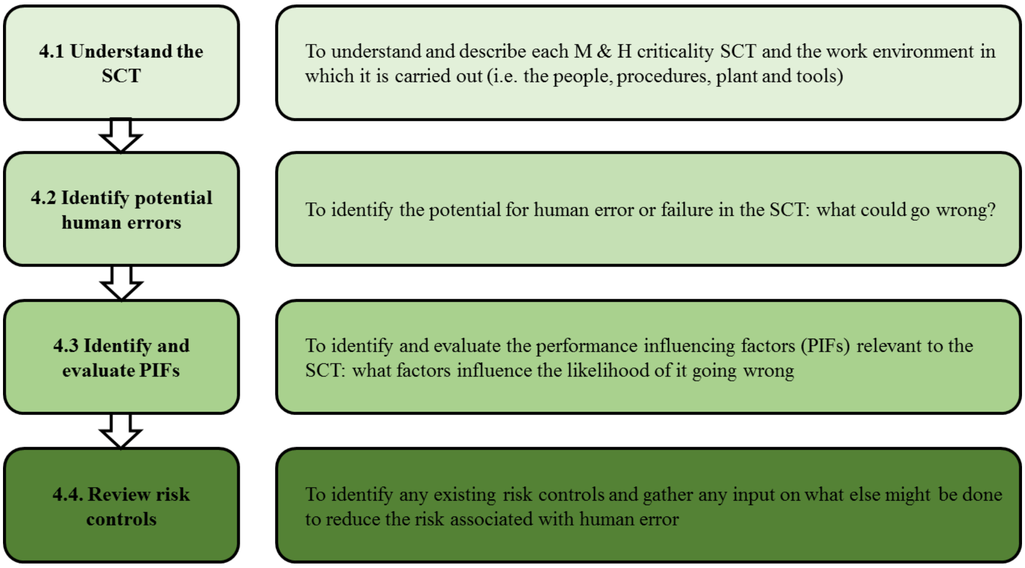

Figure 3– Process for understanding SCTs and assessing human error potential

Performance influencing factors (PIFs) are characteristics of the job, the individual or the organisation, which influence the way people perform. PIFs include, for example: the clarity of signs and signals, the adequacy of procedures, the complexity of a task, the quality of communication, or the level of supervision.

Identifying PIFs, evaluating their quality and how the quality may be improved therefore provides good opportunities for reducing the likelihood of error and reducing risk. Attachment 4 contains a checklist of possible PIFs.

PIFs should be identified at several stages during the task analysis and HEA, including during discussion with a Technician who carries out the task (e.g. PIFs relating to difficulty of worksite access) or when 'walking and talking' through the task at the worksite, with the Technician (e.g. PIFs relating to complexity of communications).

PIF evaluation should also be recorded in the HEA form. A good quality PIF should be associated with an existing risk control. A poor quality PIF (e.g. unlabelled valve) might lead to a possible additional measure being recommended as a risk control.

The final step builds on the understanding of potential human errors and PIFs and aims at identifying risk controls to further reduce the risk associated with human error. The main activities are:

- Identify existing risk controls;
- Assess the consequence of the error (if not recovered); and
- Gather information on potential additional risk controls.

The principle of inherent safety should be applied when seeking to identify and assess potential additional risk controls. Therefore, attention should first be focussed on eliminating the hazard, reducing the human contribution and hardware ('plant') controls, before improvements to procedures (a 'process' control) or human performance (a 'people' control).

This activity should combine observation by a competent SCT analyst with input from an experienced Technician. Risk controls should be specific to the error under consideration, rather than generic topics such as 'competence' or 'procedures'.

Existing risk controls, consequences and potential additional risk controls should be recorded in the HEA form, thereby completing the form to document the HEA for the SCT.

Lessons learned

Over 400 assurance, production and maintenance tasks were identified and assessed for criticality using the SCTA process. Although the application of method is simple, experience has shown that it is generally fit for purpose and effective at highlighting areas where potential human errors are of greatest concern.

When conducting the criticality ranking, one of the assessment criteria was "to what extent are ignition sources introduced into the task when it is performed?" It was noted that due to the design of the electrical equipment to be intrinsically safe, or process isolations in place prior to commencing work, this criterion usually rated a score of 0 or no exposure.

Modifications were made to enable the team to apply the criteria to marine and lifting tasks, e.g. hazard substance or condition was taken to be kinetic or stored energy in the system.

The concept of PIFs was well received by personnel involved in the SCT reviews, it was noted that the identification of PIFs per step facilitated the identification of existing and additional controls.

The linkage between PIFs and controls was well understood by personnel involved in the assessments. These sessions are time consuming, but they get quicker as experience of the users develops.

References

1. Energy Institute, 2011, Guidance on human factors safety critical task analysis.
2. Health & Safety Executive, 1999, Human Factors Assessment of Safety Critical Tasks, Offshore Technology Report OTO 1999 092.
3. Health & Safety Executive, 2005, Inspectors Toolkit: Human factors in the management of major accident hazards, Core topic 3: Identifying human failures.

Attachments

1. SCT Criticality Ranking Tool: Operations and Maintenance
2. SCT Criticality Ranking Tool: Well Operations
3. SCTA HEA Recording Form
4. PIF Checklist

Disclaimer

Attachment 1 SCT Criticality Ranking Tool: Operations and Maintenance

Question	Definition	Assessment Scale and Score			
		None (0)	Low (1)	Medium (2)	High (3)
1. How hazardous is the system involved?	Task involves systems involving intrinsically hazardous substances or conditions	System is non-hazardous	Small amount of low hazard substance or condition. Task carried out after system has been proven hazard-free	Large amount of low hazard, or small amount of high hazard substance or condition. Action taken to remove hazard, but some may remain	High amount of high hazard substance or condition. Task carried out while adjacent/related system remains live
2. To what extent are ignition sources introduced into the task when it is performed?	Task uses or may produce heat, sparks or flames	No ignition sources. No possibility of a flammable atmosphere	Static spark or low current electrical supply	High current electrical supply; sparks from grinding; very hot surfaces	Flames from welding or cutting; internal combustion engines
3. To what extent does the task involve changes to isolations or the operating configuration?	Task involves valve moves, temporary connections, opening flanges, changing isolations or change to process flows	No changes required	Simple changes to valve, equipment or process status; no change to isolations; make/break only those connections designed for routine use	Complex changes to single equipment (valves or isolations); make/break small number of bolted joints; make a single temporary connection	Complex changes to (multi-element) process units (status or isolations); make multiple temporary connections
4. To what extent could incorrect performance of the task cause release of a hazardous substance, escalate an event, or cause damage?	Errors in task could result in release of flammable or toxic substance; escalation of the event; equipment damage; or limit recovery opportunities	No release, escalation or damage. Very simple task, errors would have no consequence	Minor release or escalation of event, with opportunity for recovery; equipment weakened with potential to cause damage in the long term	Release or escalation of the event; equipment requires repair but maintains integrity	Major release or escalation of event with limited opportunity for recovery; equipment fails catastrophically
5. To what extent does the task involve defeating or overriding isolation or protection devices?	Task requires bypass or override of indications, alarms or trips	Safety systems unaffected. No safeguards defeated	Disabling gauges, meters or electronic displays Safety system may not operate as normal	Disabling alarms One of several layers of protection may be made inoperable	Overriding trip systems, isolating safety valves, inserting/removing blinds. Multiple layers of protection may be made inoperable

Attachment 2 SCT Criticality Ranking Tool: Well Operations

Task Characteristic	Assessment Scale and Score		
	Low (1)	Medium (2)	High (3)
1. Interaction with subsurface hydrocarbon reservoirs	Task does not usually involve interaction with open reservoirs	Task may involve direct interaction with open reservoirs, but pressure and other characteristics are reasonably well known	Task may involve direct interaction with newly penetrated reservoirs
2. Interaction with well pressure barriers	Task is not interacting directly with any barriers, or involves a negligible chance to remove the normal barriers	Task is carried out with all normal barriers in place, but could potentially cause the removal of one	Task is carried out with at least one of the normal barriers removed or seriously affected
3. Person to person communication	One line of communication (2 people) with many opportunities for clarification and/or recovery	More lines of communication relating to more important information with some opportunities for clarification and/or recovery	Many lines of communication relating to critical control parameters with few opportunities for clarification and/or recovery
4. Complexity	Highly practiced tasks requiring little or no conscious effort	Tasks performed less frequently, involving more conscious effort and some decision making based on <u>known</u> situations and solutions, <u>or</u> Lengthy routine tasks with many steps involving some conscious effort	Tasks performed infrequently involving intense conscious effort, more decision making and possible problem solving in <u>unfamiliar</u> or highly stressful situations
5. Monitoring and control	System shows slow rate of change. Intermittent monitoring involved that does not require fine control	System shows higher rate of change. More frequent monitoring requiring more attention to control	System shows high rate of change. Continuous monitoring requiring fine control

Sum of Scores	Criticality ranking
13 or greater	High
10-12	Medium
9 or less	Low

Attachment 3 SCTA HEA Recording Form

Safety Critical Task	
PIFs relating to the overall SCT	
Document & drawing references	

Current situation					Additional risk controls to manage human failure potential. Actions & comments	
Key step description	Potential human failure	PIFs	Risk controls & recovery mechanisms	Consequence (if failure not recovered)	Risk controls to prevent or reduce likelihood of failure	Risk controls to reduce consequences or improve recovery potential

Attachment 4 PIF Checklist

Job Factors
J1 Clarity of signs, signals, instructions and other information
J2 System/equipment interface (labelling, alarms)
J3 Difficulty/complexity of task
J4 Routine or unusual task
J5 Divided attention
J6 Procedures inadequate, inappropriate or unavailable
J7 Preparation for task (e.g. PTW, risk assessments, checking)
J8 Time available/required
J9 Tools appropriate for task
J10 Communication, with colleagues, supervision, contractors, other
J11 Working environment (e.g. noise, heat, space/access, lighting, ventilation)
Person Factors
P1 Physical capability and condition
P2 Fatigue (acute from temporary situation, or chronic)
P3 Stress/morale
P4 Work overload/underload
P5 Competence to deal with circumstances
P6 Motivation vs other priorities
Organisation Factors
O1 Work pressures (e.g. production vs safety)
O2 Level and nature of supervision/leadership
O3 Communication
O4 Staffing levels
O5 Peer pressure
O6 Clarity of roles and responsibilities
O7 Consequences of failure to follow rules/procedures
O8 Effectiveness of organisational learning (learning from experiences)
O9 Organisational or safety culture (e.g. everyone breaks the rules)
O10 Change management