Safety Critical Task Analysis Procedure

For N/A

May 2024

AB Risk Limited

www.abrisk.co.uk

Contents

.....1
1 Introduction 3
1.1 Task Inventory.....3
1.2 Prioritising tasks for analysis 3
1.3 Hierarchical Task Analysis (HTA).....3
1.4 Human Error Analysis (HEA).....4
1.5 Performance Influencing Factors (PIF) 4
1.6 Task risk evaluation 5
1.7 Analysis validation 5
2 SCTA Implementation 7
2.1 SCTA Planning.....7
2.2 Key Roles.....7
3 Implementation 8
3.1 Management of Actions 8
3.2 Operating and maintenance procedures 8
3.3 Task method deviations.....8
3.4 Incident Reporting & Investigation.....8
3.5 Management of Change 9
3.6 Management of other human factors 9
4 References 10
4.1 Guidance from the Health and Safety Executive 10
4.2 Other Guidance.....10
Appendix 1. Task Scoring Guide.....11
Appendix 2. Human Error Types 12
Appendix 3. Performance Influencing Factors (PIF) 13
Appendix 4. Abbreviations.....14

1 INTRODUCTION

The overall SCTA process involves the following activities:

1. Task inventory generation;
2. Task prioritisation;
3. Hierarchical Task Analysis (HTA);
4. Human Error Analysis (HEA);
5. Performance Influencing Factors;
6. Task risk evaluation;
7. Analysis validation;
8. Documentation.

1.1 Task Inventory.

A task inventory is simply a list of tasks performed within a defined domain. For SCTA the main interest is the tasks performed in areas that handle MAH that could cause or contribute to a major accident.

The task inventory is generated from design information (e.g. equipment list, Process Flow Diagrams) and operational experience. It is intended to be fully comprehensive for the defined domains (i.e. operations, maintenance and emergency tasks performed in areas handling oil products) for foreseeable situations. There will always be additional tasks that may be performed very infrequently or as a one-off, which will not appear on the task inventory. These are managed as individual projects that may involve some aspects of SCTA (e.g. HTA and HEA – see below).

SCTA is applied to clearly defined tasks. It does not account for all human activities performed at the facility, which will be handled by other analysis techniques. These include general maintenance, alarm management, safety critical communications, fatigue management, control room design etc.

The task inventory is maintained as an up to date, comprehensive list of operations, maintenance and emergency tasks performed at the facility.

1.2 Prioritising tasks for analysis

SCTA is a resource intensive activity but can be very beneficial if focussed on the most critical tasks. A simple scoring method is used to provide a degree of objectivity in prioritising which tasks to analyse.

The method described in Health and Safety Executive (HSE) report OTO 1999 092 - Human Factors Assessment of Safety Critical Tasks is used to systematically link tasks to the Major Accident Events. An amended versions of the scoring guidance is used (see Appendix 1). It results in scores between 0 and 15 for each task. All those scoring 8 and above are considered for detailed analysis.

1.3 Hierarchical Task Analysis (HTA)

HTA is used to describe tasks in a systematic and structured way. It involves the following stages:

1. Agree the task objective – ensure it is unambiguous and clearly defines the boundary of the task scope with a clear goal;
2. Agree the required ‘pre-conditions’ for undertaking the task – these are the assumptions regarding the starting point for the task and defines the scenario being assessed;
3. Identify the main ‘sub-tasks’ – the high-level stages of the task that gives structure to the analysis. There should normally be no more than 10 sub-tasks;

4. Identify the detailed steps within the sub-tasks to an appropriate level for human error analysis through the use of layers of ‘child boxes’;
5. Review the sub-tasks and detailed steps to ensure the sequencing captured is reflective of how the task is performed in practice.

The aim at this stage is to achieve consensus about how the task is or will be performed.

HTA is the preferred method of representing the task because it encourages a good understanding of how the task is performed, allowing anomalies and ambiguities to be identified. Simply taking the content of an existing procedure is rarely sufficient, unless it is very well written and there is strong evidence to show that it is a good representation of how the task is carried out in practice.

1.4 Human Error Analysis (HEA)

HEA involves assessing each step of a task (taken from its HTA) to determine what human errors and other failures can occur, their potential consequences and methods of controlling risks. All types of human failure (e.g. slips, lapses, mistakes and violations) are considered in the assessment. High level prompts assist with identifying what would occur if a step is:

- Omitted (not carried out);
- Incomplete;
- Performed on the wrong object;
- Mistimed (too early or late);
- Carried out at the wrong speed (too fast or slow);
- Carried out for the wrong duration (too long or too short);
- Performed in the wrong direction.

Appendix 2 shows a list of human error types that depend on the type of task step. These are considered for each step. In many cases the same consequence is likely for several different error types. In these cases the most representative error is recorded in the HEA. In some cases different errors can have different consequences. In these cases multiple lines are created and the records made for each error type.

1.5 Performance Influencing Factors (PIF)

PIFs are the characteristics of the job, individual and the organisation that affect the way people perform. The quality of those characteristics will affect the likelihood of human error. PIFs are relevant to particular tasks and more globally, it is the task element that is considered in SCTA.

During SCTA PIF identification is carried out at two levels:

1. The whole task
2. Specific steps in the task with the main emphasis where MAH consequences have been identified in the analysis.

Other PIFs may be recorded if considered appropriate.

A PIF checklist shown in Appendix 3.

In cases where a similar task may be carried out in different locations, a single HTA and HEA may cover all instances of the task but the PIFs may be different depending on location or other circumstance. In these cases an initial PIF analysis is carried out for the representative case (i.e. the one described in the HTA/HEA), followed up by an evaluation at all task locations to identify any differences, which are then recorded separately.

1.6 Task risk evaluation

The completed HTA, HEA and PIF identification will be recorded to capture the output from the analysis. Part of this includes reviewing the risk controls already considered in the design. A judgement is then made to determine the actions required during the project to achieve risks that are As Low As Reasonably Practicable (ALARP).

The hierarchy of risk controls will be in particular:

- Can hazards be eliminated?
- Can hazards be reduced through basic design?
- Can additional passive engineered controls be introduced?
- Can additional active engineered controls be introduced?
- Can additional administrative controls be introduced?

Although PIFs affect the likelihood of human error and hence task failure, they are not risk controls and so are considered in parallel with the ALARP demonstration rather than as an integral part. The aim of the PIF evaluation is to ensure PIFs are optimised.

1.7 Analysis validation

The aim during the analysis phase is to represent how tasks are performed in practice. This is achieved by involving people with relevant task experience. However, it is recognised that some assumptions may have been made and people with task experience may not be aware of how prevailing conditions could affect human performance. Validation is concerned with ensuring the findings of the SCTA accurately reflect reality. In particular that the method captured in the HTA is practical and the risk of human error is appropriate taking into account the PIFs that apply. A site visit is an important part of the validation.

It should be noted that not all critical aspects of a task can be observed directly. Where possible, observing the task being performed provides the best way of validating how the task is performed in practice. Where this is not possible a walkthrough of the task is sufficient. In some cases walkthrough is preferable because it allows time to pause for deeper discussion and examination which may not be possible when a task is actually being performed.

Particular focus during the task observation or walkthrough include:

- Labelling – if valves, instruments and other equipment are not easy to identify it can lead to errors of commission (right action on wrong object);
- Interfaces – if the data required to perform the task is badly presented or not readily available it can result in poor decision making and mean that hazardous situations are not detected or diagnosed correctly;
- Tools and equipment – if the correct or suitable items are not readily available it may require improvisation that can increase the likelihood of error;
- Working environment – poor working conditions can significantly increase the likelihood of human error. For this PIF it is important to consider how conditions may vary according to the time of day, weather etc.
- Access - if something (e.g. a valve) cannot be reached it probably means an alternative is being used to achieve a similar result;
- Logical sequences - the order of steps described in the workshop may not make so much sense in practice. This can often be due to geographic location of actions which may be difficult to fully consider during the workshop;
- Potential for confusion - things that are obvious on paper are not always so clear in practice;
- Hazards - the presence of hazards in the area may affect the way the task is performed in practice.

The results of the task observation or walkthrough are used to identify any aspects of the HTA, HEA or PIF evaluation that need to be reviewed and updated; and may require further analysis to confirm risks are being managed effectively.

Evaluating the PIFs involves interactive observation. Conducting the discussion at the worksite prompts people to mention things that may have overlooked previously. Asking the person to talk through the task whilst explaining what they would do and why they would do it in a particular way can give a deeper insight into how PIFs are affecting task performance and how they may be improved.

People will often have to refer to sources of information when performing a task including procedures and instructions, checklists, computer displays, drawings, manuals, permit to work, training documents and maintenance/asset management systems. These are reviewed as part of the analysis validation both as possible PIFs and also to determine if they need to be updated as a result of the analysis.

Photographs, print-outs or photocopies are taken to support findings from the task observation / walkthrough, PIF evaluation and review of sources of information. These are used to identify any differences where similar tasks are performed in different locations.

2 SCTA IMPLEMENTATION

2.1 SCTA Planning

Overall responsibility for site safety lies with the Site Manager, which includes ensuring this procedure is implemented to ensure safety critical tasks are properly identified, analysed and findings implemented.

SCTA output should be reviewed and updated every 5 years or if changes occur at the facility. The documents are stored on the company network.

2.2 Key Roles

Site Manager - ensuring adequate competent resources are employed to operate and maintain the plant and systems on site.

Process Safety Manager - appointments competent people to support SCTA implementation.

Shift Supervisors - ensuring the required personnel participate in SCTA and implementing the findings.

Operators/Technicians - share their experience to ensure the SCTA is an accurate representation of how tasks are performed in practice. Ensure that safety critical tasks are performed using the methods identified in the SCTA and identifying any discrepancies so that they can be rectified.

Engineers - supporting the SCTA process by providing MAH safety and technical information. Ensure that changes occurring at the facility take into account the existing SCTA output and identify requirements for updates and additions.

SCTA facilitators - support implementation of SCTA. They have proven competence in applying SCTA in MAH industries. They have Chartered membership of the Chartered Institute of Ergonomics and Human Factors (CIEHF) or equivalent.

3 IMPLEMENTATION

The objective of SCTA is ensure that safety critical operations and maintenance tasks are performed in a way that achieves ALARP.

3.1 Management of Actions

Actions are identified throughout the SCTA to improve or address deficiencies in the system. Actions may be identified during initial analyses of safety critical tasks or as part of incident investigations, reviews, audits and assessments.

Each finding that requires improvement is be added to the company action tracker. The tracker will associate a responsible person and a deadline to complete each action. The tracker will also identify the source of the action - which activity prompted the action - in order to fully appreciate the context.

3.2 Operating and maintenance procedures

Procedures for safety critical tasks are reviewed and updated following completion of HTA/HEA for the associated task. The requirement is to ensure the documented method for the task is the same in the procedure and SCTA report

Procedures have multiple potential uses. For safety critical tasks these include:

- Training and competence assurance aid;
- Support for competent people when carrying out the task.

The Shift Supervisors ensure that the most up to date versions of procedures are readily available. Personnel carrying out tasks are responsible for using the procedures as intended, which for safety critical tasks usually means that are printed, followed and signed every time the task is performed.

3.3 Task method deviations

The aim in SCTA is to analyse and document how tasks are performed in practice. In some cases the circumstances at the time a task is performed means that this is not possible. In these cases the following options are considered in order:

Where time allows the task will be rescheduled to allow the analysis to be reviewed and an amended procedure issued through the normal channels;

Where only a short delay is possible the requirements to amend the task method shall be discussed with appropriate personnel and amendments to the procedure will be agreed informally (by email, handwritten notes, verbally);

Where there is no possibility to delay the task will be performed and notes taken about the method actually used, which will be reviewed soon afterwards to capture learning etc.

The general message remains that the approved task method will always possible when safe to do so, whilst recognising that this is not always possible.

3.4 Incident Reporting & Investigation

The facility Incident Reporting & Investigation procedure provides requirements to investigate and determine the cause of any high potential incident. Part of this process is to identify opportunity to improve the SCTA process and its application. In particular:

- Were the tasks involved in the incident included in the task inventory?
- Was the task prioritisation score appropriate?
- Did the HTA describe a task method that was appropriate for the circumstances at the time of the incident?

- Did the HEA predict the type of failures that occurred and/or were risk controls ineffective?
- Did the PIF analysis consider the conditions that were present at the time of the incident?

3.5 Management of Change

The MoC procedure provides a formal means by which modifications are identified, impact assessed and managed.

Any changes to safety critical tasks will result in a review and update of the SCTA. Any changes to plant or process will use SCTA to identify any new safety critical tasks that need to be added to the inventory and analysed.

3.6 Management of other human factors

SCTA is only applied where it is most appropriate. Other human factors issues can be critical but will be handled by a separate, appropriate review and analysis using the most appropriate technique available. These wider human factors topics include:

- Alarm management;
- Human Machine Interface (HMI) design;
- Fatigue;
- Shift handover;
- Permit to work;
- Human factors in incident investigation;
- Competence management;
- Management of change;
- Human factors engineering in projects.

4 REFERENCES

4.1 Guidance from the Health and Safety Executive

- COMAH Competent Authority Inspecting Human Factors at COMAH Establishments (Operational Delivery Guide) https://www.hse.gov.uk/comah/assets/docs/hf-delivery-guide.pdf
- Performance Influencing Factors (PIFs) https://www.hse.gov.uk/humanfactors/assets/docs/pifs.pdf
- The Human Factors Inspector's Toolkit http://www.hse.gov.uk/humanfactors/toolkit.htm
- Reducing Error and Influencing Behaviour, HSG48, Second Edition, 1999 https://www.hse.gov.uk/pubns/priced/hsg48.pdf
- The Human Factors Inspector's Toolkit http://www.hse.gov.uk/humanfactors/toolkit.htm
- Human Factors Assessment of. Safety Critical Tasks. OTO 1999/092 https://abrisk.co.uk/wp-content/uploads/2023/09/OTO-1999-092.pdf (withdrawn from HSE website)

4.2 Other Guidance

- Chartered Institute of Ergonomics and Human Factors (CIEHF) How to carry out human factors assessments of critical tasks: Guidance for COMAH establishments https://ergonomics.org.uk/resource/comah-guidance.html
- Energy Institute: Guidance on Human Factors Safety Critical Task Analysis (Second Edition) https://publishing.energyinst.org/topics/human-and-organisational-factors/risk-management/guidance-on-human-factors-safety-critical-task-analysis2
- Energy Institute. Human factors briefing note no. 11 – Task analysis https://publishing.energyinst.org/topics/process-safety/leadership/human-factors-briefing-note-no.-11-task-analysis

Appendix 1. Task Scoring Guide

Operations	None	Low	Medium	High
	(Score 0)	(Score 1)	(Score 2)	(Score 3)
How hazardous is the system involved?	Non-hazardous system (operations)	Small amount of low hazard / condition	Large amount of low hazard or small amount of high hazard	High amount of high hazard / condition
	Non-hazardous system (maintenance)	Task carried out after hazardous system has been proven hazard free	Actions taken to remove hazard, but some may remain	Work carried out whilst adjacent/related systems remain live
To what extent does the task involve the introduction of energy or an ignition source?	No ignition / energy sources	Low pressure or temperature rise	Medium pressure or temperature rise. Combustion engine.	High pressure or temperature rise
	No possibility of a flammable atmosphere	Electrical switching. Electrical equipment used.	Potential for sparks or hot surfaces	Flames
To what extent does the task involve changes to the operating configuration?	No change required	Simple valve changes (few valve moves)	Complex or multiple valve changes. Use of temporary connections	Complex and multiple valve changes. Use of temporary bypass line.
		Connect/dis-connect points designed for routine use (e.g. quick coupling, plug and socket)	Make/break small number of bolted joints	Complex assembly/disassembly. Multiple components.
What is the potential for error in performing the task?	Fully automated task	The potential for error cannot be rule out although there is no specific concern	There is a recognised possibility for error	There is a significant possibility of error Task requires constant vigilance.
	Very simple and errors would have no consequence	A ‘normal’ task	Complex task	Errors are likely to be unrecoverable No automated protection.
To what extent could the task affect performance of a safety system?	No systems overridden or defeated	Task involves a deviation from an original procedure or design.	Warning devices may be made inoperable (e.g. alarms, gauges, meters)	Trip systems overridden. Safety valves isolated.
	No safety system affected by task	May affect system calibration. Safety system may not operate as normal.	One of several layers of protection may be made inoperable	Multiple layers of protection may be made inoperable. Potential for common cause failure

Appendix 2. Human Error Types

Actions errors	**Checking errors**	**Information retrieval errors**
Omitted	Omitted	Omitted (Info not obtained)
Incomplete	Incomplete	Incomplete
Right action on wrong object	Right check on wrong object	Wrong information obtained
Wrong action on right object	Wrong check on right object	Incorrectly interpreted
Too fast/too slow	Too early/too late	**Information communication errors**
Misaligned	**Selection errors**	Omitted
Mistimed, too early/too late	Omitted	Incomplete
Too long/too short	Wrong selection made	Wrong information communicated
In wrong direction	**Planning errors**	Information unclear/ambiguous
Too little/too much	Omitted	
	Incorrect	

Appendix 3. Performance Influencing Factors (PIF)

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
J5 - Procedures inadequate or inappropriate
J6 - Preparation for task (e.g. permits, risk assessments, checking)
J7 - Time available/required - Divided attention
J8 - Tools appropriate for task
J9 - Communication, with colleagues, supervision, contractor, other
J10 - Working environment (noise, heat, space, lighting, ventilation)
J11 – Access to worksite or equipment (including use of tools)
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 - Manning levels
O5 - Clarity of roles and responsibilities
O6 - Peer pressure
O7 - Consequences of failure to follow rules/procedures
O8 - Organisational learning (learning from experiences)
O9 - Organisational or safety culture, e.g. everyone breaks the rules

Appendix 4. Abbreviations

ALARP	As Low As Reasonably Practicable
CIEHF	Chartered Institute of Ergonomics and Human Factors
HEA	Human Error Analysis
EI	Energy Institute
HSE	Health and Safety Executive
HTA	Hierarchical Task Analysis
MoC	Management of Change
PIF	Performance Influencing Factors
SCTA	Safety Critical Task Analysis