Guidance Note

Hazard identification at a major hazard facility

Advice for operators of major hazard facilities on identifying major incident hazards.

April 2011

1. Introduction

The major hazard facility parts of the Occupational Health and Safety Regulations 2007 (OHS Regulations) set out legal duties for control of risks from operating a major hazard facility (MHF). They apply to the operator of a facility who is the employer with management or control of the facility.

To obtain a licence to operate an MHF in Victoria, operators are required to submit a Safety Case which sets out how the facility will be operated safely.

This guidance note is intended to assist the operator through the process of conducting hazard identification which forms part of the Safety Case. The process identifies potential major incidents and associated hazards and causes which could lead to the major incidents. It helps determine the level of detail required in the Safety Case.

Two of the key components of a Safety Case for an MHF are the identification of all major incidents which could occur at the MHF and the identification of all major incident hazards, as required by the MHF regulations. The MHF regulations also require that the operator document all aspects of identification, including the methods and criteria used for identification and any external conditions under which the hazards might give rise to a major incident.

The outcomes of the hazard identification process are to:

- identify all major incidents which could occur at the facility (irrespective of existing control measures)
- provide the employer and workers with sufficient knowledge, awareness and understanding of the causes of major incidents to be able to prevent and deal with them

- provide a basis for identifying, evaluating, defining and justifying the selection (or rejection) of control measures for eliminating or reducing risk
- show clear links between hazards, causes and potential major incidents
- provide a systematic record of all identified hazards and major incidents, together with any assumptions.

1.1. Features of hazard identification

The following factors lead to successful hazard identification:

- the hazard identification process should be workable and relevant to the facility
- a fresh view should be taken of any existing knowledge and it should not be automatically assumed that no new knowledge is required
- the information is provided to persons who require it to work safely
- an appropriate group of workers is actively involved and consultation occurs
- uncertainties are explicitly identified and recorded for later analysis
- all methods, results, assumptions and data are documented
- it is regularly maintained and used as a live document.

Knowledge of hazards and their implications is necessary for the next steps of the Safety Case process, including Safety Assessment, but is only worthwhile if it informs and improves decision-making and seeks to identify all potential hazards and major incidents. Figure 1.1 shows the important steps in effective hazard identification.

Figure 1.1 – Key steps in hazard identification

Hazard identification

Identify all hazards that could cause or contribute to causing a major incident, and associated controls

Define major incident

What are the major incidents?

Incidents which:

- are uncontrolled eg emission, loss
- involve release of schedule 9 material
- pose a serious and immediate threat to health and safety.

Identify hazards

What hazards are associated with each major incident?

Hazards might be of the following types:

- maintenance (lack of)
- dropped object
- procedural error
- process upset
- etc.

Preliminary control identification*

What are the controls for each hazard?

Identify controls for each hazard. Controls might:

- prevent the hazard from occurring
- eliminate the hazard altogether
- reduce the risk from the hazard
- mitigate against the effects from the hazard
- be either existing or proposed (potential).

Control measures

Establish the validity of the data gathered in the hazard identification

Verification

Confirmation of the information gathered in defining major incidents, identifying hazards and controls.

Questions to ask:

- is the definition of major incident too broad or too narrow?
- are the hazards realistic?
- do the controls for each hazard really exist?
- do the controls really work?

* Preliminary control identification to be further considered during Safety Assessment

1.2. Key definitions

Control measure (control): Any system, procedure, process, device or other means of eliminating, preventing, reducing or mitigating the risk of major incidents arising at an MHF. Controls include physical equipment, process control systems, management processes, operating or maintenance procedures, the emergency plan and key personnel and their actions.

Hazard (related to an MHF): Any activity, procedure, plant, process, substance, situation or any other circumstance that could cause, or contribute to causing, a major incident.

Hazard identification: The process of identifying hazards as described in this guidance note.

Major incident (related to an MHF): An uncontrolled incident, including an emission, loss of containment, escape, fire, explosion or release of energy, that:

(a) involves Schedule 9 materials, and

(b) poses a serious and immediate risk to health and safety.

Safety Assessment: The Safety Assessment process is consistent with international risk assessment standards, including the risk assessment process described within AS/NZS ISO 31000 *Risk management*. A Safety Assessment involves an investigation and analysis of the major incident hazards and major incidents to provide the operator with a detailed understanding of all aspects of risk to health and safety associated with major incidents, including:

(a) the nature of each hazard and major incident

(b) the likelihood of each hazard causing a major incident

(c) in the event of a major incident occurring –

 (i) its magnitude, and

 (ii) the severity of its consequences to persons both on-site and off-site

(d) the range of control measures considered.

So far as is reasonably practicable: To reduce risk to a level so far as is reasonably practicable involves balancing reduction in risk against the time, trouble, difficulty and cost of achieving it. This requires consideration of:

(a) the likelihood of the hazard or risk concerned eventuating

(b) the degree of harm that would result if the hazard or risk eventuated

(c) what the person concerned knows, or ought reasonably to know, about the hazard or risk and any ways of eliminating or reducing the hazard or risk

(d) the availability and suitability of ways to eliminate or reduce the hazard or risk and

(e) the cost of eliminating or reducing the hazard or risk.

The WorkSafe guidance note – *Requirements for demonstration* provides further information on so far as is reasonably practicable as applied to major incident risk. More information on key terms is found in other MHF guidance material available from the WorkSafe website and in the definitions of the OHS Regulations (reg 1.1.5).

2. Planning and preparation

2.1. Coordinating the Safety Case approach

The MHF regulations require the operator to produce and submit a Safety Case outline (see the guidance note – *Safety Case outline for an MHF*) prior to developing the Safety Case. WorkSafe recommends that this process is used to look at the overall requirements of the Safety Case and to identify areas in which the operator can save time and resources in developing the Safety Case. How each step is planned will need to be structured to suit the facility.

The steps for developing a Safety Case process are linked. For this reason the process is not strictly linear and some steps can be combined to deliver cost and resource savings. Figure 2.1 gives one example of how particular components of the Safety Case can be structured in a logical work plan. For example, it may make sense for a workshop team to 1) identify the list of potential major incidents; 2) identify hazards and outcomes; 3) identify existing control measures; and 4) as a first pass, identify any additional control measures while the whole team is together. Step 1 in Figure 2.1 illustrates the combination used in this example.

Figure 2.1 – Suggested steps for minimising overlaps

	Step 1	Step 2	Step 3	Step 4
Hazard identification	• Identify major incidents • Identify hazards and causes			
Safety Assessment		• Assess likely frequency and consequences of each hazard without controls in place • Conduct the initial Safety Assessment to assess the level of risk posed by each major incident, taking existing controls into account.	• Ensure all practicable steps to reduce risk associated with each major incident have been considered.	• Conduct the final Safety Assessment. Assess the level of risk posed by each hazard assuming improvement actions are in place
Control measures	• Identify existing control measures	• Ensure all practicable steps to reduce risk for each major incident have been considered • Identify potential additional controls.	• Adequacy assessment of controls for each major incident.	• Identify/select potential additional controls • Prepare performance standards and ensure procedures/ audits in place.

2.2. Scope

Reg 5.2.6(1) requires the identification of all major incidents and all hazards that could lead to these major incidents. In determining the scope of the hazard identification, the operator needs to set the boundaries of the work. If there is no possibility of a major incident or events that could escalate to a major incident in some operations at the facility, these may be excluded from the hazard identification. Care must be exercised before excluding any area or operation, and reasons recorded for the purposes of demonstrating in the Safety Case that such decisions were appropriate.

Example of identifying major incidents

ABC Chemical Company has a process plant which relies on ammonia for its refrigeration units. ABC determined that ammonia is the only Schedule 9 material at its site and therefore the hazard identification will only consider operations that impact on ammonia storage and handling which are the ammonia refrigeration units and associated facilities. Even though other processes occur on site, these will not be considered. The list of major incidents identified is:

- loss of containment at tanker unloading terminal
- ammonia release at storage
- ammonia release at refrigeration facility.

Issues such as release of utilities (eg water/air) or slips, trips and falls are not included as major incidents as they are not the focus of the MHF regulations.

In selecting a hazard identification process, the operator should consider:

- the size and complexity of the facility
- pilot studies/Safety Cases from similar facilities
- the properties of the Schedule 9 materials and other dangerous goods on-site
- the nature of the processes on-site
- the range of incident types which will be considered.

The operator may consider whether a pilot study, with a single area of focus on the facility, would benefit the overall Safety Case. This may be desirable if there is any doubt about the hazard identification technique to be used. A pilot study will test the methodology for identifying hazards and demonstrating linkages between major incidents, hazards and controls. It may also assist with better estimating and planning the resources needed to complete the Safety Case.

2.3. Defining a major incident

The definition of a major incident within the MHF regulations is broad. To provide consistency during the hazard identification and the remainder of the Safety Case development, the operator should provide a clear, site-specific definition. This could involve:

- using quantitative terms to define the risk to health and safety, such as defining:
  - what a serious and immediate risk to health and safety means at the site eg the risk of a fatality or the risk of a serious injury
  - the extent of injury
- deciding whether the major incident is a 'loss of containment' or the consequence (eg fire) of the loss of containment. A 'loss of containment' event can have several outcomes (eg jet fire, toxic release). Both methods have been used by facilities. The operator should consider aspects such as the structure and maintenance of the records of the study and how clear linkages between major incidents, hazards and control measures will be demonstrated.

Examples of major incident definition

One MHF, a warehouse operator, chose to use the following definition: 'A major incident involving Schedule 9 materials that has potential to cause physical injuries or health effects resulting in hospitalisation'.

This decision was taken because they expected there would be only a small number of major incidents and they could manage the Safety Assessment on this basis without diluting the focus on major incidents.

Another facility, a chemical producer, limited its definition of major incident to one with the potential to cause a fatality. The operator expected to find a large number of potential hazards that could result in a fatality and considered that including incidents that could cause injuries alone would detract from the focus on incidents with the potential to cause a fatality.

For the previous ammonia example, ABC Chemical Company chose the following definition:

'A catastrophic failure of the refrigeration unit that results in the release of the contents (one tonne of ammonia) over a 30 minute period.'

The basis for this decision was:

- a release of this scale could have significant health effects (eg hospitalise persons for three days or more) and create off-site impacts
- there is a limited number of hazards on the site compared with a large chemical site. It was considered that including hospitalisation as an outcome would not adversely affect the focus on the most serious incidents
- it was easier to structure the hazard register around a 'loss of containment' release rather than consequence outcome.

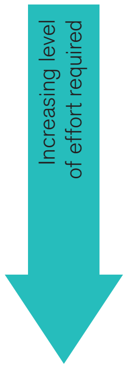
2.4. Selecting the hazard identification technique

The hazard identification process sets the foundation for the remainder of the Safety Case process. All hazards are identified during this phase so they can be assessed and safely managed. Therefore the technique selected should:

- be systematic and structured
- faster creative thinking about possible hazards that have not previously been experienced
- be appropriate for the facility
- consider which approach will extract the maximum quantity of useful information. It should be appropriate for the people involved.

There are many techniques that may apply. Some of the more common hazard identification techniques are listed in order of effort required (Figure 2.2).

Figure 2.2 – Hazard identification technique



- Incident data
- Checklist analysis
- Brainstorming
- What if?
- Guideword analysis
- Hazard and Operability Study (HAZOP)
- Failure Modes and Effects Analysis (FMEA)
- Task analysis
- Event tree
- Fault tree

A summary of the techniques, along with guidance on their use and applicability, is presented in the Appendix. Table 2.1 summarises some of the issues that should be considered in selecting a hazard identification technique.

Table 2.1 – Hazard identification technique selection issues

Issue	Check
Depending on where a facility is in its life cycle phase eg • Concept phase • Design phase • Construction/start-up • Routine operation • Decommissioning	• Prior to detailed design, it is unlikely there will be sufficient information (drawings, functional description etc) to effectively utilise detailed techniques such as HAZOP or FMEA. • During detailed design, more detailed techniques may be required to provide a greater understanding of operational concerns. • Task analysis may be of benefit for construction, start-up and decommissioning where the focus is more on procedures. • For the ongoing routine phase the technique will be influenced by factors such as the level of knowledge of hazards, the history of risk assessments and the extent of change that has occurred.
Complexity and size	The complexity and size of a facility includes the number of activities or systems, the number of pieces of equipment, the type of process and the range of potential outcomes. Some techniques get bogged down when they analyse complex problems eg event tree and fault tree analyses can become time-consuming and difficult to structure effectively. However, simple techniques may not provide sufficient focus to reach consensus, or confidence in the identification of hazards.
Type of process or activity • Engineering or procedural • Mechanical, process, or activity focussed.	• Task analysis may be appropriate (eg task analysis, procedural HAZOP) where activities are procedural or human error is dominant. • FMEA may be appropriate where knowledge of the failure modes of equipment is critical (eg control equipment). • HAZOP may be used where the facility is readily shown on a process flow diagram. • Fault tree and event tree may be beneficial where multiple failures need to combine to cause an incident or multiple outcomes are possible.

A simple, structured brainstorming technique (eg Guideword-based analysis) will satisfactorily identify the majority of hazards for many facilities. However, it may be necessary to apply a combination of different hazard identification techniques to ensure that the full range of hazards is properly considered.

For example, incident data is useful to check that known hazards have not been missed. The operator should take into account the operating history of the facility, or similar facilities within the organisation or industry. However, for the overall hazard identification process the operator should not rely solely on historical data. A recorded incident is just one example out of a vast range of potential incidents (most of which will never occur). The operator must identify and control all potential incidents that may occur, not just prevent repetitions.

The operator will also need to decide when it is appropriate to use a more detailed technique. Situations where a more detailed technique may be needed are where:

- there is uncertainty as to the underlying causes of a particular incident
- the complexity of a particular hazard is high
- a more detailed breakdown of the major incident is required to adequately assess the likelihood during the Safety Assessment phase (see guidance note – *Safety Assessment*)
- the facility is new and the operator has no operating experience. A more detailed technique may provide greater insight into the operability of the facility.

Regardless of which method/s is chosen, the level of effort should be proportional to the seriousness of the potential incidents the operator expects to find. In cases where it is not clear what method may be successful, a 'pilot' study on a selected area of the facility may be beneficial.

Example of chosen hazard identification technique

For the ABC Chemical Company ammonia example, the process is relatively simple. A HAZOP had been completed as part of the original design. The personnel on-site also have some knowledge about the hazards of ammonia.

The company decided that a simple approach, such as a 'Guideword' or 'What if?' technique would be sufficient due to the existing knowledge of the facility. While both techniques were considered adequate, it elected to use a guideword-based approach as the workers were already familiar with this technique.

Furthermore, ammonia facilities are common and the following information was available:

- a checklist of safety features for ammonia storage and refrigeration facilities
- sufficient and useful worldwide incident history.

The checklist and the incident history were used after the guideword-based hazard identification workshop to verify whether any hazards were missed.

The facility was also planning driver-only unloading of ammonia. Some personnel questioned how safe this would be and whether additional controls were necessary. Given the level of uncertainty and the potential for human error during the unloading procedure, the company also decided to complete a task analysis on the unloading procedure.

2.5. Selecting the hazard identification team

Because ownership of the Safety Case process is the responsibility of the whole organisation from management to shop floor, and because of the amount of work required to demonstrate a case for safety, developing a Safety Case requires a large commitment in terms of site personnel at all stages, including hazard identification. When carrying out hazard identification it is recommended that the following aspects are considered:

- provide the right mix of expertise and involve all relevant work groups – hazards not evident to individual work groups may be identified in the interaction between the various work groups
- involve contractors and suppliers as necessary eg truck drivers provide a different perspective on loading operations
- include an operations person who has a thorough knowledge of the facility and its history

- include someone with sufficient technical expertise in areas relevant to the facility, such as those with chemical knowledge or of maintenance procedures, and designers to capture design intent.

The operator may also need to employ a third party to provide guidance on the way forward (ie a workshop facilitator) or bring in technical expertise in a specific area.

Example of a hazard identification team

The workshop team for ABC Chemical Company hazard identification is:

- facilitator
- electrical maintenance worker
- mechanical maintenance worker
- two shift workers
- area supervisor
- ammonia truck driver/s.

Even though the ammonia truck drivers are not ABC Chemical Company workers, the drivers were invited for the hazard identification when dealing with ammonia unloading. As they are the ones carrying out this work, they have an insight into hazards and controls which the workers will not have.

It is not usually possible to involve all workers in the hazard identification workshops; however, it is important to provide feedback to those not directly involved. This feedback should be in the form of training on the hazards that are present and the controls that are in place. It should also provide an opportunity for the workers to review and comment on the hazard identification output. This is an important quality control activity.

Sufficient time needs to be allocated to the hazard identification phase of the Safety Case project plan. The plan should allow time for the workshop and to verify information to be used in the workshop and post-workshop verification activities. Some contingency should be allowed in the schedule for additional hazard identification activity that may arise from the Safety Assessment.

Table 2.2 shows the estimated site commitment for a medium-sized site with 20 major incident scenarios identified. The time specified is based on most information being gathered using a workshop format.

Table 2.2 – Site commitment for hazard identification

Process	Personnel	Time commitment	Notes
Planning and preparation	Safety Case coordinator HSR	Two weeks Two days	Some planning would be carried out at the same time as planning for other steps in the Safety Case. Excluded from this time commitment is the time required to check that drawings and information to be used in the workshop are correct.
Hazard identification workshops	Workshop participants (six-eight people) Facilitator and scribe	Daily workshops over two-week period (10 workshops)	This is based on full day workshops. An alternative is to have part day workshops over a longer period of time. More time may be required depending on the complexity of the hazard scenarios. Extra time may be required if the need for more detailed studies is identified during the hazard identification.
Review of the hazards and their dynamics	Safety Case coordinator HSR Management Facilitator and scribe Other workers	Two days Two days Two days One day Two days	This is about checking that the hazard scenarios are correct and control measures do exist. Management will also need to devote some time.

2.6. Workforce requirements and health and safety representatives

The operator should develop a role for all workers in the Safety Case development process that allows them to contribute and gain knowledge in relation to hazard identification and recognising where a hazard could contribute to causing a major incident. The operator needs to be particularly vigilant in ensuring that information is considered on the basis of technical/working knowledge and not on the seniority of the contributor. Decision-making should be transparent and based on the same basis.

Health and safety representatives (HSR) should be involved in the process to the extent that they can ensure appropriate workforce involvement. Therefore, it is recommended that the HSR is involved in:

- development of the process
- team composition and workshop scheduling
- some workshops
- reviewing the workshop results
- implementation of any actions arising from the process.

2.7. Scheduling

Once the operator has established the scope, selected personnel and gathered relevant information, the hazard identification workshops can be scheduled. The workshops should be conducted promptly to maintain momentum.

The Safety Assessment and control measure assessment steps of the Safety Case can be time-consuming, particularly for an older facility. Completing the hazard identification early allows more time to complete the other steps.

The following should be considered when scheduling workshops:

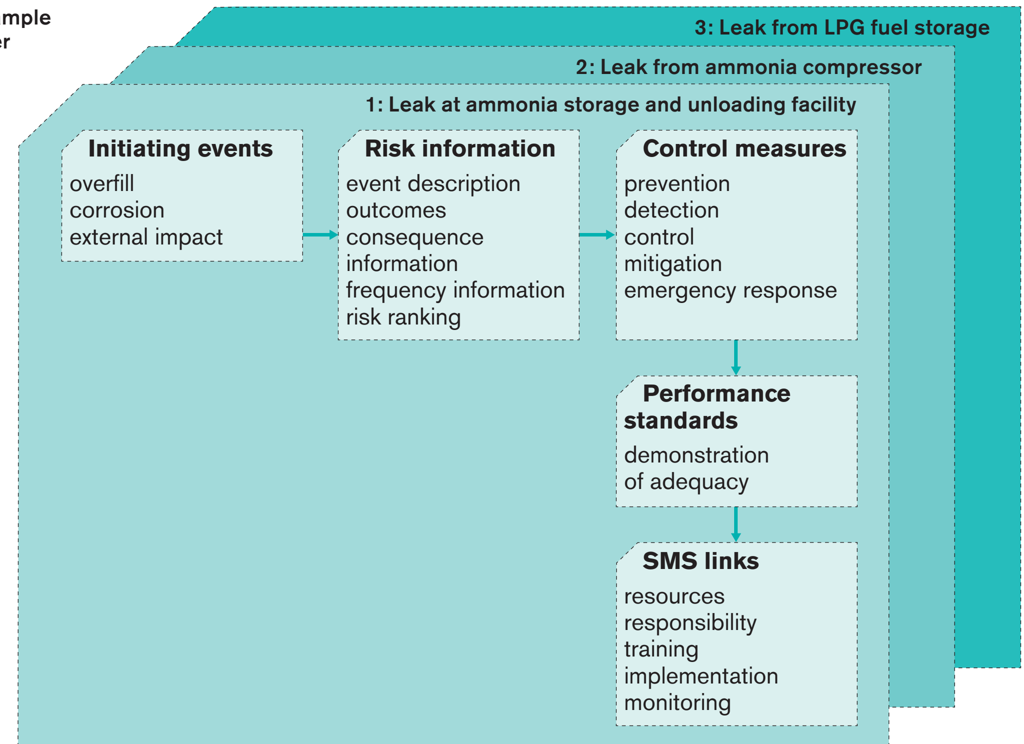
- the availability of key personnel
- the need to maintain production
- the need to maintain mental alertness
- the need for continuity and consistency.

To avoid mental fatigue, meetings should not exceed four to six hours per day. Once the workshops have been completed, it is important that a review is conducted on the information gathered. Workshop participants should be encouraged to provide feedback in the weeks following these workshops, as they might see things when they are back in the workplace which were not included during the workshops.

2.8. Documentation and linkages

A key output of the hazard identification is the documentation records such as a hazard register (Figure 2.3). This lists all potential major incidents and hazards along with the underlying causes, control measures and any assumptions. It forms the basis for the later steps of Safety Case development. The outcomes from hazard identification should clearly and logically link with the Safety Assessment and control measure steps.

Figure 2.3 – Example – hazard register



Time should be spent upfront planning how the various aspects of the Safety Case will be linked to provide a robust demonstration that the facility is safe. This avoids revamping of the Safety Case later.

The hazard identification results may be recorded on paper or electronically. The main requirements are that the records:

- clearly show linkages between incidents, hazards (including underlying causes) and control measures
- contain sufficient information to support the later steps of Safety Case development
- are maintainable. The hazard register format can directly facilitate the process of revisiting and updating the knowledge of hazards and incidents within the facility
- are managed under a document control system.

For larger facilities it is likely that an electronic hazard register (database) will be easier for ongoing maintenance of the records and keeping the Safety Case up to date.

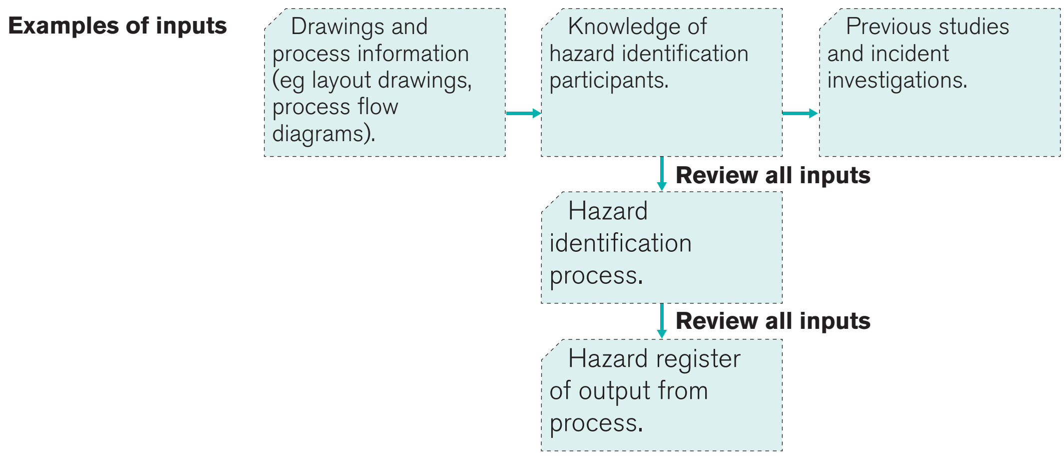
The operator should record all relevant information. While many risk techniques (eg HAZOPs) might record by exception (eg where improvement is required), the Safety Case requires all hazards to be documented regardless of whether action items result. The complete documentation for the hazard identification could be substantial and therefore a simple method of linking and communicating the information together should also be considered eg bow tie diagrams.

3. The hazard identification process

3.1. Preparing information for hazard identification

The operator must base the hazard identification process on a comprehensive and accurate description of the facility, including all necessary diagrams, process information, existing conditions, modifications and material safety data sheets (MSDS). Prior to conducting the hazard identification, the operator should collect all relevant information, compile it and then check it for accuracy. Figure 3.1 shows some sources of hazard identification input.

Figure 3.1 – Sources of hazard identification input



The hazard identification may be supported by past risk assessments and historical incident data. The operator should refer to previous hazard studies, if they are relevant to identifying major incidents, and consider all the issues discussed in this guidance note. However, the operator must ensure that any existing studies:

- are fully understood by the hazard identification participants
- are still relevant for the current operating conditions and condition of the facility
- were conducted to an acceptable standard
- addresses identified gaps.

While previous studies can be helpful, it cannot be assumed that they are correct eg the absence of identified hazards in previous risk studies should not be taken as an indication that there are no hazards to be identified. It may be that the previous hazard identification process was inadequate, hazards were screened out and/or there have been changes to the facility since the risk study.

It is useful to have a record of the facility and industry's incidents or near misses at the hazard identification workshop. Incidents or near misses, either at the facility or at similar facilities, provide a clear indication of what has gone wrong in the past and could go wrong again. This information is best used as a quality check at the workshop to avoid missing potential hazards and major incident scenarios. The operator should review its own plant operating history and conditions (eg corrosion, breakdowns and maintenance) for potential scenarios. However, major incidents are rare and historical incidents are unlikely to represent the full range of potential incidents. Incident data should be used to supplement more systematic hazard identification techniques.

Another useful source of information on the hazards associated with storage and handling of hazardous materials are MSDS. It is also worth referring to the technical literature provided by material suppliers on their products.

3.2. Identifying major incidents and hazards

Ensuring hazard identification is comprehensive, accurate and complete is important for the later steps of Safety Case development. The operator needs to consider:

- hazards that are present continuously or occasionally
- worst case events and not only those events used for the design basis of the facility. The worst case will depend on a large number of factors such as materials normally or not normally present, extreme process conditions (eg overfill, abnormal reactions), the potential failure of isolation systems, the proximity and layout of vessels and presence of personnel
- the full range of factors that can result in a hazard with the potential for a major incident. This includes the technology used, the people, the systems in place, the type of task, the operating mode and external factors (see Figure 3.3)
- hazards relating to the installation and commissioning phases for new facilities
- any changes/modifications intended at the time of submitting the Safety Case. This includes any changes to current conditions such as facility modifications, increased or reduced throughput, increased or reduced manning, material or equipment changes.

A generic description of a hazard identification workshop process is provided in Figure 3.2. It describes what is required to demonstrate a robust hazard identification process.

Figure 3.2 – Hazard identification process

Divide the system into sections

Divide the facility into manageable sections to provide sufficient focus to fully identify potential major incidents and hazards. The sections could be defined according to:

- similarity of hazard or activity
- the chemicals involved or
- geographical location.

The complexity of the section should control the size of each section. Ensure there are no gaps between sections.

Describe each section

The equipment, materials, human activities and process operations to be covered should be clearly defined and understood. For each section describe:

- the Schedule 9 materials involved
- the activities that are, or could be, conducted
- the design intent and any limitations to activities or operations
- any changes that have occurred over time and the current condition of equipment.

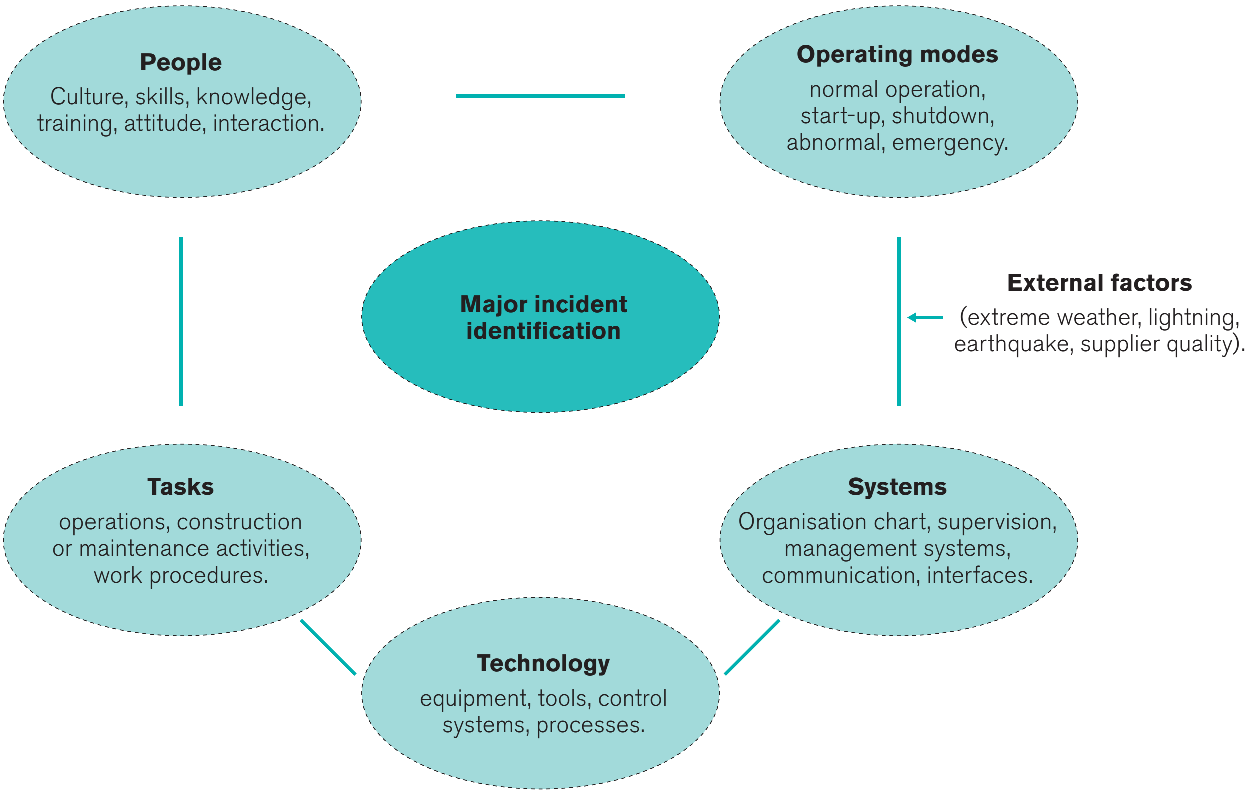
Apply hazard identification technique

Apply selected hazard identification technique to identify all hazards, incidents, causes and controls. The technique needs to:

- consider the full range of factors that could result in or influence a major incident (Figure 3.3)
- avoid inappropriate screening of hazards (section 3.3)
- provide adequate depth of analysis including sufficient detail to explain why, when, where and how (section 3.4)
- use lateral thinking and realism in hazard identification (section 3.5)
- fully document the hazard identification.

The identification of controls can occur during the hazard identification, separately or during the Safety Assessment. The operator may find it beneficial to identify all (or as many as possible) of the potential major incidents prior to identifying the hazards that may give rise to the major incident. This may also assist in dividing the facility into sections for the hazard identification process.

Figure 3.3 – Factors influencing major incidents



For each section the operator should ask the following questions in relation to these factors:

- What materials are present? Are they a potential source of major incidents in their own right? Or could they cause an incident involving another material? Could two or more materials interact with each other to create additional hazards?
- Could other materials, not normally or intended to be present, be introduced?
- Can the process deviate from the design intent or 'safe operating envelope'? What activities are conducted and how could they go wrong?
- What abnormal or infrequent activities can be conducted, and how could they go wrong?
- What equipment within the section could fail or be impacted by internal or external hazardous events? What are the possible events?
- What could happen in this section to create additional hazards eg temporary storage, road tankers?
- Could this section of the facility interact with other sections (eg adjacent equipment, an upstream or downstream process, or something sharing a service), in such a way as to cause an incident?

Analysis should consider the interaction between influencing factors eg a safety system may be bypassed in start-up mode and personnel may not be adequately trained for start-up due to its infrequent occurrence.

Figure 3.4 – Example – hazard register recording sheet

Hazard register **Area under review:** Ammonia facilities **Incident:** Ammonia release at storage	**Hazard no:** 1
Hazards	**Existing and potential control measures:**
Equipment corrosion (component failure)	• NDT inspection program • Equipment specification and design to ABC standards
Maintenance error eg fitting tightened too far, wrong component – not fit for purpose (component failure)	• Trade – qualified personnel • Valve and flange fitting training
Leak from flange/seal gasket failure	• Equipment specification and design to ABC standards • Valve and flange fitting training
On-site vehicle collides with storage tank (storage tank punctured)	• Storage designed and engineered to Australian Standards • Storage area is protected (chained off/vehicle barriers) to restrict access • Speed limits on-site
Dropped object (lifting over storage tank) (storage tank punctured)	• ABC site lifting register • Lifting gear inspection, maintenance and testing • *Build a barrier around storage tank to prevent lifts over it* (*potential*)

If control measures are recorded during the hazard identification, then hazard identification should be documented in such a way that it is clear which control measure/s control a specific hazard, as shown in the example in Figure 3.4. This is important because:

- it assists third parties to understand that all identified hazards have controls
- when combined with performance indicators and other relevant information, it helps to demonstrate adequacy of hazard and major incident risk reduction measures.

It may be helpful to display the linkage between incidents, hazards and controls diagrammatically eg using a bow tie or a fault tree diagram. An example of a bow tie diagram and more detailed guidance on control measures is provided in the guidance note – *Control measures*.

The operator can also consider upfront if it is possible to group certain types of hazards, especially if they can occur site-wide or on every bow tie (eg natural hazards, power loss or security threats). This can reduce the level of effort required if the operator is considering these hazards generically and not for each part of the site – unless special circumstances apply to a part of the site and it needs to be considered individually (eg particularly vulnerable to loss of power).

3.3. Screening hazards

The operator should include all relevant and conceivable scenarios in the hazard identification. Each scenario should be transparently assessed as part of the Safety Assessment process. The operator should not screen out hazards simply because they have a very low likelihood, rather, they should be rejected only if they are inconceivable (see example below). Note also that a decision on 'inconceivable' should not rely on controls which have been implemented.

Example of screening hazards

An example of an incident that has been incorrectly screened relates to the puncturing of a drum by the tyne of a forklift in a warehouse. This will normally only result in a limited release, however, it may, in rare circumstances, escalate. Therefore the hazard identification should include the escalated scenario in the results of this step. Decisions on likelihood are left to the next step – Safety Assessment.

For the ammonia storage example, a conceivable hazard includes terrorism. This hazard is thought to have a low likelihood due to other more high profile targets within the city. However, it cannot be considered inconceivable as the facility is in an area where there is the potential for multiple fatalities off-site.

An inconceivable hazard may be an aircraft crash, if the facility is well away from flight paths.

The operator may be tempted to screen out events because they are perceived to be unlikely. The assessment of low likelihood can often result from an assumption that the existing controls are highly effective. This type of screening is not recommended for the following reasons:

- the control (thought to eliminate the risk) may not be as robust as thought
- controls will not be adequately managed if their importance is not recognised
- the initial assessment may not be based on adequate grounds, and further detailed assessment may indicate that the risk is higher due to site-specific considerations
- knowledge of all potential events is essential for emergency planning.

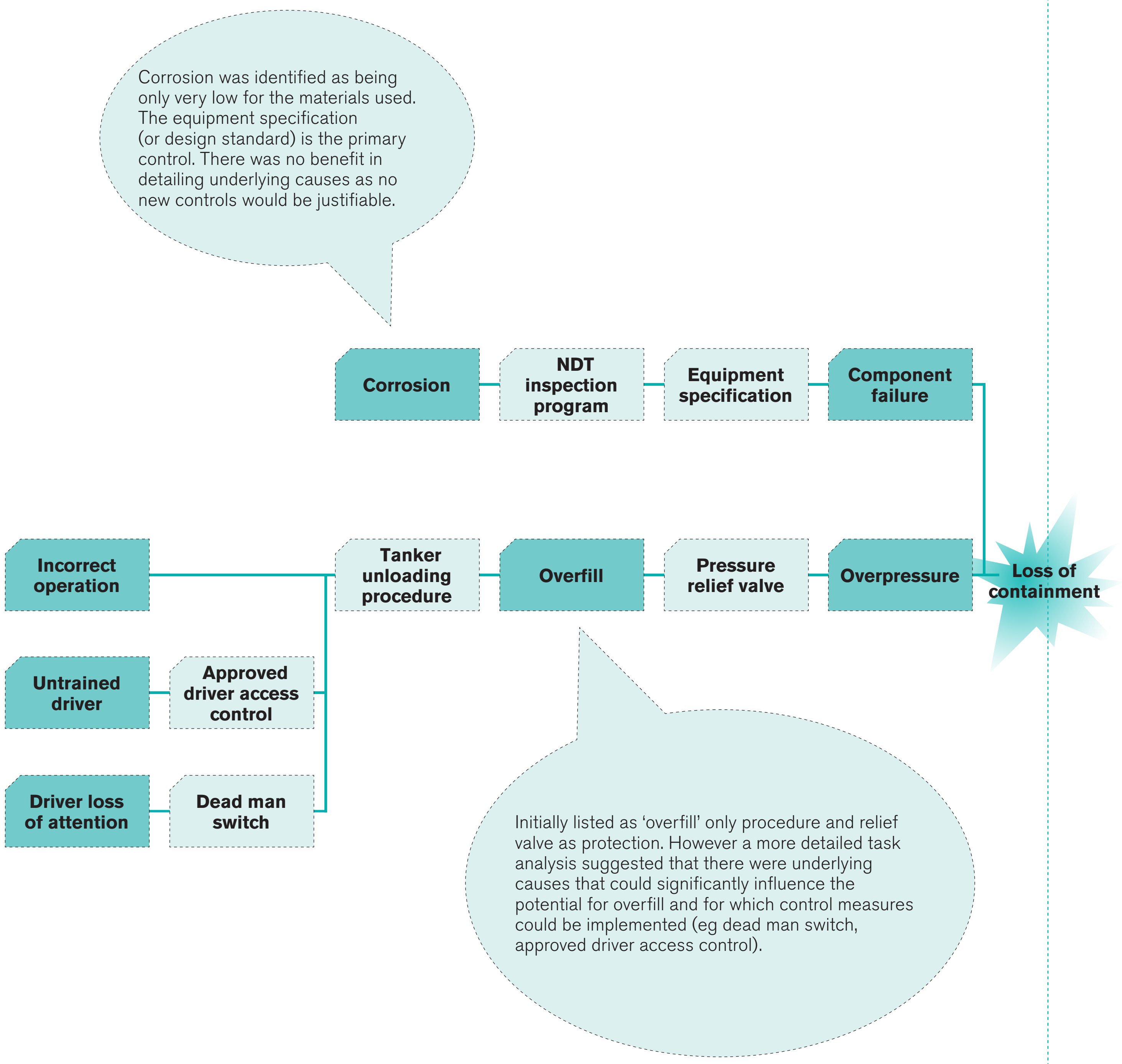
3.4. Providing an adequate depth of analysis

Hazard identification should provide sufficient detail for the operator to fully understand the nature of each hazard and identify the controls necessary – whether existing or alternative for the management of each hazard (see the guidance note – *Control measures*).

Example of depth of analysis

ABC Chemical Company initially identified overpressure as a primary hazard leading to loss of containment from their ammonia storage tank with two causes identified (overfill and thermal radiation from the sun).

During the verification phase of the hazard identification, it was questioned whether this analysis went deep enough. Filling is to be done solely by the tanker driver in the future. A more detailed task analysis was then undertaken resulting in overfill being broken down into a number of underlying causes. This resulted in several potential controls being recommended.



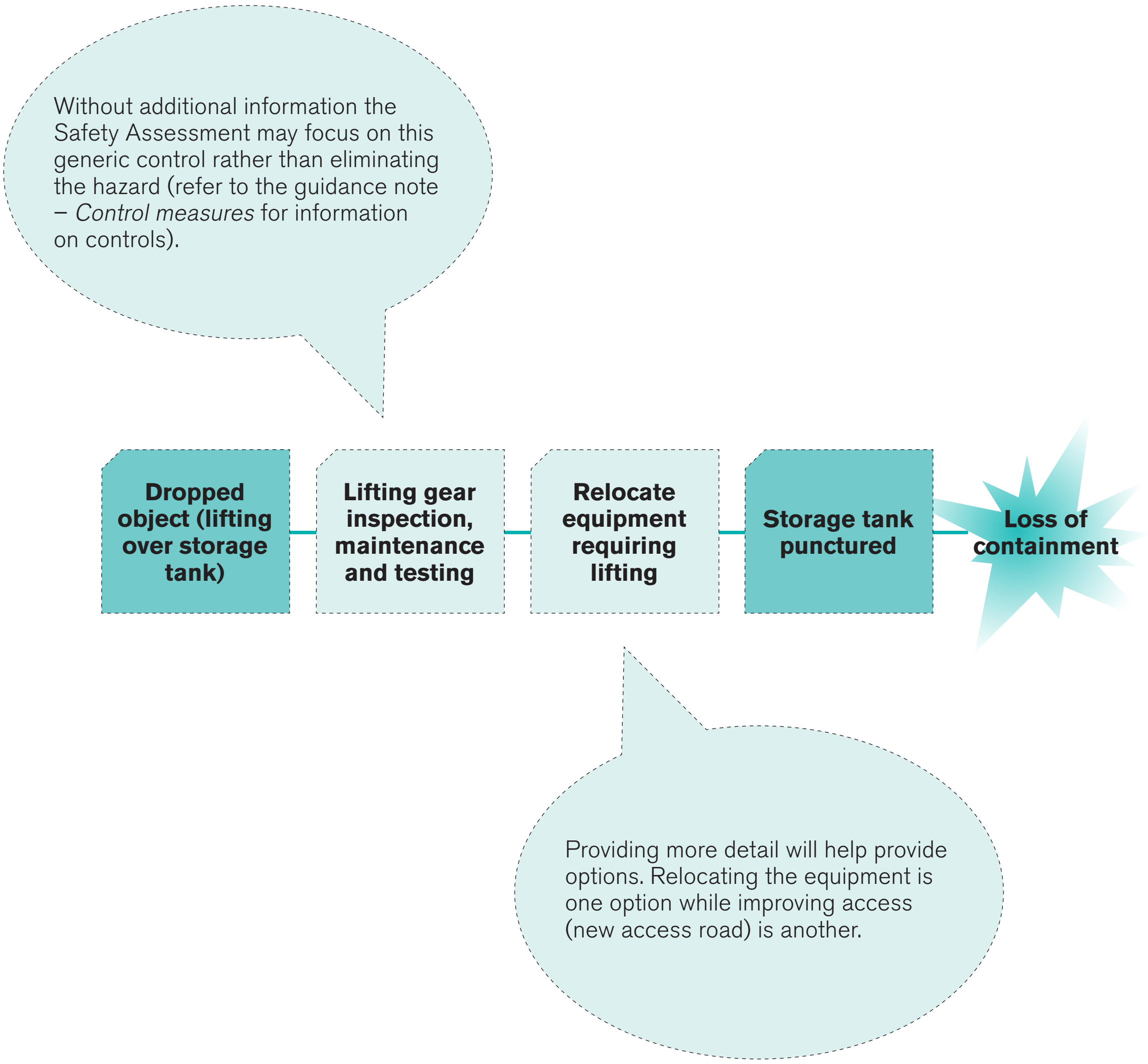
It is important to get to the most basic/root cause (or hazard) leading to a major incident, similar to the process used in an incident investigation. Identification of the most basic cause may result in a control being put in place which significantly reduces the likelihood of the direct cause (or hazard).

During the hazard identification, where this helps understanding of the hazard, the operator should detail when, where and why the hazard is present. Being specific during hazard identification helps in the assessment of the relevant control measures (see the guidance note – *Control measures*) and the Safety Assessment (see the guidance note – *Safety Assessment*).

Example of the root cause for a loss of containment

An object dropped on an ammonia storage which punctured the vessel was identified as a hazard. For this hazard it would be useful to know what objects are lifted and why. For example:

'An unreliable compression facility is near the tank and access to this equipment for maintenance is limited in wet weather as a crane would get bogged. The crane therefore lifts over the tank to limit access problems. The item lifted is often the compressor and therefore a substantial weight.'



3.5. Lateral thinking and realism in hazard identification

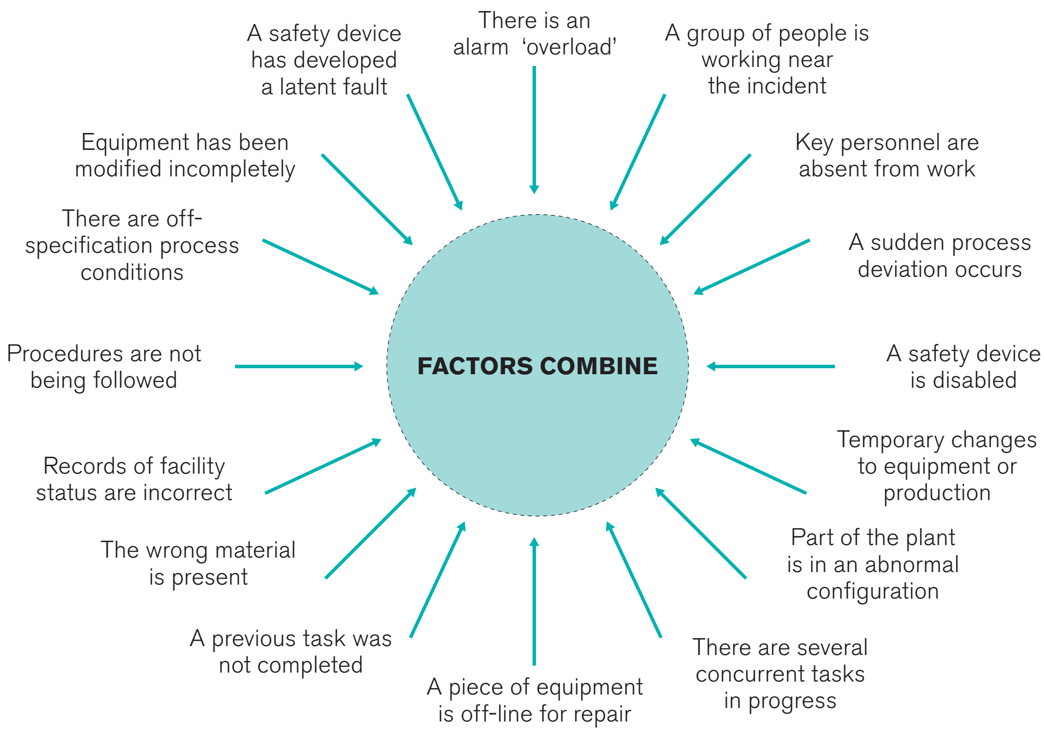
It is important to employ realism and lateral thinking in hazard identification. The operator must not only identify 'obvious' accidental events but also look for potentially complex events eg those consisting of a sequence of failures, or a set of concurrent problems.

The hazard identification team should:

- challenge assumptions and existing norms of design and operation to test whether they may contain weaknesses
- think beyond the immediate experience at the specific MHF
- explore the effect of failure of management systems, controls and procedures
- consider how relatively minor problems may grow into major incidents because of other problems that arise in addition.

Figure 3.5 shows some common factors which may combine into a major incident.

Figure 3.5 – Factors that may combine to result in a major incident



Combinations of factors such as those above have led to major incidents. In many cases operators had never considered these combinations or had dismissed them as not credible. This could happen when:

- using the traditional HAZOP approach eg combinations of events that could lead to high consequence incidents may be dismissed as 'double contingency' events
- companies and individuals exhibit 'corporate blindness' when identifying or reporting hazards eg assuming that the systems and procedures in place only ever function as intended.

The hazard identification needs to be realistic and needs to recognise that events of low likelihood are nonetheless still possible, and that apparently unconnected and minor events and failures may combine to cause catastrophic consequences.

4. Outputs

4.1. Documenting results

The key output of hazard identification is a list of all potential major incidents and hazards along with any relevant information that was discussed during the workshops such as control measures, underlying assumptions and rejected potential causes.
Several key features which should be considered are:

- a numbering system for hazards and controls to allow easy identification of Safety Case findings and tracking of linkages
- a logical structure for listing and linking of the hazards and controls. This helps find specific hazards and their causes and helps demonstrate that all major incidents and hazards have been identified
- all relevant information discussed during the hazard identification should be recorded with a clear link to hazards, causes and controls. This includes assumptions, uncertainties, debated issues, gaps in knowledge, details of hazards, incidents and control measures.

This allows the operator to describe the basis for a decision at a later time. Operators should not rely on the memory of those present during the hazard identification to later recall specific details.

4.2. Uses of hazard identification outcomes

Hazards must be understood and acted upon, not just identified. The operator can use the output of the hazard identification in the following ways:

- as an input to the Safety Assessment (see the guidance note – *Safety Assessment*) where all major incidents and hazards identified in the hazard identification must be considered
- to provide hazard awareness training to workers. This will ensure that all workers have sufficient knowledge of the hazards to enable them to carry out their roles safely, regardless of whether or not they are involved in the hazard identification itself
- the hazard register should facilitate the process of revisiting and updating the knowledge of hazards and incidents within the facility
- the identified control measures can be taken into account in the Safety Assessment which would normally involve consideration of their effectiveness and viability (see the guidance note – *Control measures*).

5. Review and revision

It is the operator's ongoing responsibility to identify hazards and major incidents before conditions arise where these hazards could result in a major incident. Therefore hazard identification must be a dynamic process which stays ahead of any changes in the facility that could introduce new hazards. Hazard identification must be an integral part of 'Management of Change' and operations management systems so that the hazard identification process will be implemented before changes are made. The example below shows some of the triggers for hazard identification review. There are also additional review and revise requirements associated with MHF licence renewal and Safety Case update (refer to the guidance note – *Renewal of a major hazard facility licence*).

Examples of triggers for review of hazard identification

Triggers include:

- changes in the workforce which could lead to changes in working practices or in knowledge of the facility
- physical modification to facility or changes to operations as these could introduce new hazards
- review of previously identified hazards prior to certain activities, particularly rarely performed ones
- a new chemical is introduced or handled
- abnormal conditions have arisen or critical operating parameters have been approached or exceeded
- process or condition monitoring may indicate potential hazards. Understanding these early warning signals can be important to avoiding incidents
- incidents and corrective actions may record hazards or concerns about potential hazards
- incident or near miss investigations should consider whether additional hazards are now recognised. Reports of incidents or near misses at other facilities should also be reviewed.

6. Quality assurance

At the completion of the hazard identification phase, a quality assurance process should be in place. Table 6.1 outlines the key activities and checks that should be undertaken to ensure quality in the hazard identification process. These checks will also assist in ensuring that all major incidents and all major incident hazards have been identified.

Table 6.1 – Key activities and checks for quality assurance

Activity	Check
Verify all major incidents and hazards have been identified.	Review company-wide and industry incident data and verify all potential incidents have been identified during the hazard identification process or are inconceivable. If they are inconceivable, record why those particular incidents cannot occur at the facility.
	Have personnel who were not present at the meeting reviewed the hazard identification records?
	Consider the use of an independent person to review the results.
	Review previous risk assessments to identify incidents not identified during the hazard identification.
	Review other documents that may indicate other hazards or causes. For example: • cause and effect diagrams for protective system • manufacturer (of plant) manuals • MSDS etc.
Verify accuracy of information.	An individual could conduct a sample check of the information used during the hazard identification to verify the hazard identification team worked on the basis of accurate information.
Verify the hazards and major incidents are clearly linked with controls.	Use personnel not present at the meeting to verify that each incident and its hazards, both primary and secondary, are linked correctly. It is useful to verify that any existing controls that were identified in the hazard identification workshops are actually in place and linked to the correct causes or pathways. However, this could be deferred until the Safety Assessment stage (see the guidance note – *Safety Assessment*) if preferred.
Verify the outcomes (hazards, controls and consequences) have been communicated.	Have training programs that include hazard awareness information been updated? Has refresher training with revised material been scheduled and/or delivered?

7. Compliance checklist

The following checklist contains information on the MHF regulations as they relate to hazard identification.

Table 7.1 – MHF regulations relating to hazard identification

Section	Requirement
Reg 5.2.6(1)	The operator of a major hazard facility must identify (a) all major incidents which could occur at the major hazard facility, and (b) all major incident hazards.
Reg 5.2.6(2)	The operator must document all aspects of any identification made under this regulation, including (a) the methods and criteria used for identifying major incidents and major incident hazards (b) any external conditions under which those major incident hazards might give rise to a major incident.
Reg 5.2.7(1)	The operator of an MHF must conduct a comprehensive and systematic Safety Assessment… in relation to all potential major incidents and all major incident hazards.
Reg 5.2.12(1)	The operator of an MHF who has identified major incident hazards and possible major incidents under reg 5.2.6… must review and, if necessary, revise those matters to ensure that the risk control measures adopted are such that the operator continues to comply with reg 5.2.8.
Reg 5.2.12(2)	Reviews and revisions under this regulation must be conducted: (a) at the direction of the Authority (b) before a modification is made to the major hazard facility (c) after a major incident occurs at the major hazard facility (d) when an effectiveness test indicates a deficiency in a control measure (e) if there has been a change to the circumstances that formed part of the original Property Protection. Assessment under reg 5.2.36. (f) if a health and safety representative requests the operator to conduct a review and in any event at least once each five years.
Reg 5.2.13(1)	The operator of an MHF must develop a role for the operator's employees, including the specific procedures they are required to follow to assist the operator to identify major incident hazards and possible major incidents under reg 5.2.6…
Reg 5.2.13(2)	The operator must review the role for employees developed under this regulation if there is a change of circumstances, including a modification to the MHF that would require additional or different knowledge and skills on the part of the employees to perform the role.
Reg 5.2.15(1)	The Safety Case prepared or revised under this part must… contain a summary of the documentation prepared under reg 5.2.6…
Reg 5.2.18	The operator of an MHF must consult in relation to identifying major incidents and major incident hazards under reg 5.2.6.
Reg 5.2.19(1)	The operator of an MHF must provide information, instruction and training to employees of the operator in relation to: (a) the kind of major incidents that could occur at the facility (b) all major incident hazards…
Reg 5.2.36	For the purpose of complying with regulation 5.2.35, the operator of an MHF must conduct a comprehensive and systematic Property Protection Assessment in accordance with this regulation for matters relating to protection of property that have not previously been considered in divisions 3 and 4.
Schedule 10 (4.1)	(The Safety Management System documentation must include…) In relation to each part of the documented Safety Management System that describes the means of compliance with part 5.2 division 3 of these regulations, an annotation or cross-reference identifying the specific provision of these regulations being complied with.

8. Further reading

General reference

The following are recommended as sources of general information and may be useful in addition to the information provided in this guidance note.

Lees, F. P., *Loss Prevention in the Process Industries*, 3rd edition, Butterworth–Heinemann, UK, 2005.

Kletz, T., *An Engineer's View of Human Error*, 2nd edition, Institution of Chemical Engineers (IChemE), Rugby, 2001.

Specific topics

Centre for Chemical Process Safety (CCPS), *Guidelines for Hazard Evaluation Procedures*, 2nd edition, American Institute of Chemical Engineers (AIChE), New York, 1992.

Centre for Chemical Process Safety (CCPS), *Guidelines for Preventing Human Error in Process Safety*, American Institute of Chemical Engineers (AIChE), New York, 1994.

CONCAWE Ad–Hoc Risk Assessment Group, *Methodologies for Hazard Analysis and Risk Assessment in the Petroleum Refining and Storage Industry*, Fire Technology, Vol. 20, No. 3, 1984.

Crawley, F. and Taylor, B., *Hazard Identification Methods*, European Process Safety Center, 2003.

Frank, W.L. and Whittle, D.K., *Revalidating process hazard analyses*, Center for Chemical Process Safety (CCPS), American Institute of Chemical Engineers (AIChE), New York, 2001.

New South Wales DUAP, *Hazard and Operability Studies*, Hazardous Industry Planning Advisory Paper No. 8 (HIPAP No. 8), Sydney, 1995.

Standards Australia, *Hazard and operability studies* (HAZOP studies) – Application guide , (AS IEC 61882–2003), Standards Australia, 2003.

Reason, J.T., *Generic Error–Modelling System (GEMS), A Cognitive Framework for Locating Common Human Error Forms*, New Technology and Human Error, ed. J. Rasmussen, K. Duncan and J. Leplat, 1987.

Montague, D. F., *Process Risk Evaluation – What Method to Use?*, Reliability Engineering and System Safety, Vol. 29, No. 1, Elsevier Science, England, 1990, pp27–53.

Procedures for Performing a Failure Mode, Effects and Criticality Analysis, MIL–STD–1629A, U.S. Navy, 1977.

9. Appendix

Hazard identification techniques

Technique	Summary
HAZOP	A highly structured technique that delivers a detailed understanding of the possible 'deviations from design intent' to identify hazards and operability concerns. The primary focus is on chemical process systems. HAZOP is less suitable for identification of hazardous scenarios associated with mechanical integrity failures and external events such as collisions or dropped objects. It is therefore a good technique for identifying process-related hazards at manufacturing facilities involving materials processing, reactions etc. It is not as useful for a facility devoted to material storage and transport such as a dangerous goods warehouse. HAZOP seeks to identify causes and consequences from a deviation whereas the Safety Case is seeking causes for major incidents. The information is present but may require manipulation to create a useable hazard register. Also, since HAZOP analysis uses a 'section by section' approach, it may not identify hazards associated with the interactions between different nodes. HIPAP No. 8 (DUAP 1995) describes the HAZOP methodology in greater detail.
Checklists	Can be an effective way of capturing and passing on the experience of others, and therefore are a valuable hazard identification tool. There are many hazard checklists available, each of which can be used to guide the identification of hazards. However, checklists should only be used as a final check that nothing has been neglected or missed by other studies eg have plastic or plastic-coated piping systems been adequately grounded to avoid static build-up? Which lines can plug and what are the hazards of plugged lines? They should not be used as the sole tool in a hazard identification process, since they may not cover all types of hazard, particularly facility-specific hazards, and they do not encourage lateral thinking. These can be used effectively to demonstrate compliance with an engineering standard.

Historical records of incidents	Information on actual incidents and near misses that have occurred provide insight into how incidents have actually occurred. The operator should consider its own site, company and industry history. There are a number of publicly accessible databases that contain summaries of accidents and near misses that have occurred in hazardous processes around the world. However, major incidents are rare and the range of incidents that has actually occurred may not be the entire range of possible incidents. No MHF in Victoria has relied on this as its only technique for hazard identification but some facilities found it to be a useful additional check.
What if?	A set of pre–prepared and customised 'What if?' questions on potential deviations and upsets at the facility. For example: • what if there is moisture left in the line? • what if the wrong material were added to the reactor? The questions are often based on the experience of others and hence this technique has some of the same limitations as a checklist approach. The rigour of this approach can be improved by increasing the structure of the What if? An advantage of this approach over HAZOP is that hazards associated with interactions between sections of the plant may be more readily identified. In general, this tool delivers results that are less detailed than HAZOP. This technique was used successfully by some Victorian MHFs which have a large number of similar facilities where the experiences gained at one facility may indicate potential hazards at another.
Task analysis	Specifically developed to identify hazards associated with human factors, procedural errors and the 'man-machine interface'. The technique can be applied to working environments such as control rooms, or to specific jobs such as start-up or shutdown processes. Types of hazard identified may include procedure failures, human resources issues, hazardous human errors and incorrect responses to alarms. The assessment can be time-consuming and therefore only used when areas of a facility have a low 'fault-tolerance', or where human error could easily take a plant out of its safe operating envelope (eg a facility handling explosives). This technique can also be effectively used for warehousing and transport applications where procedures and human error play a large part. The level of the analysis should be fit for its purpose.
FMECA and FMEA	Highly structured techniques that break down the overall system into a set of related sub-systems, then a set of smaller sub-systems, and so on down to component level. Failures of individual systems, sub-systems and components are then systematically analysed to identify potential causes (which stem from failures at the next lower-level system), and to determine their possible effects (which are potential causes of failure in the next higher-level system). These techniques are most often applied to a complex item of mechanical or electrical equipment which contains a number of sub-systems and components. They analyse the level of safety achievable by safety critical mechanical or electrical plant items such as firewater pumps, gas detection devices or trip systems. Most often applied to a complex item of mechanical or electrical equipment, which contains a number of sub-systems and components.
Brainstorming	A relatively unstructured group process, brainstorming can be effective at identifying obscure hazards of a type that may be overlooked by the more systematic methods. It can be used to complement other techniques but should not be used as a replacement as hazards are likely to be missed.

Guideword-based techniques	This structured brainstorming technique splits hazard identification into sections which may be areas, processes or activities. Guidewords are then raised to prompt creative thinking. This technique is different from a checklist approach. Rather than focus on a specific list of desired design or operating features, guidewords are more general and focus on hazard categories, eg 'overpressure', 'corrosion', 'leak' or more general categories such as 'fire', 'external events' and explosion. Guidewords prompt creative thought about the underlying causes for each hazard category. Thus guidewords provide focus while not limiting the options in the same way as a checklist. The technique is good at identifying major hazards but is not as detailed as techniques such as a HAZOP. Other techniques may need to be applied at the detailed design phase of a project. This technique's greatest advantage is where similar hazards exist across a facility and the guidewords are based at a level that provides specific focus (ie overpressure). This approach was successfully used by a number of chemical companies. The technique is not as useful for warehousing and transport companies.
Fault Tree and Event Tree Analysis	Fault trees describe an incident (eg loss of containment) in terms of the combinations of underlying failures that can cause them (eg a control system upset combined with failure of alarm, shutdown and relief systems). Event trees describe the possible outcomes of a hazardous event, in terms of the failure or success of reduction and mitigation measures such as isolation and fire-fighting systems. Fault tree and event tree analysis is time-consuming and it may not be practicable to use these methods for more than a small number of incidents eg a fault tree approach for a large, complex facility is not practicable. The technique requires incidents to be identified first, before working backwards to hazards. For complex facilities, if this were the only technique used for hazard identification, some incidents or scenarios could be inadvertently screened out of consideration before the studies begin. Nevertheless, the technique is useful for detailed identification of hazards related to highly critical or high consequence incidents, such as control of reactors with runaway potential. The methods also include control measures in a transparent way, can be reformatted into a bow tie diagram (see the guidance note – *Safety Assessment*) and are amenable to quantification as part of Safety Assessment. The method is further described in Rasmussen (1975) and CCPS (1992).

Further Information

Contact the WorkSafe Victoria Advisory Service on 1800 136 089 or go to worksafe.vic.gov.au

Related WorkSafe publications

Guidance note – *Renewal of a major hazard facility licence*

Guidance note – *Control measures*

Guidance note – *Safety Assessment*

Guidance note – *Requirement for demonstration*

Guidance note – *Safety Case outline for a major hazard facility*