System Safety
M4 Preliminary Hazard Analysis (PHA) V1.2

Matthew Squair

UNSW@Canberra

12 October 2014
Except for images whose sources are specifically identified, this copyright work is licensed under a Creative Commons Attribution-Noncommercial, No-derivatives 4.0 International licence.

To view a copy of this licence, visit http://creativecommons.org/licenses/by-nc-nd/4.0/
1 Introduction
2 Overview
3 Methodology
4 Hazard identification
5 Evaluate risks
6 Define hazard controls
7 Documenting the analysis
8 Limitations, advantages and disadvantages
9 Conclusions
10 Further reading
Introduction

Overview

Methodology

Hazard identification

Evaluate risks

Define hazard controls

Documenting the analysis

Limitations, advantages and disadvantages

Conclusions

Further reading
Learning outcomes

Outcomes

To be able to appropriately conduct a preliminary hazard analysis

To understand the strengths and weaknesses of the analysis as an element of a safety program
“Hazard identification can sound like an intimidating process. Stare at a blank page, then a miracle occurs; then read the final product…”

— Nancy Leveson (MIT Safeware website)
Key definitions

**Preliminary.** coming before and usually forming a necessary prelude to something. (The PHA is *normally* be done on the preliminary or concept design, although it can be used at any point in the system lifecycle

**Hazard.** Hazards are notional precursor system states that may lead to an accident. We use our control of such identified states as a metric for safety

**Analysis.** An examination of the elements of a system, separation of a whole into its component parts

**PHA.** An initial system safety analysis. It is a list or inventory of system hazards and includes qualitative, *not quantitative*, assessments of risk for each hazard

**PHL.** A precursor to the PHA system safety analysis. It is a simple list (in source/outcome form) of potential hazards and mishaps
PHA and the system lifecycle

For maximum effect the PHA is normally programmed into the upfront part of the program.
PHA objectives

The PHA is carried out *early* in the system development lifecycle so that it can influence the design in the most cost effective fashion.

Forms, along with the SSPP, the *safety baseline* for the project.

**Definition**

The safety baseline is the identified *and agreed* scope of safety effort for the project. The safety baseline comprises the activities defined in the SSPP and the hazards and controls identified in the PHA.

Think of the safety baseline as the *basis of estimate* for the safety program.
Methodology

1. Introduction
2. Overview
3. Methodology
4. Hazard identification
5. Evaluate risks
6. Define hazard controls
7. Documenting the analysis
8. Limitations, advantages and disadvantages
9. Conclusions
10. Further reading
PHA inputs and outputs

System Models
- Functional Flow Block Diagrams (FFBD)
- Reliability Block Diagrams (RBD)
- Indentured Equipment List (IEL)

System Design
- Architecture
- Functions
- Operations

Hazard Sources
- PHL (if done)
- Hazard checklists
- TLM checklists

Analysis

PHA Worksheet

PHA Report
- Hazards (S,M,O)
- TLM
- Risk (I,F)
- Controls
- MoV
- Responsibilities
- Traceability
- Status
System definition

We need to define the system to bound our analysis
- what’s the system boundary (for the purpose of analysis)
- Mission, mission phases and environment
- System design, major components, functions and operations
- Supporting system models (FFBD, RBD and IEL)

We also need to establish a set of analytical criteria
- design safety criteria and hierarchy of controls
- safety principles and guidelines
- what is considered a safety critical
- risk criteria, decision thresholds
- system level of risk evaluation and acceptance
Planning the PHA

Ideally we refer to the SSPP which defines the scope and techniques to be used for the PHA.

Planning is then a tactical exercise of aligning resources (people, data, meeting rooms) on a convenient date for the project.

In practice getting N > 1 project design staff in a room during the concept design phase is like herding cats.

Technique selected also drives resources, for example Hazards and Operability Study (HAZOPS) is far more thorough (and time intensive) than Structured What If Technique (SWIFT).
Acquire data

Having bounded the analysis, defined it’s scope and planned for it we need to collect the necessary data

- design data
- previous hazard analyses (PHL and TLM lists)
- hazard checklists
- statutory or regulatory ’you must address’ hazard lists
- accident and near miss data
PHL and PHA relationship

If there’s a preceding analysis it should be reviewed

The MIL-STD-882 analysis that precedes the PHA is the PHL it is (in essence) a PHA without a risk assessment that focuses on abstract hazards (source/outcomes) and mishaps

The list of Top level Mishaps (TLM) contained in the PHL is developed into a System Mishap Model (SMM) to assist in structuring the PHA

The entire list of potential hazards developed in the PHL should be an input to the PHA

- The first step is to identify any hazards not applicable
- Categorise the remaining hazards using the risk indices
- The list should then be scrubbed for applicability
PHL ‘Outcome (Source)’
Hazard Description
‘Inadvertent stage separation’

Root Causal Event (TLM)

Pyrotechnic Fault
RF Induced Current
Software/Timer Fault
Inadvertent Switch Depression

Hardware
Environment
Software
Human Factors

PHA adds ‘Mechanism’ to Hazard Description
‘Pyrotechnic fault (mechanism) leads to inadvertent stage separation (outcome) during Flight (source)’

Figure: PHL to PHL relationship (JSSG SW Safety Hdbk)
4 Hazard identification

5 Evaluate risks

6 Define hazard controls

7 Documenting the analysis

8 Limitations, advantages and disadvantages

9 Conclusions

10 Further reading
Hazard identification techniques

Is an unknown cause, unknown effect (exploratory) analysis type, techniques fall into two broad classes, structured or unstructured.

We’ll look at a couple of examples:

- Experience
- Checklists
- Structured What If Technique (SWIFT)
- TRIZ

The rule of requisite coarseness

While other techniques such as FMECA or HAZOP can be used, their use requires a level of detail *not* present in the conceptual design phase.
Class exercise - hazard identification

Consider the functions of a set of train doors, in 5 minutes list the possible hazards associated with their operation

How do we know whether your list is complete?
Hazard identification

Why use a method/technique?

Common law and legislation recognises a duty of care for reasonably foreseen hazards.

Conversely what constitutes a reasonably unforeseeable hazard?

To satisfy the 'foresee' part both a sound method and the conduct of the activity by experts is required.

A structured and disciplined approach (methodology/technique):

- Focuses all team members on the key issues systematically.
- Ensures that a cost/effective set of resources has been applied.
- Provides objective evidence that the job has been done properly.
Experience

An unstructured technique

A list of hazards is created by a person or group after discussion

Alternatively, experts are interviewed by a facilitator who elicits hazards

Usually assisted by accidents/mishap data, embodied in a TLM list

Effective for small systems or a specialised/complex element of a larger system

Advantage is it is very lightweight, but its unstructured nature lends itself to incompleteness and cognitive biases such as attentional blindness
Checklists

Checklists can be used to assist in recognising hazards associated with the system.

Checklists suitable for use in a PHA can cover:

- Hazard sources (e.g. Kinetic energy, compressed fluids etc)
- Potential initiating mechanisms (e.g fuel leakage)
- Lists of potential mishaps
- Lists of safety critical functions

Advantage is that they can be used to trap corporate knowledge. However such lists are never complete, and do not substitute for thinking critically about the specific hazard scenario.

The Preliminary Hazards List (PHL) is often conducted using checklists to evaluate the functions, energy, hardware and failure states of the system.
Checklists (cont’d)

Creative checklists is a more structured checklist method

1. A system specific checklist is created
   - Brainstorm system hazards, perturbations and events
   - Existing generic checklists are used to structure & assist
   - Should ideally completely cover all areas of concern

2. Matrices are created for system elements

3. Checklist items are reviewed for relevance to a system element

4. If relevant investigate the hazard/element combination

Advantage is that it provides structure and specificity to the analysis, however it is still a primarily checklist driven process

---

1 Number and type depend on the systems conceptual completeness
Structured What If Technique (SWIFT)

SWIFT is a structured *brainstorming* method

1. Develop a set of preplanned 'what if’ questions identified from the system mission, accident data, checklists, process descriptions, design standards etc

2. Structures questions around functions, task steps, process flow

3. Chair poses questions at workshop e.g 'what if X doesn’t happen..’

4. Multidisciplinary team of SME answer these ‘what ifs’

Advantage is that it focuses on brainstorming (creativity) and is quick and easy to implement. The technique can be conducted on any level of conceptual design. Does rely on a thorough setup
Theory of Solving Problems Inventively (TRIZ)

TRIZ is a set of analytical techniques to solve problems requiring innovative answers

Originally developed by Russian academicians

Reverse TRIZ can be applied to identify hazards

1. Identify the safety problem or hazard
2. Reverse the problem
3. Exaggerate the reversed problem
4. Consider what resources are needed to create this

TRIZ can be used as a specific brainstorming technique in hazard identification workshops, is more a supporting technique than a methodology
TRIZ (Explosion hazard in refinery example)

<table>
<thead>
<tr>
<th>Step</th>
<th>Descriptor</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Problem</td>
<td>Decrease explosion risk</td>
</tr>
<tr>
<td>2</td>
<td>Reverse</td>
<td>Increase explosion risk</td>
</tr>
<tr>
<td>3</td>
<td>Exaggerate</td>
<td>Lots of explosions, every day!</td>
</tr>
<tr>
<td>4</td>
<td>Resources</td>
<td>Lots of piping joints, poor maintenance etc</td>
</tr>
</tbody>
</table>

By reversing and exaggerating we put the team in a creative and aggressive mindset

They can therefore find more hazards than traditional techniques
How to run effective hazard workshops

Much of hazard identification is done in workshops, some lessons:

1. Don’t circulate ’what if’ questions in advance
2. Ensure reference material is to hand
3. No more than 8 in a workshop (including chair & scribe)
4. Full coverage of experts in design, operation & maintenance
5. A good chair/facilitator is vital
6. Someone needs to be there to record

The workshop chair

The workshop chair needs to have well developed people skills, as much as technical, and should ideally be independent of the project. A strong but tactful personality is a plus
The completeness problem

The heart of the problem is that if we perform any one analysis we don’t know whether we have identified all the risks.

In fact there’s good empirical evidence to indicate that there are significant incompletenesses [Potts et al 2014].

If we have two separate attempts to identify risks in the system, under certain assumptions, we can apply a capture-recapture methodology [Chapman 1951] to estimate the total number of hazards.
Capture recapture

If $X_1$ is the number of hazards identified with the first analysis method, and $X_2$ is the number identified by a second method while $X_{12}$ is the number of hazards that both identified, then the estimator for the total number of hazards is:

$$\hat{N} = \frac{X_1 \cdot X_2}{X_{12}}$$

Sense checking for (in)completeness

The smaller the overlap between analyses ($X_{12}$) the greater the indication of a hidden population.
Hazard description and logging

In order to avoid confusing a hazard with the consequences we utilise the Source, Mechanism & Outcome template.

As we are generating a list of hazards, categorising them is useful:

- Hazard type (physical or function source)
- Mission phase or mode (Startup, contingency)
- System architecture (subsystem, equipment)
- Location (Facility zones)
- function or subsystem (Solar panel array, Abort motor)

The hazard coding scheme, should be functional and applied uniformly.
Example hazard identification

**DESCRIPTION:** LOSS OF ATTITUDE CONTROL DURING FLIGHT (M4) DUE TO ACTUATOR (ACT) FAILURE

**HAZARD ID:** ACT.M4.01
Hazard tracking

To provide effective management of overall safety risk we need to an ability to track the status of the following:

- Progress towards eliminating or controlling the hazard risk
- Association of hazards to top level mishaps (TLM)
- Hazards that exceed acceptable risk thresholds
- Actions required to eliminate the hazard or reduce the risk
- The status of safety verification activities
- the hazard’s lifecycle phase (raised, accepted, closed etc)

The PHA report should document all of the above

We may transfer this data to a hazard log
Hazard tracking (cont’d)

Figure: UK Cassandra hazard log
Hazard tracking (cont’d)

If the system is assessed as low to negligible risk after the PHA we may decide not to take the safety analysis program further.

We then maintain an audit trail of references to meetings at which the PHA results were discussed.

Annotate specifications and design documents with references to the PHA to provide traceability or if we use a hazard log update it with such references.
Evaluate risks

1. Introduction
2. Overview
3. Methodology
4. Hazard identification
5. Evaluate risks
6. Define hazard controls
7. Documenting the analysis
8. Limitations, advantages and disadvantages
9. Conclusions
10. Further reading
Evaluating risk

For Each Hazard/Target Combination in Each Operational Phase:

1. Evaluate severity (worst-credible outcome (1))
2. Evaluate probability (of worst-credible outcome)
3. Consult risk assessment matrix
4. Evaluate operational constraints imposed by the hazard

Some hazards turn-out to not be applicable. We document these in the PHA report but their risk is not further assessed.

We evaluate the risk before & after we have applied controls.

**Note.** Credible is of course a subjective term and introduces an element of judgement to the analysis and is here intended to denote the exclusion of ‘possible’ but completely unrealistic scenarios.
At what level should we evaluate and accept risk?

If we evaluate risk at a low level on the hierarchy the risk associated with individual component failures will be significantly less than if we evaluate it at the subsystem level. While this may make signoff of the hazard easier, it may also mask the true criticality of the higher level subsystem.

Selecting the level at which to evaluate risk

Evaluating hazard risk at the wrong level in the system hierarchy can mask critical risks.
Define hazard controls

1. Introduction
2. Overview
3. Methodology
4. Hazard identification
5. Evaluate risks
6. Define hazard controls
7. Documenting the analysis
8. Limitations, advantages and disadvantages
9. Conclusions
10. Further reading
Hazard controls precedence

For those hazards whose risk exceeds tolerance thresholds we can:

- abandon the enterprise (rarely done in practice)
- transfer the risk to others (insure)
- obtain waivers (accept for a period of time)
- develop controls that reduce the risk

Selecting controls

Controls should be selected on the basis of their effectiveness, feasibility, and cost (both initial and lifecycle). Controls should not reduce system performance or introduce new hazards.
Hazard controls

Hazard controls reduce the likelihood or the severity of outcome

Example

By placing an electrical enclosure (a safety device) around a 240V AC power supply the probability of contact with an energised conductor is reduced. The severity is unchanged.

Example

By changing from a high voltage (240V AC) to low-voltage (28V DC) power system (a design alternation), severity has been reduced. The probability of contact with an energised conductor is unchanged.
Define hazard controls

Hazard controls feasibility

What does feasibility mean?

A checklist:

- Is this countermeasure reasonably do-able?
- Is it available when needed?
- Does it pose installation difficulties?
- Will it interface with existing equipment?
- Does it pose unusual maintenance demands?
- Is staffing or equipment available for such demands?
- Does this countermeasure fit? can it be installed without forcing intolerable modifications to other equipment?
Define hazard controls

Hazard controls precedence

Some countermeasures are more effective than others, we work through the hierarchy of controls from the highest to the lowest.

<table>
<thead>
<tr>
<th>Code</th>
<th>Title</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>D</td>
<td>Design change</td>
<td><em>Eliminate</em> or <em>substitute</em> a less hazardous item</td>
</tr>
<tr>
<td>S</td>
<td>Safety barriers</td>
<td><em>Isolate</em> through fixed passive barriers</td>
</tr>
<tr>
<td>E</td>
<td>Engineering control</td>
<td><em>Control</em> through <em>engineered</em> active devices</td>
</tr>
<tr>
<td>W</td>
<td>Warning device</td>
<td><em>Control</em> through <em>engineered</em> warning devices</td>
</tr>
<tr>
<td>P</td>
<td>Procedures</td>
<td><em>Administrative</em> controls</td>
</tr>
</tbody>
</table>

Hierarchy of hazard controls and the law

Workplace Health and Safety legislation requires controls to be considered in priority order.
Hazard ameliorators

Some controls do not reduce the likelihood of a hazard occurring
Instead they reduce the severity of the *outcome*

Examples of such controls:
- fire suppression systems
- tank bunds and blast walls
- personnel protective equipment

Example
By placing an earth leakage detector on a 240V AC power supply the probability of contact with an energised conductor is unchanged. The control reduces the severity of the outcome
Documenting the analysis

1. Introduction
2. Overview
3. Methodology
4. Hazard identification
5. Evaluate risks
6. Define hazard controls
7. Documenting the analysis
8. Limitations, advantages and disadvantages
9. Conclusions
10. Further reading
The PHA report

Primarily driven by the PHA worksheet content, typically includes:

- Hazard descriptions (source, mechanism, outcome (TLM))
- Duration of exposure
- Type of hazard
- Targets (people, equipment etc)
- Subjective risk per hazard (Likelihood and Severity)
- Hazard controls
- Safety verification
- Actions required and clarifying notes
- Administrative details (ID, status, names etc)

There is normally a covering report or letter
Documenting the analysis

PHA worksheet

**Brief Descriptive Title (Portion of System/Sub-system/Operational Phases covered by this analysis):**
Pressurized UnFo₃ Containment and Replenishment Reservoir and Piping / Startup, Routine Operation, Standard Stop, Emergency Shutdown

**Probability Interval:** 25 years

**Date:** 25 Feb. 1993

**Risk Before**

<table>
<thead>
<tr>
<th>Hazard Target</th>
<th>Severity</th>
<th>Probability</th>
<th>Risk Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>P E T</td>
<td>I II III</td>
<td>D O C</td>
<td>2 3</td>
</tr>
</tbody>
</table>

**Description of Countermeasures**

Identify countermeasures by appropriate code letter(s):
- D = Design Alteration
- E = Engineered Safety Feature
- S = Safety Device
- W = Warning Device
- P = Procedures/Training

Surround flange with sealed annular stainless steel catchment housing with gravity runoff conduit led to Defecto-Box™ containing detector/alarm device and chemical neutralizer (S/W). Inspect flange seal at 2-month intervals, and re-gasket during annual plant maintenance shutdown (P). Provide personal protective equipment (Schedule 4) and training for response/cleanup crew(S/P).

**Risk After**

<table>
<thead>
<tr>
<th>Risk Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>I II III</td>
</tr>
</tbody>
</table>

**Prepared by/Date:**

**Target Codes:**
- P = Personnel
- E = Equipment
- T = Downtime
- R = Product
- V = Environment

**Approved by/Date:**

**Figure:** PHA worksheet [Clements 1996]
A PHA can produce a significant amount of data, organising principles are essential for a coherent end product

Some best practices

- Use the S-M-O model to describe hazards
- Where more than one mechanism with the same source may independently cause the same outcome (OR), treat as individual hazards
- Where more than one mechanism with the same source is required to cause an outcome (AND), treat as one hazard
- Develop a TLM list and associate each hazard with a TLM (the System Mishap Model)
- Describe hazards in sufficient detail so that meaningful likelihoods can be estimated
Limitations, advantages and disadvantages

1. Introduction
2. Overview
3. Methodology
4. Hazard identification
5. Evaluate risks
6. Define hazard controls
7. Documenting the analysis
8. Limitations, advantages and disadvantages
9. Conclusions
10. Further reading
Limitations, advantages and disadvantages

Limitations

The PHA is an upfront technique intended to identify hazards at a high level, by its nature not intended to deliver detailed causal reasoning sufficient to identify complex accident causes or assess risk quantitatively.

The objective of the PHA is to influence the design by establishing a set of safety requirements, it is not to define the subsequent implementation that satisfies those requirements.

The fidelity versus timeliness problem

Data available for the PHA is usually incomplete & informal during conceptual design. The analysis should be structured to allow for reviews and updating as the design matures.
Limitations, advantages and disadvantages

Advantages

A PHA can

- Provide a good launch for the safety program
- Be done early in the system development
- Provide an inventory of hazards, for a system
- Assess hazard risks in a *qualitative* fashion
- Establish the safety program baseline (with the SSPP)
- Provides management data on which to base decisions
- Identify incomplete requirements
Disadvantages

A PHA cannot

- Guarantee all hazards have been identified
- Provide a statement of total system risk (use a PRA)
- Evaluate the combined effects of common cause events
- Evaluate the combined effects of coexisting failures
Conclusions

1 Introduction

2 Overview

3 Methodology

4 Hazard identification

5 Evaluate risks

6 Define hazard controls

7 Documenting the analysis

8 Limitations, advantages and disadvantages

9 Conclusions

10 Further reading
Conclusions

A PHA has the lowest requirements for hazard analytical skills but also the highest payoff in terms of identifying and controlling risk.

The purpose of the PHA is *not* to affect control of all risks but to fully recognise the hazardous states and the system implications.

A single pass analysis provides no evidence of the completeness (or otherwise) of the PHA.

The PHA is the *start* of the safety program not the end, subsequent analyses will refine and modify the initial list of hazards.
Bibliography


