System Safety
M5 Energy Trace/Barrier Analysis V1.2

Matthew Squair
UNSW@Canberra
12 October 2015
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 Energy sources, barriers and targets

5 Manage hazardous energy flows

6 Limitations, advantages and disadvantages

7 Conclusions

8 Further reading
Introduction

Overview

Methodology

Energy sources, barriers and targets

Manage hazardous energy flows

Limitations, advantages and disadvantages

Conclusions

Further reading
Learning outcomes

To be able to appropriately apply the energy barrier analysis method as part of a hazard analysis

To understand the strengths and weaknesses of the method
Overview

Introduction

Overview

Methodology

Energy sources, barriers and targets

Manage hazardous energy flows

Limitations, advantages and disadvantages

Conclusions

Further reading
Overview

ET/BA is a qualitative known cause, unknown effect analysis methodology used to develop more detailed knowledge of hazards.

Hazards are identified by tracing flows of energy through a system.

Simple mishap model where mishap = unwanted transfer of energy[Nettney, Trost 1995]

**ET/BA accident model**

"unwanted transfer of energy that produces injury to persons or property is due to a lack of barriers or controls over the energy"
ET/BA is a useful analytical tool to use during the PHA

Forms the basis of methods such as Management Oversight and Risk Tree (MORT) [Johnson 1980] and Control Change Cause Analysis (3CA) methods

Fits well when dealing with energy transfer and containment where safe design relies on design margins and standards rather than probabilistic assessments of component failures
Key definitions

**Barrier.** A barrier contains an energy source or directs an energy flow, can be physical, temporal or procedural. Barriers can be classed as preventive or protective (A system with only preventive barriers is not fault tolerant)

**Energy Source.** The source of energy in the system energy can be potential, kinetic etc

**Target.** The recipient of the energy, either intended or inadvertent

**Hazard.** The potential for an uncontrolled energy flow or the potential for an inadvertent energy barrier

**ET/BA.** Energy Trace/Barrier Analysis. Note that terms such Energy Flow/Trace/Barrier Analysis are synonomous.
Methodology

1. Introduction
2. Overview
3. Methodology
4. Energy sources, barriers and targets
5. Manage hazardous energy flows
6. Limitations, advantages and disadvantages
7. Conclusions
8. Further reading
The basic question

"Where did this energy come from?" [Johnson 1980]

The basic steps

1. Trace the sequence & logic of energy flow through the system
2. For each energy type, track flow to each transfer or use point
3. Consider physical or procedural barriers to energy flow
4. Identify potential mishaps due to unintended energy flows or barriers
5. Assign hazard controls in the form of barriers/diverters
6. Evaluate barrier/diverter effectiveness
Consider barriers to energy flow

Each physical or procedural barrier to the energy must be considered to determine what harmful outcomes are likely to occur when:

- Too much or too little energy flows
- The energy flows too soon, too late, or not at all
- The energy flow is blocked or impeded in its pathway
- The energy flow conflicts with another energy flow at a transfer or use point
- A barrier degrades, is disturbed, or does not function
Identify potential mishaps

For a mishap to occur there must be either:

- an energy source with a release flow of energy to a target in the absence of adequate barriers, or
- a barrier which prevents the normal flow of energy between actors in the system

The flow or transfer of energy is the path between the energy source and the target or component of the operation being protected
Macfarland’s extension

Macfarland extended the basic model to include:

- Application of energy in amounts exceeding the resistance of the structures on which they impinge
- Interference in the normal exchange of energy between an organism and its environment (including lack of oxygen and exposure)

Systems components are active (produce energy) or inactive (constrain energy)
Energy sources

- Electrical
- Mechanical
- Thermal
- Pneumatic
- Chemical
- Radiation (ionising and non-ionising)
- Noise
- hydraulics
- ... many others
Barriers

Barriers vary widely as to their location, type, and function.

- **Function**:
  - Prevent
  - Control
  - Minimise

- **Location**:
  - On source
  - Between source & target
  - On target
  - Time/Space separation

- **Type**:
  - Physical
  - Procedural

Do they act as a path barrier or converter/router?
Barriers can include:

- Shielding
- distance/quantity rules
- Airbags/seat-belts
- Ablative coatings
- Paint
- Guard rails
- Interlocks
- Containment vessels
- ... many others
Targets

Can be people, equipment, materials or the environment (or a mixture of these)
Manage hazardous energy flows

Use barriers or diverters to:

- Exclude energy (disconnect energy source)
- Limit energy quantity in system (reduce voltage, pressure)
- Modify release of energy (flow restrictors, ground detectors)
- Prevent energy release (Interlocks, containment vessels)
- Separate energy & target in time/space (Q/D rule, RADHAZ rules)
- Strengthen potential target (Use F76 rather than F44 fuel)
- Modify target surface (Armour, airbags)
- Isolate by barrier (Guard rails, EMI shielding)
- Control improper energy inputs (Keyed connectors)
Limitations of the technique

ET/BA is a simple model of hazards and mishaps, it has it’s limitations:

- Focuses on energy flows so may miss non-energy flow hazards
- May not identify accidents caused by logical errors
- Focus is on controlling flows not on eliminating causal factors
- Doesn’t identify hazardous energy flow interactions (e.g. ignition sources and fuel vapour)

ET/BA is a simple technique

Don’t try to use ET/BA for complex or inappropriate scenarios, use other more appropriate techniques instead
Limitations, advantages and disadvantages
Advantages

The advantages of the technique are

- Simple
- Useful for day one of a hazard workshop
- Useful for process plants and systems
- Especially useful for energy containment and transfer systems
- Useful for EMC (RADHAZ, HERO, HERP & HERF) analysis
- Can easily derive useful metrics for overall system vulnerability
Disadvantages

The disadvantages of the technique are

- You can’t generate a likelihood of occurrence
- If there’s a plant control loop, you’ll need to use another method
- Tends to skew the focus towards consequences, versus causal factors
Conclusions

Introduction

Overview

Methodology

Energy sources, barriers and targets

Manage hazardous energy flows

Limitations, advantages and disadvantages

Conclusions

Further reading
Conclusions

The ETBA is a useful adjunct hazard analysis methodology for systems where the storage and transfer of energy is a critical part of operations. However, much like the PHA, the ET/BA cannot identify the combined effects of multiple component failures.
Bibliography


