

## Hazard and Operability Studies

**Clive Boughton**

### Why use it?

- **Codes of practice are not the whole answer to ensuring fulfilment of requirements and quality.**
- **Need to supplement CoP with imaginative anticipation of possible deviations from intent of solutions to requirements.**
- **Discover possible operator errors.**
- **Investigate possible impacts of system malfunction.**

Mike Lihou: <http://www.lihoutech.com/hzp1frm.htm>

## What is it?

- **Systematic questioning of every aspect of a model/design to establish how deviations from the intent of a design can arise.**
- **Assessment of discovered deviations (of design intent) and corresponding consequences for negative affects on safe and efficient system operation.**
- **Describing actions to remedy deviations (of design intent) that cause negative affects.**

Mike Lihou: <http://www.lihoutech.com/hzp1frm.htm>

## Essential Features

### Keywords - must be relevant to system

- **Primary - reflect design intent and operational aspects.**
- **Secondary - for suggestion of potential deviations.**

### Systematic approach.

- **Systematically applying all relevant keyword combinations to system in effort to discover potential problems.**

### Full recording.

- **Tabular record of: DEVIATION, CAUSE, CONSEQUENCE, SAFEGUARDS and ACTION.**

Mike Lihou: <http://www.lihoutech.com/hzp1frm.htm>

## Primary Keywords for a Chemical Plant

### Process-oriented:

<b>Flow</b>	<b>Pressure</b>	<b>Temperature</b>	<b>Level</b>
<b>Separate</b>	<b>Composition</b>	<b>React</b>	<b>Mix</b>
<b>Reduce</b>	<b>Absorb</b>	<b>Corrode</b>	<b>Erode</b>

### Operationally-oriented:

<b>Isolate</b>	<b>Drain</b>	<b>Start-up</b>	<b>Purge</b>
<b>Inspect</b>	<b>Maintain</b>	<b>Shutdown</b>	<b>Vent</b>

**Keywords are chosen according to the system being studied**

Mike Lihou: <http://www.lihoutech.com/hzp1frm.htm>

## Secondary Keywords for a Chemical Plant

### Used in conjunction with primary keywords:

<b>No</b>	<b>Less</b>	<b>More</b>	<b>Reverse</b>
<b>Also</b>	<b>Late</b>	<b>Early</b>	<b>Fluctuation</b>

**Not all combinations of primary and secondary keywords are appropriate**

Mike Lihou: <http://www.lihoutech.com/hzp1frm.htm>

## Systematic Approach

### **DEVIATION:**

The keyword combination being applied (e.g., Pressure/More)

### **CAUSE:**

Potential cause of deviation (e.g., High temperature)

### **CONSEQUENCE:**

From effect of deviation, and the cause itself (if appropriate)

### **SAFEGUARDS:**

Any protective device that prevents the cause or safeguards against the adverse consequences of the deviation

### **ACTION:**

- ▶ Remove the cause
- ▶ Mitigate or eliminate the consequences

Mike Lihou: <http://www.lihoutech.com/hzp1frm.htm>

## Example

### **HAZOP Study for Train-Carried ATP System**

### **Appendix B of Defence Standard 00-58 (2000)**

### Use of Data / Control Flow Diagram (Hatley/Pirbhai)

- **DFD:**
  - Contain data flows and processes
- **CFD:**
  - Contain control / event flows, processes and control specifications (any combination of STD, DT and PAT)
- **Actions:**
  - Primitive processes
  - Transitions in STD
  - DT output
  - PAT output

See DEF STAN 00-58 Annex A

### Use of Object-Oriented Diagrams (Shlaer/Mellor)

- **Information Diagram:**
  - Contains objects and relationships
- **State Transition Diagram (More):**
  - Contains states (actions), transitions and events
- **Object Communication Diagram (Asynchronous):**
  - Contains objects with lifecycles, external entities and events (communications)
- **Object Access Diagram (Synchronous):**
  - Contains objects, external entities and process names (accesses)

See DEF STAN 00-58 Annex A



# HAZOP & DEF STAN 00-58 (1)

**Example Attribute-Guide-Word Interpretations for Data /Control Flow Diagrams (Hatley/Pirbhai)**

Attribute	Guide Word	Interpretation
Flow (Data/Control)	No	No information Flow
	More	More information passed than expected
	Part Of	Incomplete information passed (group flow)
	Reverse	Information flow in wrong direction
	Other Than	Information complete, but incorrect
	Early	Information flow occurs before intended
	Late	Information flow occurs after intended
Data Rate	More	Data rate is too high
	Less	Data rate is too low
Data Value	More	Data value too high (in or out of bounds)
	Less	Data value too low (in or out of bounds)



# HAZOP & DEF STAN 00-58 (2)

**Example Attribute-Guide-Word Interpretations for State Transition Diagrams (Mealy)**

Attribute	Guide Word	Interpretation
Event (Control Flow)	No	Event does not occur
	As Well As	Another event also takes place
	Other Than	An unexpected event occurs instead of the anticipated event
Action	No	No action occurs
	As Well As	Additional (unwanted) actions occur
	Part Of	An incomplete action is performed
	Other Than	An incorrect action occurs