Human Performance during Operating Events: Can Advanced Technologies Help?

Presented by
Dennis Bley, Buttonwood Consulting, Inc.
Albuquerque, NM

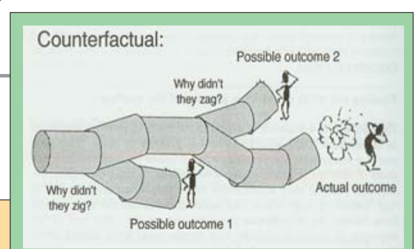
RIC 2018
Session on Advanced Technologies in Plant Operations
Operational and Safety Implications Identified through
Experimentation and Control Room Modernization Efforts

bley@buttonwoodconsulting.com

Introduction to session and motivation for discussion

- My background: operations, PRA & HRA
  - Helped develop ATHEANA, aspects of IDHEAS, & older methods
  - Supported many applications of PRA & HRA
- Focus: examine real-world events to help improve operations, PRA & HRA, and design
- Question: what can developers do to help operators determine accurate situation assessments, detect mismatch between their assessment and procedures & plans, and get early warning if the current plan is not going in the right direction?

Framing human error*



The New View of Human Error:

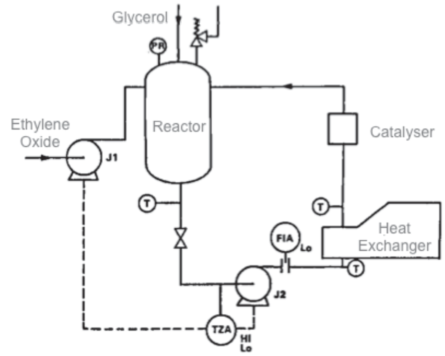
Human error is a symptom of trouble deeper inside a system

To explain failure, do not try to find where people went wrong

Instead, investigate how people's assessments and actions would have made sense at the time, given the circumstances that surrounded them

*_The Field Guide to Human Error Investigations_, Sidney Dekker

Human reliability
human-system interactions

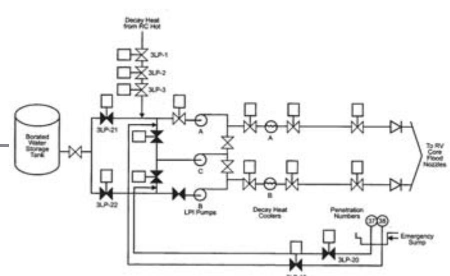


Taken from Trevor A. Kletz, What Went Wrong? Case Histories of Process Plant Disasters, Gulf Publishing Co. London, 1985. Explosion at ICI Batch Reactor.

Explosion at ICI batch reactor

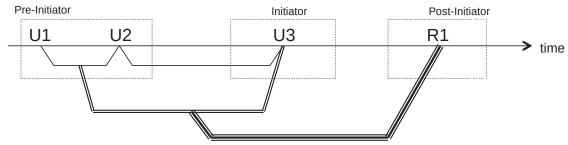
Circumvention	Operated system with no flow indication
Regime not understood	Invented rationale for why ethylene oxide not reacting
Refusal to believe evidence	Raised indicated temperature above limits because instrument "must" be wrong; opened suction valve without understanding consequences

PWR event at shutdown



- DHR cooling via LPI pump A,
  RV head off and level 12 ft above core,
- Blind flange on tailpipe of LP recirculation sump suction valve 3LP-19
- Just as test of valve begins, other problems draw operators attention:
  - Minor alarm
  - RV level 20" & decreasing - having problems with erroneous transmitter
  - RB normal sump alarm - washdown operations in progress
  - RV ultrasonic level alarm - investigate cause/enter AP "Loss of LPI in DHR mode"
  - HP in RB verifies drop in level & increasing radiation
  - LPI pump A current fluctuating downward - stop pump & open BWST suction valves
  - RCS not refilling - reclose BWST valves & send NLO to close 3LP-19 or 20

Human dependencies & surprises



U1. Blind flange for LPI sump suction installed on wrong line – LATENT ERROR
U2. Subsequent checking failed to detect incorrect flange installation – LATENT ERROR
U3. RCS drained through unblanked sump line - INITIATOR
R1. Operators isolate drainpath, restore RCS level, & restore DHR (including pump venting) RECOVERY

- Dependencies among HFEs can exist over days and weeks and can require powerful contrary evidence to break through a strong mindset because of a mistaken situation model⇨Context Important

THORP leak

- April 20, 2005 - camera inspection revealed 22,800 gal. dissolver liquor (19 T U) in cell that should be dry
  - 2 accountancy tanks
  - Initial design lateral restraints to limit tank movement
  - Changed later w/o appreciation of fatigue cracking, although tanks vibrate during processing to agitate contents
- Appears that one tank began to leak in mid-2004 & failed catastrophically in January 2005
  - Leakage not detected until April, despite a variety of indications over time that were ignored by ops & others

THORP event evaluated vs. behaviors seen in many serious accidents

- Design changes w/o recognition of safety implications
- Disregard of indications of problems
  - Sump level (safety case parameter)
    - instrument known to be faulty; history of false alarms
    - erratic indications, including a step jump in January
  - Sump temperature
    - continued to indicate abnormally high
    - not used by operators routinely
  - Sump materials samples
  - Material balance calculations
    - discrepancies up to 9% (limit 5%) dismissed "erroneous calculations"
- Belief that nothing cold go wrong
- History of ineffective corrective actions

Conclusions
Human actions & serious accidents

Serious accidents often involve human "error"

Operators act rationally

Operators are set up to fail by context, i.e., complicating physical conditions and complicating human conditions

Human performance is a multidisciplinary problem

Let's illustrate with one more real-world example

Robinson fire

- Latent Failures
  - Hardware
    - Breaker indicator light out (no control power for five months)
    - Installation errors (feeder cable; I&C jumpers for CP suction shift)
    - CCW return valve no auto open—simulator and procedure wrong
  - Operations & training
    - 86 Relay training incorrect
    - Non-standard crew led to unfulfilled assumptions & miscomunication
- Macro-cognitive problems during event
  - Lack of effective command and control
  - Training bias
  - Incomplete situation assessment
  - Operator errors