Human Error in Risk Assessment and Safety Management Systems

Chris Johnson

University of Glasgow, Scotland.
http://www.dcs.gla.ac.uk/~johnson

3rd May 2003

Glasgow Accident Analysis Group

The Queen's Anniversary Prizes
for Higher and Further Education
1998

Some Changes

- After the first few days:
  - More individual exercises;
  - More on automated systems;
  - Less on techniques….
- I'll put the revised notes on the web.

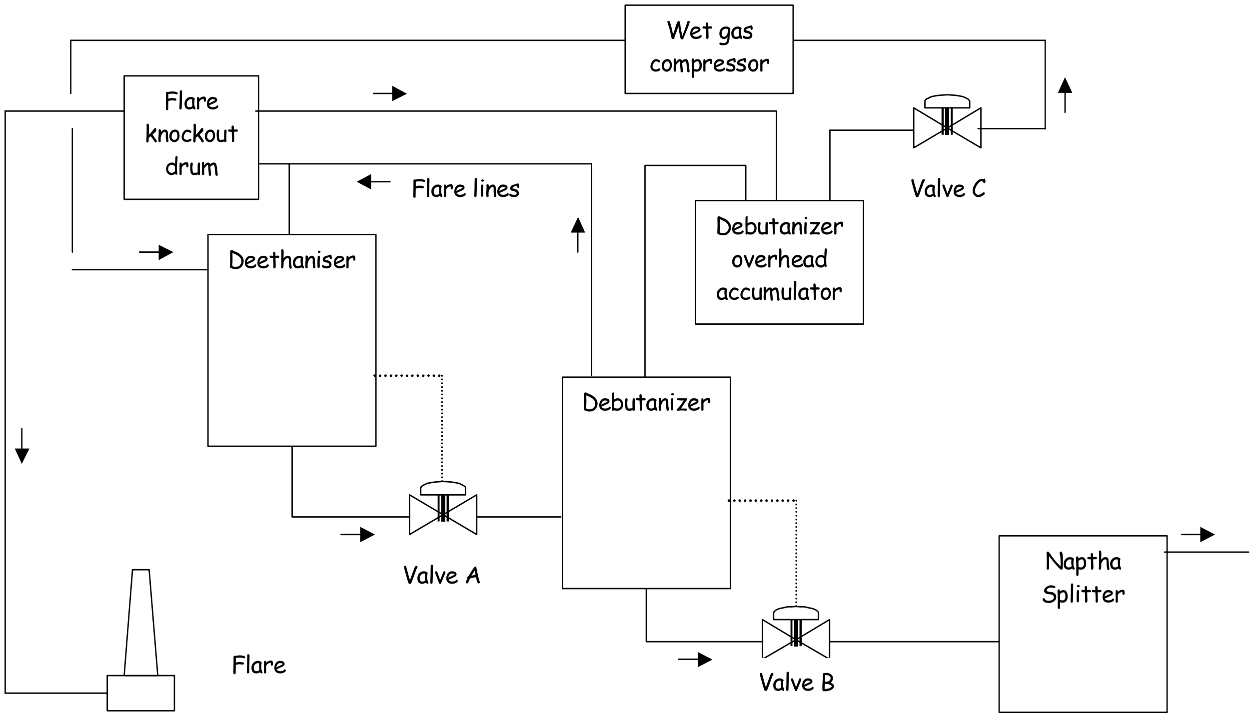
Overview

- Key topics:
  - What is human error?
  - Human error in risk assessment.
  - Human error in safety management.

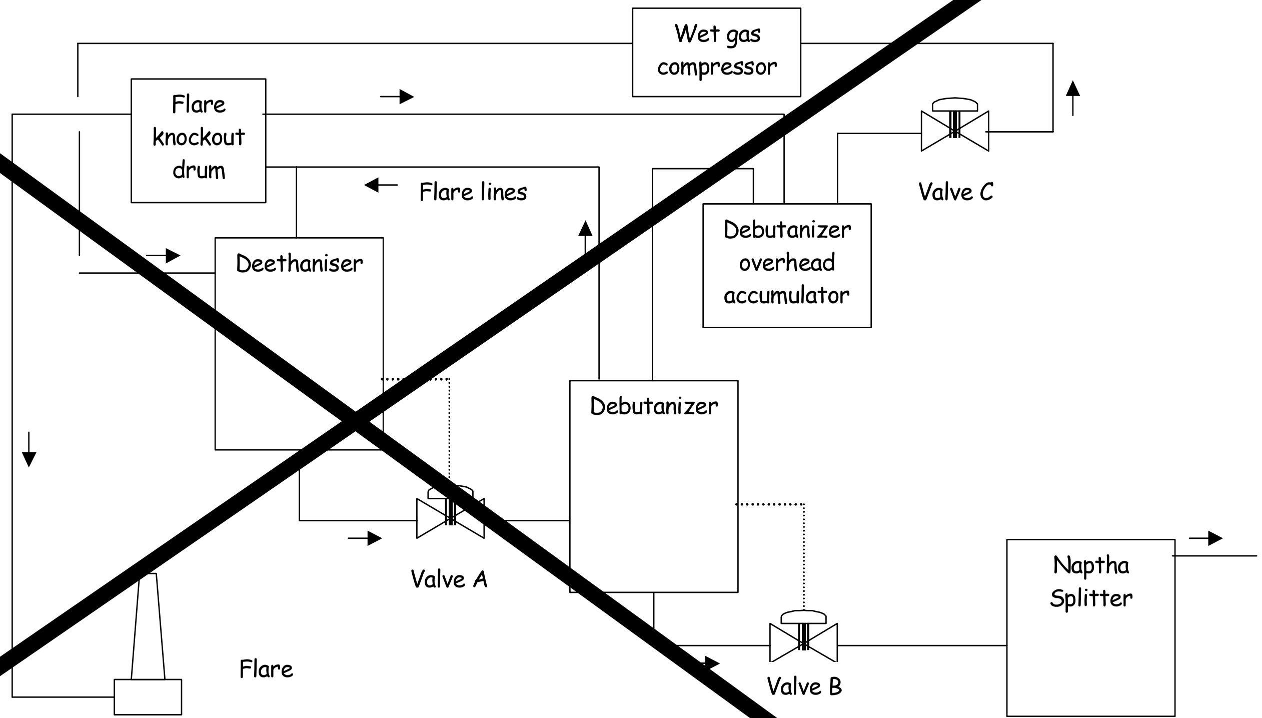
Timetable

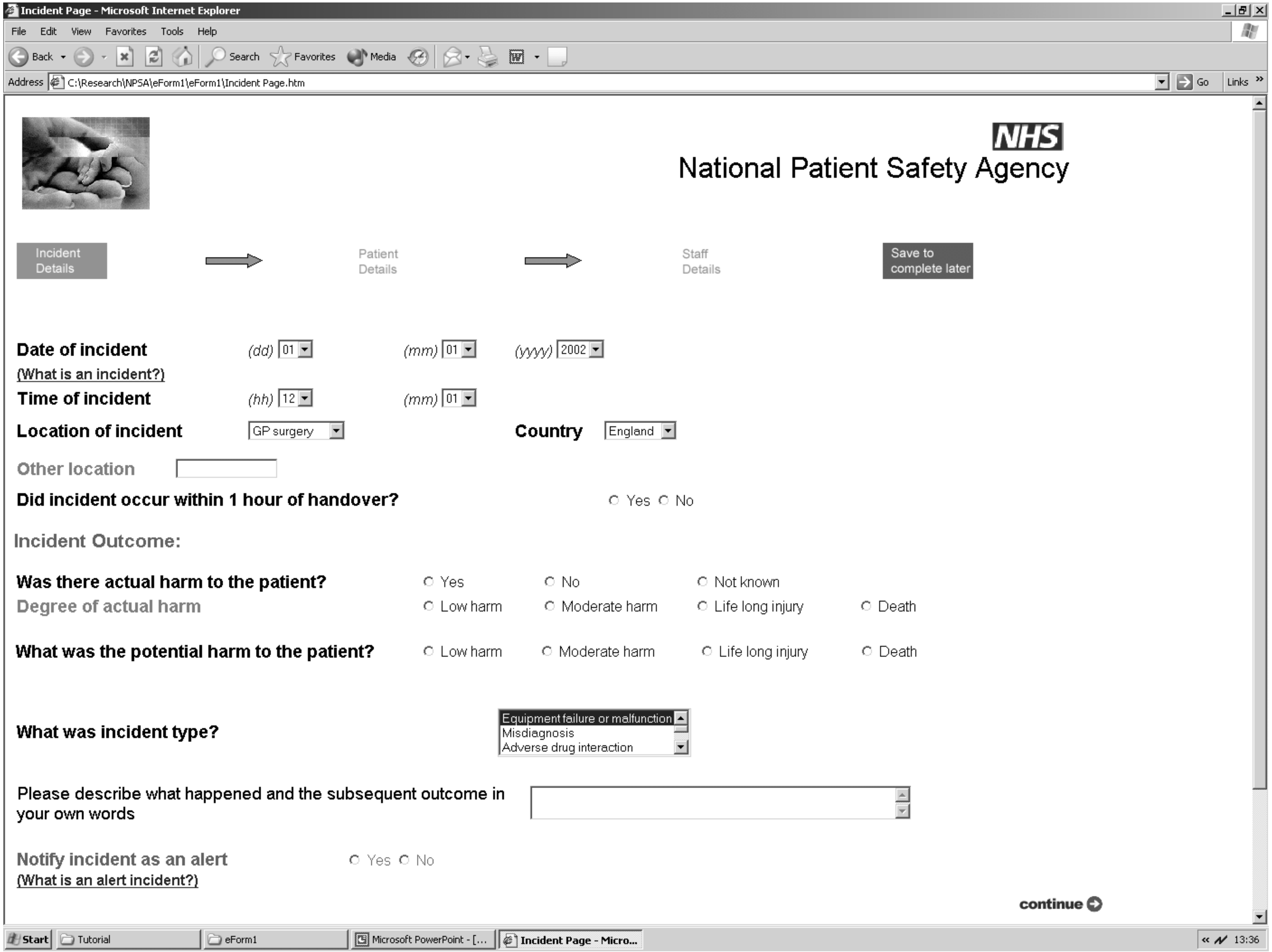
- 08.00 – registration
  - 08.30-09.30 – What is human error?
    - 09.30-10.00 – Break and group session 1 (TRIPOD analysis).
  - 10.00-11.00 - Human error & Risk analysis.
    - 11.00-11.30 – Break and group session 2 (FMECA study).
  - 11.30-12.30 - Human reliability analysis.
    - 12.30-13.00 – Break and group session 3 (HRA exercise).
  - 13.00-14.00 - Human error & Safety management.
    - 14.00-14.30 – wrap-up
- 14.30 Lunch

Motivation: Milford Haven

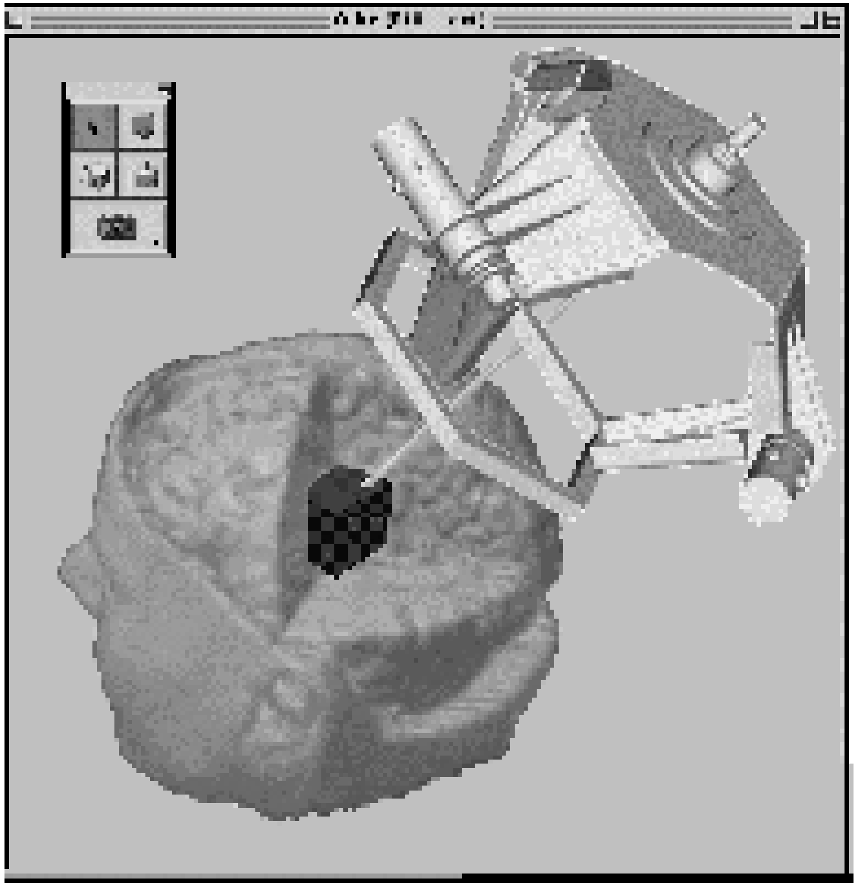


Motivation: Milford Haven





Incident Page - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address C:\Research\NPSA\eForm1\eForm1\Incident Page.htm
Go Links
NHS
National Patient Safety Agency
Incident Details
Patient Details
Staff Details
Save to complete later
Date of incident (dd) 01 (mm) 01 (yyyy) 2002
(What is an incident?)
Time of incident (hh) 12 (mm) 01
Location of incident GP surgery
Country England
Other location
Did incident occur within 1 hour of handover? Yes No
Incident Outcome:
Was there actual harm to the patient? Yes No Not known
Degree of actual harm Low harm Moderate harm Life long injury Death
What was the potential harm to the patient? Low harm Moderate harm Life long injury Death
What was incident type?
Equipment failure or malfunction
Misdiagnosis
Adverse drug interaction
Please describe what happened and the subsequent outcome in your own words
Notify incident as an alert Yes No
(What is an alert incident?)
continue
Start Tutorial eForm1 Microsoft PowerPoint - [... Incident Page - Micro...
13:36



- **Roboscope**
  The removal of deep-seated brain tumours requires endoscopic surgery and high precision. As part of a multi-national European project, a robot is being developed that holds an endoscope and allows a surgeon to manipulate it within the brain. The robot constrains motions to a specific region using the Active Constraint principle. This project is multi-disciplinary and involves MRI processing, ultrasound guidance, robotics and visualisation.

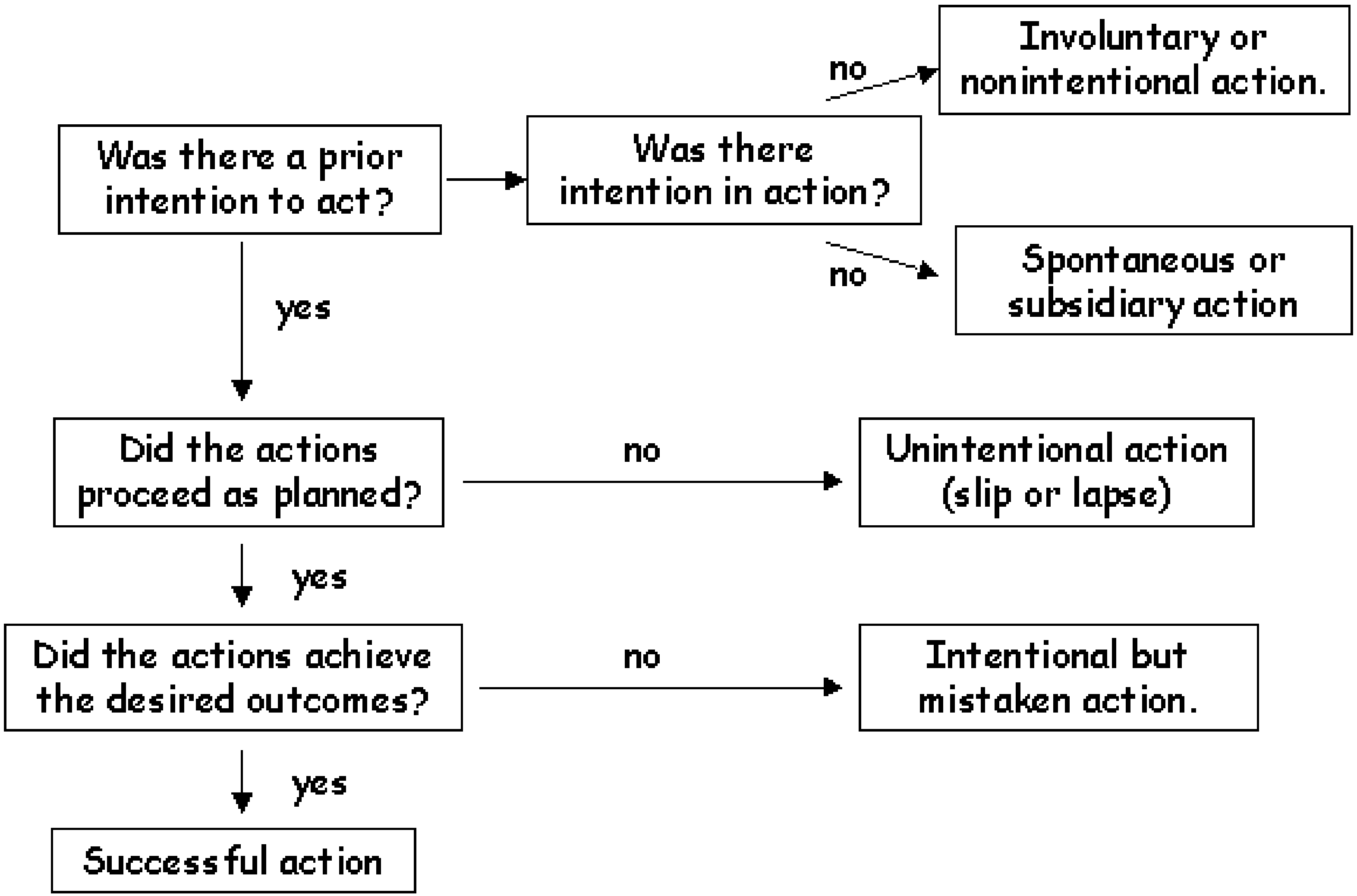
  (http://www.me.ic.ac.uk/case/mim/)

Part 1

> 1. What is human error?

2. Human error in risk assessment.
3. Human Reliability Analysis techniques.
4. Human error in safety management.

Individual Human Error



Determining System Inadequacy(ies) Responsible for Human Error

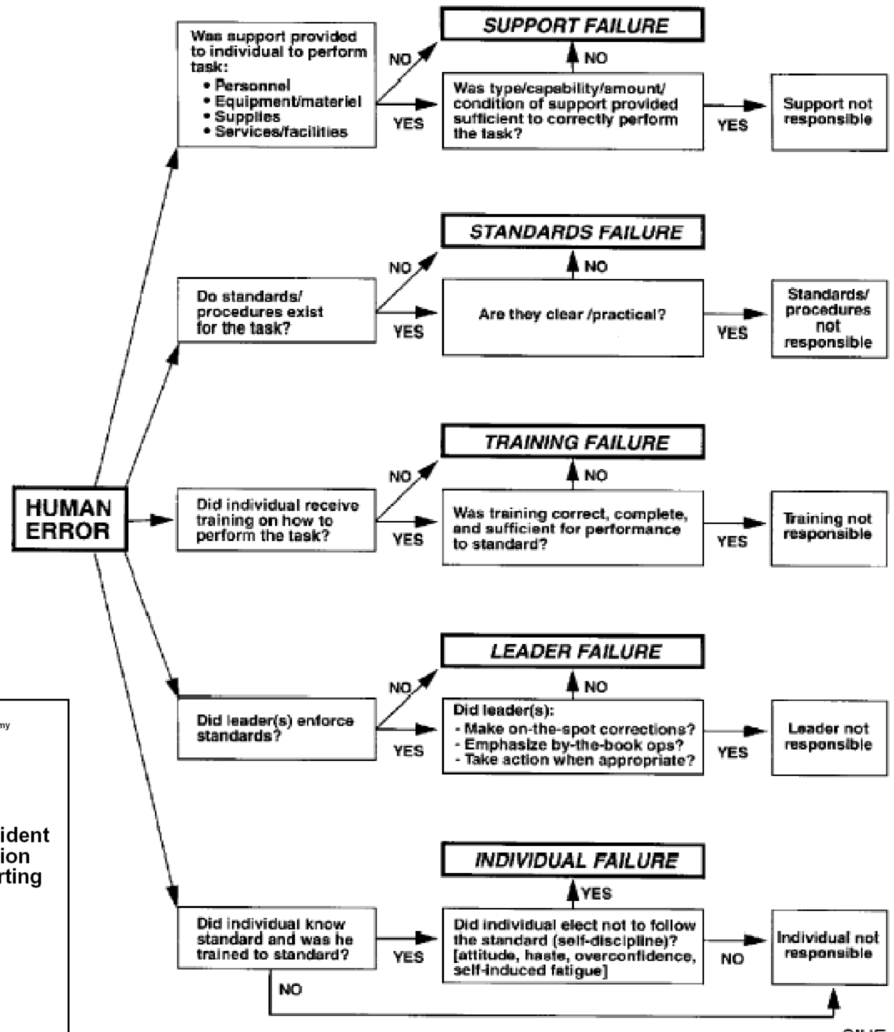
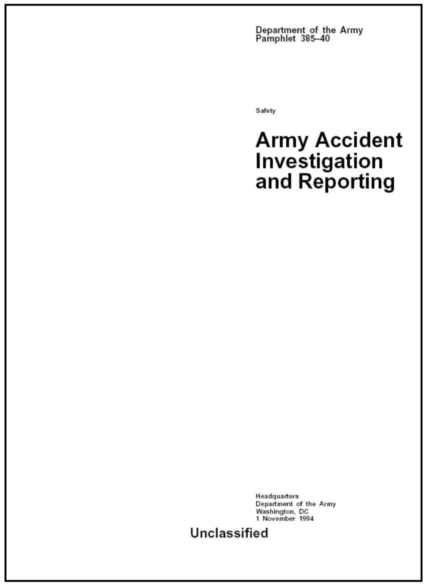


Figure 2-1. Determining system inadequacy(ies) responsible for human error


Department of the Army Pamphlet 385–40

Safety

Army Accident Investigation and Reporting

Headquarters Department of the Army Washington, DC 1 November 1994

Unclassified

System Inadequacies/Readiness Shortcomings/Root Causes

LEADER FAILURE
Code: 01 Key Word/Explanation: Inadequate/improper supervision by higher command.
Code: 02 Key Word/Explanation: Inadequate/improper supervision by staff officer.
Code: 03 Key Word/Explanation: Inadequate/improper supervision by unit command.
Code: 04 Key Word/Explanation: Inadequate/improper supervision by direct supervisor/noncommissioned officer in charge/platoon leader/instructor. NOTE: Inadequate supervision becomes a root cause when it leads to accident–causing personnel mistakes or materiel failure/malfunctions. Inadequate supervision is more clearly identifiable at the immediate–supervisor level.

INDIVIDUAL FAILURE
Code: 15 Key Word/Explanation: Fear/Excitement/Anger (inadequate composure). Each person is a part of the system. Therefore, his state of mind is a system element. Inadequate composure is a temporary state of mind that becomes a root cause when a person makes an accident–causing error because of fear, excitement, or some related emotional factor made clear, rational thought impossible.
Code: 16 Key Word/Explanation: Overconfidence/complacency in abilities. Overconfidence is a temporary state of mind that becomes a root cause when an accident is caused by a person's unwarranted reliance on: his own ability to perform a task, the ability of someone else to perform a task, the performance capabilities of equipment or other materiel.
Code: 17 Key Word/Explanation: Lack of confidence. Lack of confidence is a

Table B–5
System Inadequacies/Readiness Shortcomings/Root Causes—Continued

temporary of mind that becomes a root cause when an accident is caused by a person's unwarranted lack of reliance on: his own ability to perform the task, the ability of someone else to perform the task, the performance capabilities of equipment or other materiel.
Code: 18 Key Word/Explanation: Haste/Attitude (poor motivation). Haste/attitude (poor motivation) is a temporary state of mind that becomes a root cause when a person makes an accident–causing mistake because he/she is in a hurry (haste), or has a poor/bad attitude.
Code: 19 Key Word/Explanation: Fatigue (self–induced). Fatigue is a temporary physical and/or mental state that becomes a root cause when a person makes an accident–causing error because of reduced physical or mental capabilities resulting from previous activity and/or lack or rest.
Code: 20 Key Word/Explanation: Effects of alcohol, drugs, illness. The temporary effects of alcohol, drugs, or illness become a root causes when a person makes an accident–causing error because of reduced physical or mental capabilities resulting from one or more of these effects.
Code: 21 Key Word/Explanation: Environment conditions. Unknown or unavoidable conditions, which result in materiel failure or induce human error.
Code: 97 Key Word/Explanation: Insufficient information to determine system inadequacy/cause.

Human Error in Teams

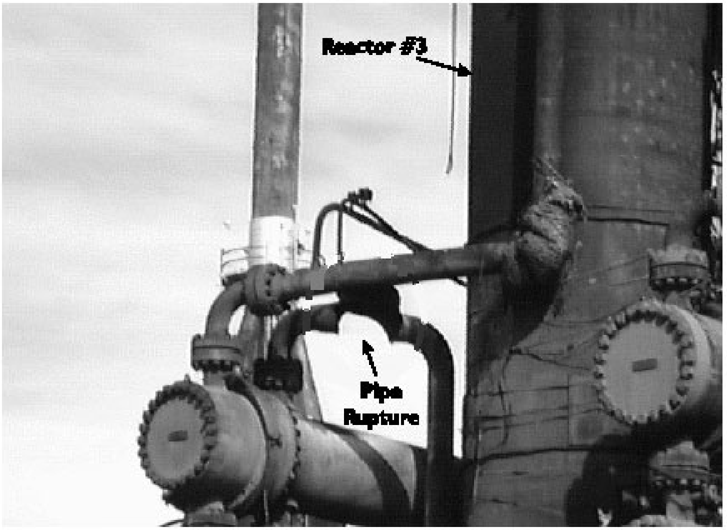
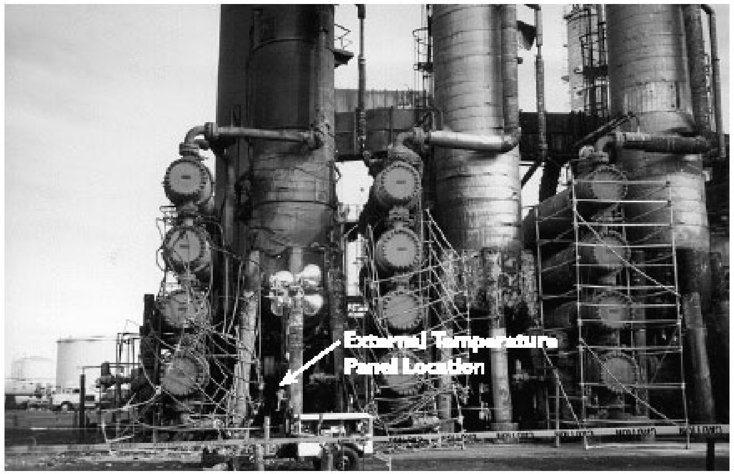


Figure 10 Reactor 3 Effluent Piping Rupture

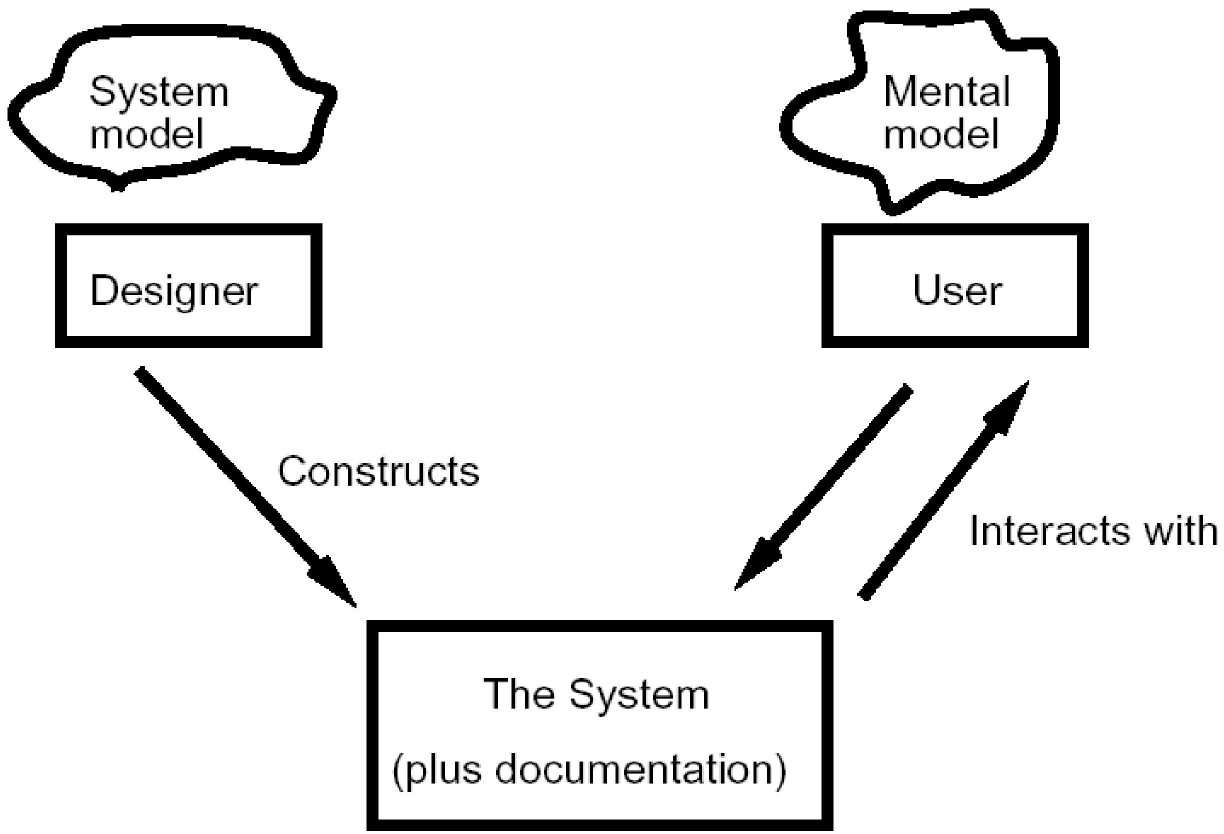


- Tosco Avon Refinery, California.
- Hydrocracker kills 1 and 46 injured.
- Reactor temperature ruptures effluent pipe.
- SOP required users to depressurize 2nd reactor:
  - if temperatures exceeds 800F.
  - But operators unsure what was occurring.
- Operator reading field panels under reactors.

"operators heard a radio message from the No. 2 Operator that was garbled and unclear. The Operator thought he heard "1250" on the radio, but wasnt sure. Two unsuccessful attempts were made to contact him. Two operators went outside to check on him. The reactor outlet temperature reading on the data logger defaulted to 0 at 7:39:40 pm."

- http://www.epa.gov/ceppo/pubs/tosco.pdf

Human Error and Technology



Human Error and Technology

- Shell Deer Park plant.

- Operators know startup SOPs if conditions normal.
- SOPs didn't cover unexpected *eg* compressor trips.
- Foremen and operators used their own discretion.
- Quickly re-start compressor after high-vibration trip.
- Should check for suction check valve's imminent failure.

- Once leak had occurred:
  - no control room indications of leak, delays operator shut down of system.
  - poor communications add to severity, hinders control room operators.

http://yosemite.epa.gov/oswer/ceppoweb.nsf/vwResourcesByFilename/shellrpt.pdf/$File/shellrpt.pdf

Human Error and Technology

Fishing boat 0.35 miles from rig, auto. radar alarm at 0.3 miles.

VHF radio off because skipper said too much distraction.

Stand-by vessel finds nobody on bridge/deck after sounding horns.

Rig goes to ‘abandon platform stations’ as a precautionary measure.

Support vessel crew find skipper asleep.

Skipper complains about being woken, says its ‘under control’.

(MAIB, 2002b).

09.30-10.00:
Break and group session 1 (incident analysis).

TRIPOD

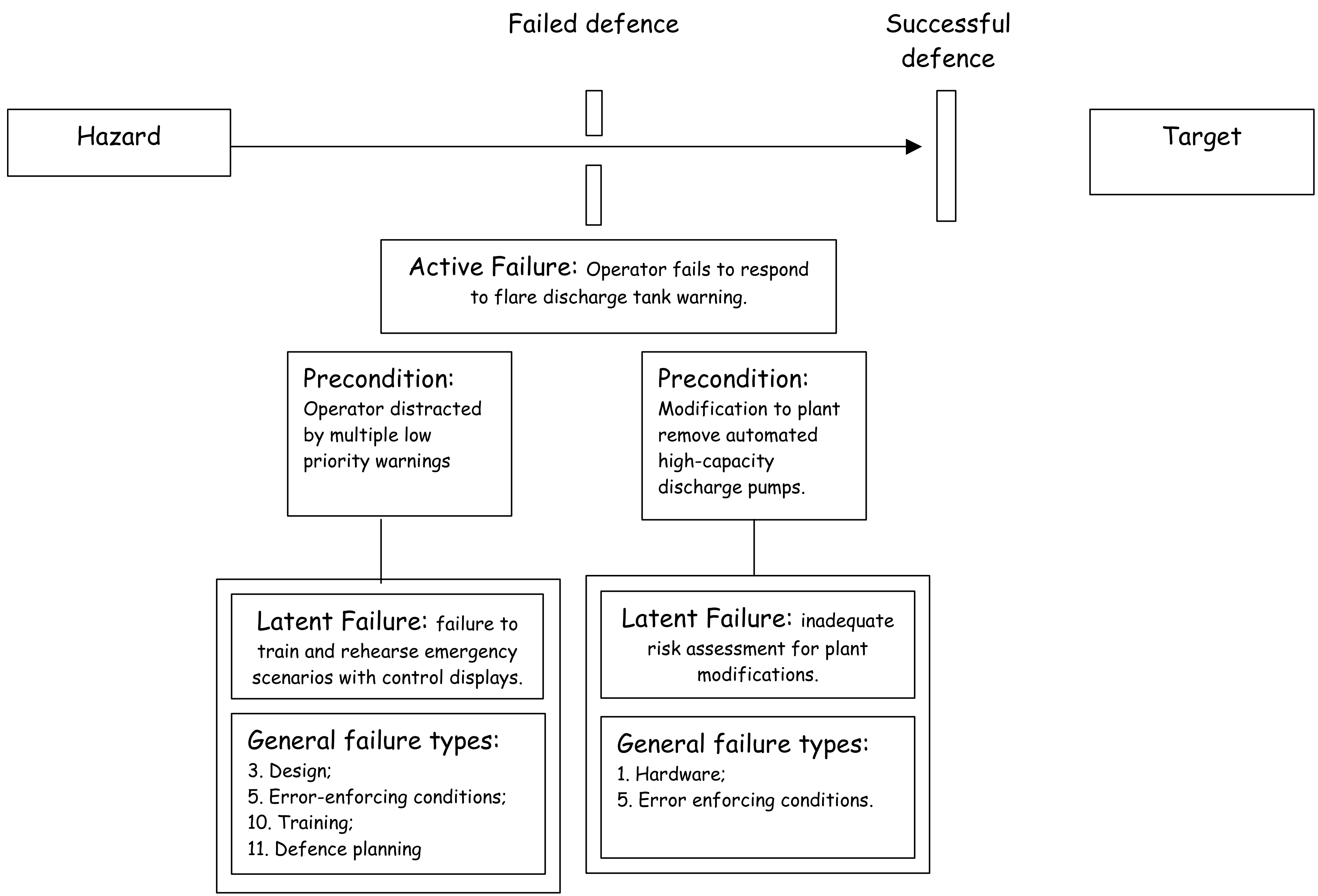
- Developed for Shell Exploration & Production.

- Two different versions:
  - Delta used for proactive safety management;
  - Beta used for incident investigation.

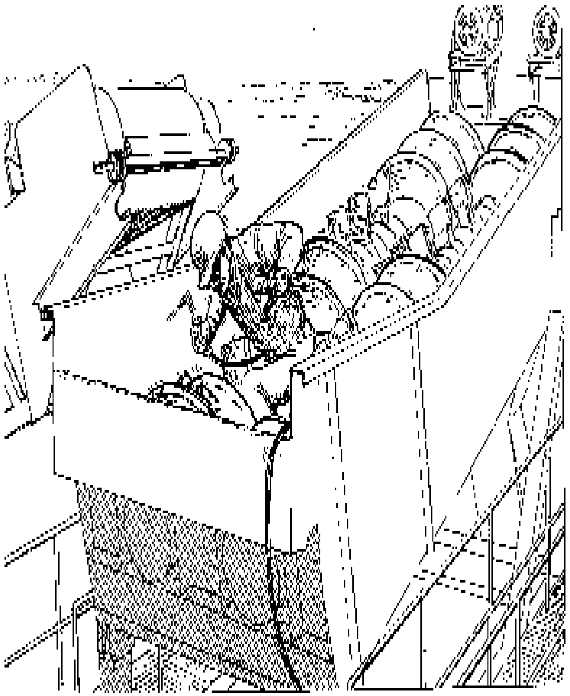
- For more information see:
  - J. Reason, *Managing the Risks of Organisational Accidents*, Ashgate, 1997, ISBN 1-84014-105-0.

TRIPOD

- General Failure Types:
  1. Hardware
  2. Maintenance management.
  3. Design.
  4. Operating procedures.
  5. Error-enforcing conditions.
  6. Housekeeping
  7. Incompatible goals
  8. Communication
  9. Organisation
  10. Training
  11. Defence planning


Failed defence
Successful defence
Hazard
Target
Active Failure: Operator fails to respond to flare discharge tank warning.
Precondition: Operator distracted by multiple low priority warnings
Precondition: Modification to plant remove automated high-capacity discharge pumps.
Latent Failure: failure to train and rehearse emergency scenarios with control displays.
General failure types:
3. Design;
5. Error-enforcing conditions;
10. Training;
11. Defence planning
Latent Failure: inadequate risk assessment for plant modifications.
General failure types:
1. Hardware;
5. Error enforcing conditions.

Case Study Incident



Blade mill pre-conditions aggregates before wet screening.

Consists of 2 screws driven by 2x40-horse power motors.

Spiral grooves interlocked to help prepare the gravel.

Motors operated by control centre in trailer 30m from mill.

US Dept. of Labor, Mine Safety and Health Administration.
http:www.msha.gov/FATALS/1997/FTL97M01.HTM

Case Study Incident

- Mechanic and foreman thaw frozen material inside mill, replace paddle tips etc.
- Mechanic signals foreman in control center to start motors to see if blades free.

- Motors start, so foreman leaves on another task away from mill.
- Before leaving, he switched mill's start/stop buttons to 'off' position.
- Foreman returns to help but called to assist electrician with faulty circuit breaker.

- Electrician switches breaker 'on' and they watched it for several minutes with no trip.
- Electrician turns it off, begins to diagnose problem, foreman returns to check mechanic.

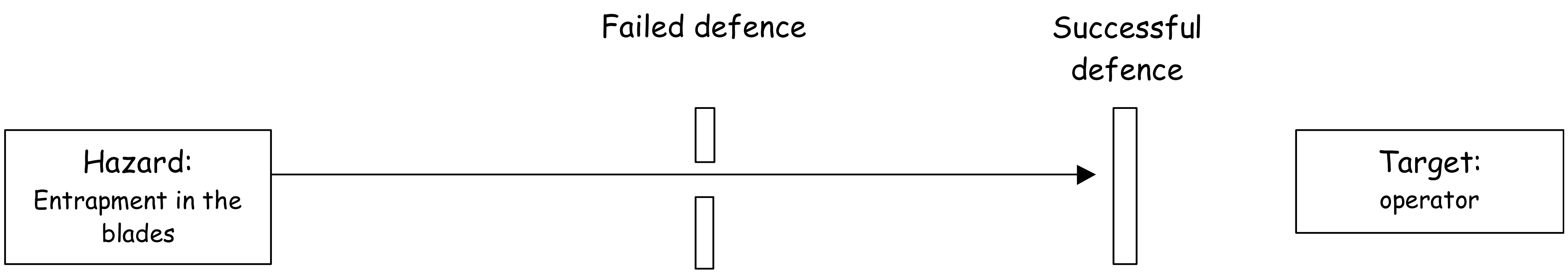
- On leaving control center, foreman noticed two blade mill buttons in "run" position.
- Pushed them "off", goes to mill where he found mechanic in the blades.

Case Study Incident

- Mechanic starts mill to clear frozen material after foreman left on 1st task away from mill.
- Blades work as mechanic expects but circuit breaker trips, before electrician’s inspection.
- For some reason, mechanic goes back to work in mill without shutting off any switches.
- Faulty breaker controls center lighting & Programmable Logic Controller (PLC) mill control.
- PLC modification, power unintentionally returned after power down if switches left "on".
- Mill operates when breaker reset during troubleshooting by foreman and electrician.

Your Task

- INDIVIDUALLY or in pairs.
- Use TRIPOD on case study.
- Identify failed barriers, latent failures…
- Here we use it post hoc but can guide design.
- How?



Active Failure: Mechanic works on blades when motor buttons are in 'on' position

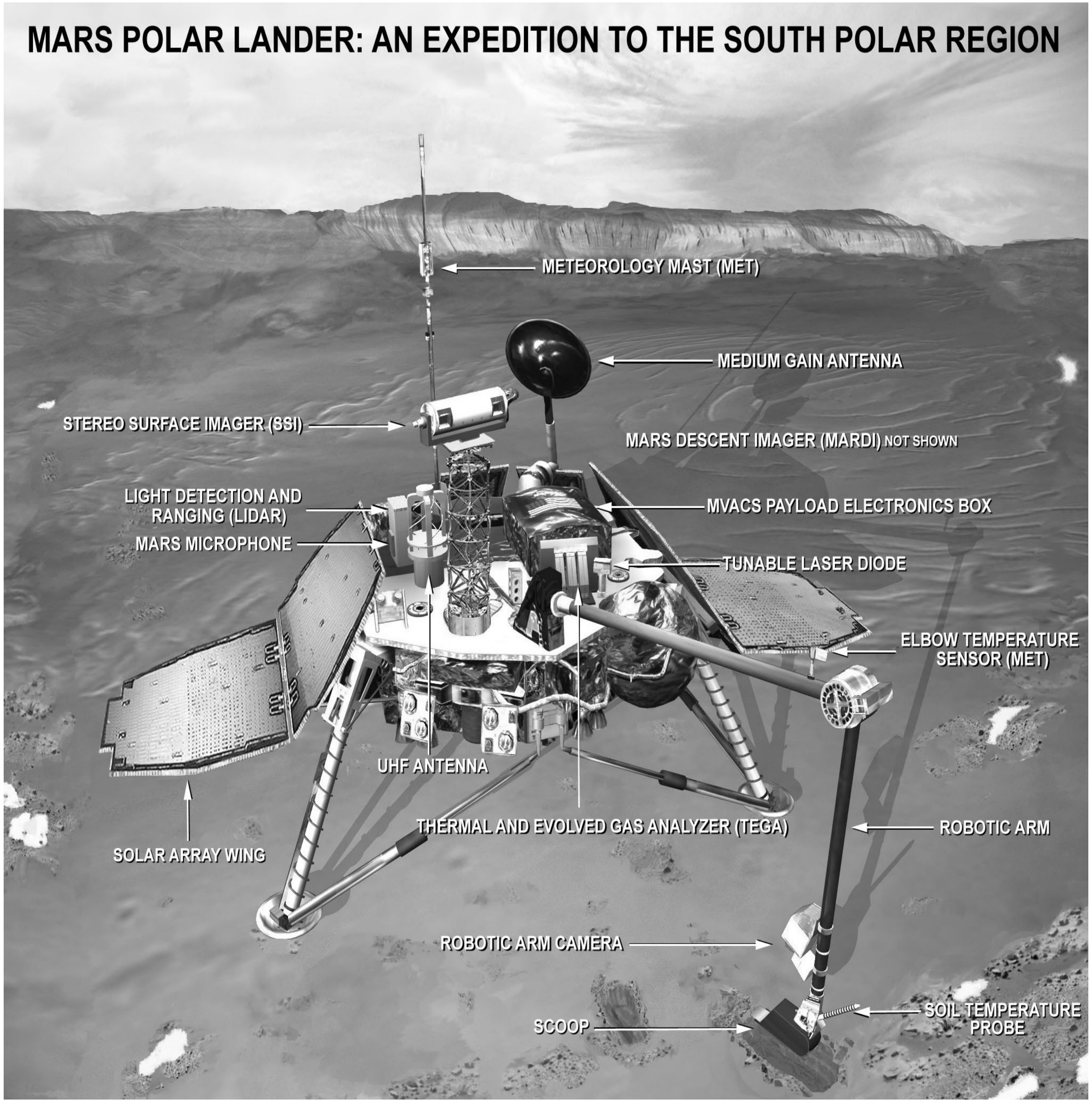
Precondition: mechanic believes motor is disabled.

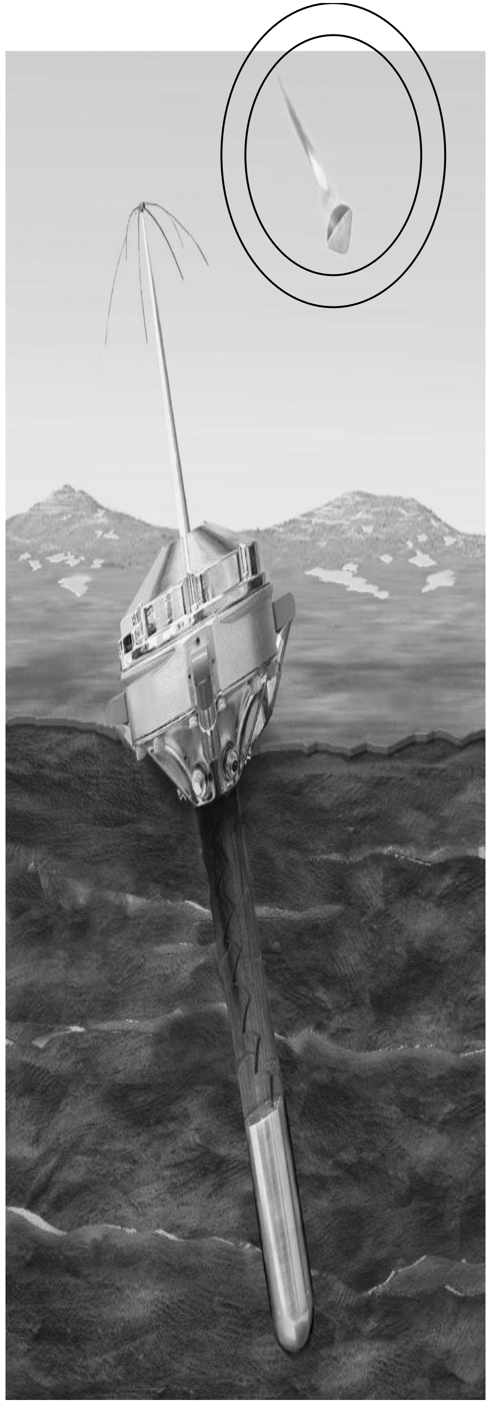
Latent Failure: blade motor controls not visible from mill.

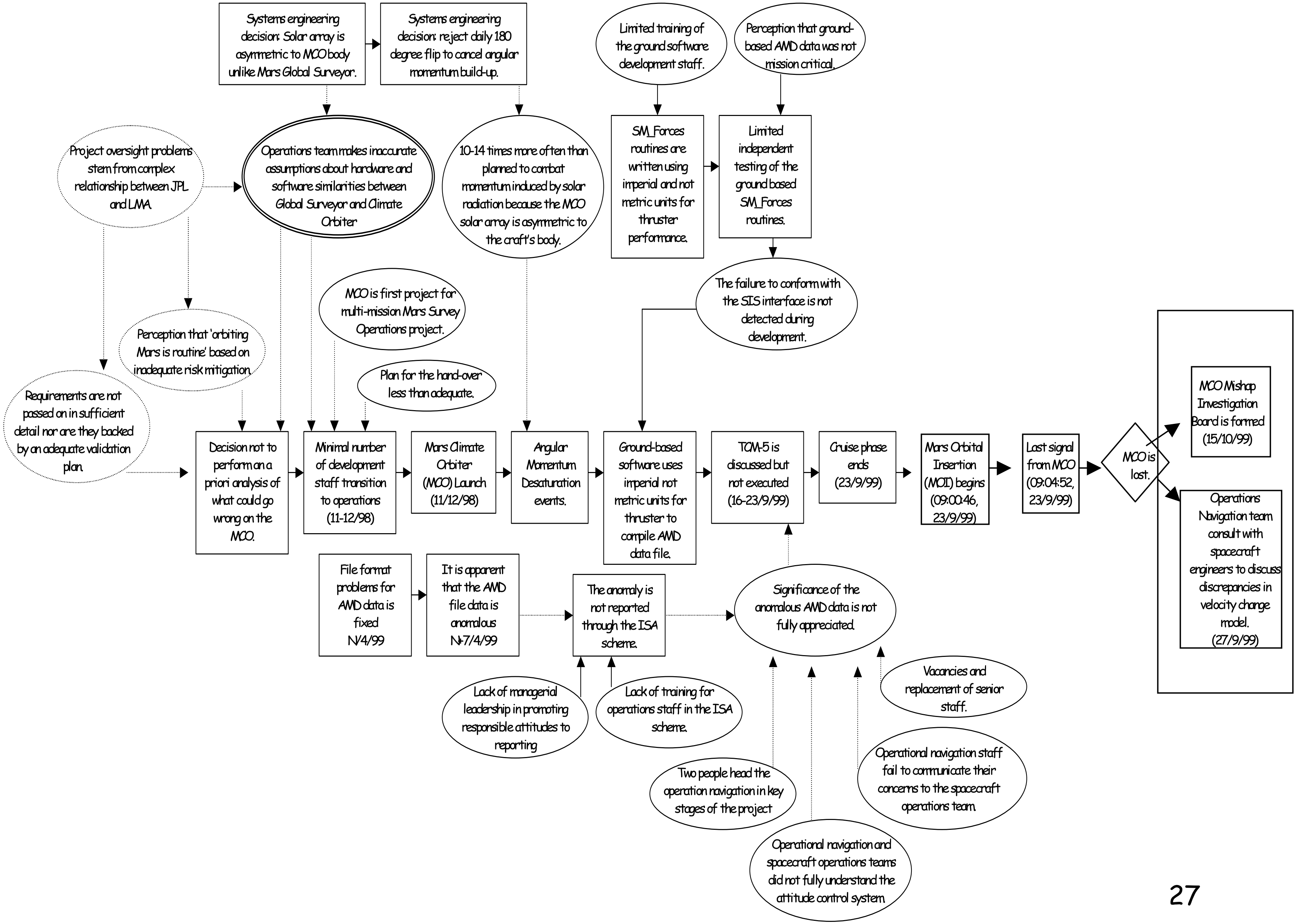
General failure types:
3. Design
5. Error enforcing conditions

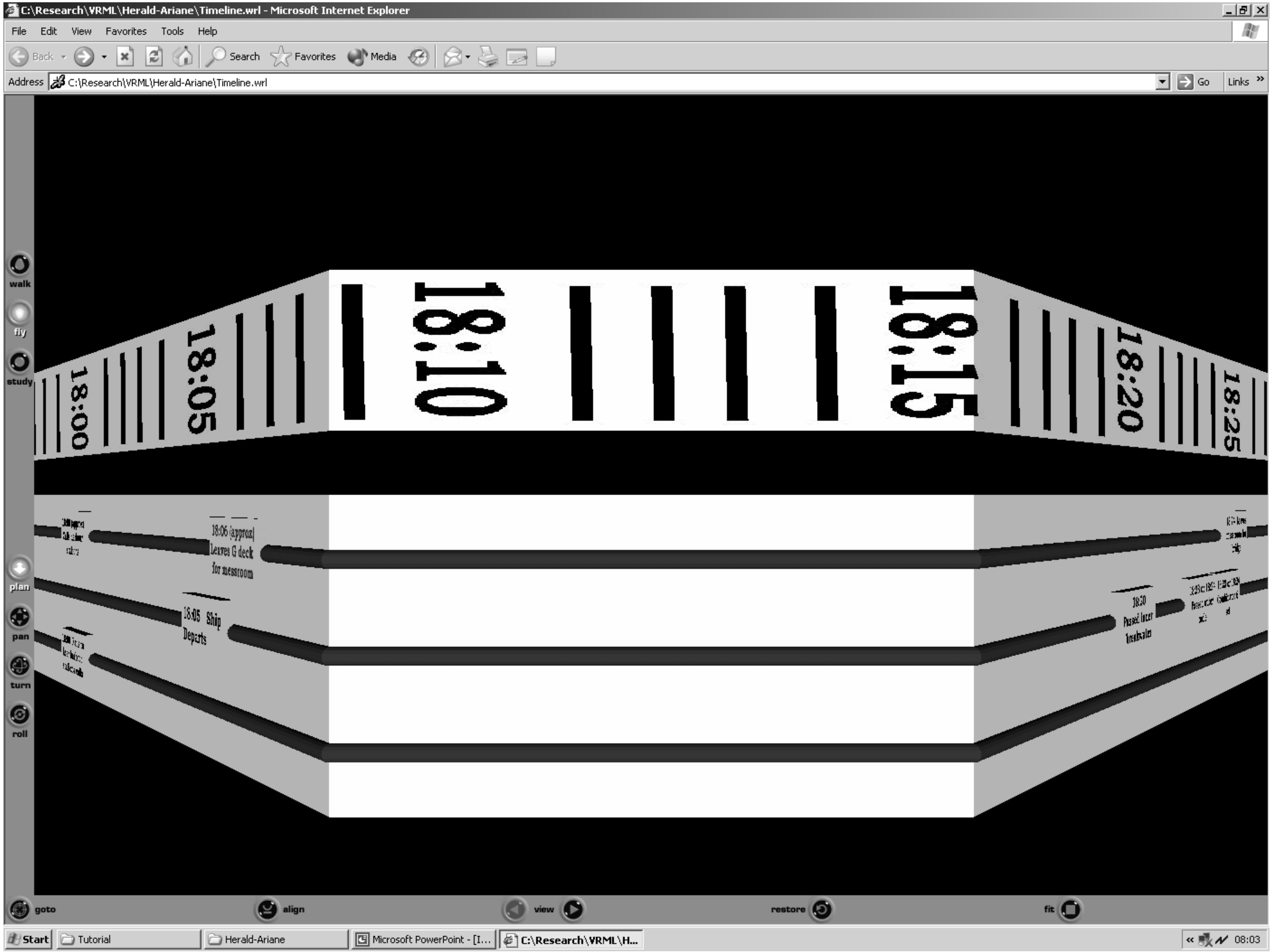
- *General Failure Types:*
1. Hardware
2. Maintenance management.
3. Design.
4. Operating procedures.
5. Error-enforcing conditions.
6. Housekeeping
7. Incompatible goals
8. Communication
9. Organisation
10. Training
11. Defence planning

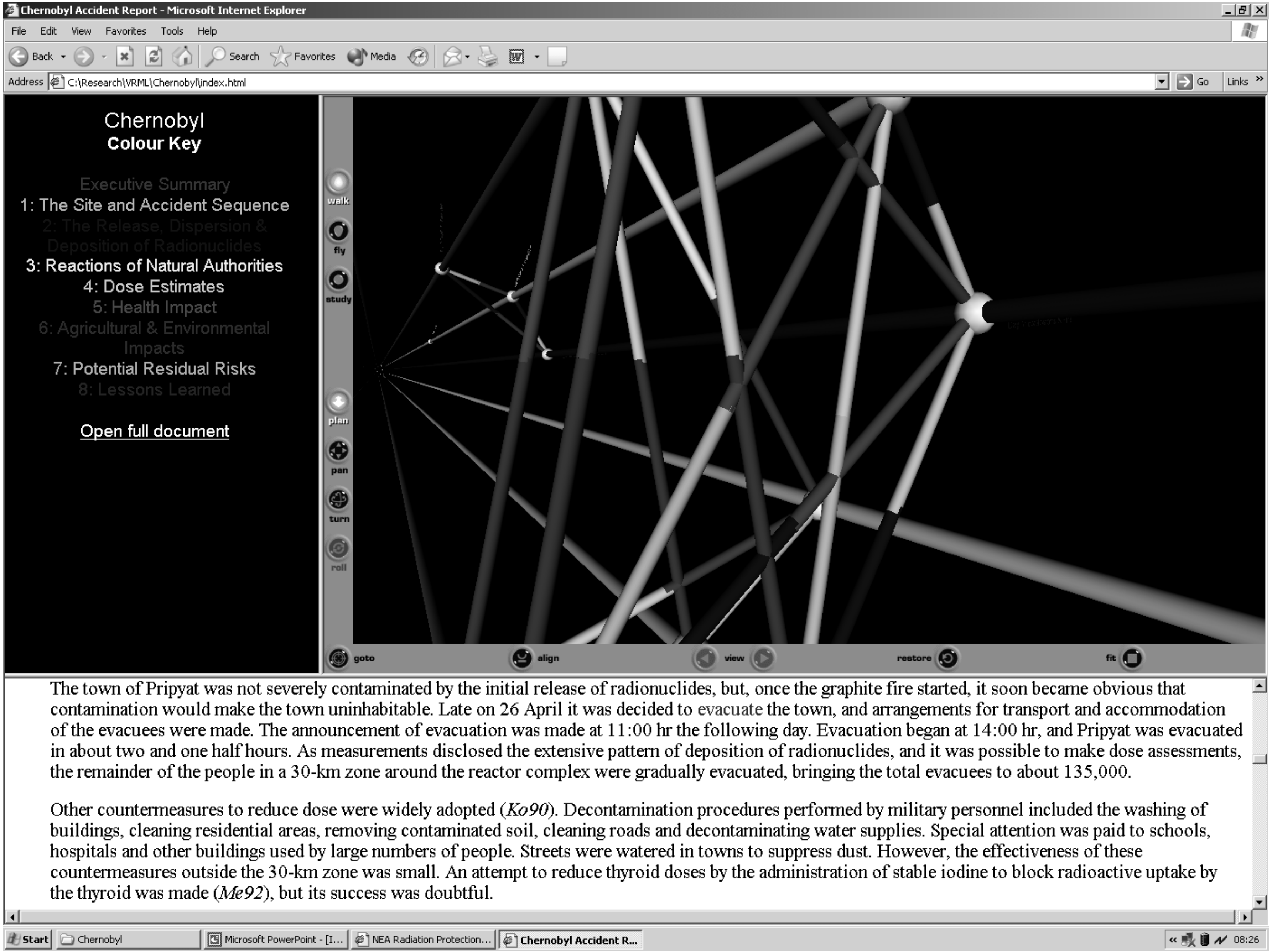
Some incident investigations can get very complex...


MARS POLAR LANDER: AN EXPEDITION TO THE SOUTH POLAR REGION
METEOROLOGY MAST (MET)
MEDIUM GAIN ANTENNA
STEREO SURFACE IMAGER (SSI)
MARS DESCENT IMAGER (MARDI) NOT SHOWN
LIGHT DETECTION AND RANGING (LIDAR)
MVACS PAYLOAD ELECTRONICS BOX
MARS MICROPHONE
TUNABLE LASER DIODE
ELBOW TEMPERATURE SENSOR (MET)
UHF ANTENNA
THERMAL AND EVOLVED GAS ANALYZER (TEGA)
ROBOTIC ARM
SOLAR ARRAY WING
ROBOTIC ARM CAMERA
SOIL TEMPERATURE PROBE
SCOOP




Systems engineering decision: Solar array is asymmetric to MCO body unlike Mars Global Surveyor.
Systems engineering decision: reject daily 180 degree flip to cancel angular momentum build-up.
Limited training of the ground software development staff.
Perception that ground-based AMD data was not mission critical.
Project oversight problems stem from complex relationship between JPL and LMA
Operations team makes inaccurate assumptions about hardware and software similarities between Global Surveyor and Climate Orbiter
10-14 times more often than planned to combat momentum induced by solar radiation because the MCO solar array is asymmetric to the craft's body.
SM_Forces routines are written using imperial and not metric units for thruster performance.
Limited independent testing of the ground based SM_Forces routines.
The failure to conform with the SIS interface is not detected during development.
MCO is first project for multi-mission Mars Survey Operations project.
Perception that 'orbiting Mars is routine' based on inadequate risk mitigation
Plan for the hand-over less than adequate.
Requirements are not passed on in sufficient detail nor are they backed by an adequate validation plan.
Decision not to perform an a priori analysis of what could go wrong on the MCO.
Minimal number of development staff transition to operations (11-12/98)
Mars Climate Orbiter (MCO) Launch (11/12/98)
Angular Momentum Desaturation events.
Ground-based software uses imperial not metric units for thruster to compile AMD data file.
TCM-5 is discussed but not executed (16-23/9/99)
Cruise phase ends (23/9/99)
Mars Orbital Insertion (MOI) begins (09:00:46, 23/9/99)
Last signal from MCO (09:04:52, 23/9/99)
MCO is lost.
MCO Mishap Investigation Board is formed (15/10/99)
Operations Navigation team consult with spacecraft engineers to discuss discrepancies in velocity change model. (27/9/99)
File format problems for AMD data is fixed N/4/99
It is apparent that the AMD file data is anomalous N+7/4/99
The anomaly is not reported through the ISA scheme.
Significance of the anomalous AMD data is not fully appreciated.
Lack of managerial leadership in promoting responsible attitudes to reporting
Lack of training for operations staff in the ISA scheme.
Two people head the operation navigation in key stages of the project
Operational navigation and spacecraft operations teams did not fully understand the attitude control system.
Operational navigation staff fail to communicate their concerns to the spacecraft operations team.
Vacancies and replacement of senior staff.


C:\Research\VRML\Herald-Ariane\Timeline.wrl - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address C:\Research\VRML\Herald-Ariane\Timeline.wrl
Go Links
18:00
18:05
18:10
18:15
18:20
18:25
18:06 (approx) Leaves G deck for messroom
18:05 Ship Departs
18:30 Passed Inner breakwater
walk
fly
study
plan
pan
turn
roll
goto
align
view
restore
fit
Start
Tutorial
Herald-Ariane
Microsoft PowerPoint - [I...
C:\Research\VRML\H...
08:03



The town of Pripyat was not severely contaminated by the initial release of radionuclides, but, once the graphite fire started, it soon became obvious that contamination would make the town uninhabitable. Late on 26 April it was decided to evacuate the town, and arrangements for transport and accommodation of the evacuees were made. The announcement of evacuation was made at 11:00 hr the following day. Evacuation began at 14:00 hr, and Pripyat was evacuated in about two and one half hours. As measurements disclosed the extensive pattern of deposition of radionuclides, and it was possible to make dose assessments, the remainder of the people in a 30-km zone around the reactor complex were gradually evacuated, bringing the total evacuees to about 135,000.

Other countermeasures to reduce dose were widely adopted (*Ko90*). Decontamination procedures performed by military personnel included the washing of buildings, cleaning residential areas, removing contaminated soil, cleaning roads and decontaminating water supplies. Special attention was paid to schools, hospitals and other buildings used by large numbers of people. Streets were watered in towns to suppress dust. However, the effectiveness of these countermeasures outside the 30-km zone was small. An attempt to reduce thyroid doses by the administration of stable iodine to block radioactive uptake by the thyroid was made (*Me92*), but its success was doubtful.

Part 2

1. What is human error?

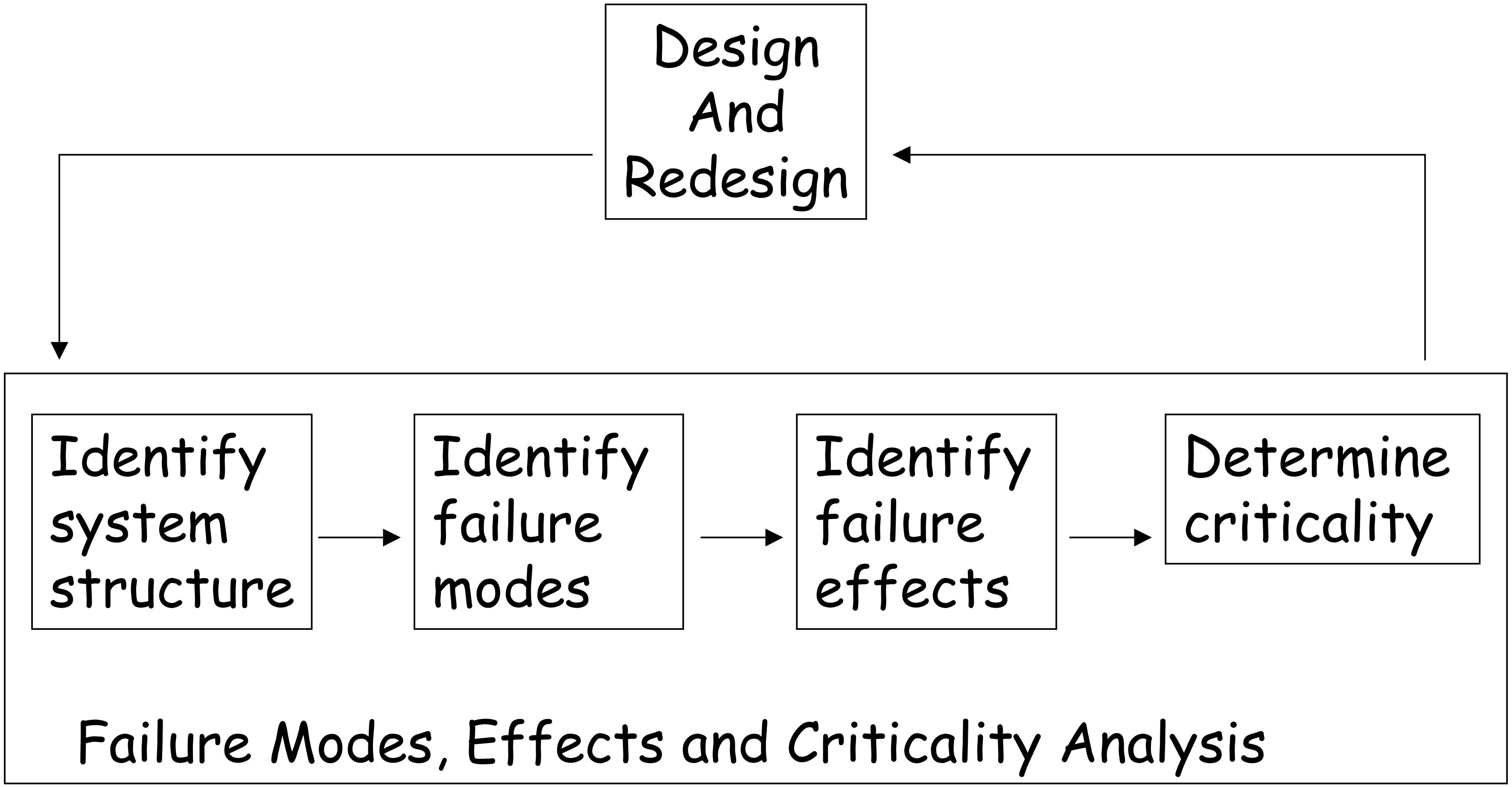
> 2. Human error in risk assessment.

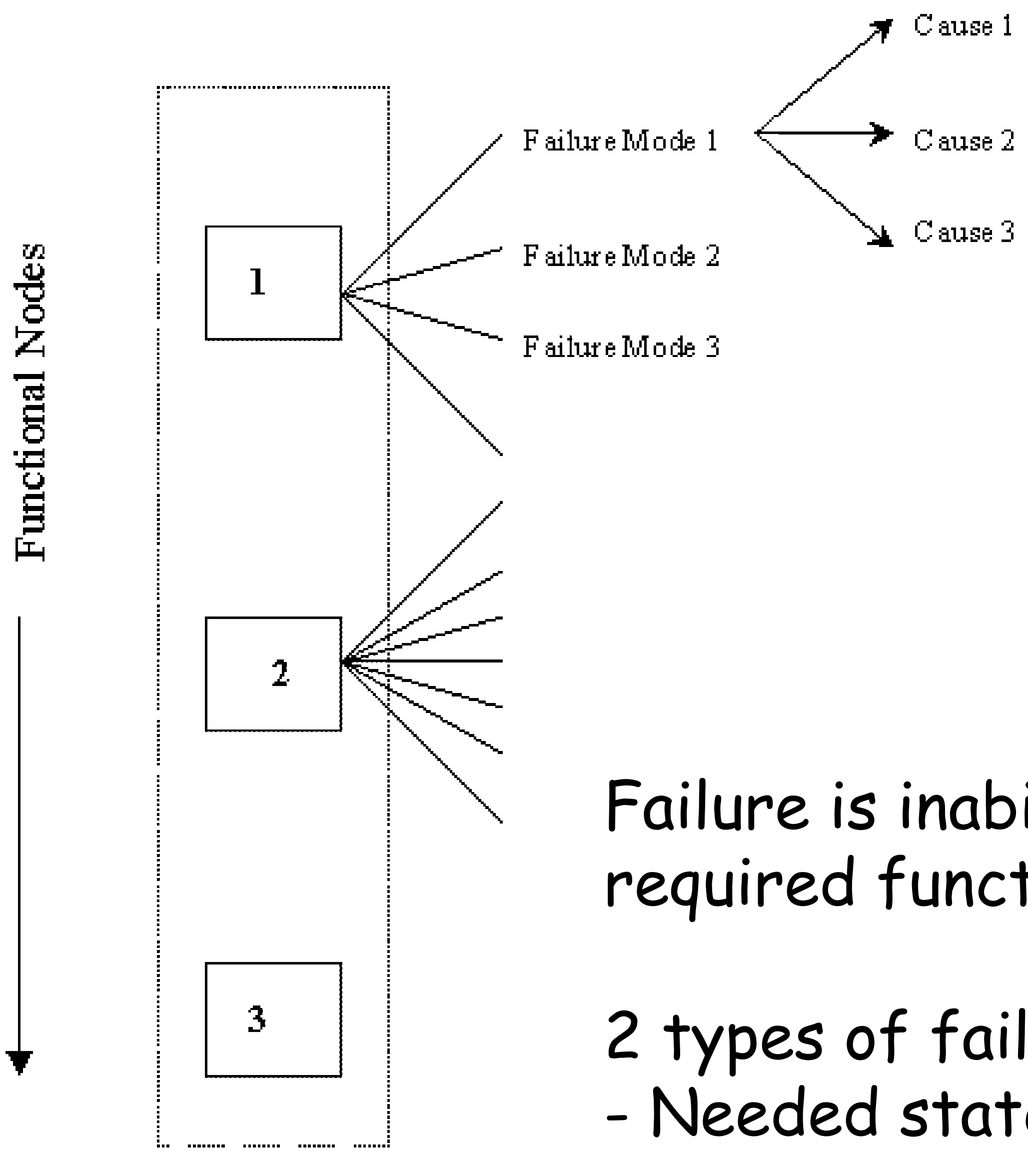
3. Human Reliability Analysis techniques.
4. Human error in safety management.

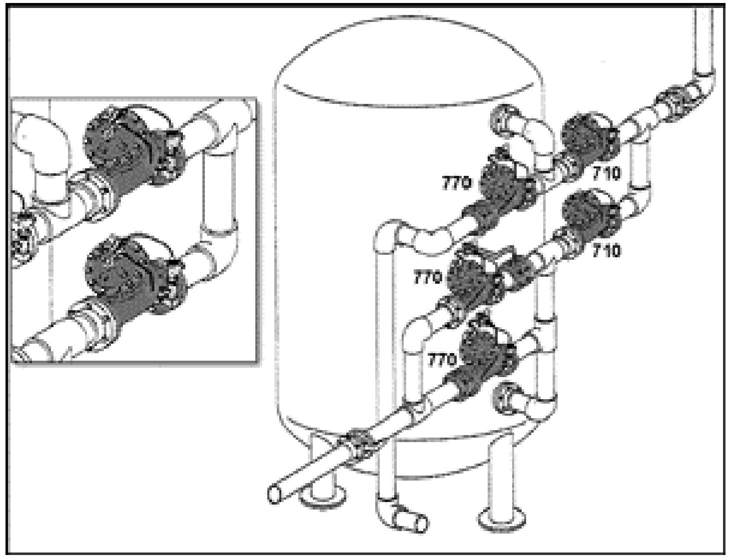
How do we go from incidents to hazard analysis?

Four Stages to Risk Assessment

1. Identify Hazards
2. Identify controls
3. Implement controls
4. Supervise and evaluate


Design
And
Redesign
Identify
system
structure
Identify
failure
modes
Identify
failure
effects
Determine
criticality
Failure Modes, Effects and Criticality Analysis





Failure is inability to perform required function

2 types of failure modes:
- Needed state change not achieved;
- Spurious state change occurs.

Failure Modes of Remotely Operated Valve

- Fail to close on command
- Fail to open on command
- Uncommanded open
- Uncommanded close
- Leakage to environment
- Leak to environment
- ...

FMECA Worksheet

System: Date: Author: Approved by:

Function	Failure Mode	Failure Effect		Severity	Occurrence rate	Detection Method	Notes
		System	Local				
Remote control block valve C2011	Uncommanded open	Pressure rise, worst case rupture	Unable to control flow into sector?	I - Catastrophic	Occasional	RCM scheduled inspections	FMECA analysis incomplete – requires more detail on failure modes.

Occurrence:
Very unlikely, 1 per 1000 years or more seldom;
Remote, 1 per 100 years;
Occasional, 1 per 10 years;
Probable, 1 per year;
Frequent, 1 per month or more often

Severity:

I – Catastrophic, may cause death;

II – Critical, injury, major property damage

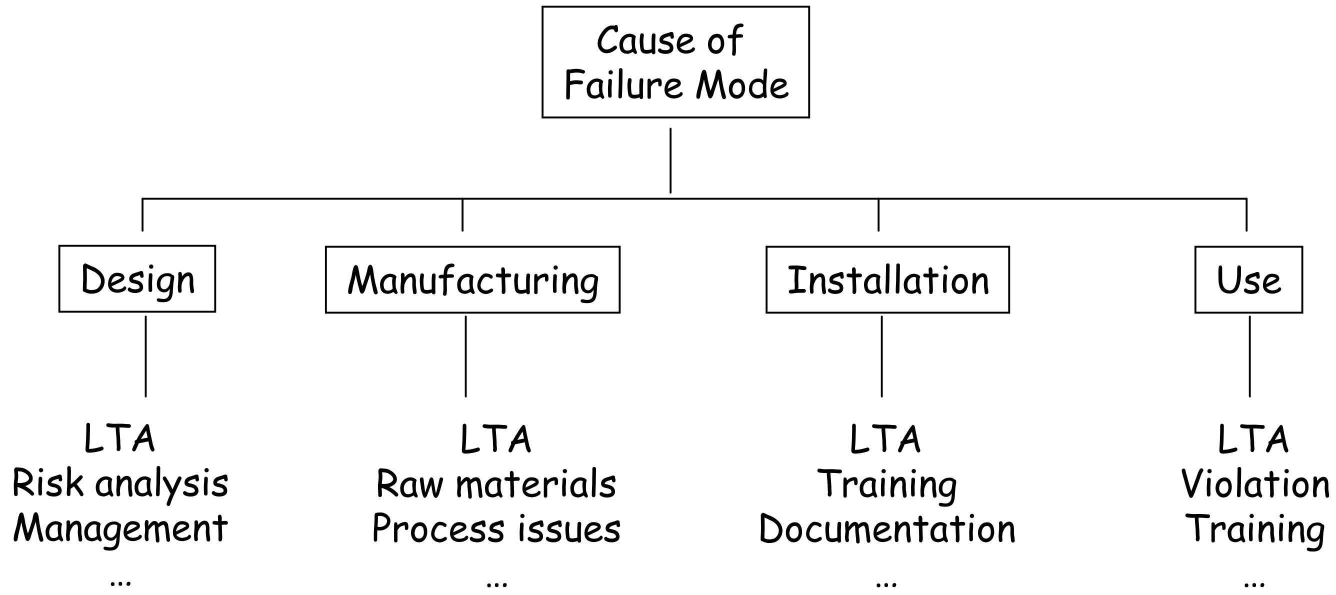
III – Marginal, minor injury, minor property damage;

IV – Minor, no injury/damage but more maintenance.

Location	Station, ft	Upstream Valve	Downstream Valve	Detection + Valve Closure Time[a], Minutes		Maximum Drain Volume		Loss During Detection and Pipeline Shutdown[b]		Total Maximum Release	
				Upstream Valve	Downstream Valve	bbl	gal	bbl	Gal	bbl	gal
Fomwood Elementary, Northwood Elementary, and Langstead Primary Schools	75600 to 76400	Remote-controlled block valve	Manual block valve	5	120[c]	3,903	164,000	781	32,800	4,684	196,800
Buescher State Park	673338 to 679884	Manual block valve	Remote-controlled block valve	120[c]	5	2,333	98,000	781	32,800	3,114	130,800
Colorado River Crossing	710033	Remote-controlled block valve MLV G-1	Check valve and manually-operated block valve	5	5	1,245	52,300	781	32,800	2,026	85,100
Onion Creek Crossing	865867	Remote-controlled block valve	Remote-controlled block valve	5	5	4,310	179,600	781	32,800	5,091	212,400
Hillcrest Elementary School	861050	Remote-controlled block valve	Remote-controlled block valve	5	5	488	20,500	781	32,800	1,269	53,300
Brown Schools	888000	Remote-controlled block valve	Remote-controlled block valve	5	5	3,996	167,800	781	32,800	4,777	200,600
Shiloh Oaks Subdivision	891264	Remote-controlled block valve	Remote-controlled block valve	5	5	2,667	112,014	781	32,800	3,448	144,814
Karst Preserve	901500	Remote-controlled block valve	Remote-controlled block valve	5	5	3,964	166,500	781	32,800	4,745	199,300
Edwards Aquifer – General	875615 to 914682	Remote-controlled block valve[d]	Remote-controlled block valve	5	5	5,240	220,080	781	32,800	6,021	252,880

US Environment Protection Agency, http://www.epa.gov/earth1r6/6en/xp/lpptab6.pdf

Why Do Failure Modes Occur?



- Fail to close on command:
  - lines blocked; worn seals, voltage regulator fails…

11.00-11.30:
- Break and group session 2 (FMECA exercise)

Case Study Incident

Facility produces pressurized containers: product + propellant to form spray.

Pressurized containers filled in 4 stages:

1. product placed in container in production building.
2. conveyor brings containers to gas house ;
3. propellant placed into container in the *Gas House*.
4. filled containers conveyed back to Production Building for leak and quality control.

Case Study Incident

Incident occurs when filling ethylene oxide containers for sterilant in hospitals.

Do not need an aerosol and just use one chemical - ethylene oxide.

All filling of ethylene oxide takes place in Gas House.

Ethylene oxide is a highly toxic chemical:

- classified by the National Fire Protection Association as a 1A flammable liquid,
- listed by EPA as “extremely hazardous substance”.

So, operator wears protective clothing and respirator during ethylene oxide filling.

Breathing air is pumped to operator’s respirator via air hose.

Case Study Incident

Steel pipe ethylene oxide liquid from storage tank to Gas House at 55-65 psig.

In Gas House, ethylene oxide fed pressurized to 600-650 psig and sent to “under-the-cup” filling machine.

Small amount of ethylene oxide released into Gas House during filling and sealing of each container.

Filling machine meters out approx. 105 grams of ethylene oxide for each 100-gram container.

Target amount for each 100-gram container is 101.5-102.5 gram.

Any excess ethylene oxide sent to reclamation tank in Gas House.

Case Study Incident

Gas House uses catalytic oxidizer to break down ethylene oxide vapor to avoid environmental release.

The pump that supplied breathing air to operator in Gas House stopped.

Unable to breathe, operator forced to shut down filling and leave.

After breathing-air pump was fixed, operator returned to Gas House to restart production.

However, he noticed that a hydrocarbon vapor alarm was triggered.

This indicated the level of hydrocarbon vapor had exceeded 40% of lower explosive limit.

Gas House is used primarily for processing hydrocarbons such as propane and iso-butane.

Ethylene oxide is not a hydrocarbon, level of ethylene oxide that would trigger alarm unknown.

Operator immediately left Gas House to check on instruments in adjacent Production Building.

Case Study Incident

Large explosion as he exited.

Operator thrown 10 feet and injured shoulder.

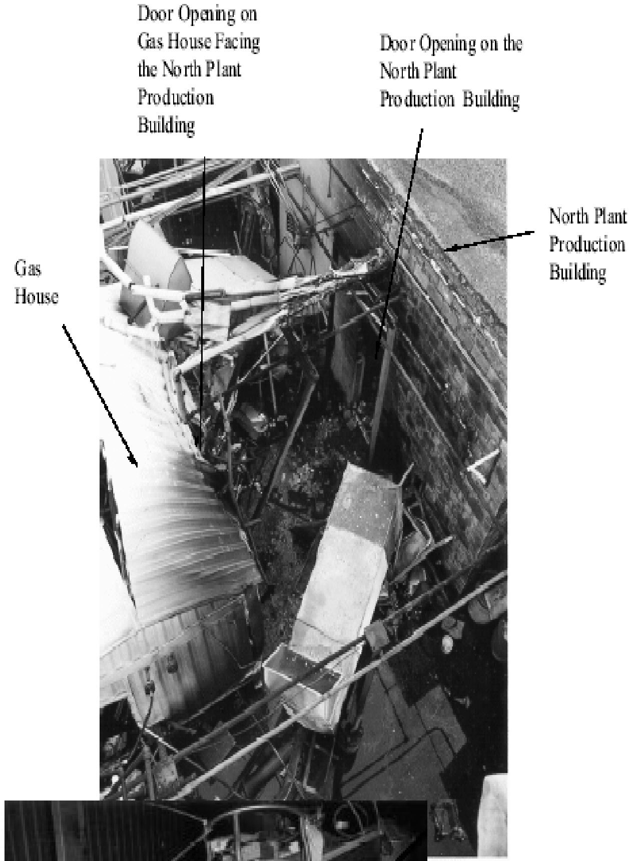
Gas House doors blown off.

Door facing Production Building impacted Production Building door.

Production building door dislodged with its frame.

They were blown into Production Building, struck and killed employee.

http://yosemite.epa.gov/oswer/ceppoweb.nsf/vwResourcesByFilename/accrapac.pdf/$File/accrapac.pdf



Your Task

- Incidents trigger re-engineering.
- Use FMECA to analyse users task…
- Identify other failures modes.

FMECA Worksheet

System: Date: Author: Approved by:

Function	Failure Mode	Failure Effect		Severity	Occurrence rate	Detection Method	Notes
		System	Local				
Operator breathing supply fails	Uncommanded stop	Total loss of control on the filling operation.	Worst assumed – loss of consciousness	I – Catastrophic	Occasional (1 in 10yrs)	Flow valve Alarm system Operator foot plate alarm.	FMECA analysis incomplete – requires more detail on failure modes.

Occurrence:
Very unlikely, 1 per 1000 years or more seldom;
Remote, 1 per 100 years;
Occasional, 1 per 10 years;
Probable, 1 per year;
Frequent, 1 per month or more often

Severity:

I – Catastrophic, may cause death;

II – Critical, injury, major property damage

III – Marginal, minor injury, minor property damage;

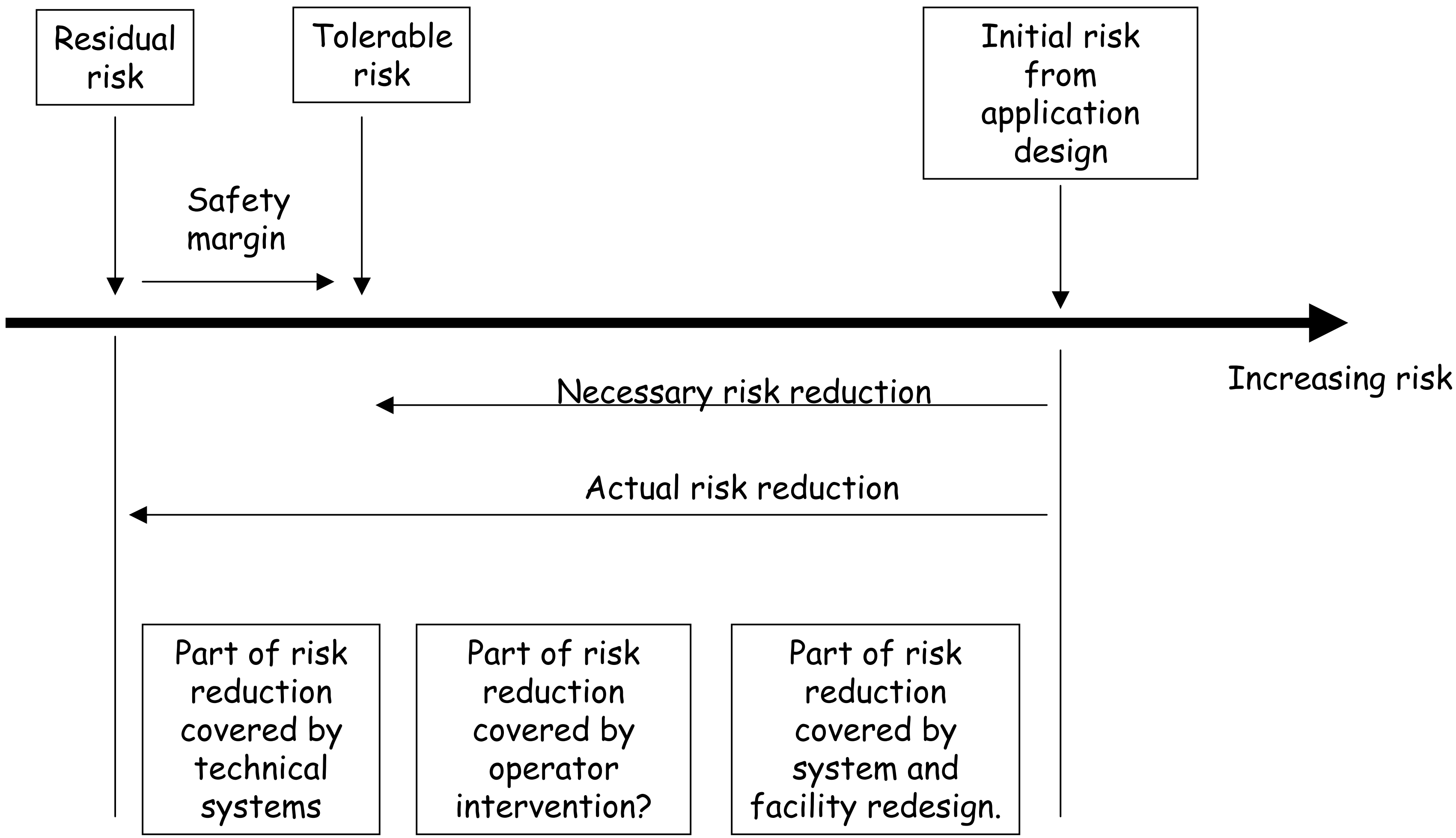
IV – Minor, no injury/damage but more maintenance.

Part 3

1. What is human error?
2. Human error in risk assessment.

> 3. Human Reliability Analysis tools.

4. Human error in safety management.


Residual risk
Tolerable risk
Initial risk from application design
Safety margin
Increasing risk
Necessary risk reduction
Actual risk reduction
Part of risk reduction covered by technical systems
Part of risk reduction covered by operator intervention?
Part of risk reduction covered by system and facility redesign.

ALARP

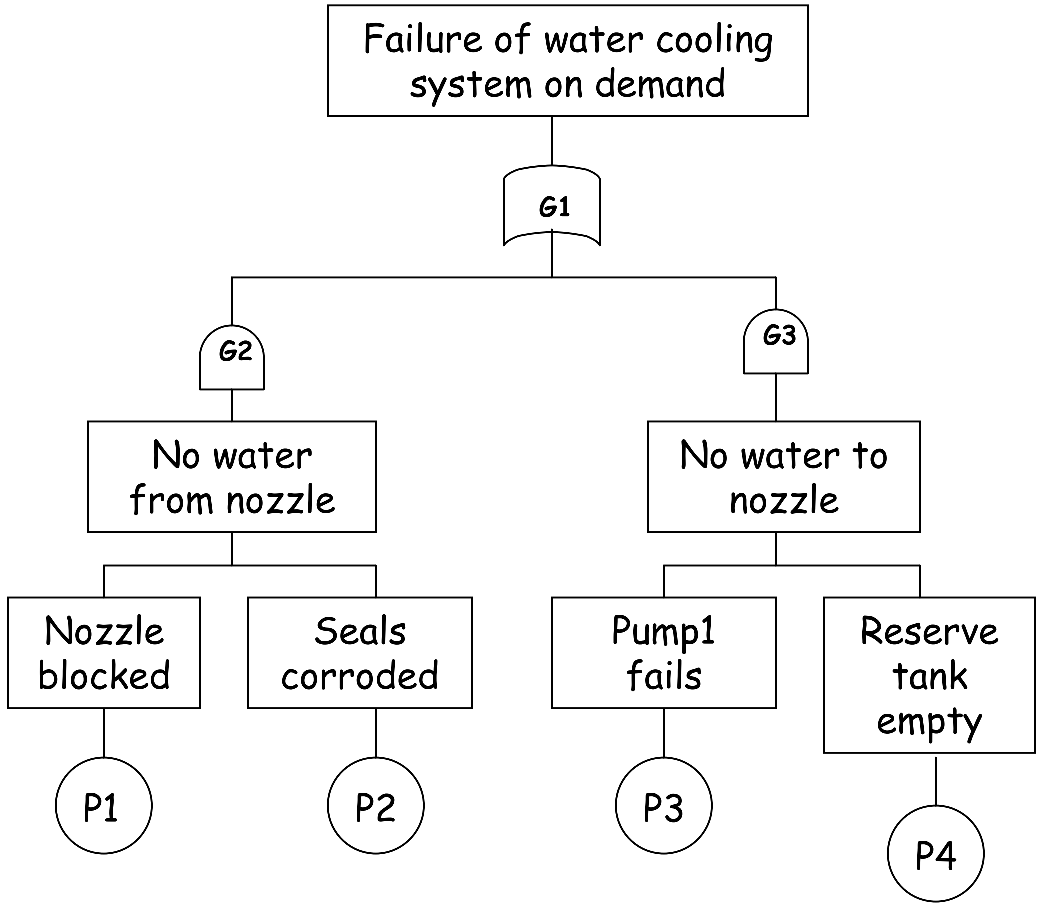
	Very likely	Remote	Occasional	Probable	Frequent
I – Catastrophic					
II – Critical					
III – Marginal					
IV - Minor					

Key

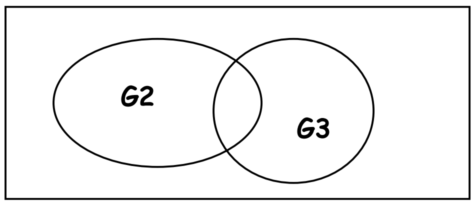
Broadly acceptable.

Acceptable only if risk as low as reasonably practicable.

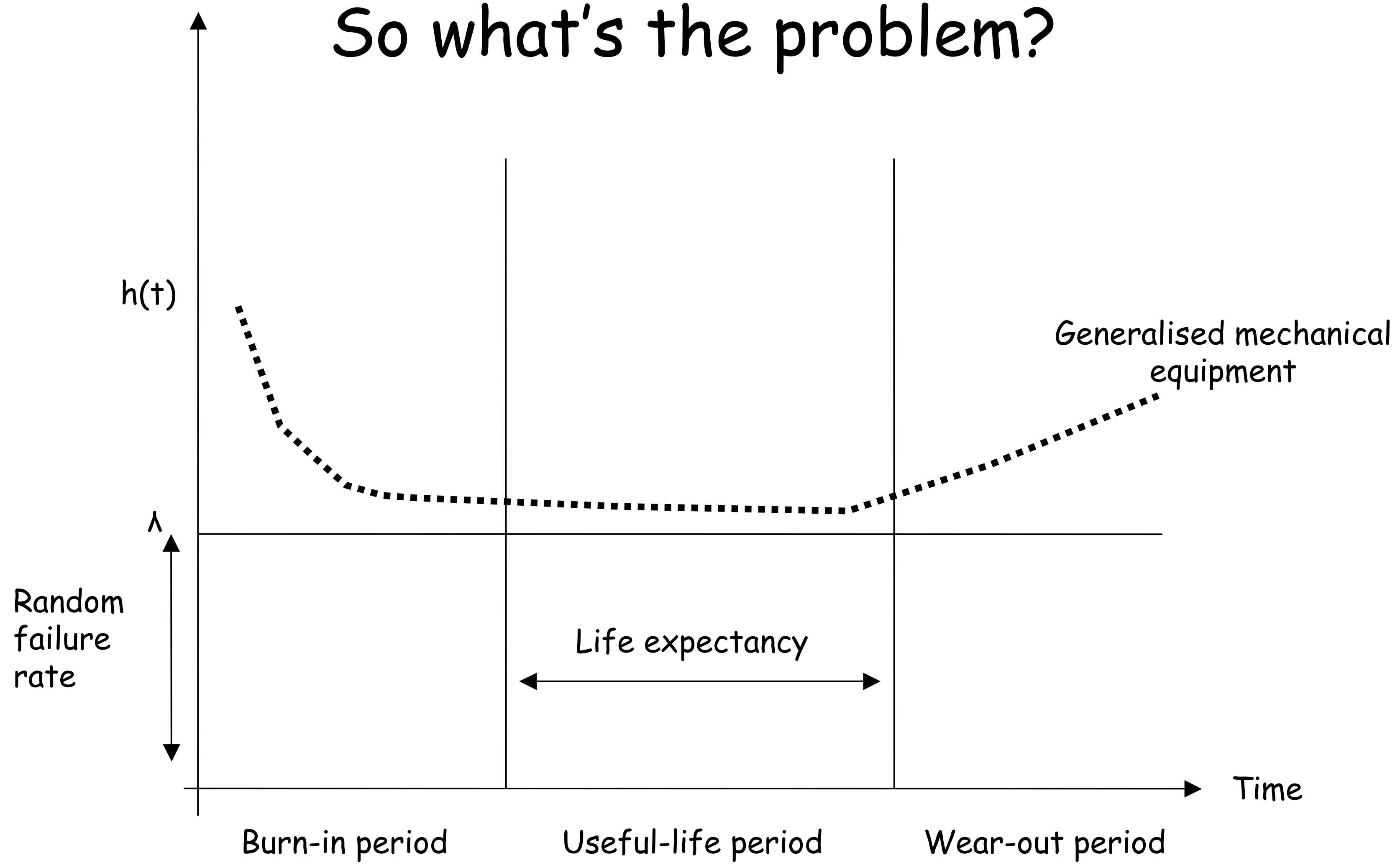
Unacceptable, risk reduction required.



$$P(G1) = P(G2) + P(G3) - P(G2).P(G3)$$
$$= (P1.P2)+(P3.P4) - (P1.P2).(P3.P4)$$



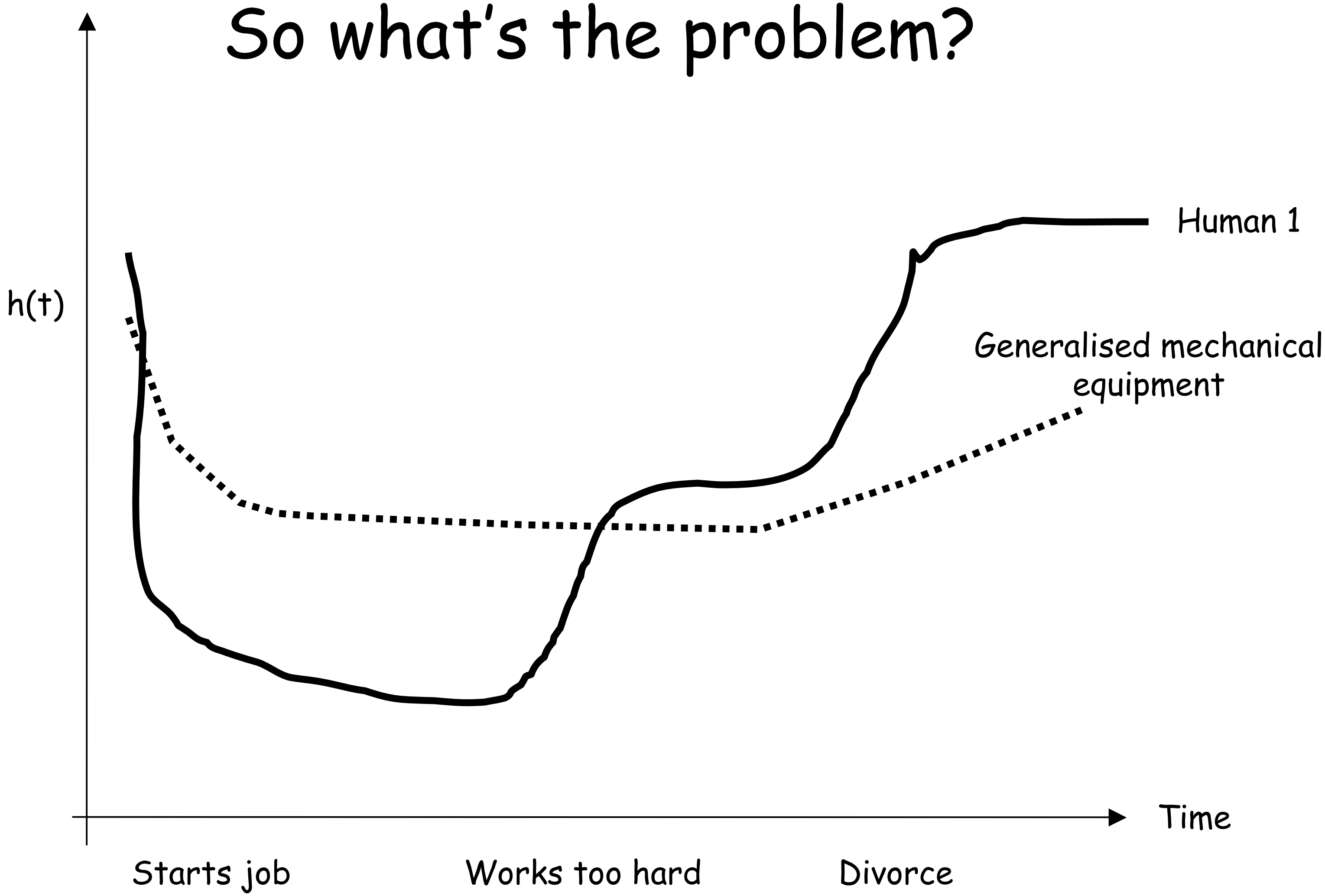
So what's the problem?



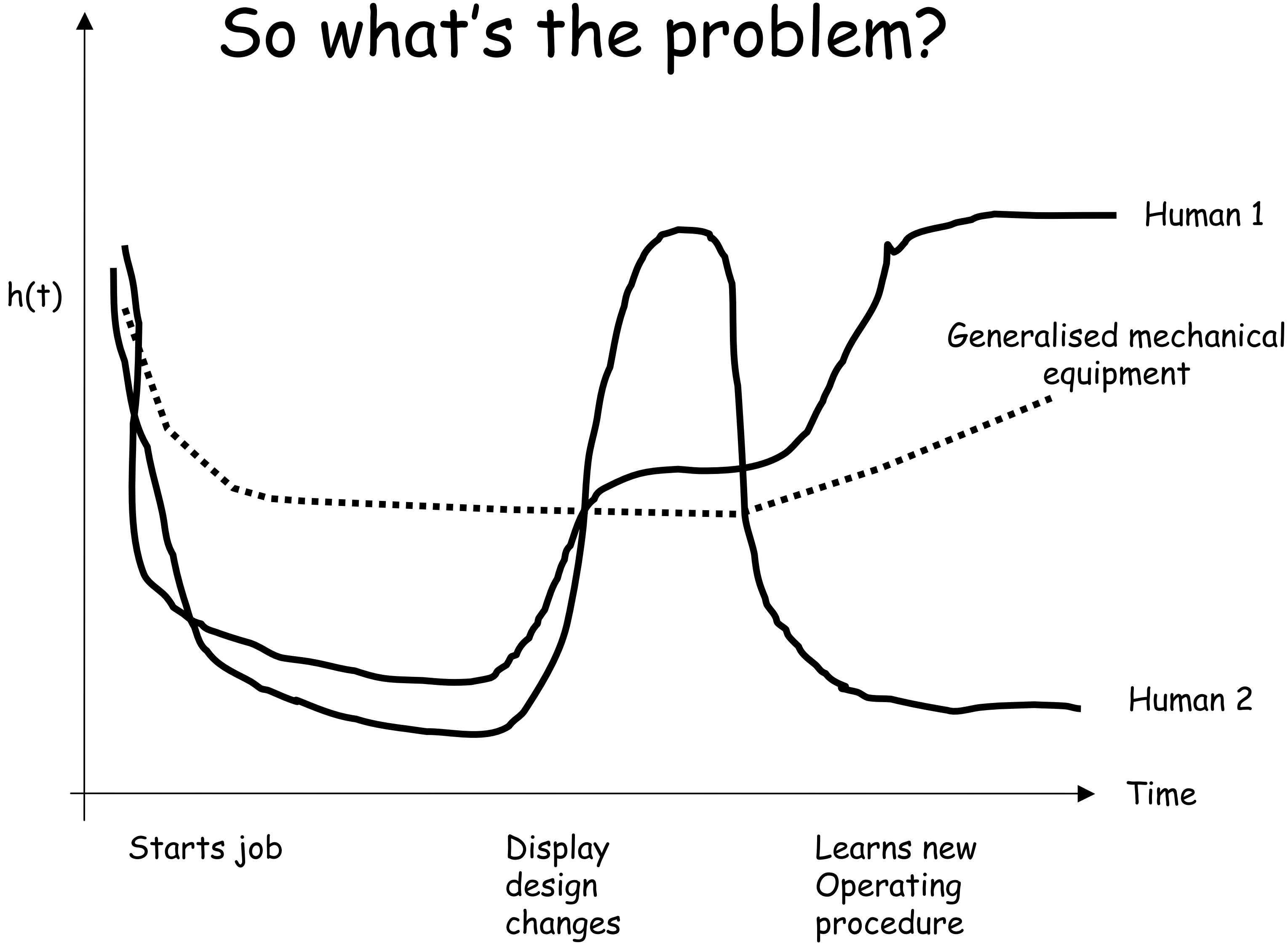
Λ or randomised failure
Rate on the previous slide

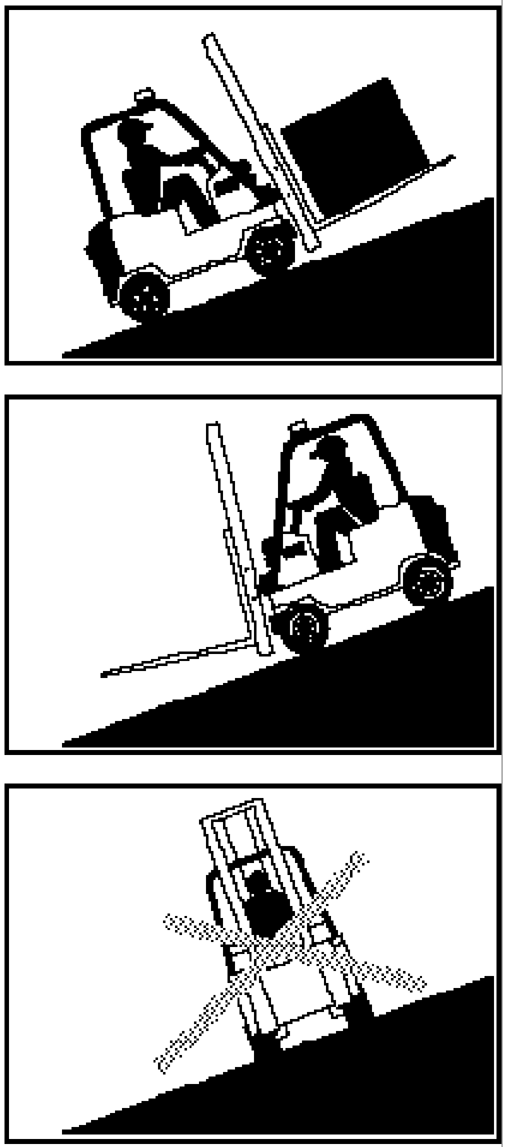
Accumulator	Leaking Seized Worn Contaminated	.47 .23 .20 .10
Actuator	Spurious Position Change Binding Leaking Seized	.36 .27 .22 .15
Alarm	False Indication Failure to Operate Spurious Operation Degraded Alarm	.48 .29 .18 .05
Antenna	No Transmission Signal Leakage Spurious Transmission	.54 .21 .25
Battery, Lithium	Degraded Output Startup Delay Short Open	.78 .14 .06 .02
Battery, Lead Acid	Degraded Output Short Intermittent Output	.70 .20 .10
Battery, Ni-Cd	Degraded Output No Output	.72 .28
...	...	...

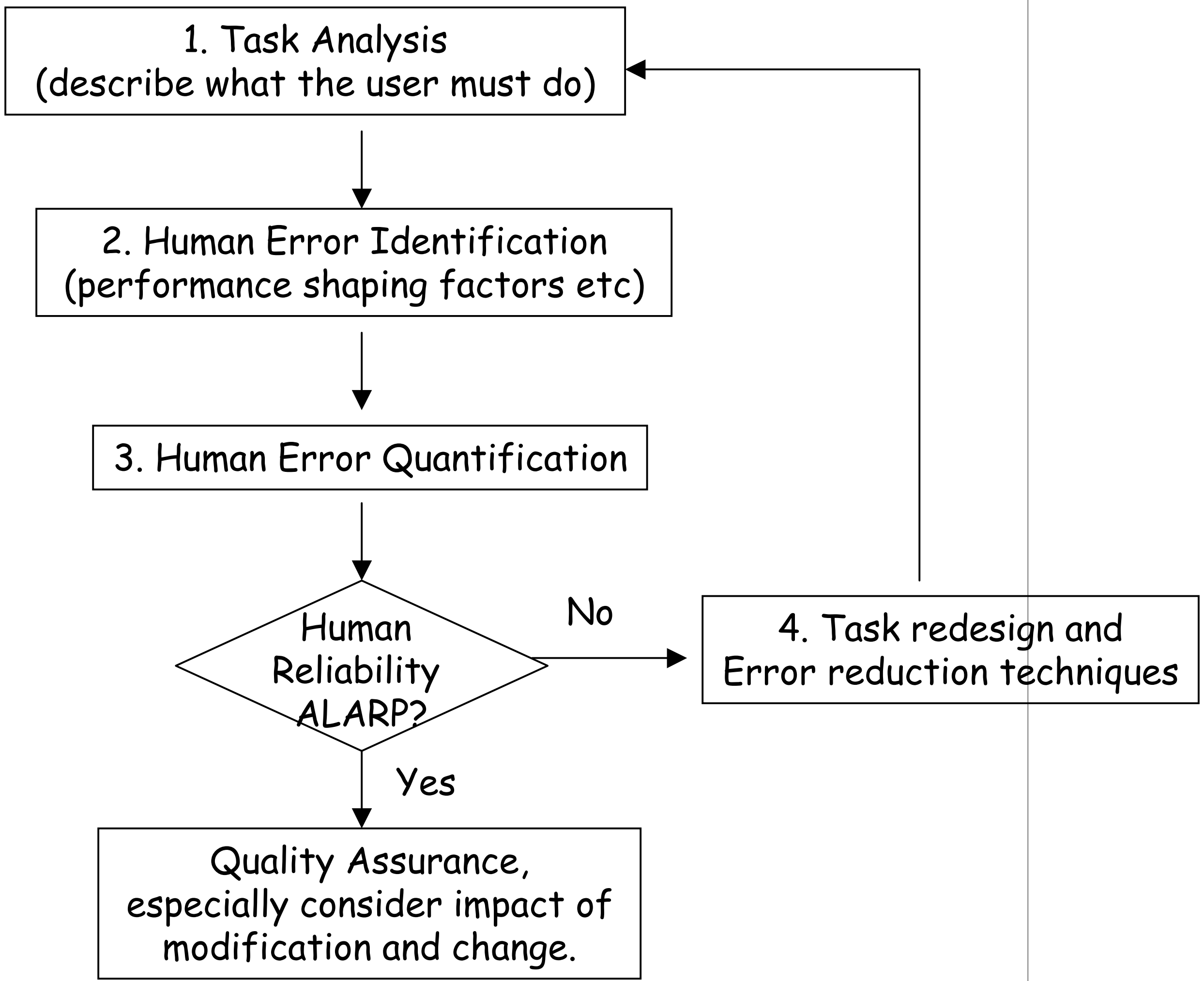
So what's the problem?



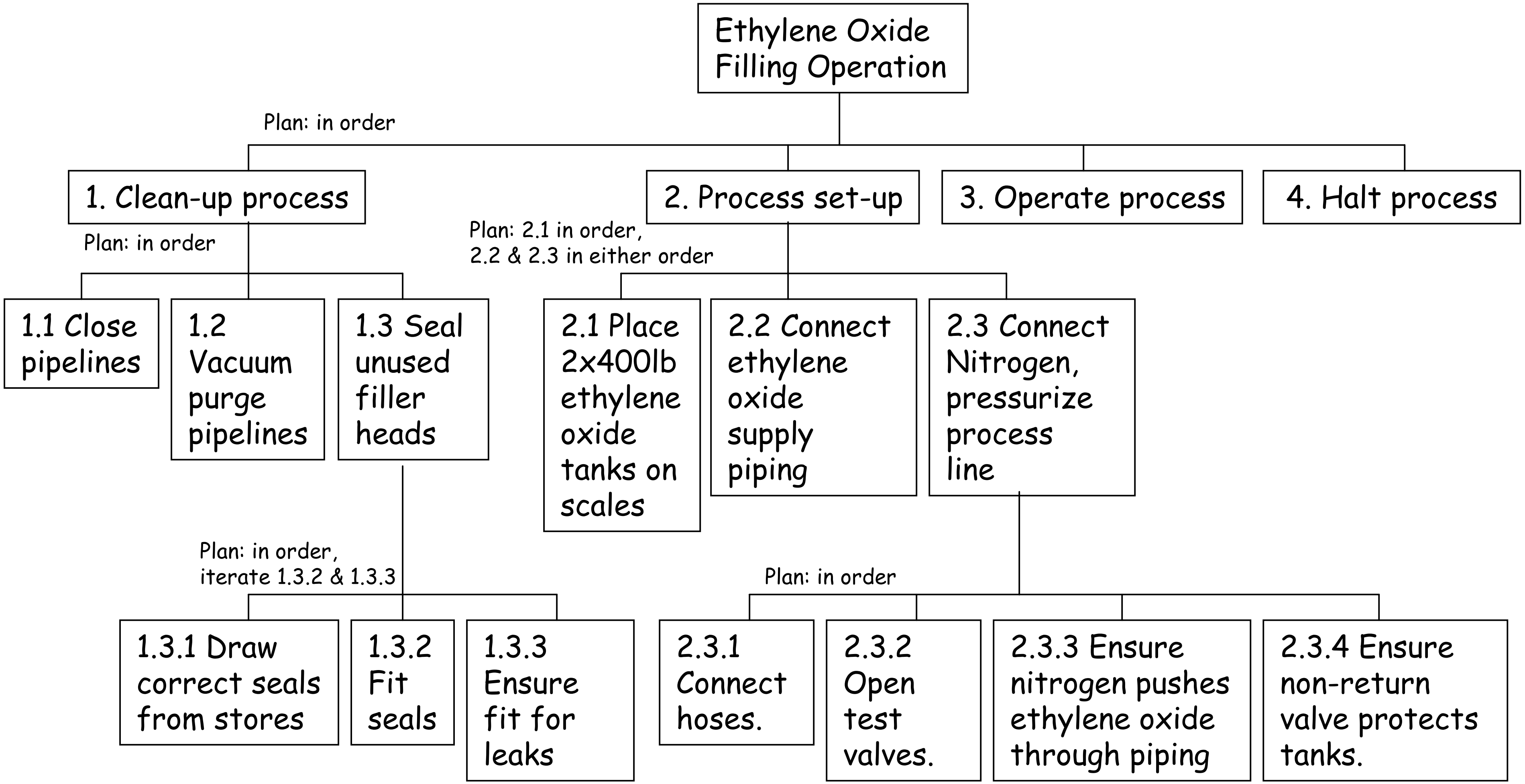
So what's the problem?





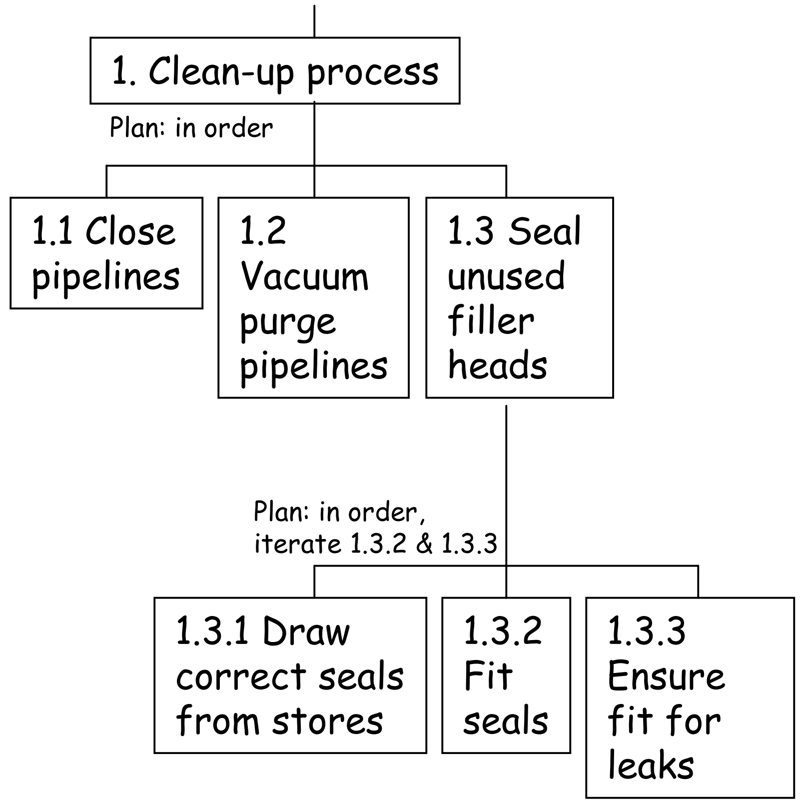

1. Task Analysis
(describe what the user must do)
2. Human Error Identification
(performance shaping factors etc)
3. Human Error Quantification
Human
Reliability
ALARP?
No
4. Task redesign and
Error reduction techniques
Yes
Quality Assurance,
especially consider impact of
modification and change.

1. Task Analysis



2. Human Error Identification

Human Error Guidewords	Example
Task omitted	Forget to seal unused filler heads (1.3)
Achieved less than goal/lapse	Only achieve a seal on some of the filler heads (1.3)
Exceeded goal	Leave test valves open during production (2.3.2)
Achieved opposite goal	Introduce contamination of pipeline during vacuum purge (1.2)
Additional task/action	Open test valves disconnects a hose (2.3.2)
Slip	Crack filler head during seal fit (1.3.2)
Erratic task performance	Ensure fit for leaks on some seals (1.3.3)
Performed goal/ task too soon	Purge pipelines before pipelines are closed (1.1 and 1.2)
Performed goal/ task too late	Attempt to seal filler heads (1.3) before vacuum purge is complete (1.2)
Calculation error	Miscalculate nitrogen pressure (2.3.3)
Installation error	Poor connection of ethylene oxide (2.2)
Scheduling error	No time for clean-up process to complete (1)



NB related to HAZOPS

But how likely are these errors?

3. Human Error Quantification

Category	Failure Probability
Simple, frequently performed task under minimal stress	0.001
More complex tasks, less time available and some care necessary	0.01
Complex, unfamiliar task with little feedback and some distractions	0.1
Highly complex task, considerable stress little time to perform it	0.3
Extreme stress, rarely performed task	1

- Generic Human Error Probabilities (Kirwan)
  - Forget to clean up process (1.) = 0.001 (1 in 1000 clean-up operations?)
  - Didn't notice leak from seals (1.3.3) = 0.3 (3 in 10 operations given leak occurs).

- But even a simple task can be complex:
  - If you're hurried;
  - If you're under stress;
  - If there are poor SOPs…

- PERFORMANCE SHAPING FACTORS…

Performance Shaping Factors

Situational characteristics (PSFs general to one or more jobs in a work situation)	Architectural features. Quality of environment: (Temperature, humidity, air quality and radiation, lighting, noise and vibration, degree of general cleanliness). Work hours/work breaks. Availability/adequacy of special equipment, tools and supplies. Shift rotation.	Staffing parameters. Organisational structure (authority, responsibility, communication channels). Actions by supervisors, co-workers, union representatives and regulatory personnel. Rewards, recognition and benefits.
Job and task instructions; single most important tool for most tasks.	Procedures required (written or unwritten). Cautions and warnings.	Written or oral communications. Work methods. Plant policies (shop practices).
Task and equipment characteristics (PSFs specific to tasks in a job)	Perceptual requirements. Motor requirements (speed, strength, precision). Control-display relationships. Anticipatory requirements. Interpretation. Decision-making. Complexity (information load). Narrowness of task. Frequency and repetitiveness. Task criticality. Long and short-term memory	Calculation requirements. Feedback (knowledge of results). Dynamic vs step-by-step activities. Team structure and communication. Man-machine interface factors (design of prime/test/manufacturing equipment, job aids, tools, fixtures).

Performance Shaping Factors

Psychological stressors (PSFs which directly affect mental stress)	Suddenness of onset. Duration of stress. Task speed. High jeopardy tasks. Threats (of failure, job loss etc). Monotonous, degrading or meaningless work. Long, uneventful vigilance periods.	Conflicts of motives about job performance. Reinforcement absent or negative. Sensory deprivation. Distractions (noise, glare, movement, flicker, colour). Inconsistent cueing.
Physiological stressors (PSFs that directly affect physical stress)	Duration of stress. Fatigue. Pain or discomfort. Hunger or thirst. Temperature extremes. Radiation. G-force extremes.	Atmospheric pressure extremes. Oxygen insufficiency. Vibration. Movement constriction. Lack of physical exercise. Disruption of circadian rhythm.

Organismic factors (characteristics of people resulting from internal and external influences)	Previous training/experience. State of current practice or skill. Personality and intelligence variables. Motivation and attitudes. Knowledge required (performance standards). Stress (mental or bodily tension).	Emotional state. Sex differences. Physical condition. Attitudes based on influence of family and other outside persons or agencies. Group identification.

3. Human Error Quantification

- Human Error Assessment & Reduction, HEART:

1. Conduct task analysis;

2. For each task assign initial human reliability;

3. For each task consider Performance Shaping Factors;

4. Likelihood of failure =
   F(initial reliability, Performance Shaping Factors).

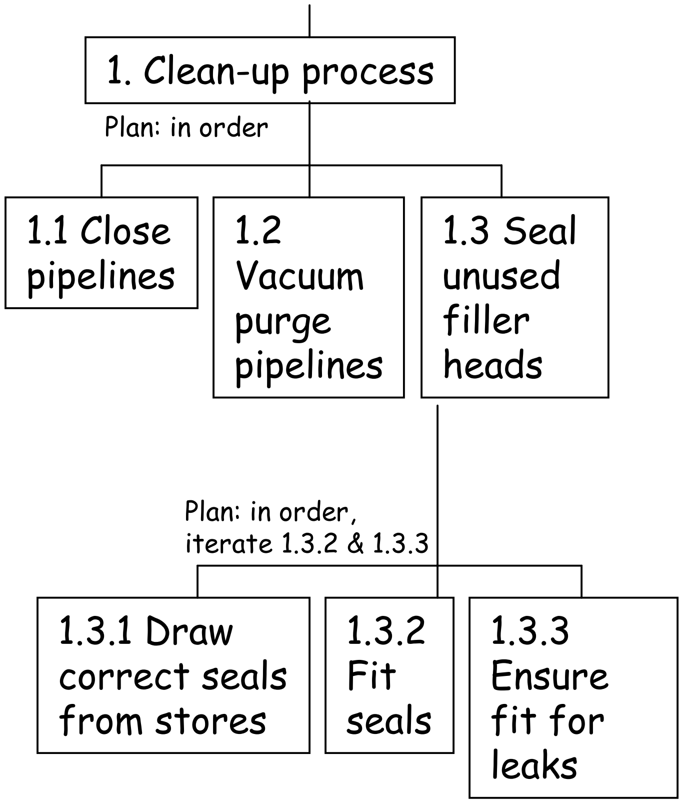
HEART: Initial Reliability Assessment

Generic task	**Proposed nominal human reliability** (5th-95th percentile)
A) totally unfamiliar, performed at speed with no real idea of the likely consequences.	0.55 (0.35-0.97)
B) Shift or restore system to a new or original state on a single attempt without supervision or procedures.	0.26 (0.14-0.42)
C) Complex task requiring high-level of comprehension and skill.	0.16 (0.12-0.28)
D) Fairly simple task performed rapidly or given scant attention.	0.09 (0.06-0.13)
E) Routine, highly-practiced rapid task involving relatively low level of skill.	0.02 (0.007-0.045)
F) Shift or restore system to a new or original state following procedures, with some checking.	0.003 (0.0008-0.007)
G) Completely familiar, well designed, highly practiced, routine task occurring several times per hour and performed to higest possible standards by trained staff…	0.0004 (0.00008-0.0009)
H) Respond correctly to system command even when there is an augmented or automated supervisory system providing accurate interpretation of system stage.	0.00002 (0.000006-0.0009)

HEART: Performance Shaping Factors

Performance Shaping Factors	**Max amount by which reliability impaired**
1. Unfamilliarity with a situation which is potentially important but which occurs infrequently or is novel	X17
2. A shortage of time available for error detection and correction.	X11
3. A low signal-to-noise ratio.	X10
4. A means of suppressing or overriding information or features which is too accessible.	X9
5. No means of conveying spatial and function information to operators in a form which they can readily assimilate.	X8
6. A mismatch between an operator's model of the world and that imaged by the designer.	X8
7. No obvious means of reversing an unintended action.	X8
8. A channel capacity overload, particularly one caused by simultaneous presentation of non-redundant information.	X6
9. A need to learn a technique and apply one which requires the application of an opposite philosophy.	X6
10. The need to transfer specific knowledge from task to task without loss.	X5.5
11. Ambiguity in the required performance standards.	X5
12. A mismatch between perceived and real risk.	X4
13. Poor, ambiguous or ill-matched system feedback.	X4
14. No clear, direct and timely confirmation of an intended action from the portion of the system over which control is to be exherted.	X4
15. Operator inexperience.	X3
16. An impoverished quality of information conveyed by procedures and person-person interaction.	X3
17. Little or no independent checking or testing of output.	X3
18. A conflict between immediate and long term objectives.	X2.5
19. No diversity of information input for veracity checks.	X2.5
20. A mismatch between the education achievement of an individual and the requirements of the task.	X2
21. An incentive to use other more dangerous procedures.	X2
22. Little opportunity to exercise mind and body outside the confines of the job.	X1.8
23. Unreliable instrumentation.	X1.6
24. A need for absolute judgements, which are beyond the capabilities or experience of an operator.	X1.6
25. Unclear allocation of function and responsibility.	X1.6
26. No obvious way to keep track or progress during an activity.	X1.4

HEART: Example



- Ensure fit for leaks.
- Mean nominal human reliability:
  - Fairly simple task performed rapidly … (0.09)
- Performance Shaping Factors :
  - Poor, ambiguous or ill-matched feedback (x4);
  - Little or no independent checking (x3)
  - Etc

Task: Ensure fit for leaks		Nominal Human Reliability = 0.09	
Error Producing Conditions	**Total HEART effect**	**Engineer's assessed portion of effect (0 to 1)**	**Assessed effect**
Poor, ambiguous or ill-matched feedback	x4	0.4	((4-1)x0.4)+1=2.2
Little or no independent checking	x3	1.0	((3-1)x1.0)+1=3.0
…	…	…	…
Net nominal likelihood of failure = 0.09 x 2.2 x 3.0 = 0.594			

4. Task Redesign

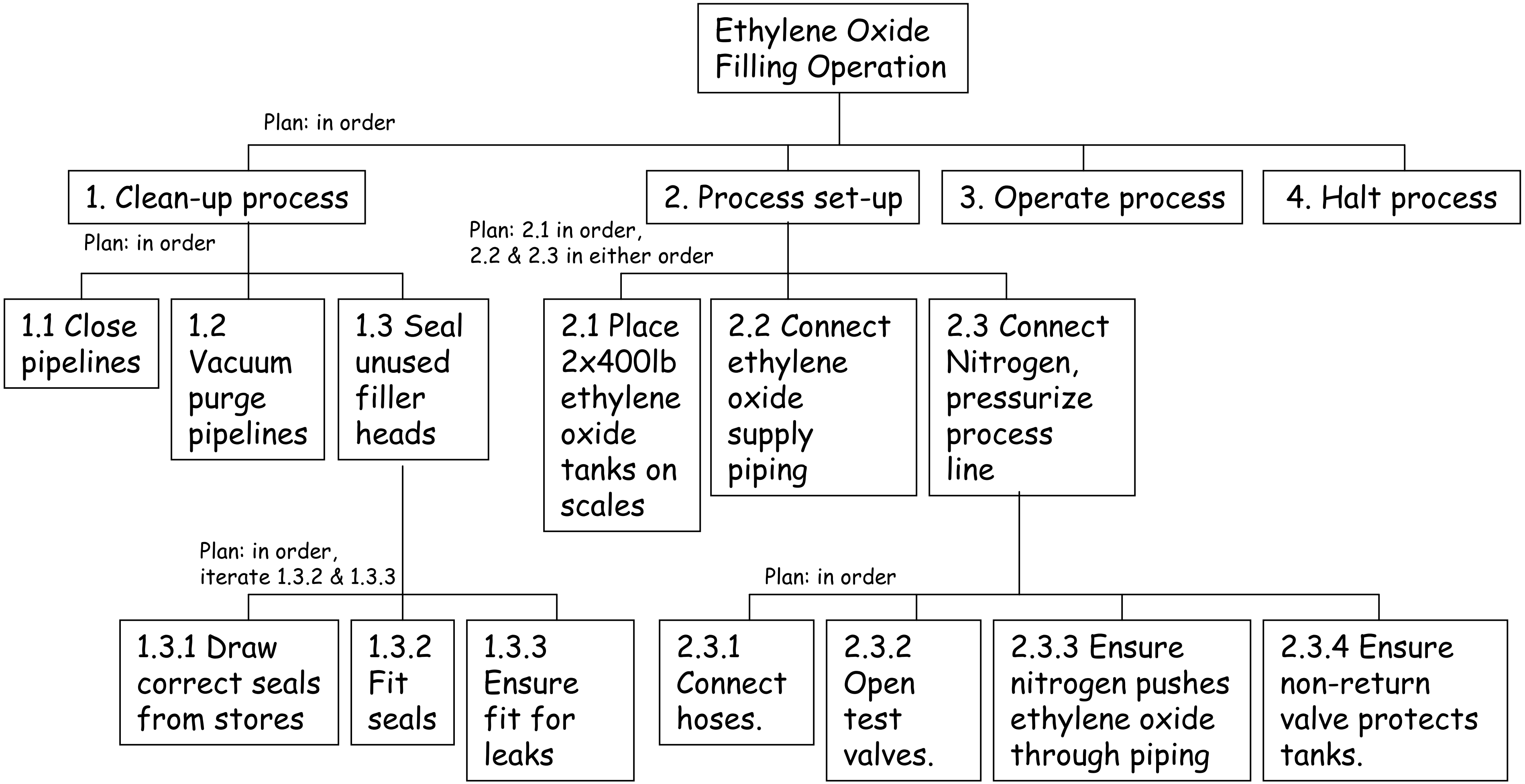
- 'Fit for leaks' net probability 0.594:
  - Clear need for intervention but what?
- Consequence reduction:
  - Focus on filtering/breathing systems.
- Error pathway blocking:
  - Prevent process set-up until fit confirmed.
- Error recovery enhancement:
  - Ensure clear evacuation procedures…

4. Task Redesign

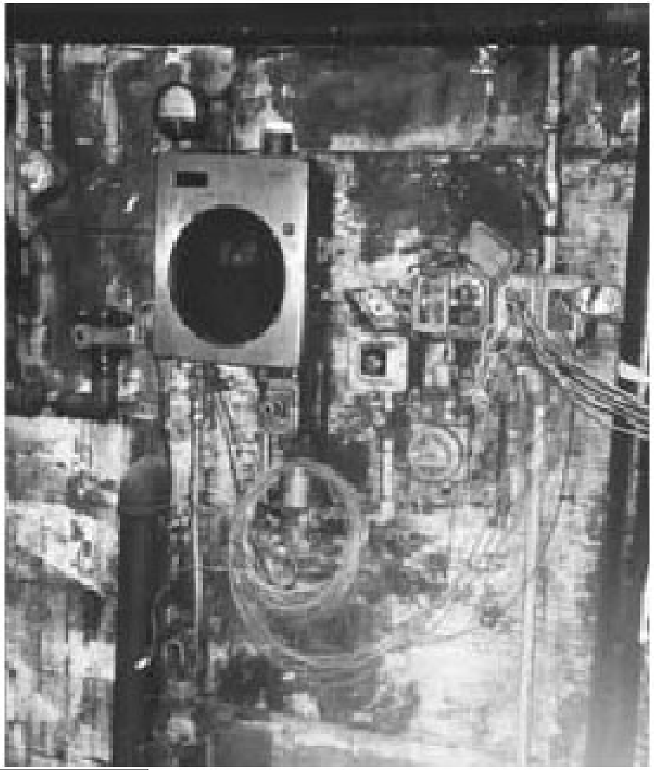
- Address performance shaping factors:
  - Reduce distractions during fit checks.
- Increase predictability:
  - Ensure caps are of good quality, standardised...
- Enhance detection:
  - Deploy pressure alarms on delivery pipes?
- Increase controllability:
  - Consider excess flow valves to cut-off leaks…
- Increase competence:
  - Emphasize consequences of failure in training.

12.30-13.00:
Break and group session 3
(HRA exercise).

1. Task Analysis



Your Task



Temperature Chart and Digital Display

The round window in the aluminum box contained the temperature chart. The rectangular cutout above and to the left of the chart contained the digital temperature readout.

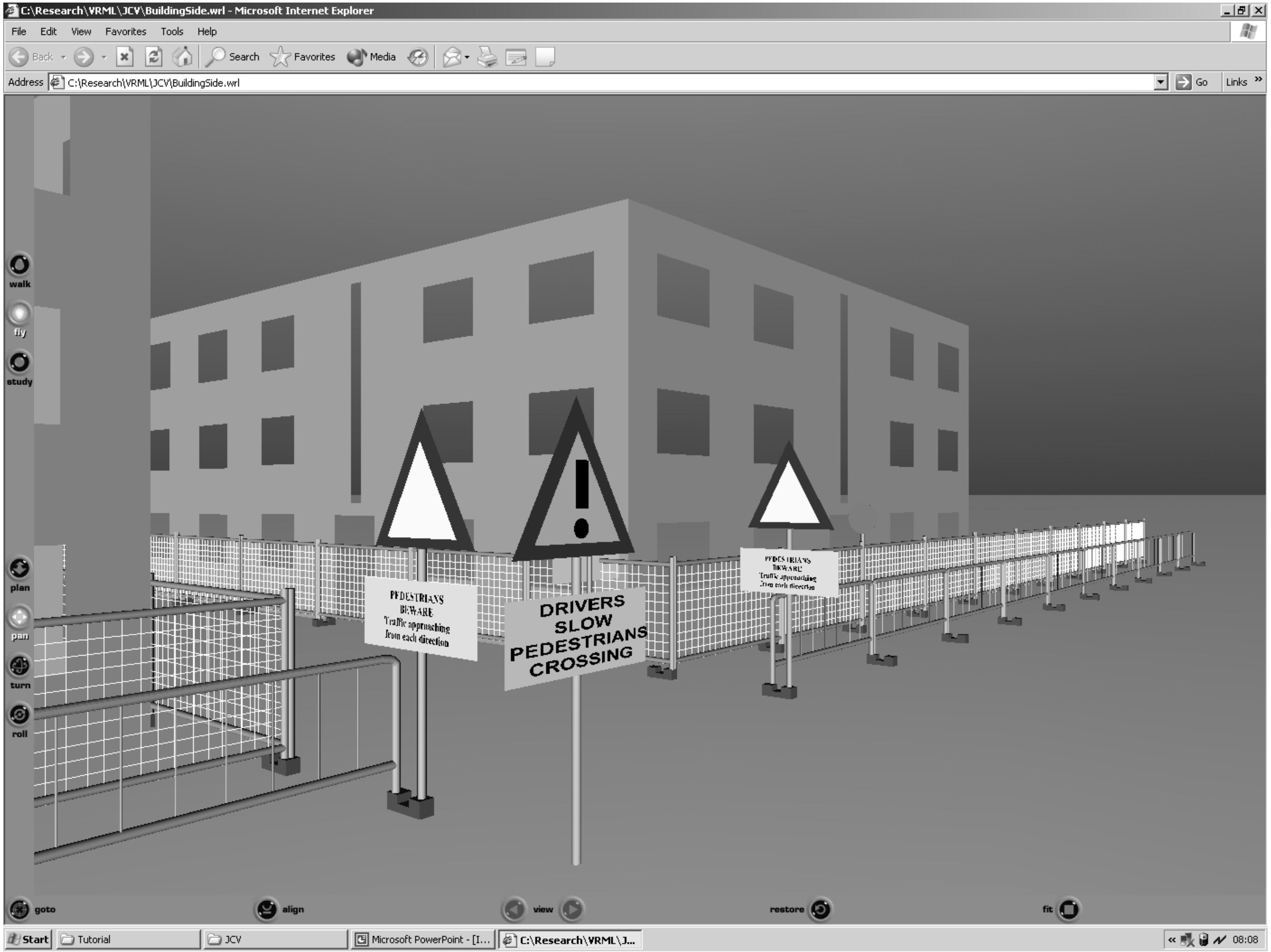
- Try HEART yourself.
- Quantify error likelihood.
- Identify remedial actions?
- BUT:
  - You will need to make assumptions.
  - What validation would you do?

Task Redesign (Cont.)

Microsoft PowerPoint - [IIRGulf_Johnson_tutorial_final]
ControlRoom.mov
File Edit Movie QTV Window Help
Start
QTVR
Microsoft PowerPoint - [I...
NEA Radiation Protection...
Chernobyl Accident Rep...
ControlRoom.mov
08:30


lukasCutterObj.mov

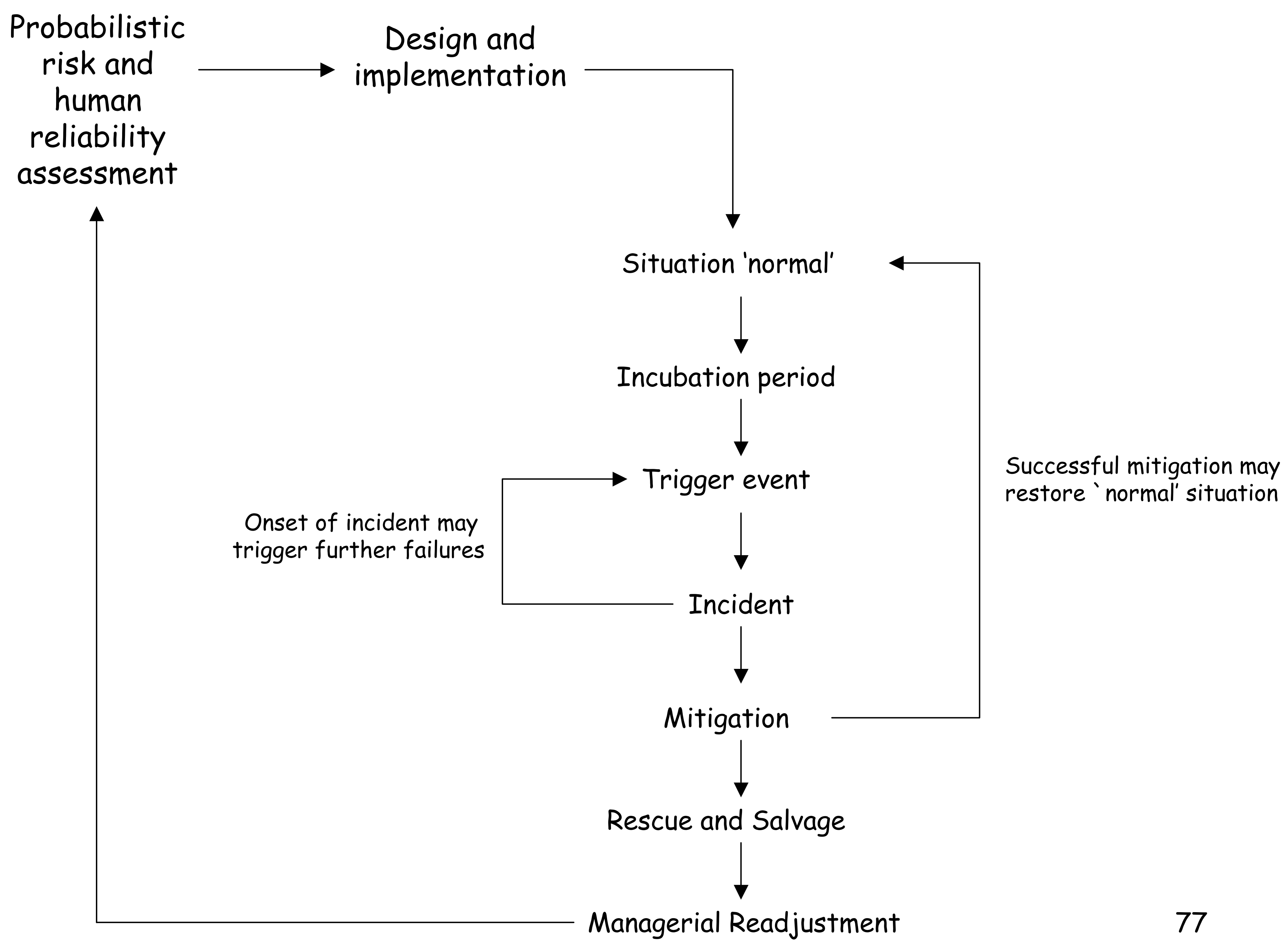

lukasCutter.mov
Lukas Dedicated
Body Cutter.....


C:\Research\VRML\JCV\BuildingSide.wrl - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address C:\Research\VRML\JCV\BuildingSide.wrl
Go Links
PEDESTRIANS BEWARE Traffic approaching from each direction
DRIVERS SLOW PEDESTRIANS CROSSING
walk
fly
study
plan
pan
turn
roll
goto
align
view
restore
fit
Start
Tutorial
JCV
Microsoft PowerPoint - [I...
C:\Research\VRML\J...
08:08

Part 4

1. What is human error?
2. Human error in risk assessment.
3. Human Reliability Analysis techniques.

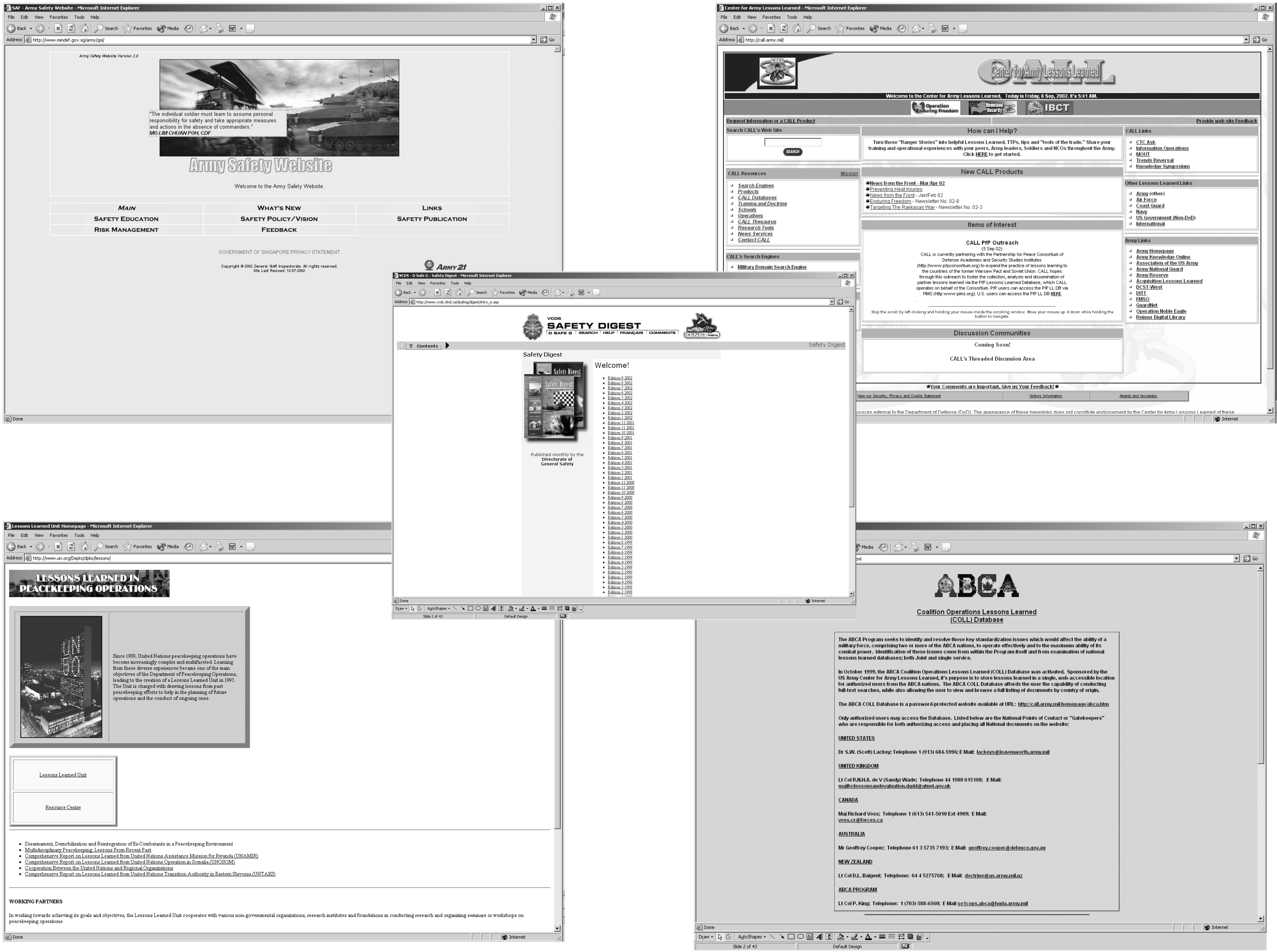
> 4. Human error in safety management.


Probabilistic risk and human reliability assessment
Design and implementation
Situation 'normal'
Incubation period
Trigger event
Incident
Mitigation
Rescue and Salvage
Managerial Readjustment
Onset of incident may trigger further failures
Successful mitigation may restore `normal' situation

So what happens in practice?

	World War II (1942-1945)	Korea (1950-1953)	Vietnam (1965-1972)	Desert Storm and Desert Shield (1990-1991)
Accidents	56%	44%	54%	75%
Friendly Fire	1%	1%	1%	5%
Enemy Actions	43%	55%	45%	20%

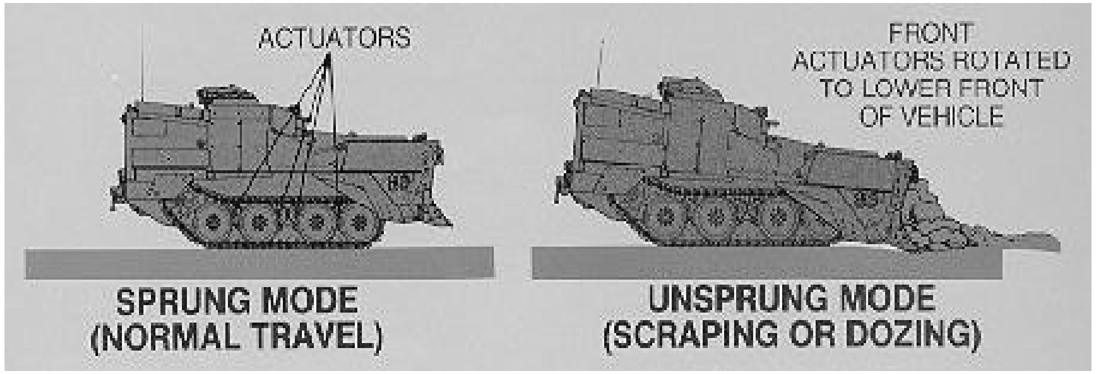
Percentage of all accounted casualties, fatal and non-fatal (US Army, Risk Management Field Manual 100-14)



SAF - Army Safety Website - Microsoft Internet Explorer
"The individual soldier must learn to assume personal responsibility for safety and take appropriate measures and actions in the absence of commanders."
MG LIM CHUAN POH, CDF
Army Safety Website
Welcome to the Army Safety Website.
MAIN
WHAT'S NEW
LINKS
SAFETY EDUCATION
SAFETY POLICY/VISION
SAFETY PUBLICATION
RISK MANAGEMENT
FEEDBACK
GOVERNMENT OF SINGAPORE PRIVACY STATEMENT
ARMY 21
Center for Army Lessons Learned - Microsoft Internet Explorer
Center for Army Lessons Learned
Welcome to the Center for Army Lessons Learned, Today is Friday, 6 Sep, 2002. It's 5:41 AM.
Operation Enduring Freedom
IBCT
Request Information or a CALL Product
Provide web site Feedback
How can I Help?
Turn those "Ranger Stories" into helpful Lessons Learned, TTPs, tips and "tools of the trade." Share your training and operational experiences with your peers, Army leaders, Soldiers and NCOs throughout the Army. Click HERE to get started.
New CALL Products
Items of Interest
CALL PfP Outreach
Discussion Communities
Coming Soon!
CALL's Threaded Discussion Area
CALL Links
Other Lessons Learned Links
Army Links
VCDS - D Safe G - Safety Digest - Microsoft Internet Explorer
SAFETY DIGEST
Safety Digest
Welcome!
Published monthly by the Directorate of General Safety
Lessons Learned Unit Homepage - Microsoft Internet Explorer
LESSONS LEARNED IN PEACEKEEPING OPERATIONS
Since 1989, United Nations peacekeeping operations have become increasingly complex and multifaceted. Learning from these diverse experiences became one of the main objectives of the Department of Peacekeeping Operations, leading to the creation of a Lessons Learned Unit in 1995. The Unit is charged with drawing lessons from past peacekeeping efforts to help in the planning of future operations and the conduct of ongoing ones.
Lessons Learned Unit
Resource Centre
Disarmament, Demobilization and Reintegration of Ex-Combatants in a Peacekeeping Environment
Multidisciplinary Peacekeeping: Lessons From Recent Past
Comprehensive Report on Lessons Learned from United Nations Assistance Mission for Rwanda (UNAMIR)
Comprehensive Report on Lessons Learned from United Nations Operation in Somalia (UNOSOM)
Cooperation Between the United Nations and Regional Organizations
Comprehensive Report on Lessons Learned from United Nations Transition Authority in Eastern Slavonia (UNTAES)
WORKING PARTNERS
In working towards achieving its goals and objectives, the Lessons Learned Unit cooperates with various non-governmental organizations, research institutes and foundations in conducting research and organizing seminars or workshops on peacekeeping operations.
ABCA
Coalition Operations Lessons Learned (COLL) Database
The ABCA Program seeks to identify and resolve those key standardization issues which would affect the ability of a military force, comprising two or more of the ABCA nations, to operate effectively and to the maximum ability of its combat power. Identification of those issues come from within the Program itself and from examination of national lessons learned databases; both Joint and single service.
In October 1999, the ABCA Coalition Operations Lessons Learned (COLL) Database was activated. Sponsored by the US Army Center for Army Lessons Learned, it's purpose is to store lessons learned in a single, web-accessible location for authorized users from the ABCA nations. The ABCA COLL Database affords the user the capability of conducting full-text searches, while also allowing the user to view and browse a full listing of documents by country of origin.
The ABCA COLL Database is a password-protected website available at URL: http://call.army.mil/homepage/abca.htm
Only authorized users may access the Database. Listed below are the National Points of Contact or "Gatekeepers" who are responsible for both authorizing access and placing all National documents on the website:
UNITED STATES
UNITED KINGDOM
CANADA
AUSTRALIA
NEW ZEALAND
ABCA PROGRAM

Decision Making and Scale

- 8+ revisions of US M9 Armored Combat Earthmover manuals in a single month in 2000:
  - TM5-2350-262-10, TM5-2350-262-10HR, LO5-2350-262-12, TM5-2350-262-20-1 & 2,
  - TM5-2350-262-20-3, TM5-2350-262-34, TM5-2350-262-24P, TM5-2815-240-34 & P.
- Problems of scale and complexity require carefully designed reporting processes.
- The US Army's (2000) Accident Investigation and Reporting Procedures Handbook
  - Department of Army 60 days to inform Army Safety Center of corrective actions.
  - Interim and follow-up reports required every 90 days until the actions are closed.



Limitation 1: Technological' Change

- M939A2 'fish-tailed'' on a steep hill:
  - Weather, road conditions good;
  - Trailor tires blew and truck rolls off road;
  - Tires well-maintained, no defects;
  - Witnesses state vehicle under speed limit.

- *Any Safety-of-Use-Messages or Ground Precautionary Messages?*
  - Unit personnel said no, M939A2s only recently replace older models;
  - Investigation board checks Army Electronic Product Support Bulletin Board;
  - 2 safety messages limit M939A2 to 45mph until antilock brakes & radials fitted;
  - When maintenance received messages they didn't have any M939A2 trucks…

Limitation 2: Organisational Change

- The US Army's Modification Work Order (MWO) program:
  - ensure 'identified operational and safety problems' consistently implemented across US Army
  - centralized database records progress of maintenance recommendations.
  - Army Headquarters & Materiel Command query if units meet timescales in safety notices.

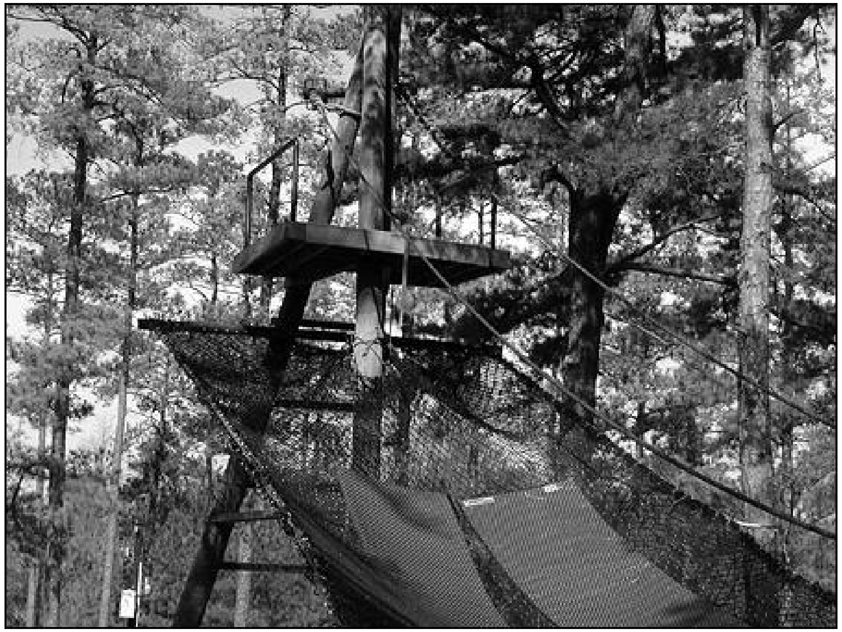
- Database discontinued following a structural reorganization in 1990:
  - Control over modification funding transferred from HQ;
  - Control given to program sponsors
  - Weapon systems, eg M1A1 tank, or product support centres, eg Squad Automatic Weapon.

- 'Army headquarters and Materiel Command officials don't have adequate overview of equipment modifications across the force, funding requirements, logistical support requirements and information for deployment decisions' (US Army Safety Center, 2001).

Limitation 3: Organizational Complexity

- Soldier falls during 'inverted' rope descent.
- Previous incidents led to US Army FM21-20:
  - include platform at top and safety net.
  - use Corps of Engineers drawing 28-13-95.
  - diagram didnt include safety net or platform!!

'Confusion exists concerning the proper design and construction of this obstacle'



Limitation 4: Safety Culture

National Defence Authorization Act:

- develop Ranger 'safety cells';
- must know geographic training area (weather etc.);
- But Act doesn't give detailed guidance.

General Accounting Office report:

- "no change from safety oversight" at time of incidents;
- focus on "checklists of procedures";
- "whether files of safety regulations and risk assessments are maintained"
- Do not monitor effectiveness of incident recommendations.

Limitation 5: Risk Analysis

- Canadian Engineering Officer hurt when fragment shatters bunker viewport:
  - 4-ply laminate glass design 100 kg of TNT at 130M with less than 2% glass loss;
  - Glazing performed as designed, 2% glass lost in the eye of a student.
- Recommendations:
  - sacrificial polycarbonate can be replaced if damaged, final protection for viewers;
  - Or plentiful supply of “offset viewblock” NSN 6650-12-171-9741 tank periscope.
- But sacrificial layers increase glass thickness and so use video?

Limitation 6: Inherent Risk

- Never under-estimate organizational complexity of human 'error'…

- "Many units stated first aid training packages lack realism. IV and morphine training were essential... During 6 months in theatre, no soldier gave artificial respiration, treated a fracture or did Heimlich manoeuvre. Treated 17 bullet-wounds, 3 shrapnel-wounds and 7 minefield cases.

As threat level dropped for latter rotations, comments on need for IV and morphine training waned. All unit medical staff strongly recommend that it not be completed because of inherent dangers in administering IVs or morphine…"

(Canadian Army's Lessons Learned Centre, NATO Implementation & Stabilization Force in Bosnia-Herzegovina. 1999)

- Balancing operational need and medical caution?

Conclusions

- Key topics:
  - What is human error?
  - Human error in risk assessment.
  - Human Reliability Analysis techniques.
  - Human error in safety management.

Questions?

Thanks are due in particular to:

David Wright,
Intensive Care Unit,
Edinburgh Western General Hospital.

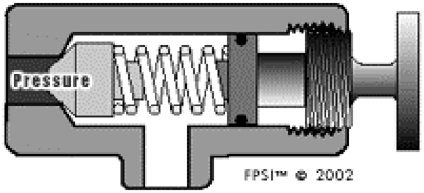
Barbara Holland,
Paediatric Intensive Care Unit,
Yorkhill Hospital, Glasgow.

Clinical Negligence and Other Risks Scheme,
Scottish Executive.

http://www.dcs.gla.ac.uk/~johnson

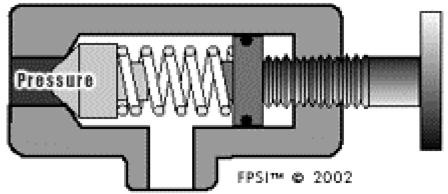
HAZOPS

- Primary keywords describe process:
  - Flow,Temperature, Pressure, Level
  - Separate (settle, filter, centrifuge)
  - Composition, React, Mix
  - Reduce (grind, crush, etc.), Absorb
  - Corrode, Erode, Isolate, Drain
  - Vent, Purge, Inspect, Maintain
  - Start-up, Shutdown



pressure relief valve
(design 1)

HAZOPS



pressure relief valve
(design 2)

- Secondary keywords describe problems:
  - No - design intent doesnt occur (e.g. Flow/No).
  - Less - decrease in design intent (e.g. Pressure/Less)
  - More - increase in design intent (e.g. Temperature/More)
  - Reverse - opposite of design intent (e.g. Flow/Reverse)
  - Also - design fulfilled but another activity also occurs (e.g. Flow/Also contamination)
  - Other - activity occurs but not in way intended (e.g. Flow/Other indicates leak)
  - Fluctuation - design achieved part of time (e.g. airlock in pipeline Flow/Fluctuation)
  - Early - step is started at the wrong time or done out of sequence
  - Late - As for Early

HAZOPS

Guide word	Deviation	Possible cause	Consequences	Safeguards	Action Required
More of	High flow	(i) Failure to close off XMV and SV (ii) Collapse of ASV membrane	Overpressure of venting system downstream.	Automated pressure detection system within specified range	Procedures to allow inspection of plates and membranes in venting system. HAZ1 – venting system needs more thorough review to identify dispersion sites.
Less of	Low flow	Blockage of inlets through contamination.	Delayed depressurisation upstream may overpressurise this section.		
No/None	No flow		No hazard – operators will detect and respond to this problem.		