Causal Analysis for Incident and Accident Investigation

(involving people and programmable systems)

Chris Johnson

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

June 2003

Rough Timings…

- 09.00-09.30 Overview
- 09.30-12.00 STAMP
  - 11.00-12.00 Group Session 1 (coffee @ 10.30)
- 12.00-13.30 Lunch
- 13.30-16.00 PARC
  - 15.00-16.00 Group Session 2 (tea @ 3)
- 16.00 End.

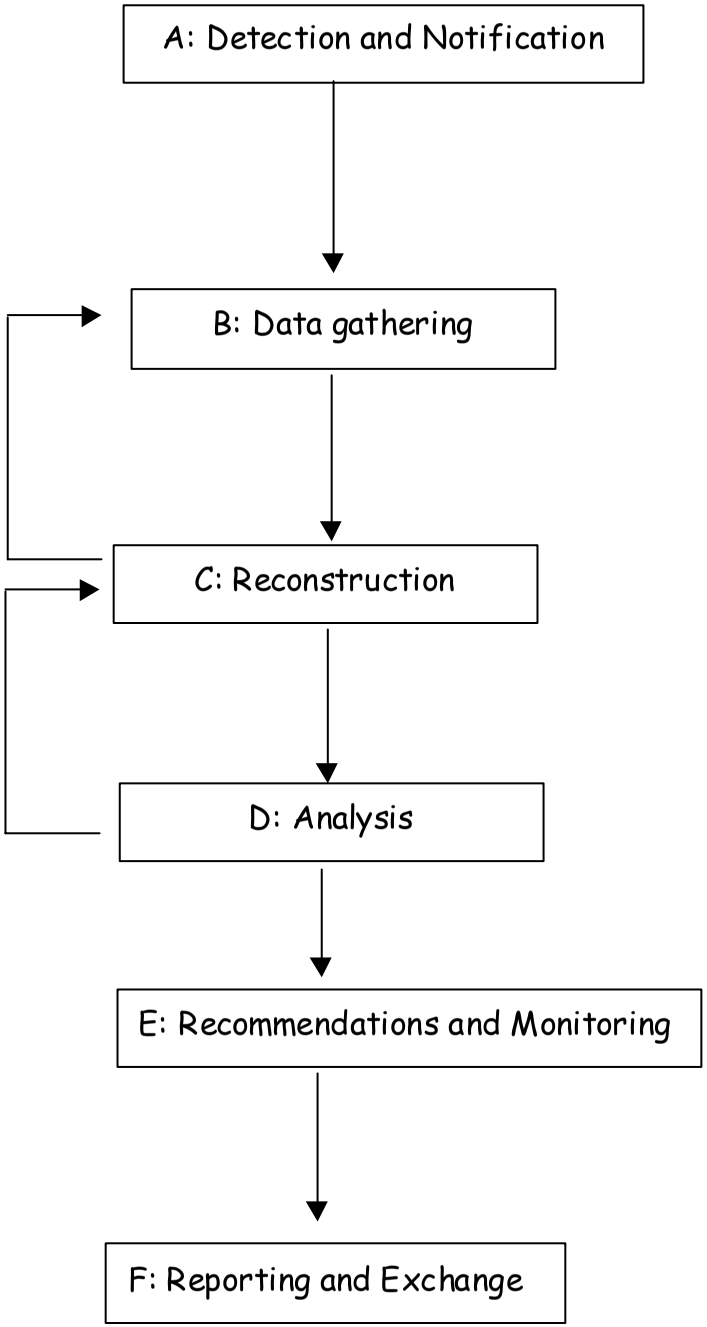
Part 1

> 1. Overview

2. STAMP: System Theoretic Accident Modelling & Processes

3. PARCEL: Programmable Electronic Systems Analysis of Root Causes.

4. Wrap-up.


A: Detection and Notification
B: Data gathering
C: Reconstruction
D: Analysis
E: Recommendations and Monitoring
F: Reporting and Exchange

Department of the Army
Pamphlet 385–40

Safety

Army Accident Investigation and Reporting

Headquarters
Department of the Army
Washington, DC
1 November 1994

Unclassified

Determining System Inadequacy(ies) Responsible for Human Error

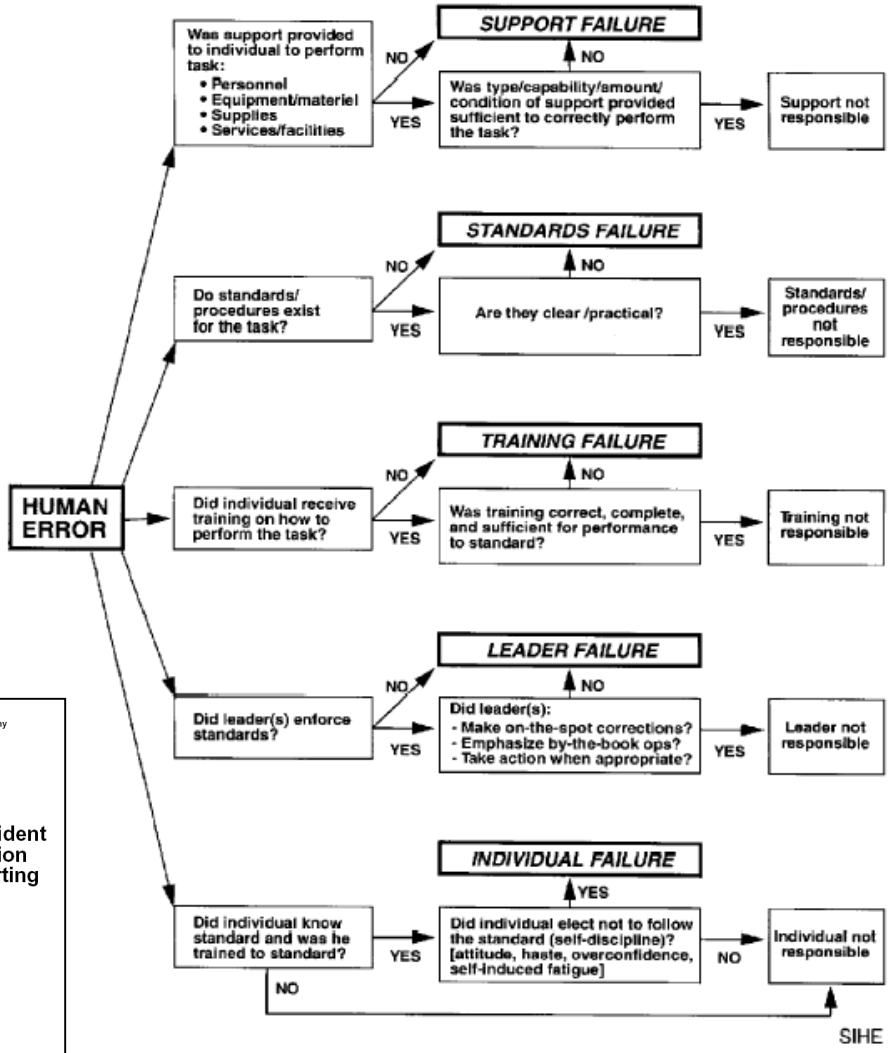


Figure 2-1. Determining system inadequacy(ies) responsible for human error

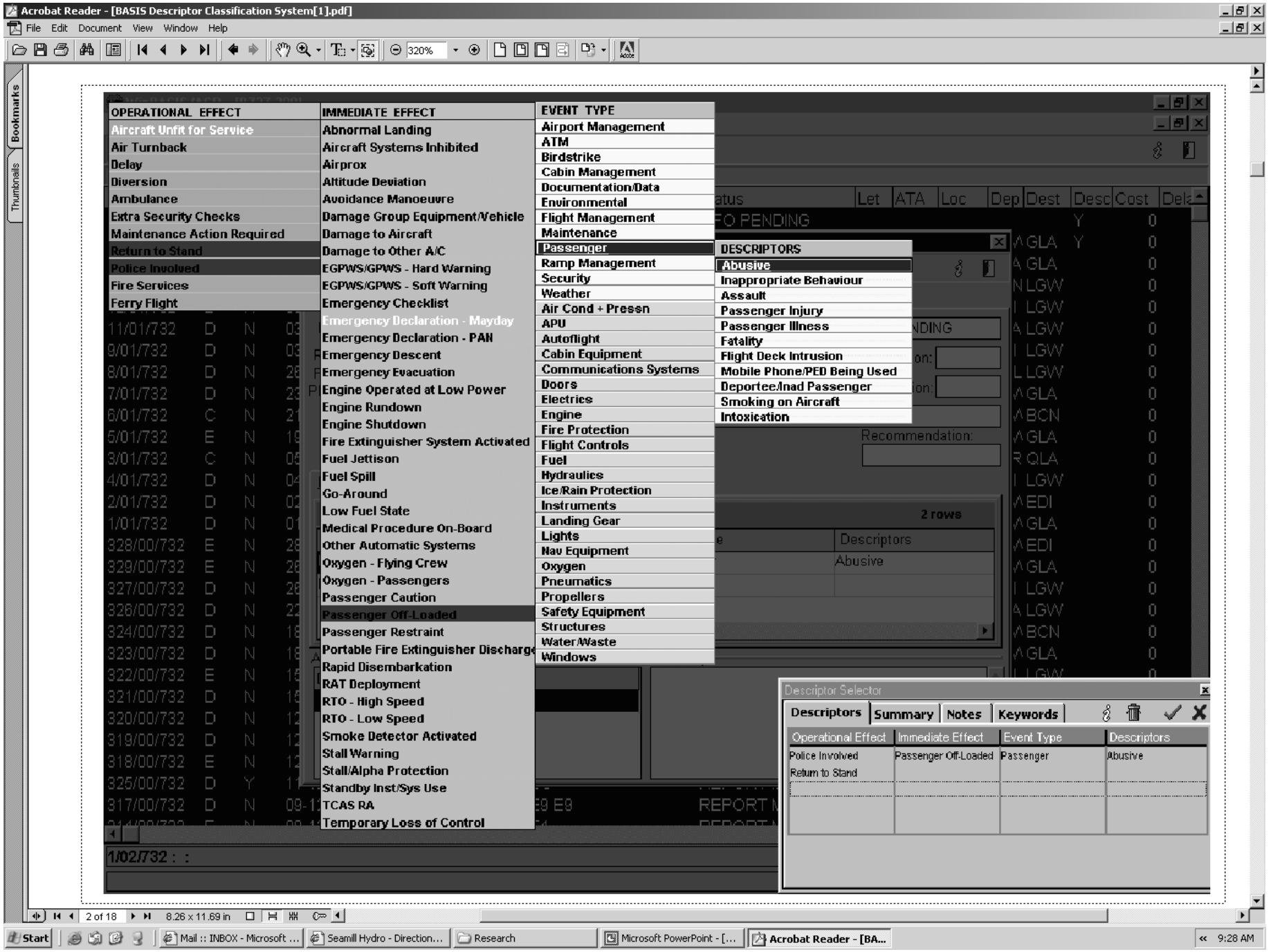
System Inadequacies/Readiness Shortcomings/Root Causes

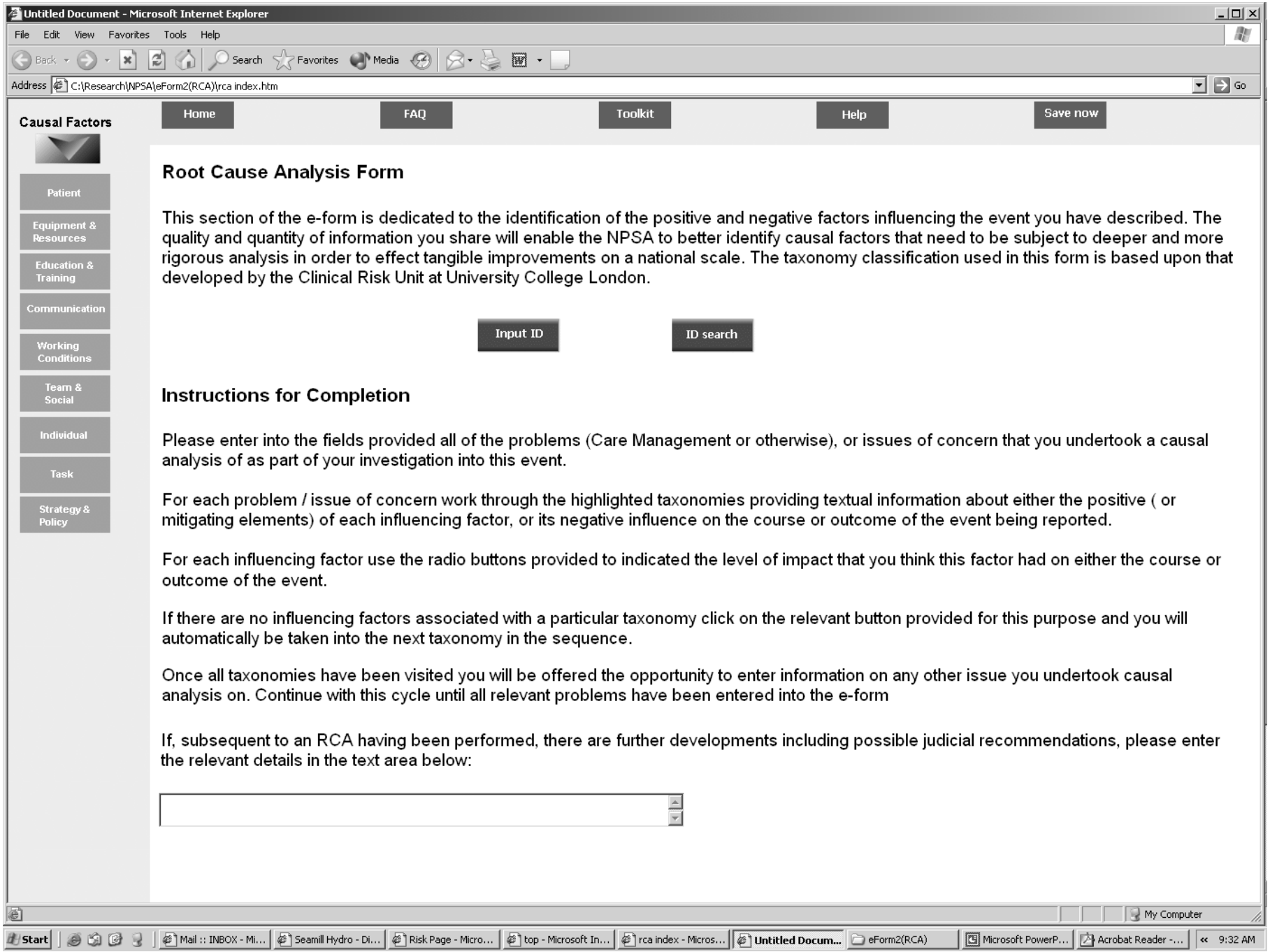
LEADER FAILURE
Code: 01 Key Word/Explanation: Inadequate/improper supervision by higher command.
Code: 02 Key Word/Explanation: Inadequate/improper supervision by staff officer.
Code: 03 Key Word/Explanation: Inadequate/improper supervision by unit command.
Code: 04 Key Word/Explanation: Inadequate/improper 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

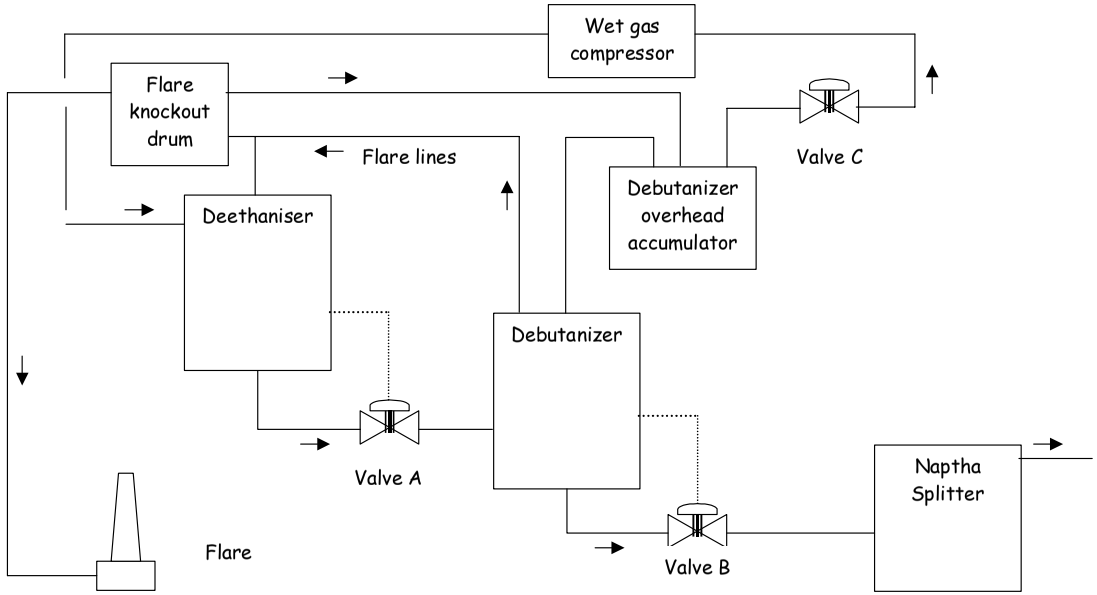
Table B–5
System Inadequacies/Readiness Shortcomings/Root Causes—Continued

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.


Acrobat Reader - [BASIS Descriptor Classification System[1].pdf]
File Edit Document View Window Help
OPERATIONAL EFFECT
Aircraft Unfit for Service
Air Turnback
Delay
Diversion
Ambulance
Extra Security Checks
Maintenance Action Required
Return to Stand
Police Involved
Fire Services
Ferry Flight
IMMEDIATE EFFECT
Abnormal Landing
Aircraft Systems Inhibited
Airprox
Altitude Deviation
Avoidance Manoeuvre
Damage Group Equipment/Vehicle
Damage to Aircraft
Damage to Other A/C
EGPWS/GPWS - Hard Warning
EGPWS/GPWS - Soft Warning
Emergency Checklist
Emergency Declaration - Mayday
Emergency Declaration - PAN
Emergency Descent
Emergency Evacuation
Engine Operated at Low Power
Engine Rundown
Engine Shutdown
Fire Extinguisher System Activated
Fuel Jettison
Fuel Spill
Go-Around
Low Fuel State
Medical Procedure On-Board
Other Automatic Systems
Oxygen - Flying Crew
Oxygen - Passengers
Passenger Caution
Passenger Off-Loaded
Passenger Restraint
Portable Fire Extinguisher Discharge
Rapid Disembarkation
RAT Deployment
RTO - High Speed
RTO - Low Speed
Smoke Detector Activated
Stall Warning
Stall/Alpha Protection
Standby Inst/Sys Use
TCAS RA
Temporary Loss of Control
EVENT TYPE
Airport Management
ATM
Birdstrike
Cabin Management
Documentation/Data
Environmental
Flight Management
Maintenance
Passenger
Ramp Management
Security
Weather
Air Cond + Press'n
APU
Autoflight
Cabin Equipment
Communications Systems
Doors
Electrics
Engine
Fire Protection
Flight Controls
Fuel
Hydraulics
Ice/Rain Protection
Instruments
Landing Gear
Lights
Nav Equipment
Oxygen
Pneumatics
Propellers
Safety Equipment
Structures
Water/Waste
Windows
DESCRIPTORS
Abusive
Inappropriate Behaviour
Assault
Passenger Injury
Passenger Illness
Fatality
Flight Deck Intrusion
Mobile Phone/PED Being Used
Deportee/Inad Passenger
Smoking on Aircraft
Intoxication
Recommendation:
2 rows
Descriptors
Abusive
Descriptor Selector
Descriptors
Summary
Notes
Keywords
Operational Effect
Immediate Effect
Event Type
Descriptors
Police Involved
Return to Stand
Passenger Off-Loaded
Passenger
Abusive
1/02/732 : :
2 of 18
8.26 x 11.69 in
Start
Mail :: INBOX - Microsoft ...
Seamill Hydro - Direction...
Research
Microsoft PowerPoint - [...
Acrobat Reader - [BA...
9:28 AM


Untitled Document - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address C:\Research\NPSA\eForm2(RCA)\rca index.htm
Go
Causal Factors
Home
FAQ
Toolkit
Help
Save now
Patient
Equipment & Resources
Education & Training
Communication
Working Conditions
Team & Social
Individual
Task
Strategy & Policy
Root Cause Analysis Form
This section of the e-form is dedicated to the identification of the positive and negative factors influencing the event you have described. The quality and quantity of information you share will enable the NPSA to better identify causal factors that need to be subject to deeper and more rigorous analysis in order to effect tangible improvements on a national scale. The taxonomy classification used in this form is based upon that developed by the Clinical Risk Unit at University College London.
Input ID
ID search
Instructions for Completion
Please enter into the fields provided all of the problems (Care Management or otherwise), or issues of concern that you undertook a causal analysis of as part of your investigation into this event.
For each problem / issue of concern work through the highlighted taxonomies providing textual information about either the positive (or mitigating elements) of each influencing factor, or its negative influence on the course or outcome of the event being reported.
For each influencing factor use the radio buttons provided to indicated the level of impact that you think this factor had on either the course or outcome of the event.
If there are no influencing factors associated with a particular taxonomy click on the relevant button provided for this purpose and you will automatically be taken into the next taxonomy in the sequence.
Once all taxonomies have been visited you will be offered the opportunity to enter information on any other issue you undertook causal analysis on. Continue with this cycle until all relevant problems have been entered into the e-form
If, subsequent to an RCA having been performed, there are further developments including possible judicial recommendations, please enter the relevant details in the text area below:
My Computer
Start
Mail :: INBOX - Mi...
Seamill Hydro - Di...
Risk Page - Micro...
top - Microsoft In...
rca index - Micros...
Untitled Docum...
eForm2(RCA)
Microsoft PowerP...
Acrobat Reader -...
9:32 AM

Milford Haven



Control system closes valve A, starves debutanizer.

Also closes valve B, heating raises debutanizer pressure.

Opens valve A, debutanizer flow restored.

Valve B should open to splitter.

Operators see misleading signals, valve B shown open.

Debutanizer fills while naptha splitter empties.

Motivation: Milford Haven

Separate displays.

Didnt check status of valve B, operators open valve C.

Debutanizer vents to flare, wet gas compressor restarts.

Should increase flow but increases debutanizer pressure.

Material vents to flare drum, corroded discharge breaks.

20 tonnes of hydrocarbon ignites, damage > £50 million.

Motivation: Milford Haven

- Human 'Error' and Plant Design/Operation

"The incident developed from the initial causative problems largely because of the combined effects of two factors. Firstly, operators were not provided with information systems configured to help them identify the root cause of such problems. Secondly, the preparation of shift operators and supervisors for dealing with a sustained upset and therefore stressful situation was inadequate.

- The alarm system was such that warnings of crucial problems were lost in the plethora of general and less important alarms…With alarms going off every two to three seconds, operators did not and could not react appropriately to each alarm."

Motivation: Milford Haven

- Safety Management Systems

"All of the key elements of the incident, and lessons drawn from it, have been seen and publicised before, in major accidents around the world. Those who are responsible for operating hazardous plants must have systems in place that bring to their attention these lessons of history.

The incident investigation demonstrated that some of the company's crucial safety management systems were not adequately performing their function. Examples are the systems for modification and inspection. The company was unaware of these defects in its safety management systems because its monitoring of their performance did not effective highlight the problems."

Motivation: Milford Haven

- Risk Assessment

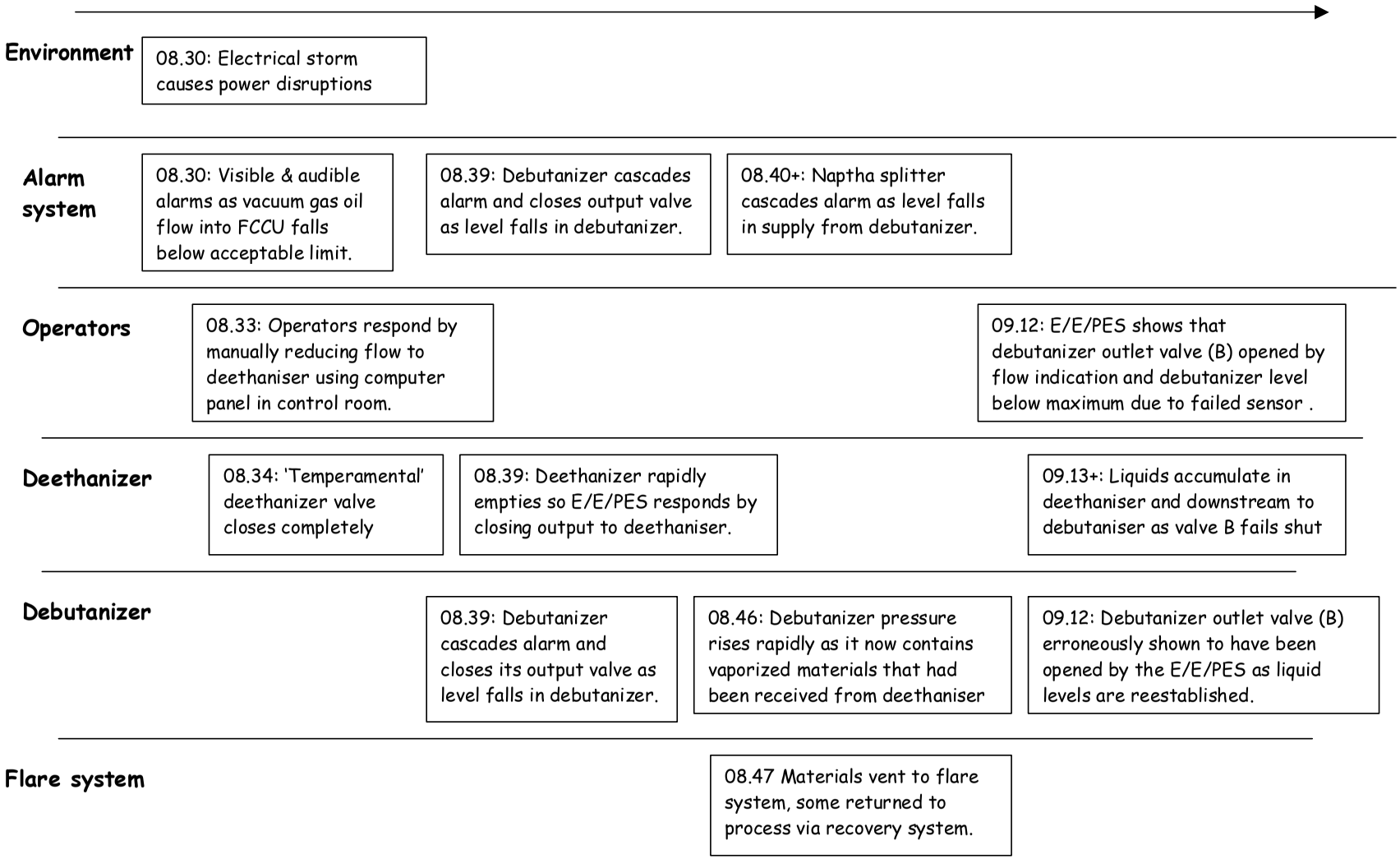
NB 3 years before the accident a modification was carried out so that automated high-capacity discharge pumps were no longer automatically started to move excess to slops when the flare discharge tank was full. Instead, low capacity pumps recycle material back to production process. Valves had to be operated manually if high-capacity pumping to slops was needed but this was seldom (never?) practiced.

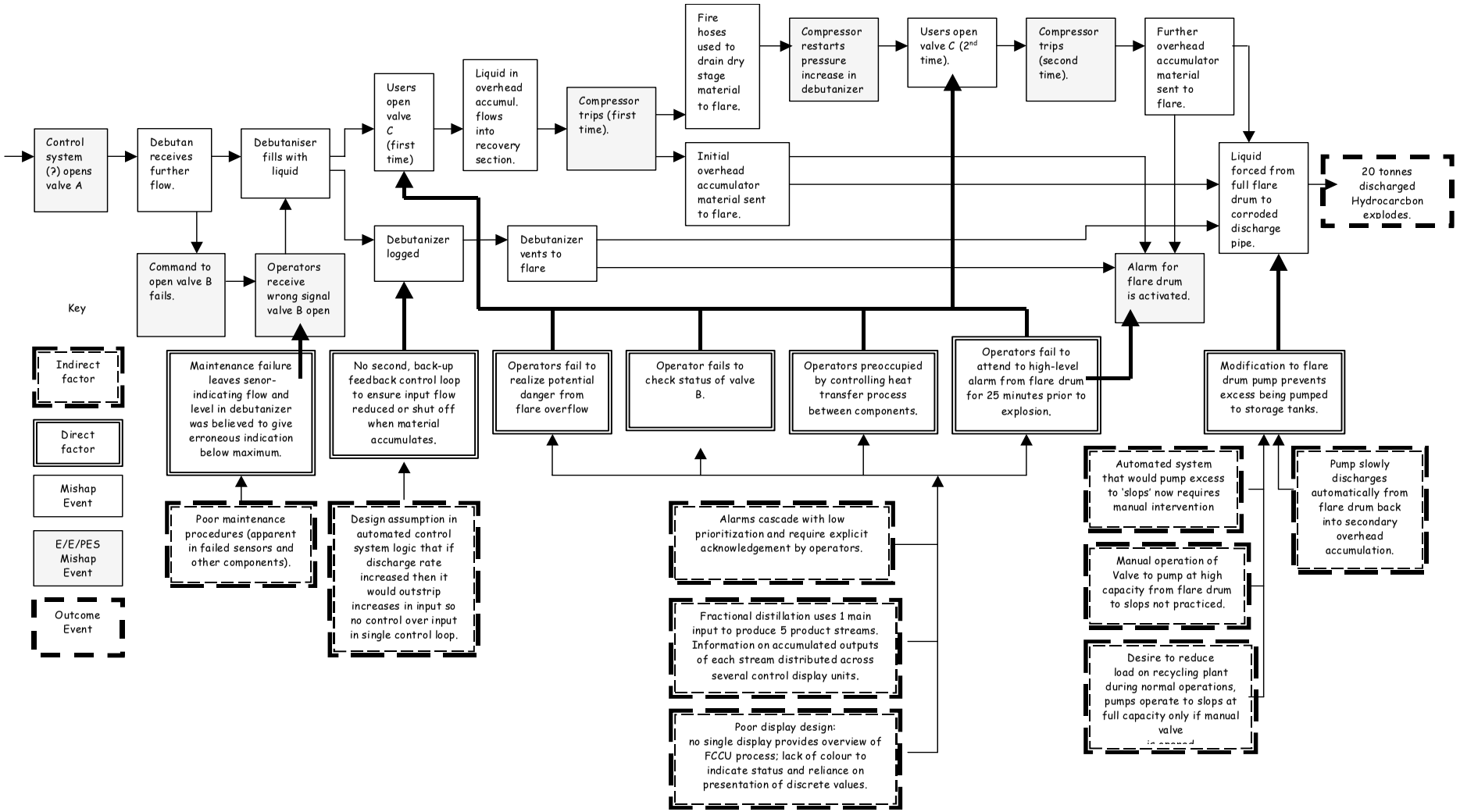
"There should be a formal, controlled procedure for hazard identification and operability analysis for modifications (including emergency modifications) that ensures all safety issues identified at the design stage are reflected in how the modification is constructed and used…"

General Causal Analysis : Elicitation and Reconstruction

Barrier	Reason for failure?
Control loops link level in each vessel to discharge rate.	No control over input to vessel so assumes discharge rate can always exceed input rate. This was not the case during the incident.
	No secondary control loop to monitor input rate and limit it if this exceeded output. Hence there was no backup or secondary control system.
	Key sensors provided erroneous information to control system.
Control system displays linked to multiple level alarms.	Operators couldnt identify reason for alarms, especially valve B was closed, displays were grouped according to sub-processes hence it was difficult to gain over view of the system state.
	Operators were progressively overloaded with alarms. In the last eleven minutes they were expected to read and confirm 275 individual alarms, with similar high severity levels.

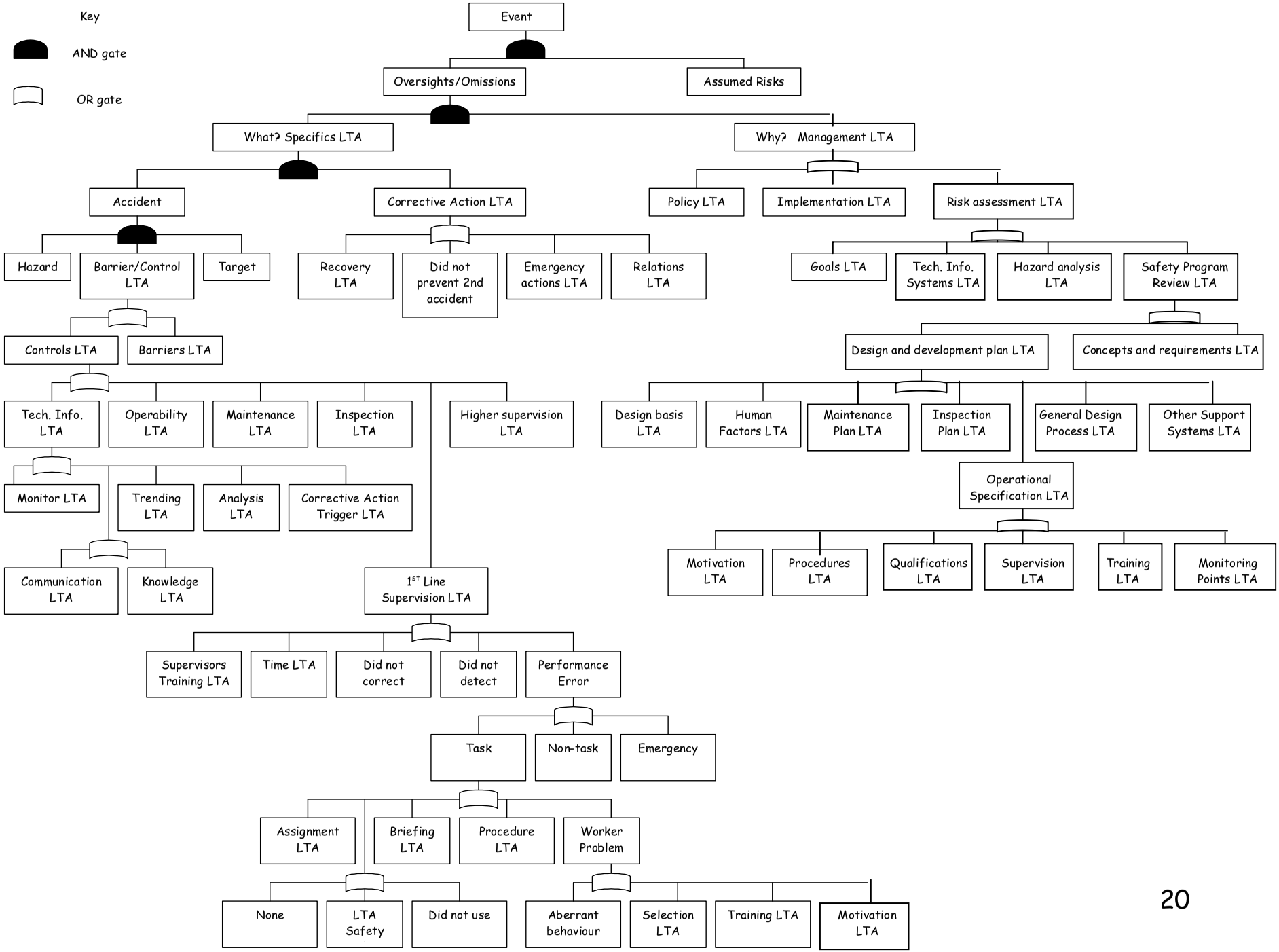
Prior/Ideal Condition	Present Condition	Effect of Change
All modifications that have safety implications should be considered by a formal hazard assessment.	The modification to the flare system that reduced the normal transfer capacity to storage tanks so that material could be recovered back to the production process was not considered in any formal safety assessment.	Assumed operators would manually restore system configuration so high-capacity pumps could remove excess materials from flare knockout drum. Operators unprepared to do this by lack of training and difficulty of diagnosing the state of their system.
Maintenance procedures should ensure that E/E/PES applications have accurate and timely information to meet control requirements.	After the incident 40 control loops tested. 24 required maintenance from minor mechanical damage to major faults. Only faulty debutanizer outlet valve (labeled B) occurred on the day of the incident. All of the rest were either known about or had not been detected for some time.	Maintenance issues created latent conditions for lightening strike to act as catalyst. Key readings confused operators. E/E/PES sensors downstream report valve B closed. However, flow indicator closest to valve indicated a flow and level in debutanizer that was below maximum even though full.


Environment
08.30: Electrical storm causes power disruptions
Alarm system
08.30: Visible & audible alarms as vacuum gas oil flow into FCCU falls below acceptable limit.
08.39: Debutanizer cascades alarm and closes output valve as level falls in debutanizer.
08.40+: Naptha splitter cascades alarm as level falls in supply from debutanizer.
Operators
08.33: Operators respond by manually reducing flow to deethaniser using computer panel in control room.
09.12: E/E/PES shows that debutanizer outlet valve (B) opened by flow indication and debutanizer level below maximum due to failed sensor .
Deethanizer
08.34: 'Temperamental' deethanizer valve closes completely
08.39: Deethanizer rapidly empties so E/E/PES responds by closing output to deethaniser.
09.13+: Liquids accumulate in deethaniser and downstream to debutaniser as valve B fails shut
Debutanizer
08.39: Debutanizer cascades alarm and closes its output valve as level falls in debutanizer.
08.46: Debutanizer pressure rises rapidly as it now contains vaporized materials that had been received from deethaniser
09.12: Debutanizer outlet valve (B) erroneously shown to have been opened by the E/E/PES as liquid levels are reestablished.
Flare system
08.47 Materials vent to flare system, some returned to process via recovery system.


Control system (?) opens valve A
Debutan receives further flow.
Debutaniser fills with liquid
Users open valve C (first time)
Liquid in overhead accumul. flows into recovery section.
Compressor trips (first time).
Fire hoses used to drain dry stage material to flare.
Compressor restarts pressure increase in debutanizer
Users open valve C (2nd time).
Compressor trips (second time).
Further overhead accumulator material sent to flare.
Initial overhead accumulator material sent to flare.
Liquid forced from full flare drum to corroded discharge pipe.
20 tonnes discharged Hydrocarcbon explodes.
Debutanizer logged
Debutanizer vents to flare
Command to open valve B fails.
Operators receive wrong signal valve B open
Alarm for flare drum is activated.
Key
Indirect factor
Direct factor
Mishap Event
E/E/PES Mishap Event
Outcome Event
Maintenance failure leaves senor-indicating flow and level in debutanizer was believed to give erroneous indication below maximum.
No second, back-up feedback control loop to ensure input flow reduced or shut off when material accumulates.
Operators fail to realize potential danger from flare overflow
Operator fails to check status of valve B.
Operators preoccupied by controlling heat transfer process between components.
Operators fail to attend to high-level alarm from flare drum for 25 minutes prior to explosion.
Modification to flare drum pump prevents excess being pumped to storage tanks.
Poor maintenance procedures (apparent in failed sensors and other components).
Design assumption in automated control system logic that if discharge rate increased then it would outstrip increases in input so no control over input in single control loop.
Alarms cascade with low prioritization and require explicit acknowledgement by operators.
Fractional distillation uses 1 main input to produce 5 product streams. Information on accumulated outputs of each stream distributed across several control display units.
Poor display design: no single display provides overview of FCCU process; lack of colour to indicate status and reliance on presentation of discrete values.
Automated system that would pump excess to 'slops' now requires manual intervention
Manual operation of Valve to pump at high capacity from flare drum to slops not practiced.
Desire to reduce load on recycling plant during normal operations, pumps operate to slops at full capacity only if manual valve
Pump slowly discharges automatically from flare drum back into secondary overhead accumulation.


Key
Indirect factor
Direct factor
Mishap Event
E/E/PES Mishap Event
Outcome Event
Users open valve C (2nd time).
Compressor trips (second time).
Further overhead accumulator material sent to flare.
Liquid forced from full flare drum to corroded discharge pipe.
20 tonnes discharged Hydrocarcbon explodes
Operators preoccupied by controlling heat transfer process between components.
Operators fail to attend to high-level alarm from flare drum for 25 minutes prior to explosion.
Modification to flare drum pump prevents excess being pumped to storage tanks.
Fractional distillation uses 1 main input to produce 5 product streams. Information on accumulated outputs of each stream distributed across several control display units.
Alarms cascade with low prioritization and require explicit acknowledgement by operators.
Poor display design: no single display provides overview of FCCU process; lack of colour to indicate status and reliance on presentation of discrete values.
Automated system that would pump excess to 'slops' now requires manual intervention
Pump slowly discharges automatically from flare drum back into secondary overhead accumulation.
Manual operation of Valve to pump at high capacity from flare drum to slops not practiced.
Desire to reduce load on recycling plant during normal operations, pumps operate to slops at full capacity only if manual valve

General Causal Analysis Techniques: Flow Charts


Key
AND gate
OR gate
Event
Oversights/Omissions
Assumed Risks
What? Specifics LTA
Why? Management LTA
Accident
Corrective Action LTA
Policy LTA
Implementation LTA
Risk assessment LTA
Hazard
Barrier/Control LTA
Target
Recovery LTA
Did not prevent 2nd accident
Emergency actions LTA
Relations LTA
Goals LTA
Tech. Info. Systems LTA
Hazard analysis LTA
Safety Program Review LTA
Controls LTA
Barriers LTA
Design and development plan LTA
Concepts and requirements LTA
Tech. Info. LTA
Operability LTA
Maintenance LTA
Inspection LTA
Higher supervision LTA
Design basis LTA
Human Factors LTA
Maintenance Plan LTA
Inspection Plan LTA
General Design Process LTA
Other Support Systems LTA
Monitor LTA
Trending LTA
Analysis LTA
Corrective Action Trigger LTA
Operational Specification LTA
Communication LTA
Knowledge LTA
1st Line Supervision LTA
Motivation LTA
Procedures LTA
Qualifications LTA
Supervision LTA
Training LTA
Monitoring Points LTA
Supervisors Training LTA
Time LTA
Did not correct
Did not detect
Performance Error
Task
Non-task
Emergency
Assignment LTA
Briefing LTA
Procedure LTA
Worker Problem
None
LTA Safety
Did not use
Aberrant behaviour
Selection LTA
Training LTA
Motivation LTA

MORT

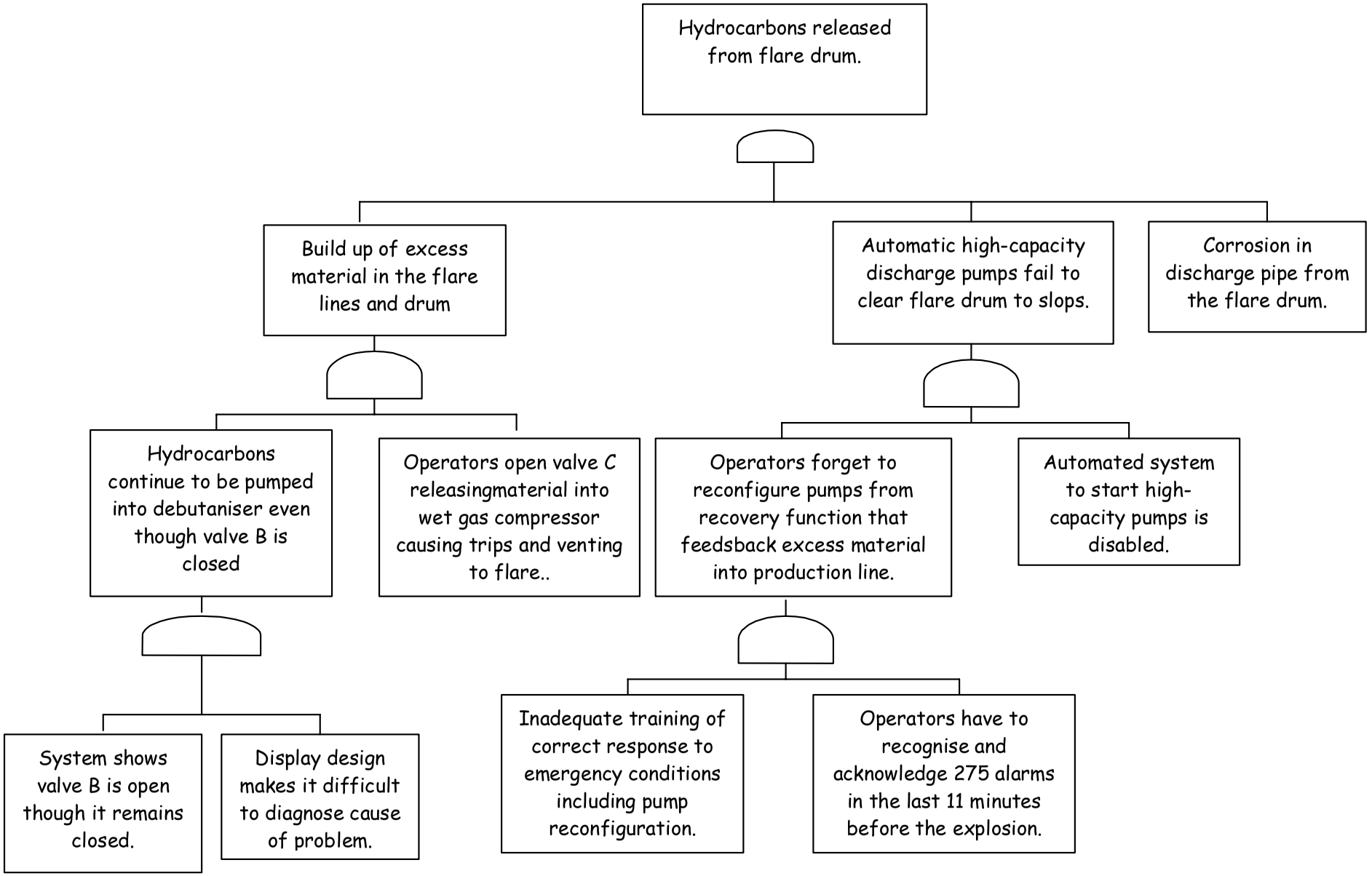
Sub-tree: Management LTA

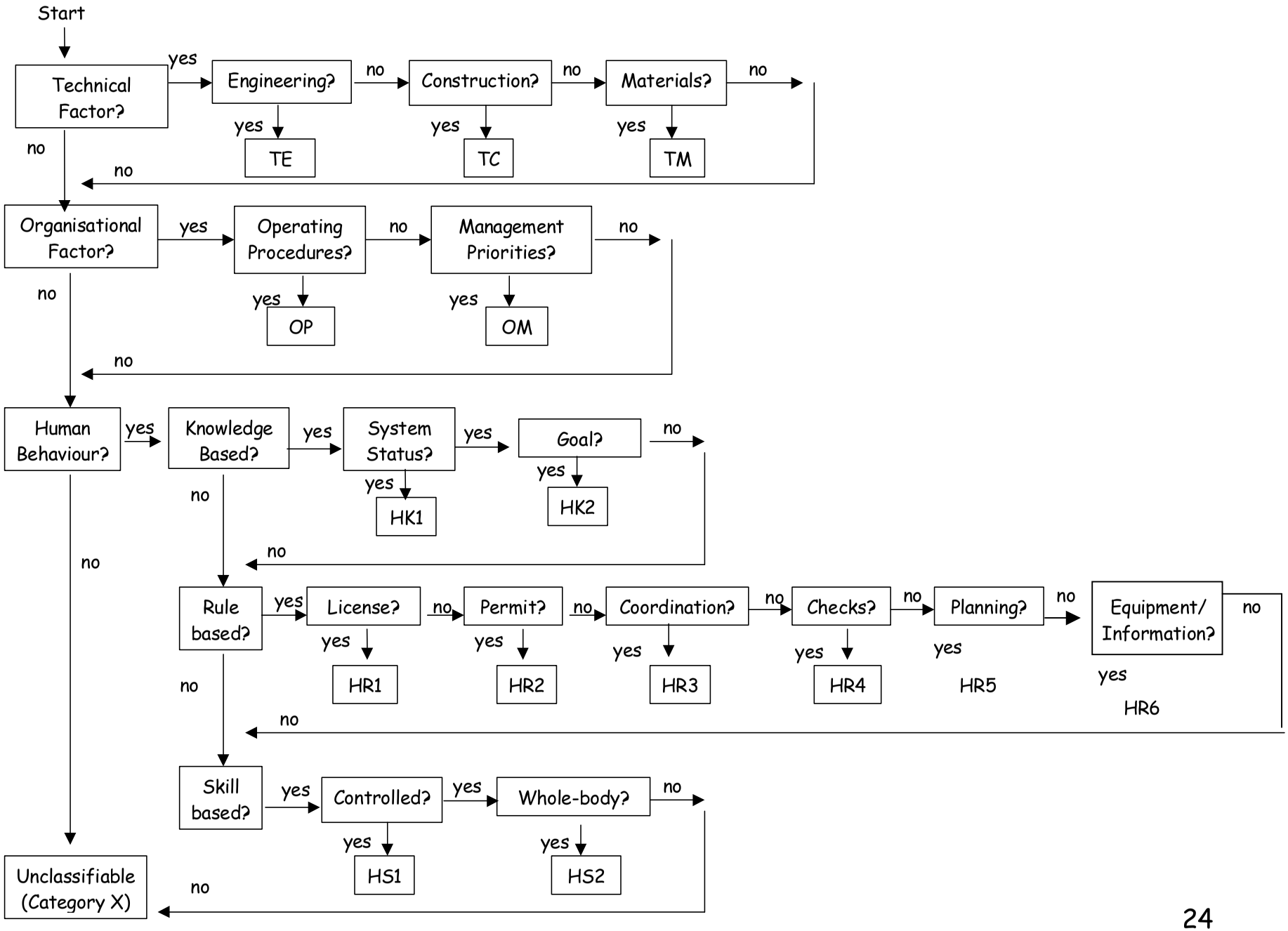
Risk Assessment LTA	Hazard	Release of hydrocarbons into environment after leak from over-pressurized flare drum.
	Target	People and systems in the plant and the wider environment…
Hazard Analysis LTA	Control operability problems	No risk assessment of change to emergency pumping system; now requires operator intervention to reconfigure flow from retrieval to evacuation…

MORT (Stage 2) Analysis Form

PRISMA

- Anaesthesia study:
  - 15 incidents:
  - 78 root causes (5.2 ave);
  - 27% organisational causes;
  - 40% (direct) human causes;
  - 26% technical causes.
- A&E study:
  - 19 incidents:
  - 93 root causes (4.9 ave);
  - 45% organisational causes;
  - 41% (direct) human causes.


Hydrocarbons released from flare drum.
Build up of excess material in the flare lines and drum
Automatic high-capacity discharge pumps fail to clear flare drum to slops.
Corrosion in discharge pipe from the flare drum.
Hydrocarbons continue to be pumped into debutaniser even though valve B is closed
Operators open valve C releasingmaterial into wet gas compressor causing trips and venting to flare..
Operators forget to reconfigure pumps from recovery function that feedsback excess material into production line.
Automated system to start high-capacity pumps is disabled.
System shows valve B is open though it remains closed.
Display design makes it difficult to diagnose cause of problem.
Inadequate training of correct response to emergency conditions including pump reconfiguration.
Operators have to recognise and acknowledge 275 alarms in the last 11 minutes before the explosion.


Start
Technical Factor?
yes
Engineering?
no
Construction?
no
Materials?
no
yes
TE
yes
TC
yes
TM
no
no
Organisational Factor?
yes
Operating Procedures?
no
Management Priorities?
no
yes
OP
yes
OM
no
no
Human Behaviour?
yes
Knowledge Based?
yes
System Status?
yes
Goal?
no
yes
HK1
yes
HK2
no
no
no
Rule based?
yes
License?
no
Permit?
no
Coordination?
no
Checks?
no
Planning?
no
Equipment/ Information?
no
yes
HR1
yes
HR2
yes
HR3
yes
HR4
yes
HR5
yes
HR6
no
no
Skill based?
yes
Controlled?
yes
Whole-body?
no
yes
HS1
yes
HS2
Unclassifiable (Category X)
no

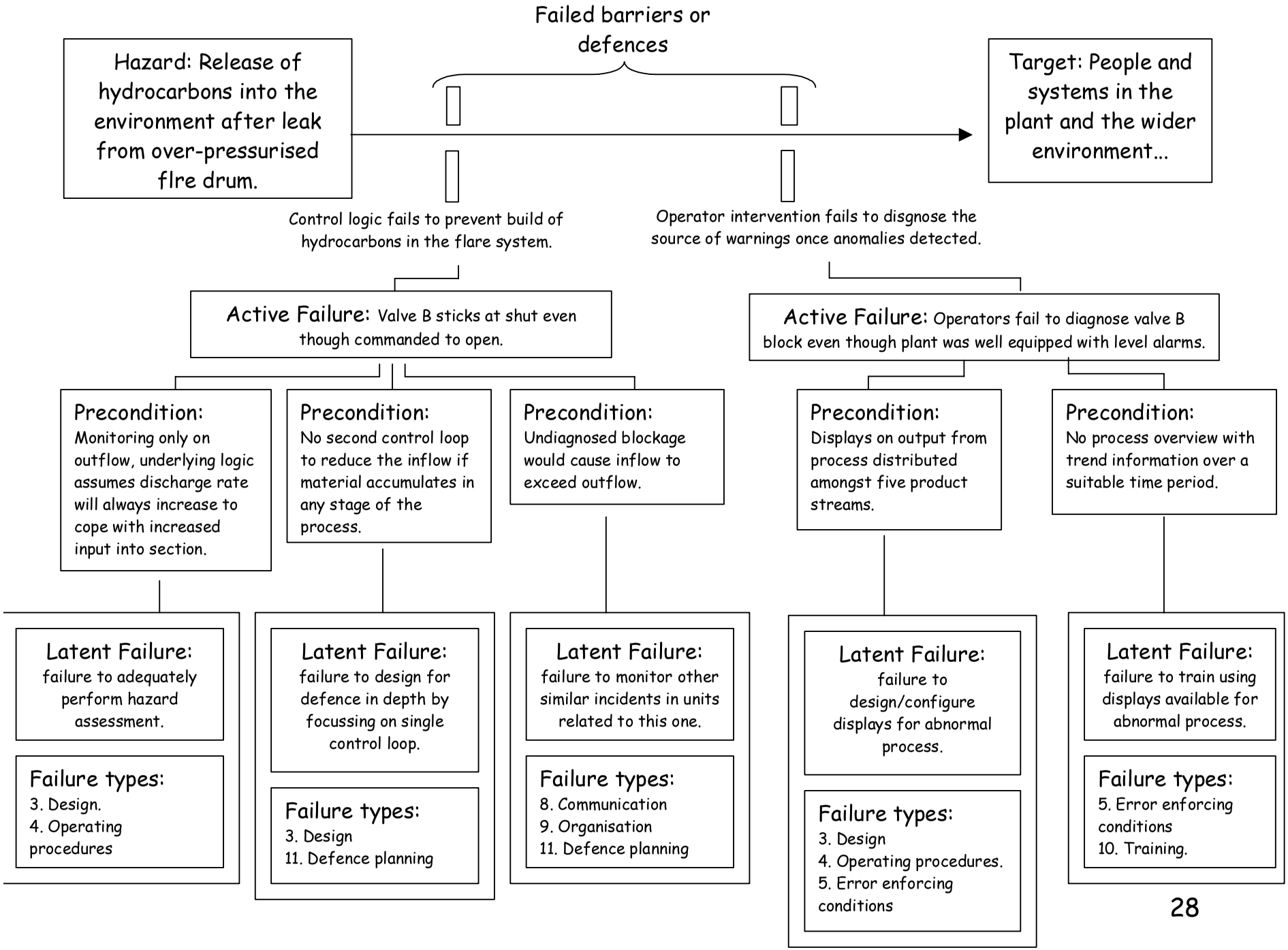
Example PRISMA Classification/Action Matrix

	External Factors (O-EX)	Knowledge Transfer (OK)	Operating procedures (OP) &	Manag. priorities (OM)	Culture (OC)
Inter-departmental communication	X				
Training and coaching		X			
Procedures and protocols			X		
Bottom-up communication				X	
Maximise reflexivity					X

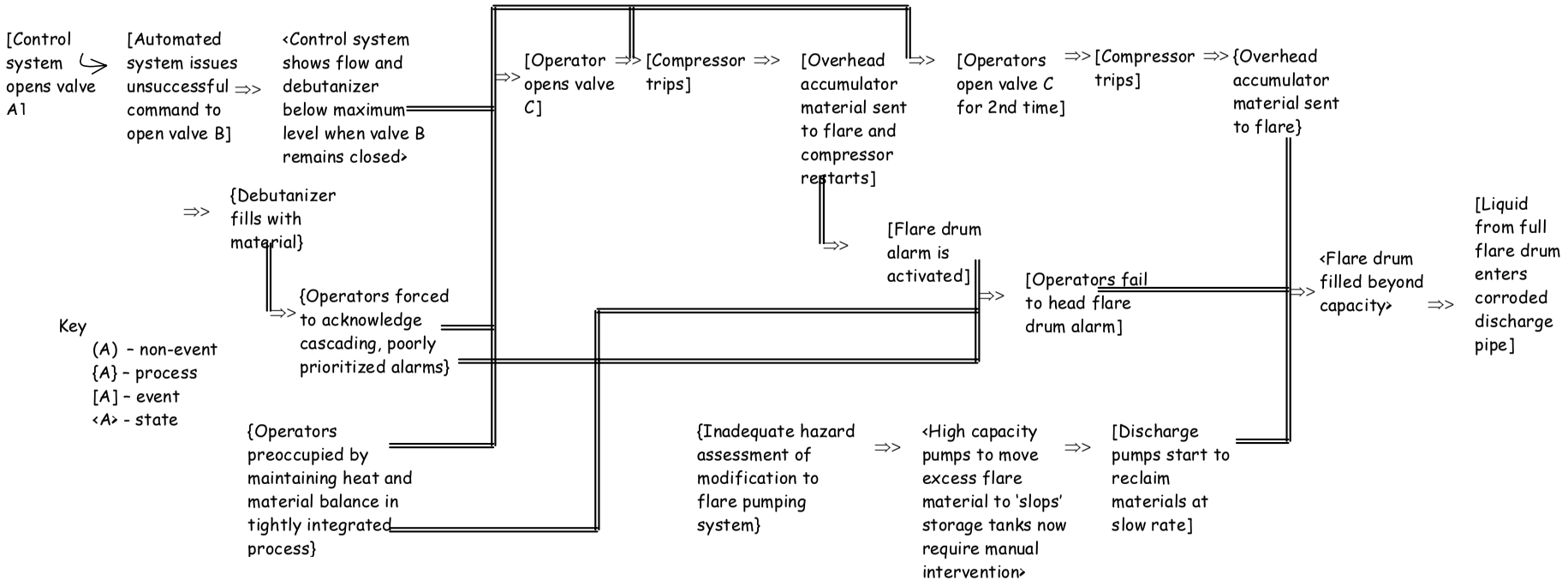
General Causal Analysis Techniques: Accident Models

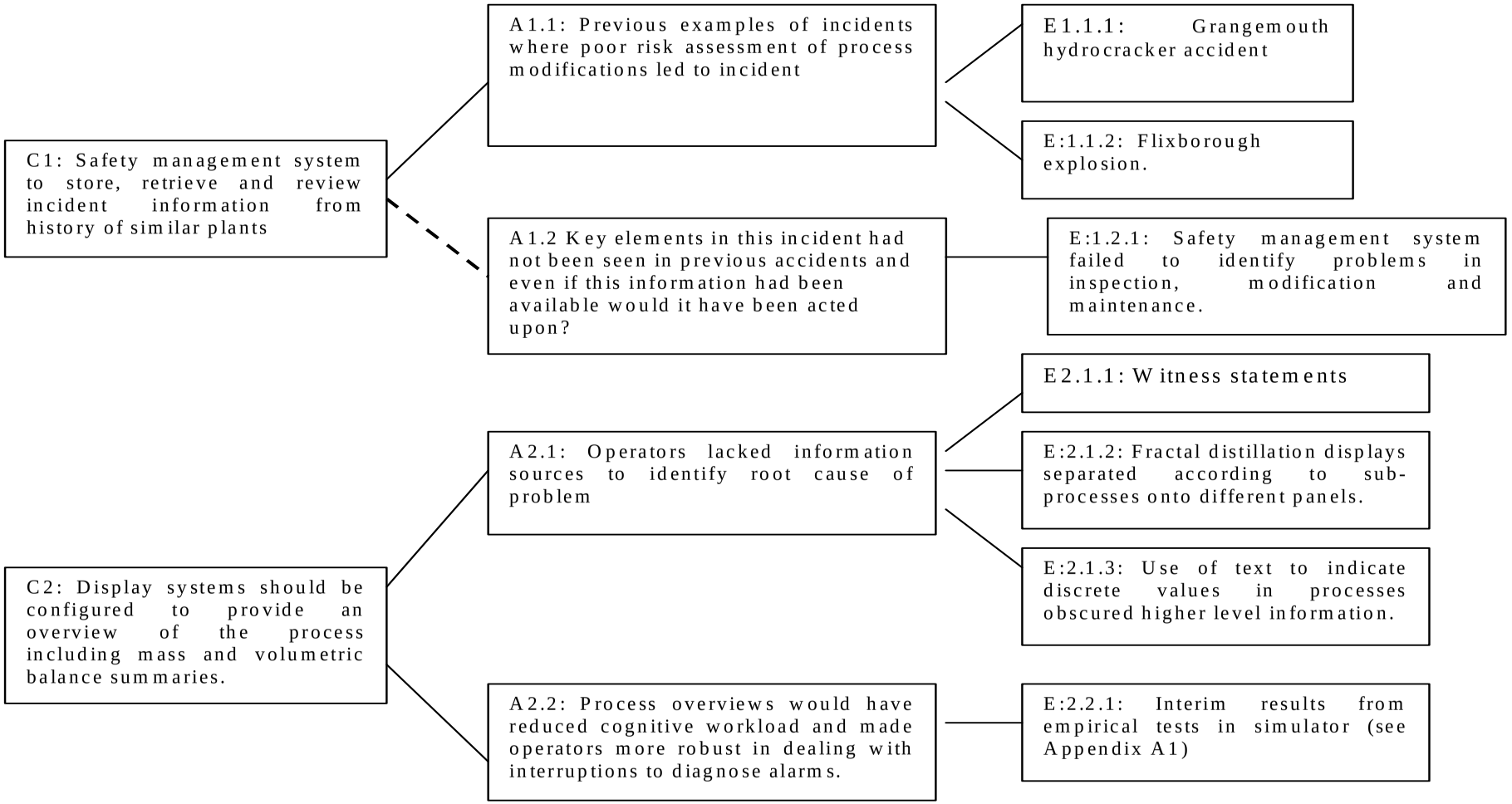
TRIPOD

- General Failure Types:
  - Hardware
  - Maintenance management.
  - Design.
  - Operating procedures.
  - Error-enforcing conditions.
  - Housekeeping
  - Incompatible goals
  - Communication
  - Organisation
  - Training
  - Defence planning


Failed barriers or defences
Hazard: Release of hydrocarbons into the environment after leak from over-pressurised flre drum.
Target: People and systems in the plant and the wider environment...
Control logic fails to prevent build of hydrocarbons in the flare system.
Operator intervention fails to disgnose the source of warnings once anomalies detected.
Active Failure: Valve B sticks at shut even though commanded to open.
Active Failure: Operators fail to diagnose valve B block even though plant was well equipped with level alarms.
Precondition: Monitoring only on outflow, underlying logic assumes discharge rate will always increase to cope with increased input into section.
Precondition: No second control loop to reduce the inflow if material accumulates in any stage of the process.
Precondition: Undiagnosed blockage would cause inflow to exceed outflow.
Precondition: Displays on output from process distributed amongst five product streams.
Precondition: No process overview with trend information over a suitable time period.
Latent Failure: failure to adequately perform hazard assessment.
Failure types: 3. Design. 4. Operating procedures
Latent Failure: failure to design for defence in depth by focussing on single control loop.
Failure types: 3. Design 11. Defence planning
Latent Failure: failure to monitor other similar incidents in units related to this one.
Failure types: 8. Communication 9. Organisation 11. Defence planning
Latent Failure: failure to design/configure displays for abnormal process.
Failure types: 3. Design 4. Operating procedures. 5. Error enforcing conditions
Latent Failure: failure to train using displays available for abnormal process.
Failure types: 5. Error enforcing conditions 10. Training.

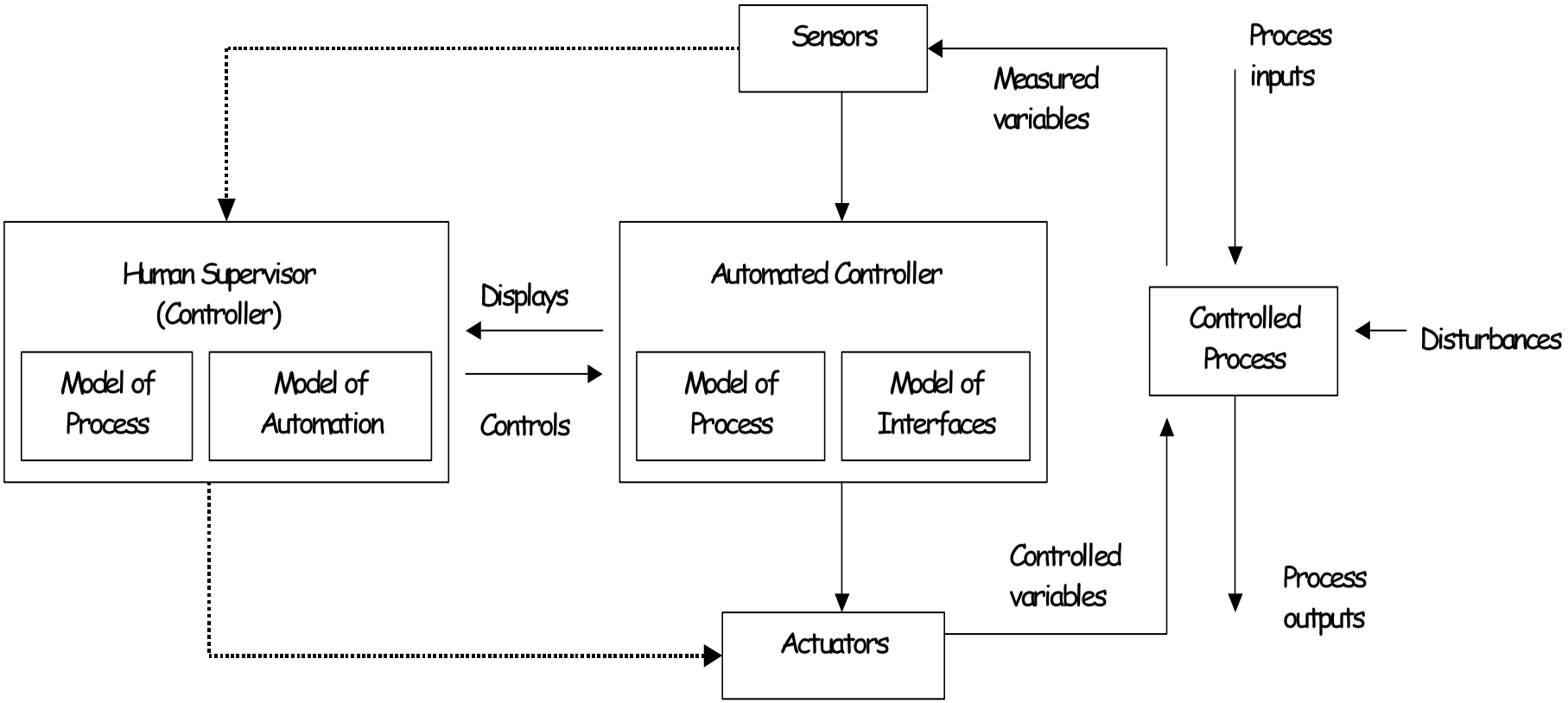
General Causal Analysis Techniques: Argumentation Techniques

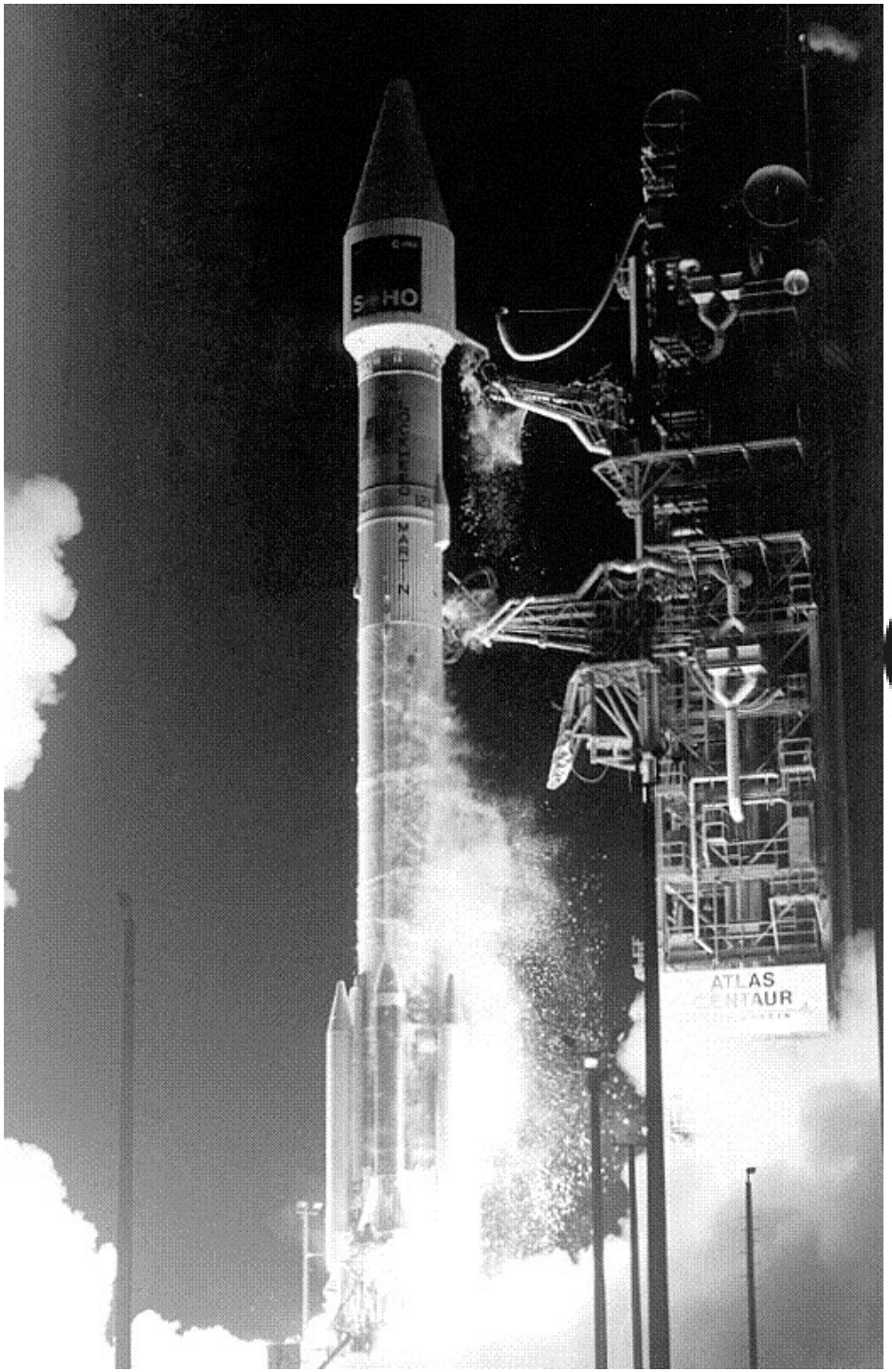

[Control system opens valve A1
[Automated system issues unsuccessful command to open valve B]
<Control system shows flow and debutanizer below maximum level when valve B remains closed>
[Operator opens valve C]
[Compressor trips]
[Overhead accumulator material sent to flare and compressor restarts]
[Operators open valve C for 2nd time]
[Compressor trips]
{Overhead accumulator material sent to flare}
{Debutanizer fills with material}
[Flare drum alarm is activated]
[Operators fail to head flare drum alarm]
<Flare drum filled beyond capacity>
[Liquid from full flare drum enters corroded discharge pipe]
{Operators forced to acknowledge cascading, poorly prioritized alarms}
Key
(A) – non-event
{A} – process
[A] – event
<A> - state
{Operators preoccupied by maintaining heat and material balance in tightly integrated process}
{Inadequate hazard assessment of modification to flare pumping system}
<High capacity pumps to move excess flare material to 'slops' storage tanks now require manual intervention>
[Discharge pumps start to reclaim materials at slow rate]

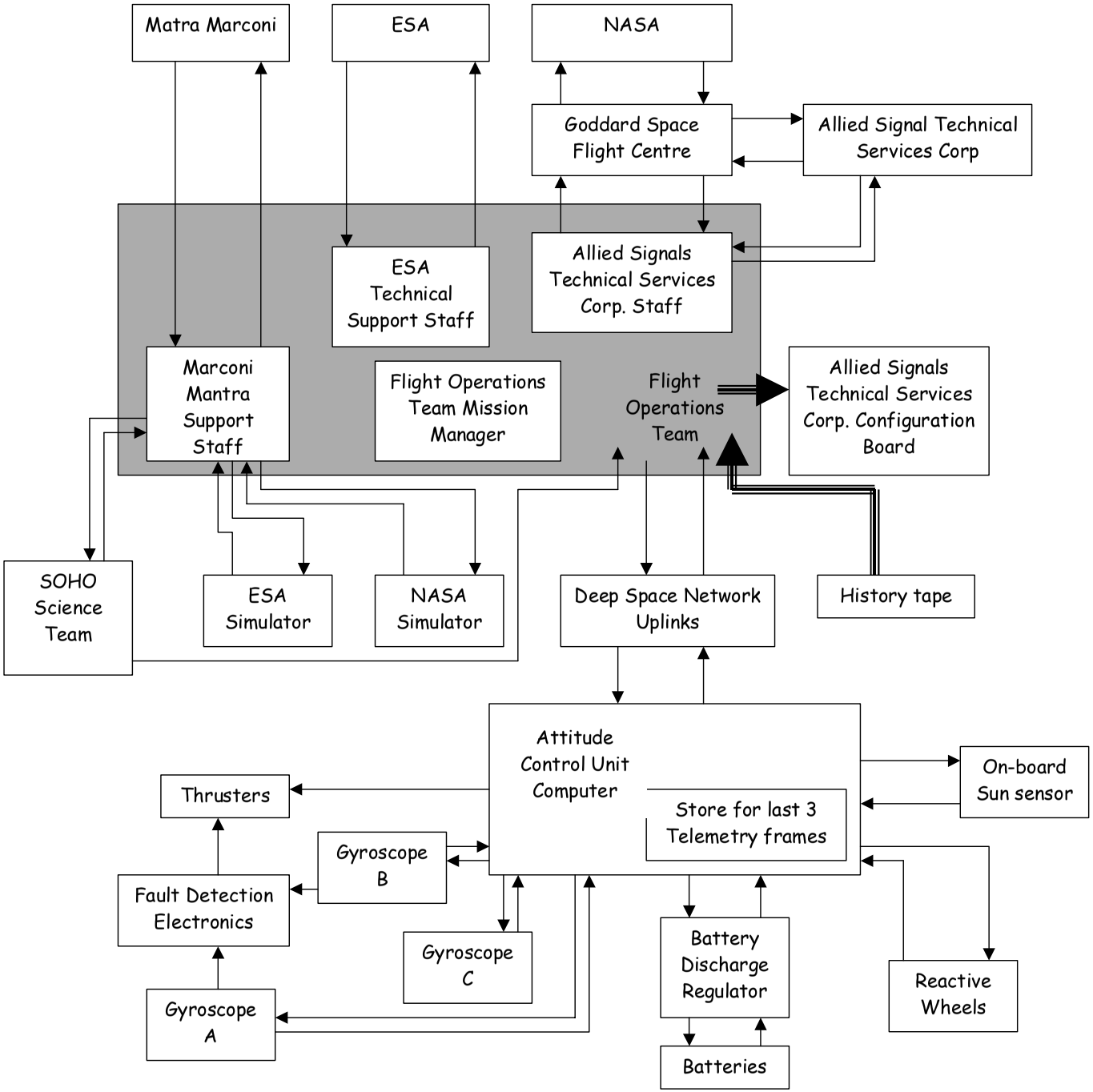

C1: Safety management system to store, retrieve and review incident information from history of similar plants
A1.1: Previous examples of incidents where poor risk assessment of process modifications led to incident
E1.1.1: Grangemouth hydrocracker accident
E:1.1.2: Flixborough explosion.
A1.2 Key elements in this incident had not been seen in previous accidents and even if this information had been available would it have been acted upon?
E:1.2.1: Safety management system failed to identify problems in inspection, modification and maintenance.
C2: Display systems should be configured to provide an overview of the process including mass and volumetric balance summaries.
A2.1: Operators lacked information sources to identify root cause of problem
E2.1.1: Witness statements
E:2.1.2: Fractal distillation displays separated according to sub-processes onto different panels.
E:2.1.3: Use of text to indicate discrete values in processes obscured higher level information.
A2.2: Process overviews would have reduced cognitive workload and made operators more robust in dealing with interruptions to diagnose alarms.
E:2.2.1: Interim results from empirical tests in simulator (see Appendix A1)

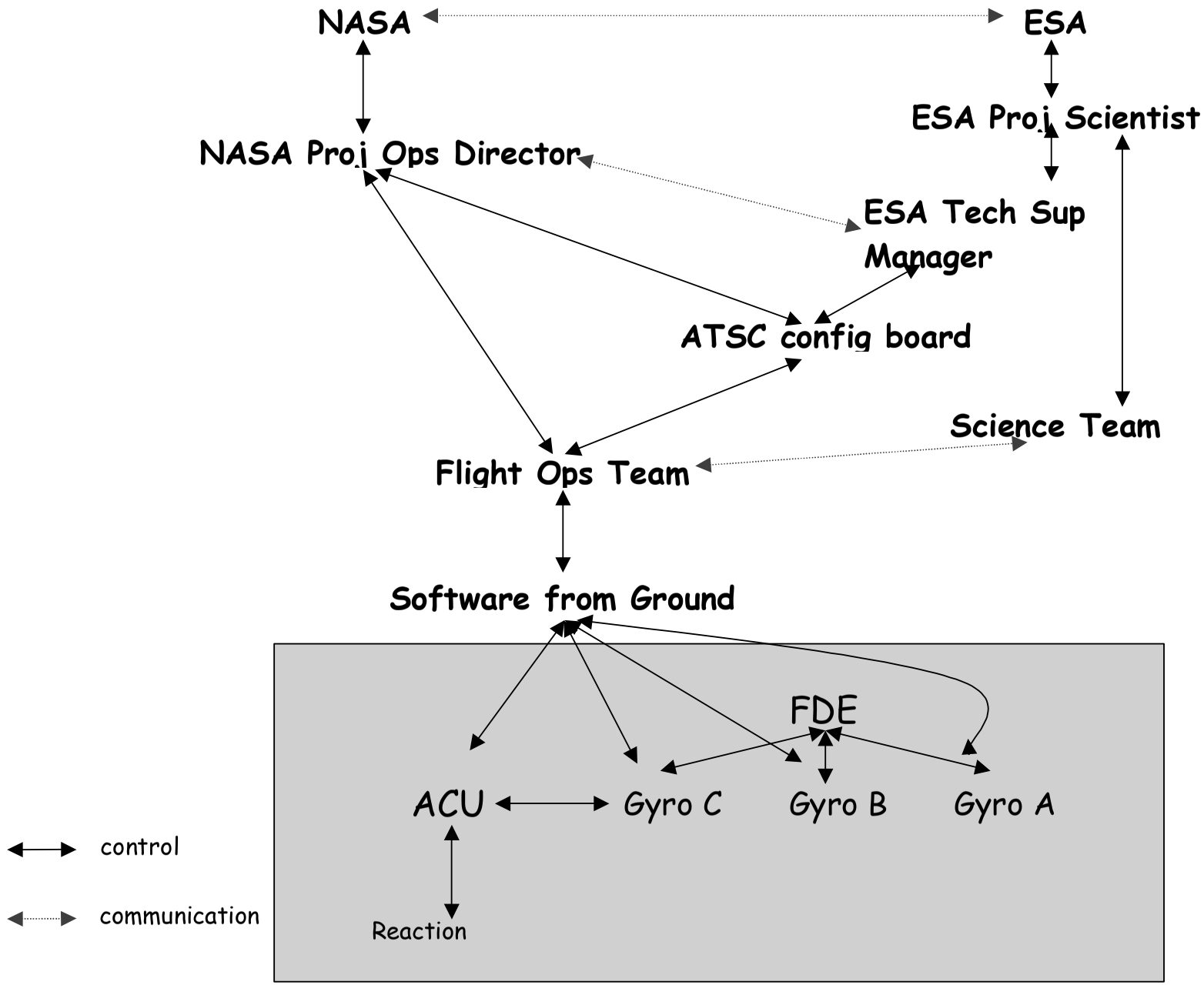
Part 2

1. Overview.
> 2. STAMP
3. PARCEL.
4. Wrap-up.

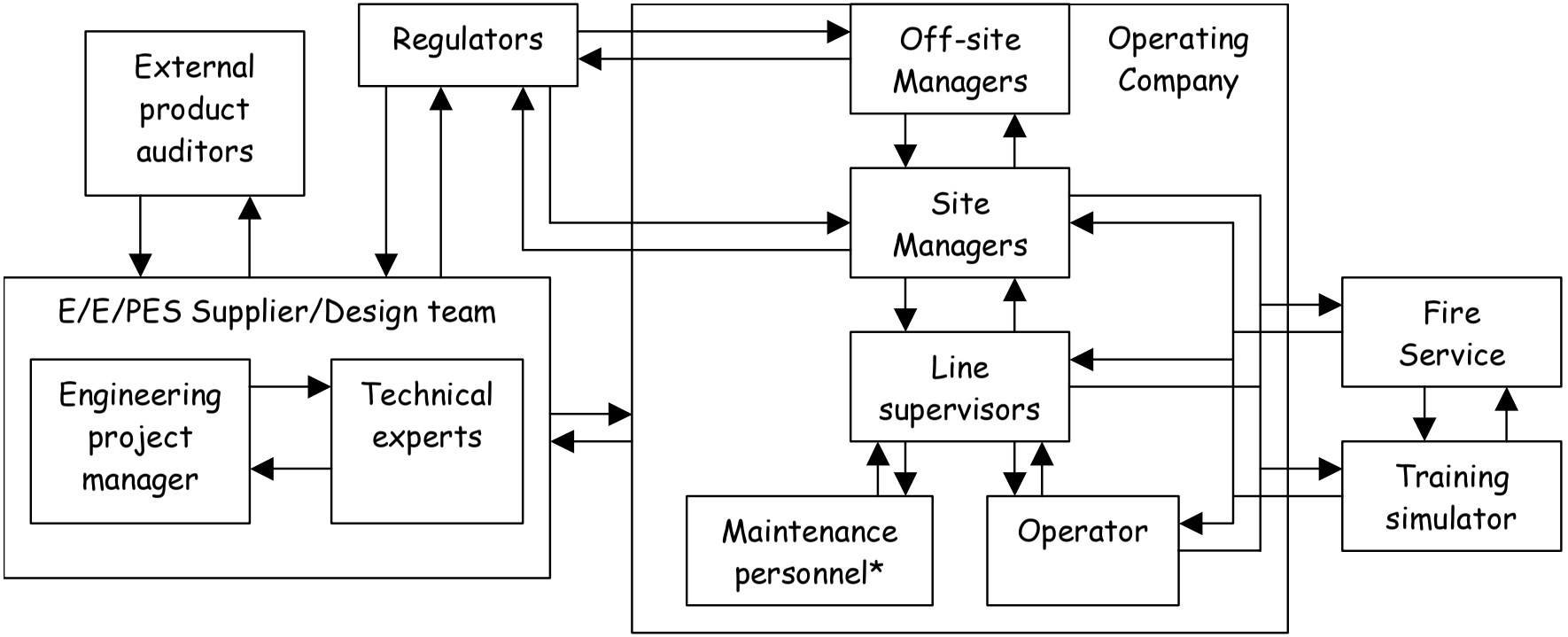

Sensors
Measured variables
Process inputs
Human Supervisor (Controller)
Model of Process
Model of Automation
Displays
Controls
Automated Controller
Model of Process
Model of Interfaces
Controlled Process
Disturbances
Controlled variables
Process outputs
Actuators

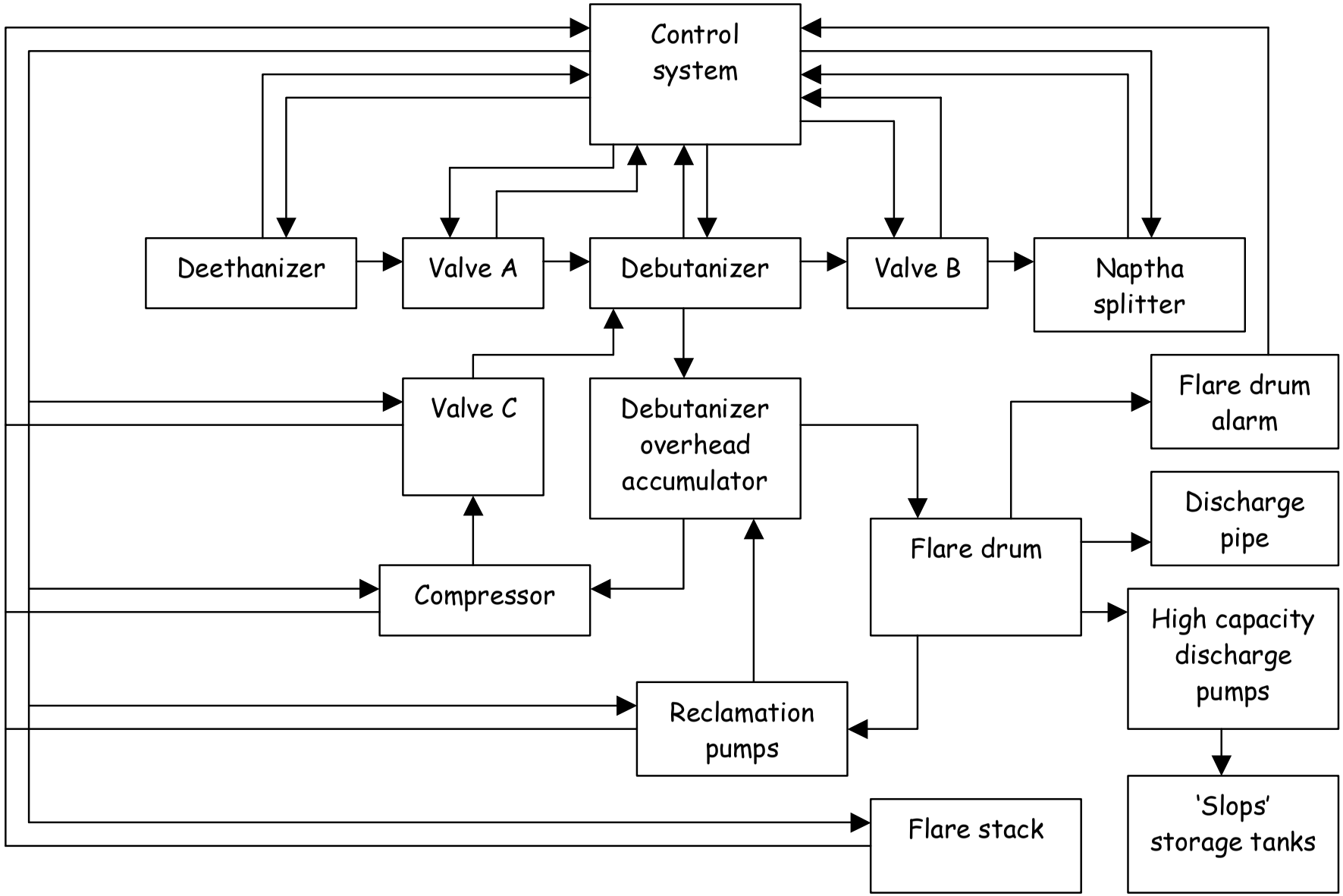

SOHO
MARTIN
ATLAS
CENTAUR

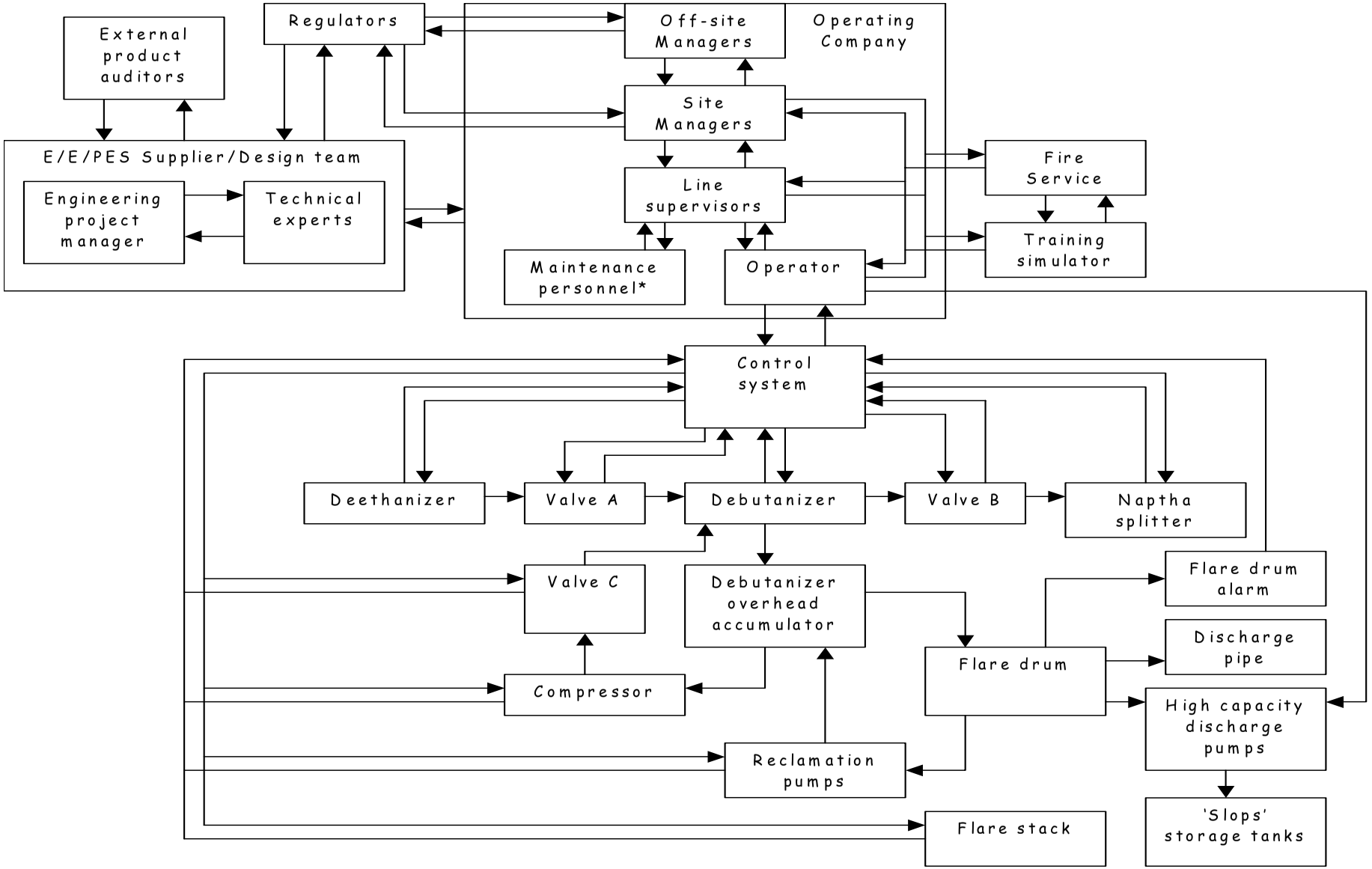

Matra Marconi
ESA
NASA
Goddard Space Flight Centre
Allied Signal Technical Services Corp
ESA Technical Support Staff
Allied Signals Technical Services Corp. Staff
Marconi Mantra Support Staff
Flight Operations Team Mission Manager
Flight Operations Team
Allied Signals Technical Services Corp. Configuration Board
SOHO Science Team
ESA Simulator
NASA Simulator
Deep Space Network Uplinks
History tape
Attitude Control Unit Computer
Store for last 3 Telemetry frames
On-board Sun sensor
Thrusters
Gyroscope B
Fault Detection Electronics
Gyroscope C
Battery Discharge Regulator
Reactive Wheels
Gyroscope A
Batteries


NASA
ESA
ESA Proj Scientist
NASA Proj Ops Director
ESA Tech Sup Manager
ATSC config board
Science Team
Flight Ops Team
Software from Ground
FDE
ACU
Gyro C
Gyro B
Gyro A
Reaction
control
communication

Back to Milford Haven


External product auditors
Regulators
Off-site Managers
Operating Company
Site Managers
E/E/PES Supplier/Design team
Engineering project manager
Technical experts
Line supervisors
Fire Service
Training simulator
Maintenance personnel*
Operator


Control system
Deethanizer
Valve A
Debutanizer
Valve B
Naptha splitter
Valve C
Debutanizer overhead accumulator
Flare drum alarm
Discharge pipe
Flare drum
Compressor
High capacity discharge pumps
Reclamation pumps
'Slops' storage tanks
Flare stack

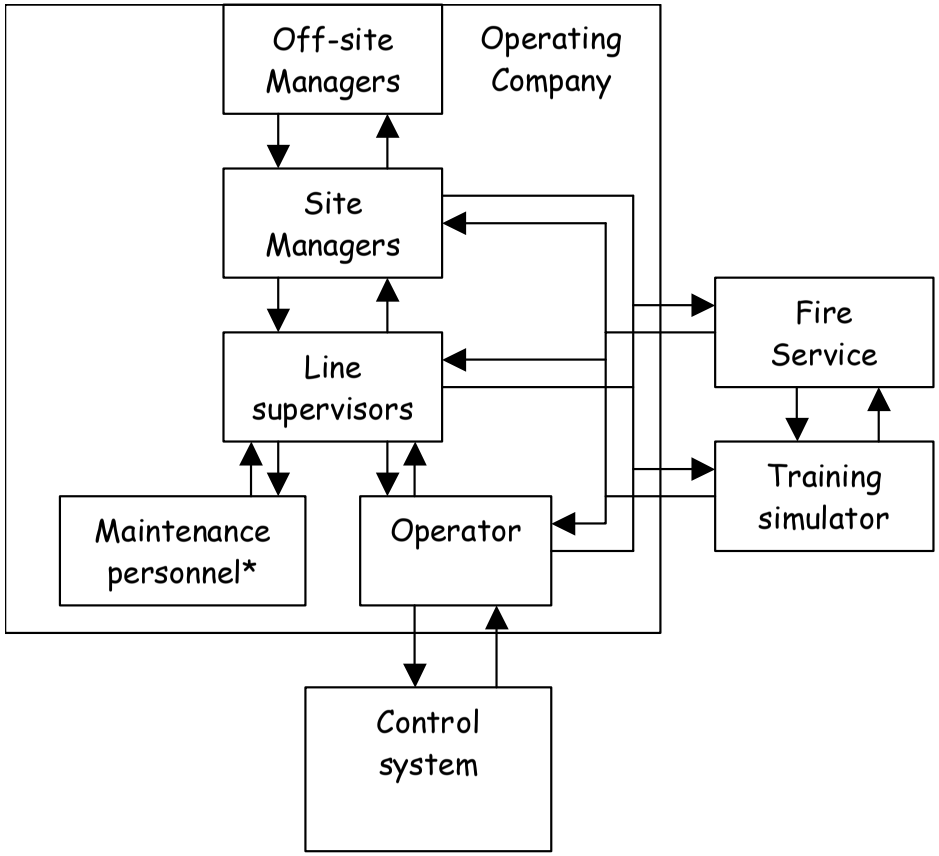

External product auditors
Regulators
Off-site Managers
Operating Company
Site Managers
E/E/PES Supplier/Design team
Engineering project manager
Technical experts
Line supervisors
Fire Service
Training simulator
Maintenance personnel*
Operator
Control system
Deethanizer
Valve A
Debutanizer
Valve B
Naptha splitter
Valve C
Debutanizer overhead accumulator
Flare drum alarm
Discharge pipe
Flare drum
Compressor
High capacity discharge pumps
Reclamation pumps
'Slops' storage tanks
Flare stack

Control Flaws

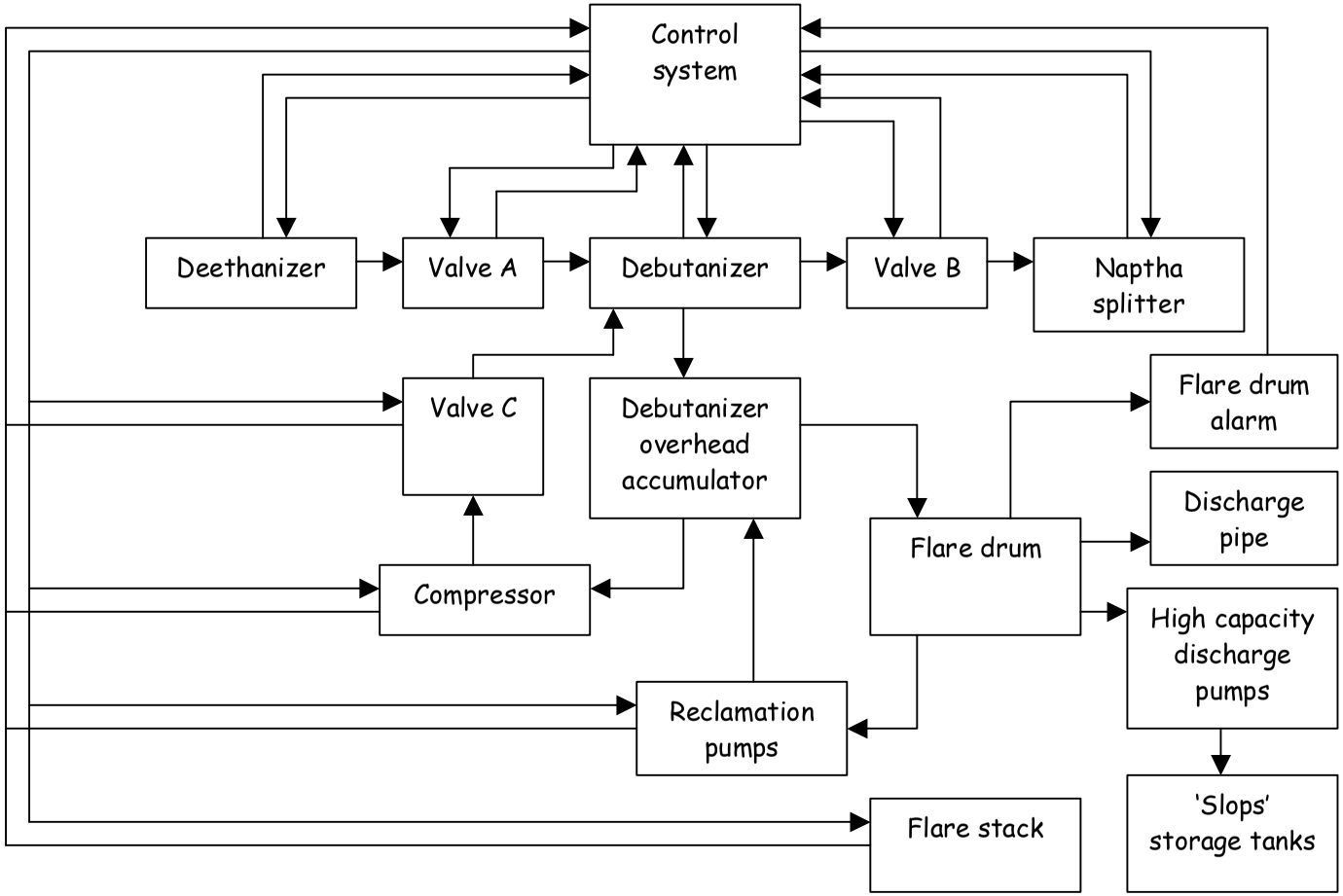
- **1. Inadequate Enforcements of Constraints (Control Actions)**
  - 1.1 Unidentified hazards
  - 1.2 Inappropriate, ineffective or missing control actions for identified hazards
    - 1.2.1 Design of control algorithm (process) does not enforce constraints
      - Flaws in creation process
      - Process changes without appropriate change in control algorithm (asynchronous evolution)
      - Incorrect modification or adaptation.
    - 1.2.2 Process models inconsistent, incomplete or incorrect (lack of linkup)
      - Flaws in creation process
      - Flaws in updating process (asynchronous evolution)
      - Time lags and measurement inaccuracies not accounted for
    - 1.2.3 Inadequate coordination among controllers and decision makers

- **2 Inadequate Execution of Control Action**
  - 2.1 Communication flaw
  - 2.2 Inadequate actuator operation
  - 2.3 Time lag

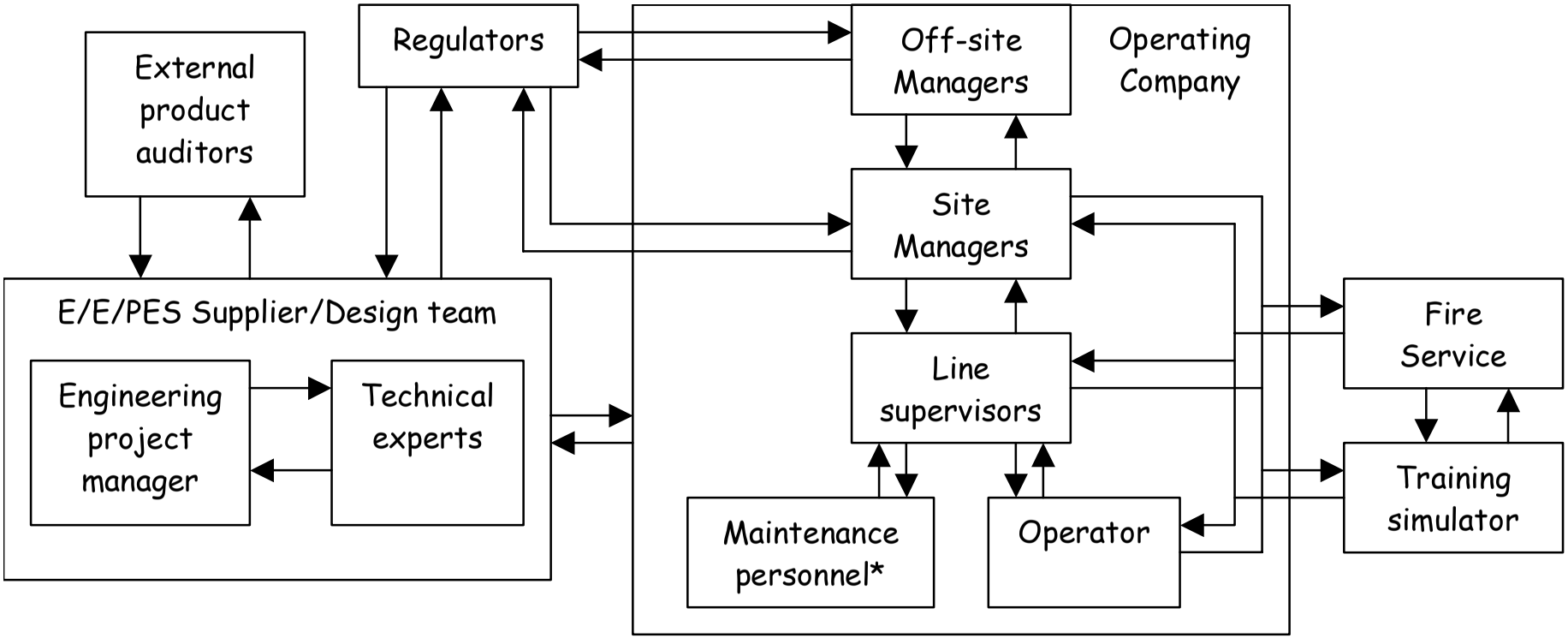
- **3 Inadequate or Missing Feedback**
  - 3.1 Not provided in system design
  - 3.2 Communication flow
  - 3.3 Time lag
  - 3.4 Inadequate sensor operation (incorrect or no information provided)



Control Relationship	Constraint violation	Justification
[Operator-> Control System]	1.2 Inappropriate, ineffective or missing control action for identified hazard	Operator failed to check valve B and instead opened valve C – repeatedly forcing hydrocarbons into the flare system.
[Control System -> Operator]	3.4 Inadequate sensor operation	System failed to show correct state of valve B.
	3.2 Communication flow	System failed to provide necessary process overview.



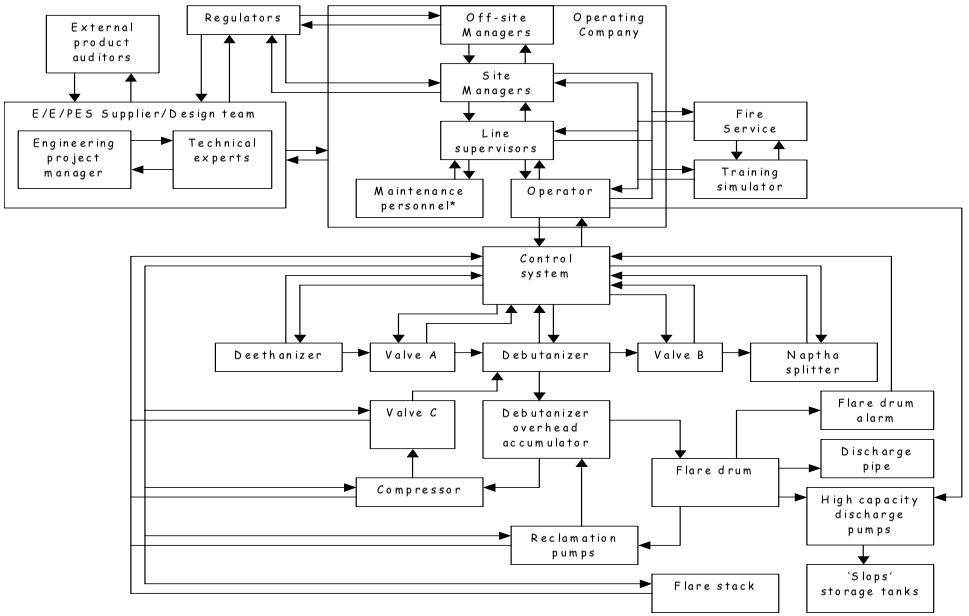
Control Relationship	Constraint violation	Justification
[Valve A-> debutaniser-> Valve B]	1.2.1 Design of control process does not enforce constraints- flaws in creation process	Assumption that outflow from debutanizer via valve B will always be capable of exceeding the inflow via valve A.



Control Relationship	Constraint violation	Justification
[Offsite managers-> Site managers-> Operators]	1.1 Process models inconsistent, incomplete or incorrect (lack of linkup)	Failure to realize that additional operator training and simulations would be required to prepare change over from reclamation configuration to initiation of high-capacity discharge pumps.
[Regulators <-> Offsite managers]	1.1 Unidentified hazards	Failure to assess hazards associated with build-up of material in the flare drum without starting discharge pumps.

Concerns 1: Responsibility

- Senior Management controls everything??



- How to represent their impact on design??

Concerns 2: Success or Failure?

- Organisational structures always look bad:
  - What does successful organisation look like?
  - Informal, messy, complex – flexible?
  - Milford Haven managers 'help out' operators.

- Also, pressure to simplify control models.

Concerns 3: Omissions?

- How do we represent missing controls?
  - Inadequate risk assessment on flare modification.
- How do we represent missing entities?
  - No review board for operation post flare modification.
- Also, pressure to simplify control models.

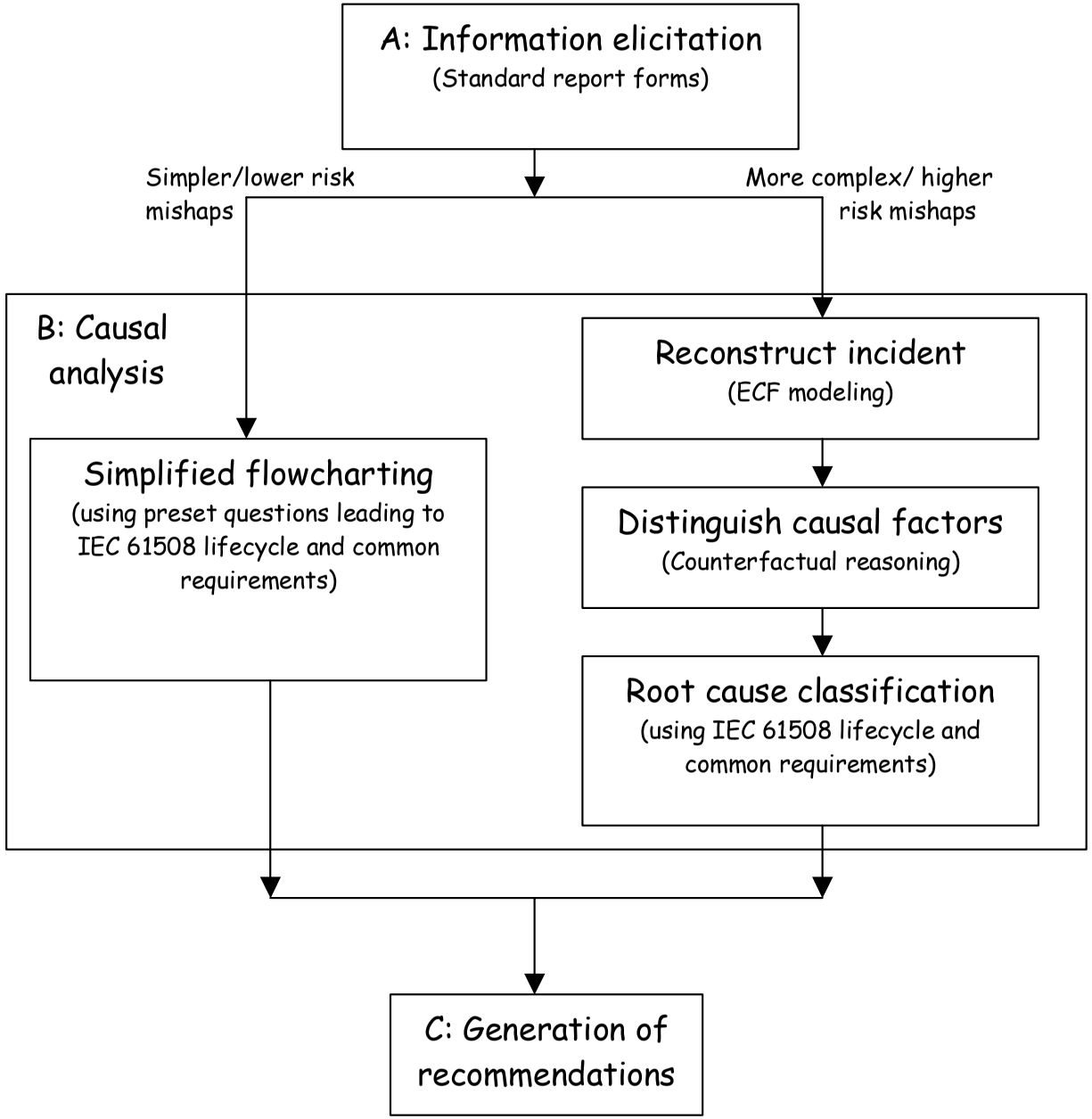
	Analyst 1	Analyst 2
1 Inadequate Enforcement of Constraints		
1.1 Unidentified hazards	Factor 2: "Failure to perform risk analysis of a modified procedure… •Factor 4: "Failure to properly respect autonomous Safe Mode triggers	Factor 2: Failure to perform risk analysis of a modified procedure set. Factor 7: Failure to recognise risk posed by operations team overload
1.2 Inappropriate, ineffective or missing control actions for identified hazards		Factor 6: Failure to Question Telemetry discrepancies
1.2.1 Design of control algorithm does not enforce constraints	Factor 1: Flight operations team modified flight-demonstrated ground operations procedures as a part of the ISTP Ground System re-engineering… Factor 10: Over reliance of flight operations team on ESA and MMS representatives…	
1.2.2 Process model inconsistent, incomplete or inaccurate	Factor 6: Failure to Question Telemetry discrepancies Factor 9: Emphasis on science return at expense of spacecraft safety Factor 13: Failure to validate the planned sequence of events in advance.	Factor 1: Flight operations team modified flight-demonstrated ground operations procedures as a part of the ISTP Ground System re-engineering… Factor 9: Emphasis on science return at expense of spacecraft safety
1.2.3 Inadequate coordination among controllers and decision makers	Factor 7: Failure to recognise risk posed by operations team overload Factor 8: Failure to recognise shortcomings in implementation of ESA/NASA agreements…	Factor 10: Over reliance of flight operations team on ESA and MMS representatives…
2 Inadequate Execution of Control Actions		
2.1 Communication flaw		Factor 5: Failure to follow the operations script; failure to evaluate primary and ancillary data…
2.2 Inadequate actuator operation	Factor 5: Failure to follow the operations script; failure to evaluate primary and ancillary data… Factor 11: Dillution of observatory engineering support…	Factor 12: Failure to resolve a critical deficiency report in a timely manner Factor 4: Failure to properly respect autonomous Safe Mode triggers
2.3 Time lag	Factor 12: Failure to resolve a critical deficiency report in a timely manner	
3. Inadequate or Missing Feedback		
3.1 Not provided in system design		Factor 13: Failure to validate the planned sequence of events in advance.
3.2 Communication flaw	Factor 3: Failure to communicate change	Factor 3: Failure to communicate change
3.3 Time lag		
3.4 Inadequate sensor operation		Factor 8: Failure to recognise shortcomings in implementation of ESA/NASA agreements… Factor 11: Dillution of observatory engineering support…

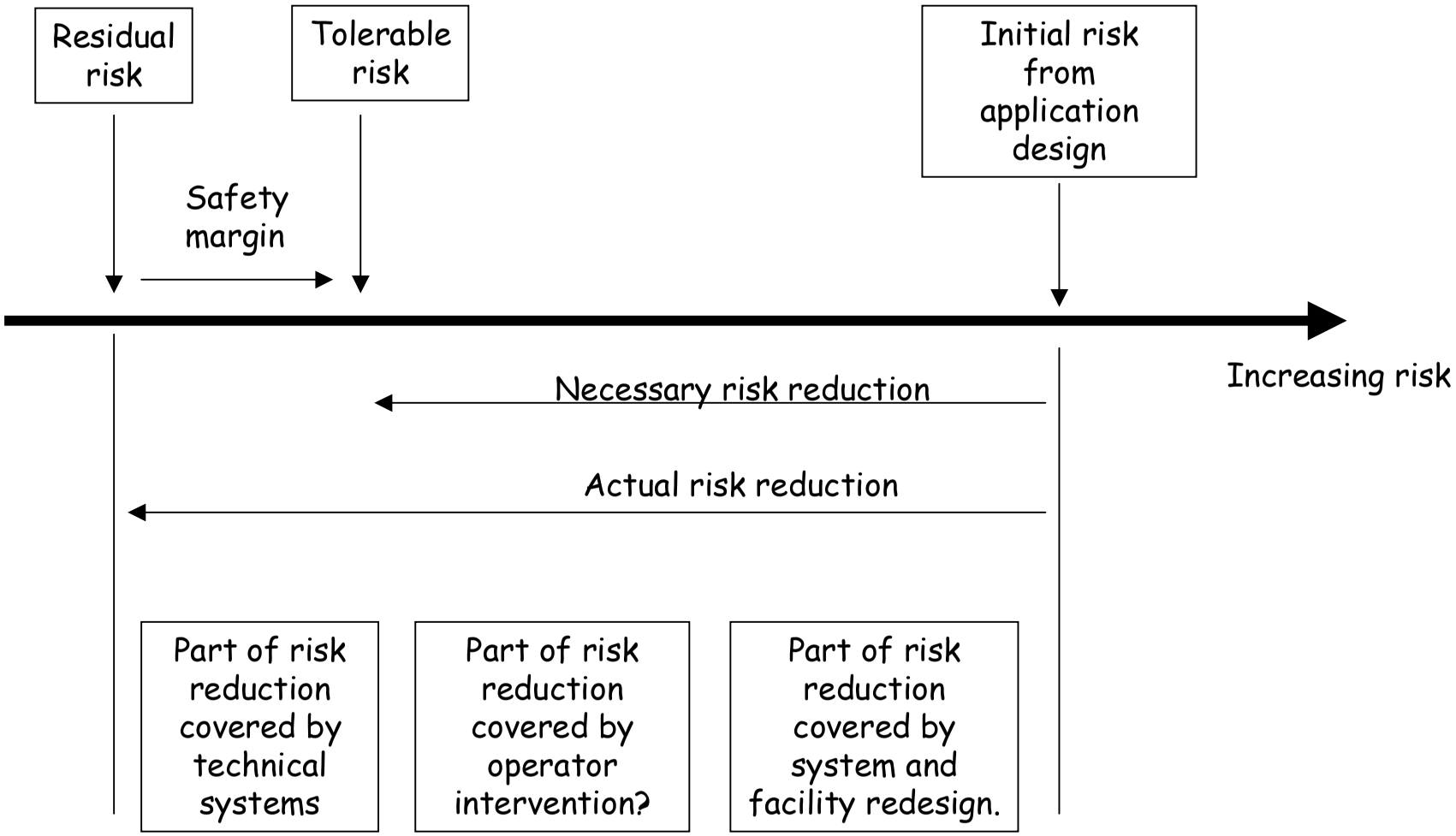
Part 3

1. Overview.
2. STAMP
> 3. PARCEL
4. Wrap-up.

	Elicitation and Analysis techniques		Event Based Techniques		Flowcharts and taxonomies		Accident Models		Argumentation Techniques	
	Barrier Anal.	Change Anal.	Timelines	Accident Fault Trees	MORT	PRISMA	TRIPOD	STAMP	WBA	CAE
IEC 61508 Lifecycle phase										
Concept	F	F	U	U	F	P	F	P	U	F
Scope	F	F	U	U	F	P	F	P	U	F
Risk Assessment	P	P	P	P	F	P	P	F	U	F
Safety Requirement	F	F	U	U	P	P	F	F	U	F
Allocation	F	P	P	U	P	P	F	P	U	U
Planning of Validation, Operation & maintenance	U	P	P	P	F	F	U	P	P	U
Realisation	U	F	F	P	U	P	U	F	F	U
Installation / Commission	U	P	F	P	P	P	P	P	F	P
Validation	P	P	F	P	P	P	P	U	F	P
Operation & Maintenance	P	F	F	P	P	P	F	F	F	P
Modification	U	F	F	P	P	P	U	F	F	P
IEC 61508 Common Requirements										
Competency	P	P	P	P	P	P	F	P	P	P
Lifecycle	U	P	P	P	P	P	P	P	P	P
Verification	P	P	P	P	P	F	P	P	P	P
Safety management	P	P	P	P	P	P	P	P	P	P
Document.	P	P	P	P	P	P	P	P	P	P
Functional safety assessment	P	P	P	P	P	P	P	P	P	P

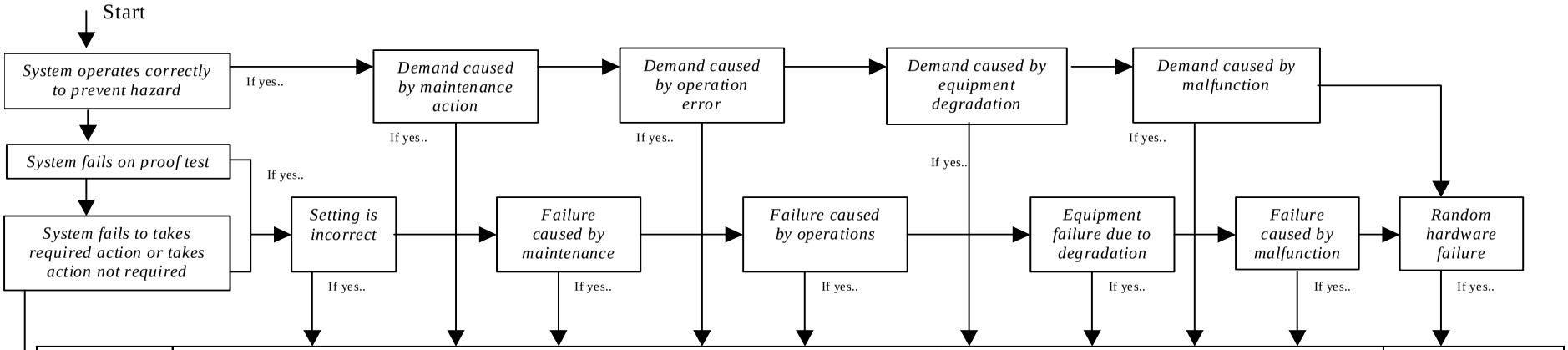
Key: (U)nsupported, (P)artially supported, (F)ully supported


A: Information elicitation
(Standard report forms)
Simpler/lower risk mishaps
More complex/ higher risk mishaps
B: Causal analysis
Reconstruct incident
(ECF modeling)
Simplified flowcharting
(using preset questions leading to IEC 61508 lifecycle and common requirements)
Distinguish causal factors
(Counterfactual reasoning)
Root cause classification
(using IEC 61508 lifecycle and common requirements)
C: Generation of recommendations


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.

IEC 61508 common requirements		
Competency	1. LTA operations competency 2. LTA maintenance competency 3. LTA modification competency	6.2.1 h 6.2.1 h 6.2.1 h
Lifecycle	1. LTA definition of operations accountabilities 2. LTA definition of maintenance accountabilities 3. LTA definition of modification accountabilities	7.1.4 7.1.4 7.1.4
Verification	1. LTA verification of operations 2. LTA verification of maintenance 3. LTA verification of modification	7.18.2, 7.9 (2) 7.18.2, 7.9 (2) 7.18.2, 7.9 (2)
Safety management	1. LTA safety culture 2. LTA safety audits 3. LTA management of suppliers	6.2.1 6.2.1 6.2.5
Documentation	1. documentation unclear or ambiguous 2. documentation incomplete 3. documentation not up to date	5.2.6 5.2.3 5.2.11
Functional safety assessment	1. LTA O & M assessment 2. modification assessment LTA 3. assessment incomplete 4. insufficient skills or independence in assessment team	8.2 8.2 8.2.3 8.2.11/12/13/14

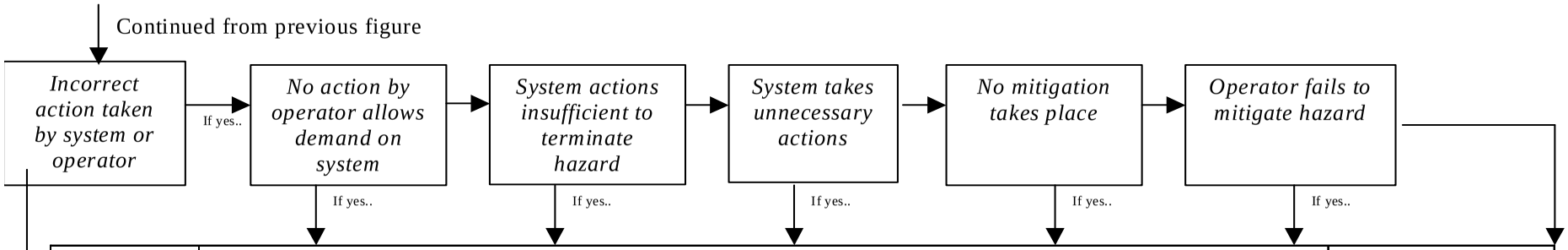
Key: LTA is Less Than Adequate, IEC 61508 references are to Part 1 except as indicated by parentheses e.g. (2)



	Would the incident have been prevented if:					
Hazard and Risk Assessment	- hazard and risk analysis had considered all modes of operation and causes	- hazard and risk analysis had considered all modes of operation and causes	- hazard and risk analysis had considered all modes of operation and causes			Log failure and check -if dangerous failure rate is in line with design assumptions -if all expected actions occurred and no unexpected actions occurred -if safe failure causes any unexpected actions Log demand and check if -demand rate is in line with design assumptions -demand cause was predicted in H & RA
Design	- different equipment selected? - installation design different? - configuration was correct	- maintenance facilities had been designed adequately	- operations facilities had been designed correctly	- different equipment selected? - installation design had been different?	- different equipment selected? - the installation design had been different? -configuration was correct	
Installation & Commission	- the equipment had been installed according to design	- the maintenance facilities had been installed according to design	- the operations facilities had been installed according to design	- the equipment had been installed according to design	- the equipment had been installed according to design	
Validation	- the setting had been checked during validation	- maintenance facilities had been fully checked	- operations facilities had been fully checked	- equipment condition had been fully checked	- equipment condition had been fully checked	
Operation & Maintenance	- maintenance procedures were applied - maintenance procedures were improved - maintenance tools better - test interval was reduced	- correct maintenance procedure had been used - maintenance procedure was improved - permit procedures better	- correct operation procedure was used - operation procedure was improved - permit procedures improved	- maintenance procedures applied - maintenance proc. better - test interval was reduced - additional protection provided	- maintenance procedures were improved - maintenance tools improved - test interval was reduced - additional protection provided	
Modification	- setting had been reviewed during impact analysis	- maintenance facilities or procedures had been reviewed during impact analysis	- operation facilities or procedures had been reviewed during impact analysis	- equipment used or installation design has been reviewed during impact analysis	- equipment used or installation design has been reviewed during impact analysis	

	Would the incident have been prevented if:					
	Competency	Lifecycle	Verification	Safety management	Documentation	Safety assessment
Operation & Maintenance	- operation or maintenance staff were more competent	- responsibilities were defined better	- a better verification scheme had been in place	- safety culture was improved - audits were more frequent	- documentation was clear and sufficient	- assessment had been carried out on O&M phase
Modification	- modification carried out by more competent staff	- modification lifecycle was better defined	- a better verification scheme had been in place	- accountabilities better defined - suppliers not reviewed	- documentation updated	- assessment carried out on modification

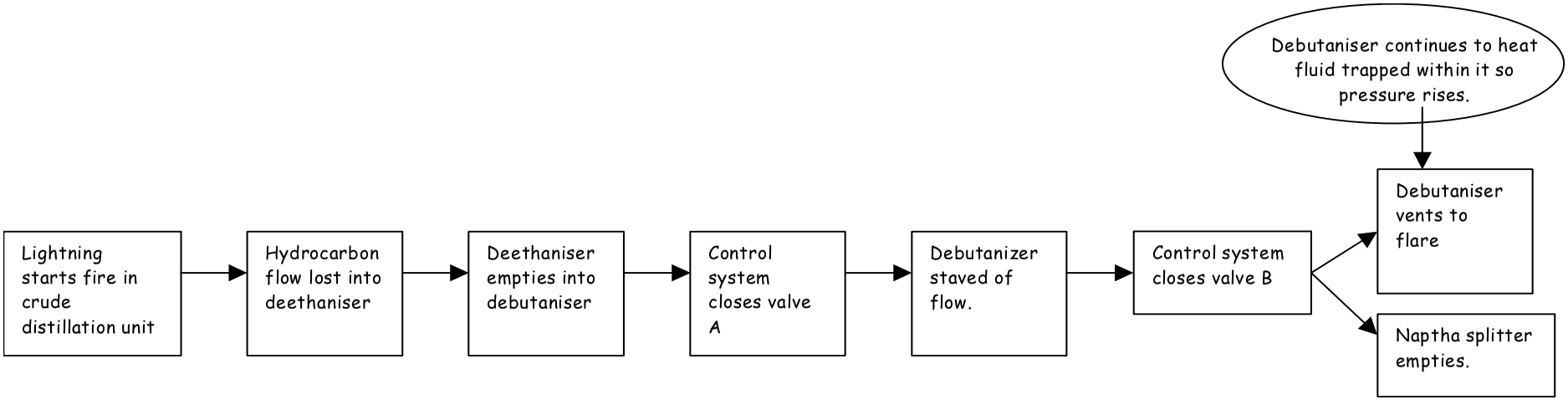
Continued …

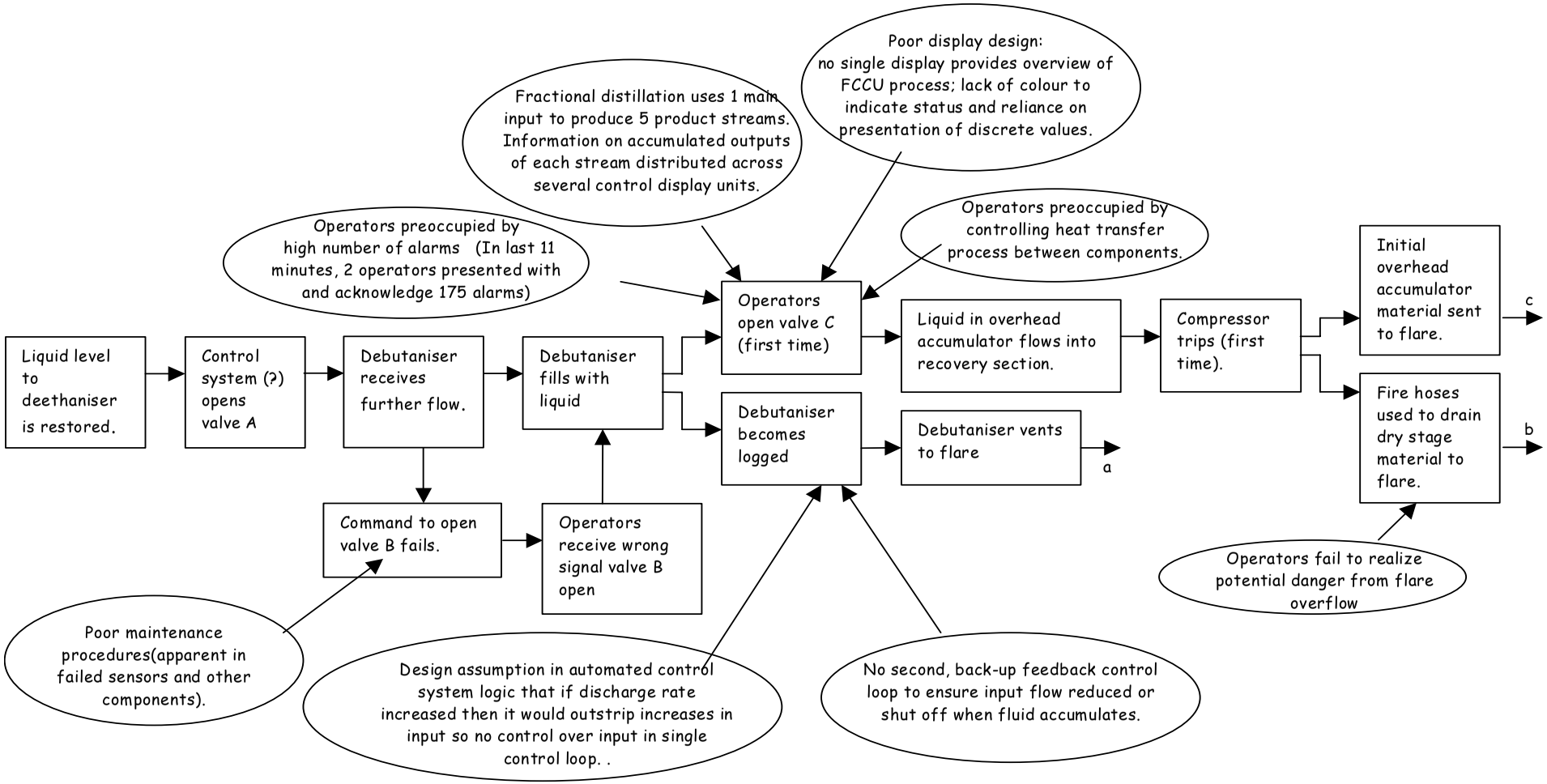


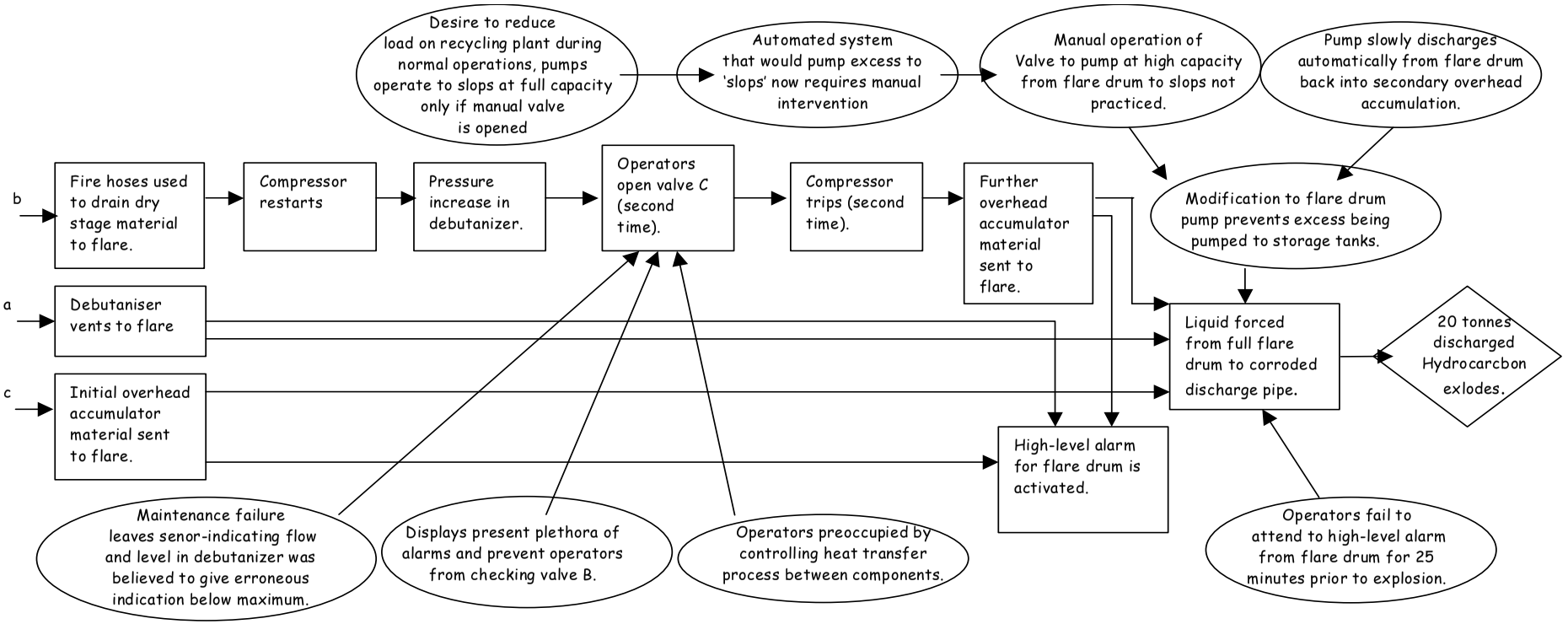
	Would the incident have been prevented if:					
Hazard and Risk Assessment	- hazard & risk analysis had considered all modes of operation & causes	- hazard & risk analysis had considered all modes of operation & causes	- hazard & risk analysis had considered all modes of operation & causes	- hazard & risk analysis had considered all modes of operation & causes	- hazard & risk analysis had considered all modes of operation & causes	Log failure and check -if dangerous failure rate is in line with design assumptions -if all expected actions occurred and no unexpected actions occurred -if safe failure causes any unexpected actions Log demand and check if - demand rate is in line with design assumptions - demand cause was predicted in H & RA
Design	- operator facilities wer designed better - installation design had been different?	- additional actions were specified - actions were faster - final actuation device were improved	- design requirements were better documented	- mitigation system had been specified - mitigation system had been better designed	- operator facilities had been designed better - the installation design had been different?	
Installation & Commissioning	- equipment had been installed according to design	- the equipment had been installed according to design	- the equipment had been installed according to design	- mitigation system had been installed according to design	- equipment had been installed according to design	
Validation	- operator facilities had been checked during validation	- operation facilities had been checked during validation	- operations facilities had been fully checked	- mitigation system had been fully checked	- operator facilities had been fully checked	
Operation & Maintenance	- operation procedures were applied - operation procedures were improved	- correct maintenance procedure had been used - maintenance procedure was improved - proof testing was more frequent	- correct operation procedure was used - operation procedure was improved - permit procedures were improved	- mitigation procedures were applied - mitigation procedures were improved - mitigation system was proof checked more frequently	- operation procedures had been applied - operation facilities or procedures were improved	
Modification	- operation facilities had been reviewed during impact analysis	- necessary system actions had been reviewed during impact analysis	- necessary system actions had been reviewed during impact analysis	- need for mitigation had been reviewed during impact analysis	- need for mitigation had been reviewed during impact analysis	

	Would the incident have been prevented if:					
	Competency	Lifecycle	Verification	Safety management	Documentation	Safety assessment
Operation & Maintenance	- operation or maintenance staff were more competent	- responsibilities were defined better	- a better verification scheme had been in place	- safety culture was improved - audits were more frequent	- documentation was clear and sufficient	- assessment had been carried out on O&M phase
Modification	- modification had been carried out by more competent staff	- modification lifecycle was better defined	- a better verification scheme had been in place	- accountabilities were better defined - suppliers not reviewed	- documentation had been updated	- assessment ad been carried out on modification

Causal Event	IEC 61508 Classification	Route through flow chart	Rationale
Decision to open valve C.	**Validation**	Incorrect action taken by system or operator-> Operator fails to mitigate hazard -> Accident would have been avoided if operator facilities had been fully checked.	The operators intervened in the automated control system to open valve C this twice led the compressor to trip and forced excess fluid into the flare system. The poorly designed displays prevented them from diagnosing the source of the increased pressure in the debutanizer and the potential hazard from their actions in opening C. Improved display design might have occurred if they had been validated against a wider range of operational scenarios.
Failure to open valve B.	**Operation and maintenance**	System fails to take required action -> Failure caused by maintenance -> Accident would have been avoided if maintenance procedure were improved.	The computer control system was designed to automatically open valve B when flow was restored to the debutanizer. This command failed. Subsequent investigation found of 39 instrument loops 24 needed attention ranging from minor mechanical damage to major maintenance faults.


Debutaniser continues to heat fluid trapped within it so pressure rises.
Lightning starts fire in crude distillation unit
Hydrocarbon flow lost into deethaniser
Deethaniser empties into debutaniser
Control system closes valve A
Debutanizer staved of flow.
Control system closes valve B
Debutaniser vents to flare
Naptha splitter empties.


Poor display design:
no single display provides overview of FCCU process; lack of colour to indicate status and reliance on presentation of discrete values.
Fractional distillation uses 1 main input to produce 5 product streams. Information on accumulated outputs of each stream distributed across several control display units.
Operators preoccupied by high number of alarms (In last 11 minutes, 2 operators presented with and acknowledge 175 alarms)
Operators preoccupied by controlling heat transfer process between components.
Liquid level to deethaniser is restored.
Control system (?) opens valve A
Debutaniser receives further flow.
Debutaniser fills with liquid
Operators open valve C (first time)
Liquid in overhead accumulator flows into recovery section.
Compressor trips (first time).
Initial overhead accumulator material sent to flare.
c
Fire hoses used to drain dry stage material to flare.
b
Debutaniser becomes logged
Debutaniser vents to flare
a
Command to open valve B fails.
Operators receive wrong signal valve B open
Operators fail to realize potential danger from flare overflow
Poor maintenance procedures(apparent in failed sensors and other components).
Design assumption in automated control system logic that if discharge rate increased then it would outstrip increases in input so no control over input in single control loop. .
No second, back-up feedback control loop to ensure input flow reduced or shut off when fluid accumulates.


Desire to reduce load on recycling plant during normal operations, pumps operate to slops at full capacity only if manual valve is opened
Automated system that would pump excess to 'slops' now requires manual intervention
Manual operation of Valve to pump at high capacity from flare drum to slops not practiced.
Pump slowly discharges automatically from flare drum back into secondary overhead accumulation.
b
Fire hoses used to drain dry stage material to flare.
Compressor restarts
Pressure increase in debutanizer.
Operators open valve C (second time).
Compressor trips (second time).
Further overhead accumulator material sent to flare.
Modification to flare drum pump prevents excess being pumped to storage tanks.
a
Debutaniser vents to flare
c
Initial overhead accumulator material sent to flare.
Liquid forced from full flare drum to corroded discharge pipe.
20 tonnes discharged Hydrocarcbon exlodes.
High-level alarm for flare drum is activated.
Maintenance failure leaves senor-indicating flow and level in debutanizer was believed to give erroneous indication below maximum.
Displays present plethora of alarms and prevent operators from checking valve B.
Operators preoccupied by controlling heat transfer process between components.
Operators fail to attend to high-level alarm from flare drum for 25 minutes prior to explosion.

Causal Event	Associated Conditions	IEC 61508 Lifecycle Classification	Justification	IEC 61508 Common Requirements Violation	Justification
Liquid forced from full flare drum to corroded discharge pipe.	Modification to flare drum pump prevents excess being pumped to storage tanks.	**Modification:** 1 impact analysis incorrect.	After modification in normal operation automated pumps would now reclaim materials from the flare. Manual intervention was required to restore high velocity pumping to slops under 'emergency' conditions. Operators did not intervene in this manner and the impact of this was not considered.	**Functional Safety Assessment:** 2. Modification assessment LTA.	Assessment of the modification had identified the need to override low capacity transfer of materials in flare but had not considered what would happen if manual intervention did not occur.
		Modification: 4 LTA verification and validation	Inadequate testing to see if operators would intervene once switch was made away from automated default use of high velocity pumps to slops.	**Verification:** 3 LTA verification of modification	There appears not to have been any verification to determine whether operators could or would intervene to perform the necessary manual reconfiguration that was necessary to start high velocity pump transfer to storage tanks from the flume tank.
	Operators fail to attend to high-level alarm for flare drum during 25 minutes prior to explosion.	**Operation and maintenance:** 9 LTA procedures to monitor system performance	Operators were presented with deluge of automated alarms and lacked technical/procedural support to discriminate high priority alarms.	**Functional Safety Assessment:** 1. LTA Operations and Maintenance assessment. **Safety management:** 2. LTA Safety Audits	The incident was caused by a number of problems in the way in which the system was both maintained and operated. Maintenance failures meant that automated systems and operators could not rely on some sensor readings. The tight integration of heat transfer operations together with poor alarm handling created immense burdens for system operators under abnormal situations and these demands appear not the have been assessed in a systematic manner.
Operators open valve C	Maintenance failure leaves sensor indicating that the flow and level in the debutanizer was believed to give erroneous indication below maximum.	**Operation and maintenance:** 2: maintenance procedures need improvement	The programmable systems and operator alarms depended on accurate sensor information. Inadequate maintenance created systemic vulnerabilities that were likely to lead to mishaps.		
	Display presents plethora of alarms that prevent operators from checking status of valve B.	**Allocation:** 4. Installation design	Operators had to acknowledge almost 400 alarms in the last 12 minutes of the mishap. This took away from time to diagnose the problem and plan their intervention.		
	Operator preoccupied by controlling heat transfer process between components	**Overall safety requirements:** 4. Installation design.	Heat generated as a by-product of one sub-process was used elsewhere in the system rather than dissipated by cooling systems. This created delicate dependencies that would be disturbed and impose additional burdens on operators during emergency situations.		

Causal Event	Associated Conditions	IEC 61508 Lifecycle Class.	IEC 61508 Common Requirements Violation	Recommendation	Priority	Responsible authority	Deadline for response	Date Accepted/ Rejected
Liquid forced from full flare drum to corroded discharge pipe.	Modification to flare drum pump prevents excess being pumped to storage tanks.	**Modification:** 1 impact analysis incorrect	**Functional Safety Assessment:** 2. Modification assessment LTA	1. Flare system must be redesigned to provide effective removal of slops from knock-out drum at adequate rate to prevent overfilling.	High	Production engineering team manager	1/4/2003	Accepted 15/2/2003
			Verification: 3. LTA verification of modification	2. There should be a formal controlled procedure for hazard identification following all modification proposals.	High	Plant safety manager	1/6/2003	Accepted 15/2/2003
		Modification: 4 LTA verification and validation		3. Control and protection systems should be independent, particularly where they involve programmable systems.	High	Plant safety manager	1/6/2003	Accepted 15/2/2003
	Operators fail to attend to high-level alarm for flare drum during 25 minutes prior to explosion.	**Operation and Maintenance:** 9. LTA procedures to monitor system performance.	**Functional Safety Assessment:** 1. LTA Operations and Maintenance assessment. **Safety management:** 2. LTA Safety Audits	4. Display systems to be redesigned to provide clearer indication of source of flow problems. Greater prioritisation of alarms will assist in this (see rec 7).	Medium	Production engineering team manager & Plant safety manager	1/5/2003	
Operators open valve C	Maintenance failure leaves sensor indicating that the flow and level in the debutanizer was believed to give erroneous indication below maximum.	**Operations and maintenance:** 2. maintenance procedures need improvement.		5. Safety management system to record and review incident information from other similar plants, causes of mishap already well documented.	Medium	Plant safety manager	1/5/2003	
				6. Safety management system to include monitoring of its own performance – for instance over assessment of modifications.	High	Plant safety manager	1/4/2003	Accepted 15/2/2003
	Display presents plethora of alarms that prevent operators from checking the status of valve B.	**Allocation.** 4. installation design.		7. Training of staff will focus on high-stress situations as well as production critical issues. (see also recommendation 4)	Medium	Plant safety manager	1/5/2003	
	Operators preoccupied controlling heat transfers process between components.	**Overall safety requirements:** 4. installation design.						

Concerns 1:Flow Chart Validation

- The flow chart is very simplistic.
- Will people be able to use it consistently?
- How much must we change for each industry?
- Can it really be used by:
  - developers, vendors, integrators and end-users?

Concerns 2: Human Factors

- PARCEL is narrowly based on IEC61508.
- IEC61508 is poor on human factors issues.

Operation & Maintenance	- operation procedures were applied - operation procedures were improved	- correct maintenance procedure had been used - maintenance procedure was improved - proof testing was more frequent	- correct operation procedure was used - operation procedure was improved - permit procedures were improved	- mitigation procedures were applied - mitigation procedures were improved - mitigation system was proof checked more frequently	- operation procedures had been applied - operation facilities or procedures were improved

- But HSE and others are addressing this?

Concerns 3: IEC61508?

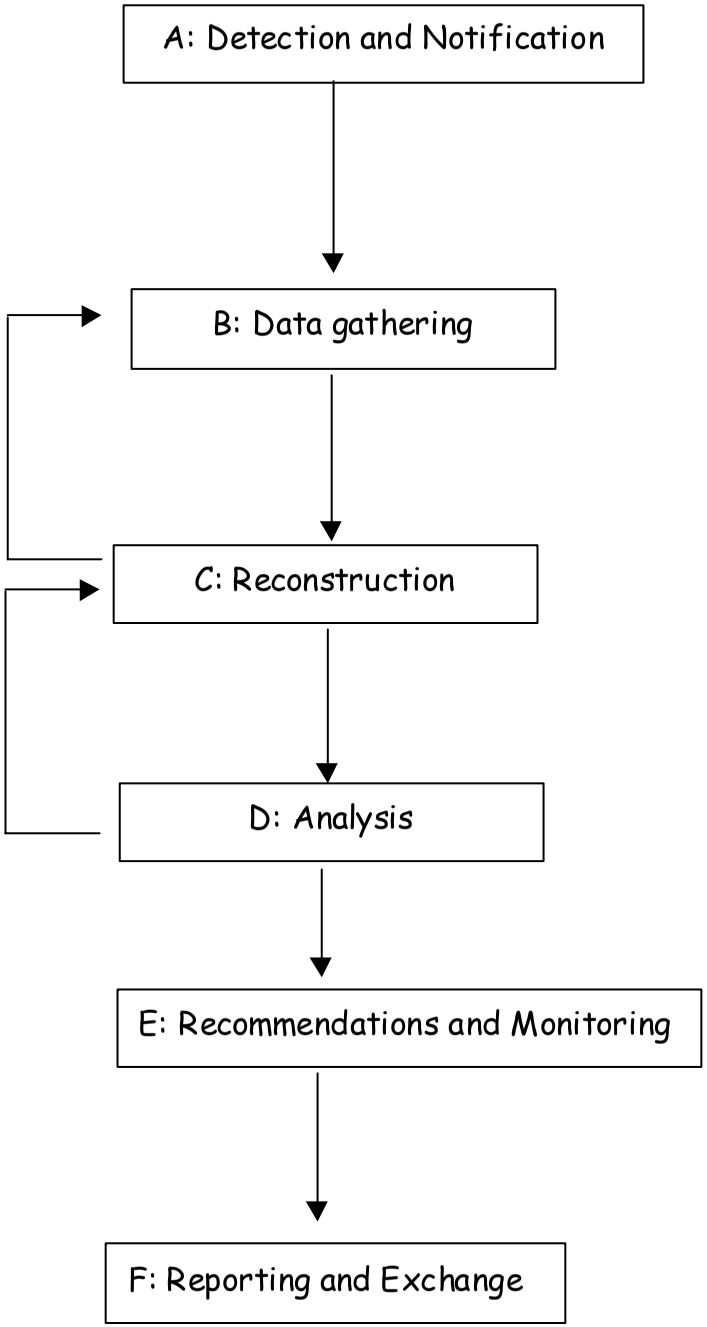
- PARCEL embodies IEC61508:
  - Can we use it with other standards?
  - Will it really help spot problems in 61508?

- PARCEL embodies flowcharts and ECF:
  - We could use flowcharts and STAMP?
  - Must match tool complexity to industry need.

Part 4

1. Coffee and overview.
2. STAMP
3. PARCEL

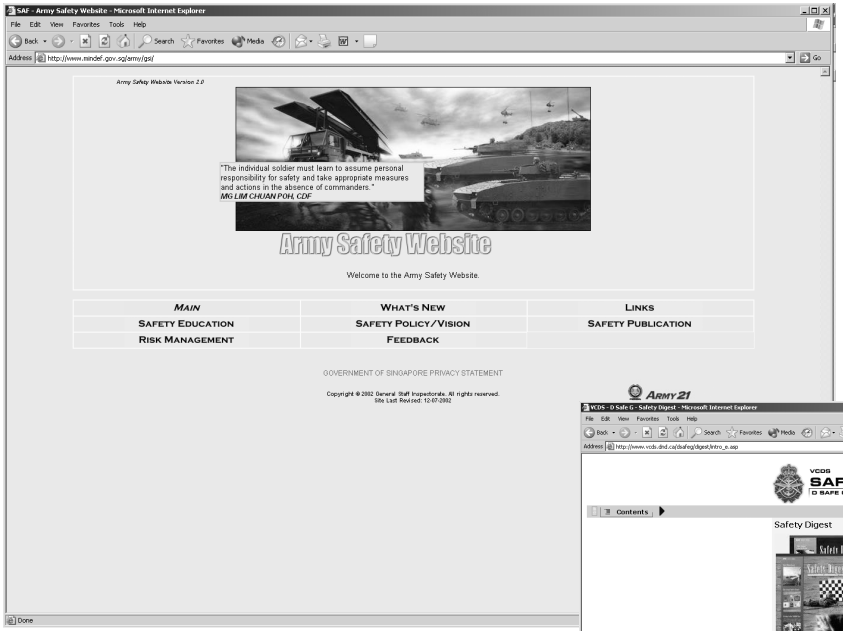
> 4. Wrap-up.


A: Detection and Notification
B: Data gathering
C: Reconstruction
D: Analysis
E: Recommendations and Monitoring
F: Reporting and Exchange

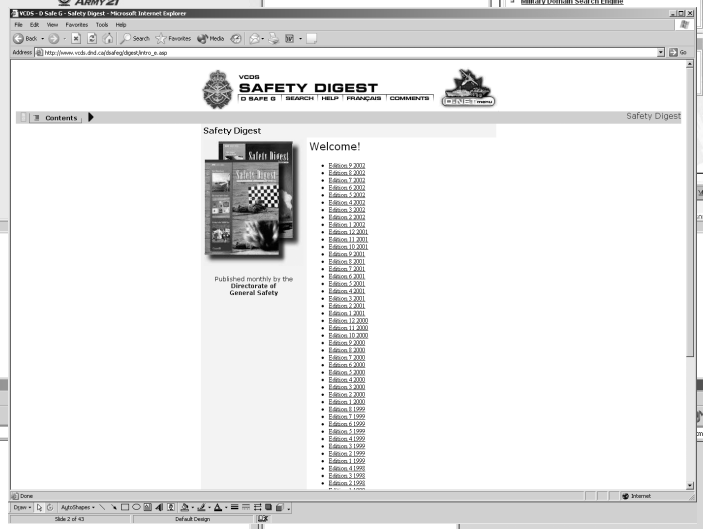
So what happens in practice?

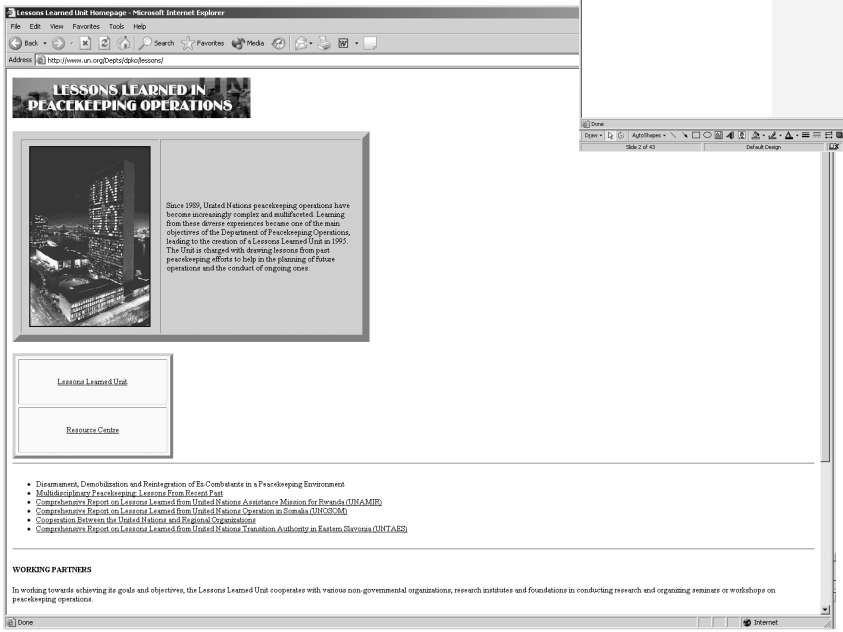
	World War II (1942-1945)	Korea (1950-1953)	Vietnam (1965-1972)	Desert Storm and Desert Shield (1990-1991)
Accidents	56%	44%	54%	75%
Friendly Fire	1%	1%	1%	5%
Enemy Actions	43%	55%	45%	20%

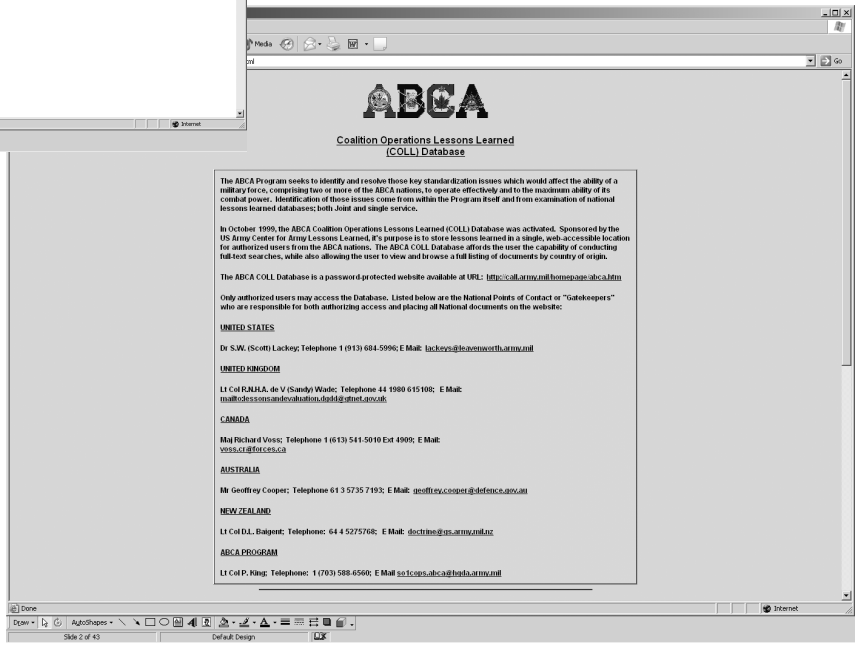
Percentage of all accounted casualties, fatal and non-fatal (US Army, Risk Management Field Manual 100-14)


SAF - Army Safety Website - Microsoft Internet Explorer
Army Safety Website Version 2.0
"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
Copyright © 2002 General Staff Inspectorate. All rights reserved.
Site Last Revised: 12-07-2002
ARMY 21


Center for Army Lessons Learned - Microsoft Internet Explorer
CALL
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
Homeland Security
IBCT
Request Information or a CALL Product
Provide web site Feedback
Search CALL's Web Site
SEARCH
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.
CALL Links
CTC Ask
Information Operations
MOUT
Trends Reversal
Knowledge Symposium
CALL Resources
Mission
Search Engines
Products
CALL Databases
Training and Doctrine
Schools
Operations
CALL Thesaurus
Research Tools
News Services
Contact CALL
New CALL Products
News from the Front - Mar/Apr 02
Preventing Heat Injuries
News from the Front - Jan/Feb 02
Enduring Freedom - Newsletter No. 02-8
Tangeling The Rakkasan Way - Newsletter No. 02-3
Other Lessons Learned Links
Army (other)
Air Force
Coast Guard
Navy
US Government (Non-DoD)
International
CALL's Search Engines
Military Domain Search Engine
Items of Interest
CALL PfP Outreach
(6 Sep 02)
CALL is currently partnering with the Partnership for Peace Consortium of Defense Academies and Security Studies Institutes (http://www.pfpconsortium.org) to expand the practice of lessons learning to the countries of the former Warsaw Pact and Soviet Union. CALL hopes through this outreach to foster the collection, analysis and dissemination of partner lessons learned via the PfP Lessons Learned Database, which CALL operates on behalf of the Consortium. PfP users can access the PfP LL DB via PIMS (http://www.pims.org). U.S. users can access the PfP LL DB HERE.
Army Links
Army Homepage
Army Knowledge Online
Association of the US Army
Army National Guard
Army Reserve
Acquisition Lessons Learned
DCST-West
DITT
FMSO
GuardNet
Operation Noble Eagle
Reimer Digital Library
Discussion Communities
Coming Soon!
CALL's Threaded Discussion Area
Your Comments are Important, Give us Your Feedback!
Internet


VCDS - D Safe G - Safety Digest - Microsoft Internet Explorer
VCDS
SAFETY DIGEST
D SAFE G | SEARCH | HELP | FRANÇAIS | COMMENTS
Contents
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.

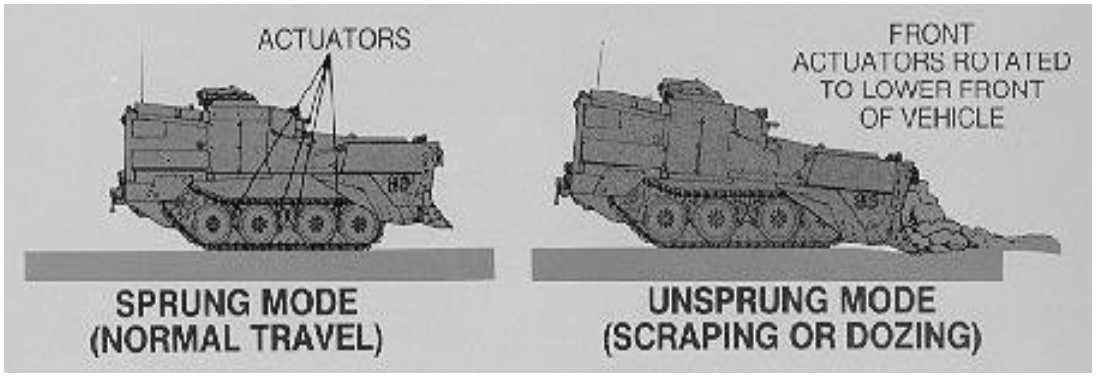

ABCA
Coalition Operations Lessons Learned
(COLL) Database
The ABCA Program seeks to identify and resolve those key standardization issues which would affect the ability of a military force, comprising two or more of the ABCA nations, to operate effectively and to the maximum ability of its combat power. Identification of these 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
Dr S.W. (Scott) Lackey; Telephone 1 (913) 684-5996; E Mail: lackeys@leavenworth.army.mil
UNITED KINGDOM
Lt Col R.N.H.A. de V (Sandy) Wade; Telephone 44 1980 615108; E Mail: mailtodessonsandevaluation.dgdd@gtnet.gov.uk
CANADA
Maj Richard Voss; Telephone 1 (613) 541-5010 Ext 4909; E Mail: voss.cr@forces.ca
AUSTRALIA
Mr Geoffrey Cooper; Telephone 61 3 5735 7193; E Mail: geoffrey.cooper@defence.gov.au
NEW ZEALAND
Lt Col D.L. Baigent; Telephone: 64 4 5275768; E Mail: doctrine@qs.army.mil.nz
ABCA PROGRAM
Lt Col P. King; Telephone: 1 (703) 588-6560; E Mail so1cops.abca@hqda.army.mil

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

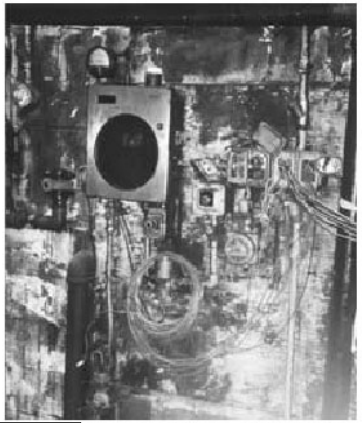
- Never under-estimate organizational complexity of human 'error'…

- "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…"

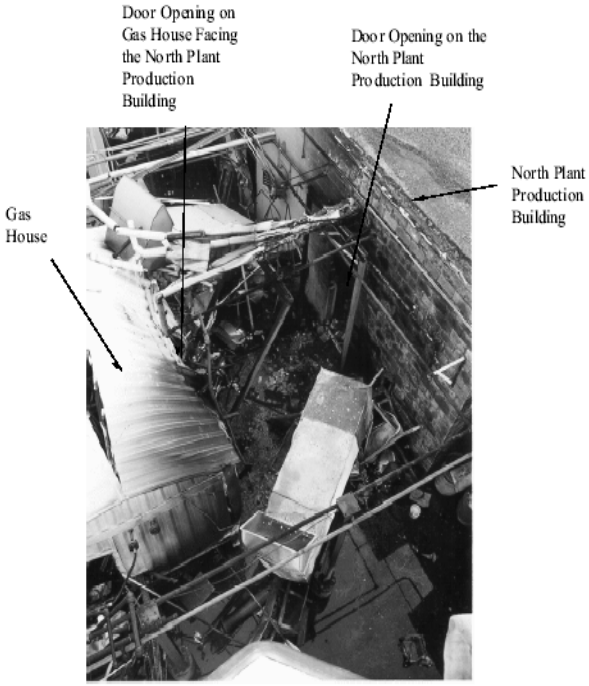
(Canadian Army's Lessons Learned Centre, NATO Implementation & Stabilization Force in Bosnia-Herzegovina. 1999)

- Balancing operational need and medical caution?



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.



Any Questions?