Lloyd's Register Educational Trust

UNIVERSITY OF Southampton
School of Engineering Sciences

Safety and risk

by

Professor Vaughan Pomeroy

The LRET Research Collegium
Southampton, 16 July – 7 September 2012

UNIVERSITY OF Southampton
School of Engineering Sciences

Safety and Risk

Professor Vaughan Pomeroy
July 2012

Icebreaker

- Think of a maritime application that you are familiar with
- How safe is the application?
- What do you think is the greatest risk to your safety and your activity?

UNIVERSITY OF Southampton
School of Engineering Sciences

Introduction to Maritime Safety and Risk

What is safety?

- Freedom from danger
- Freedom from unacceptable risks and/or personal harm

- Is cost a valid consideration?

- How safe is safe enough?
  - From whose perspective?

What is safety?

- Individual safety
  - Occupational health and safety
  - Individual behaviours
  - Workplace environment
  - EASY TO MEASURE – LOST TIME ACCIDENTS etc
- Process, unit or societal safety
  - Safety management
  - Management of risks outside individual's control
  - ONLY MEASURABLE BY FAILURES, POST EVENT

What is risk?

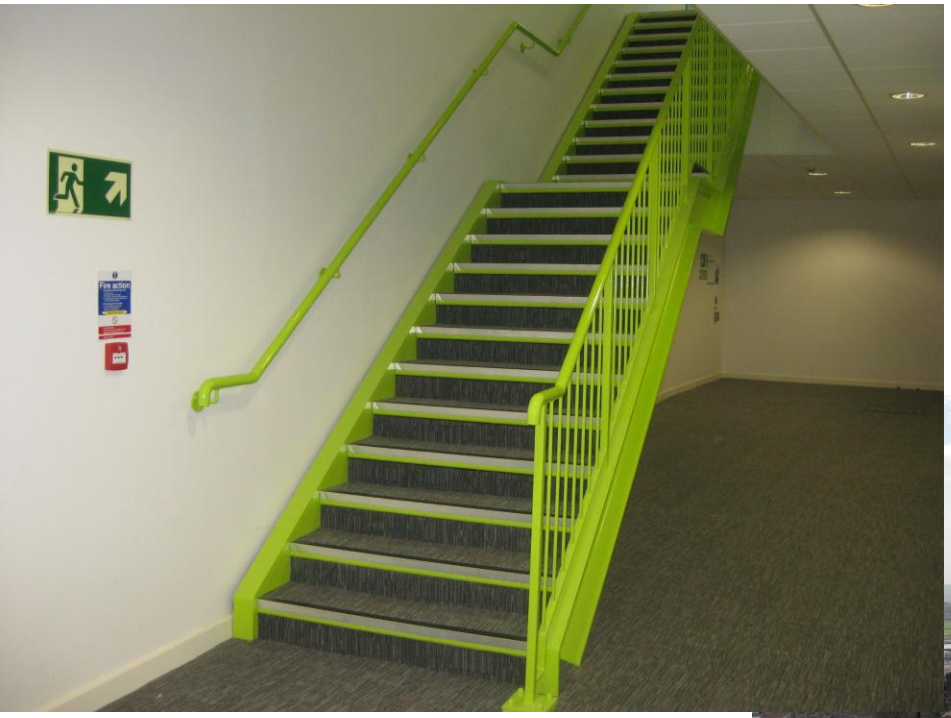
- A hazard
- The chance of a ‘loss’

Risk is a ‘probabilistic measure’

- Risk = (probability of occurrence) x (consequence)

Whose risk?

Attitudes to managing risks



What does this imply?

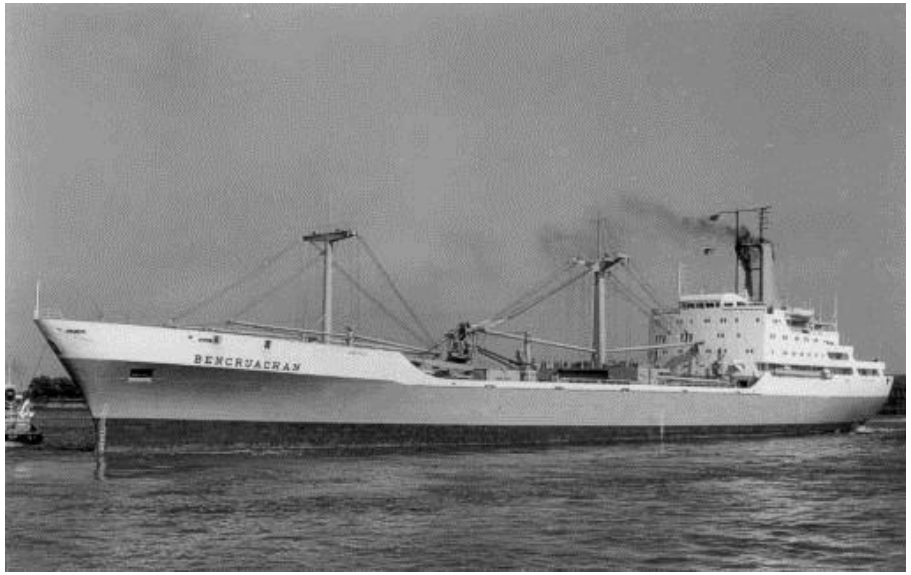
Maritime hazards and risks

- Which hazards can be managed?
- Which risks are changed by human choice and action?
- Where are the uncertainties?

Tsunami

Natural environment

UNIVERSITY OF Southampton
School of Engineering Sciences



Pasha Bulker

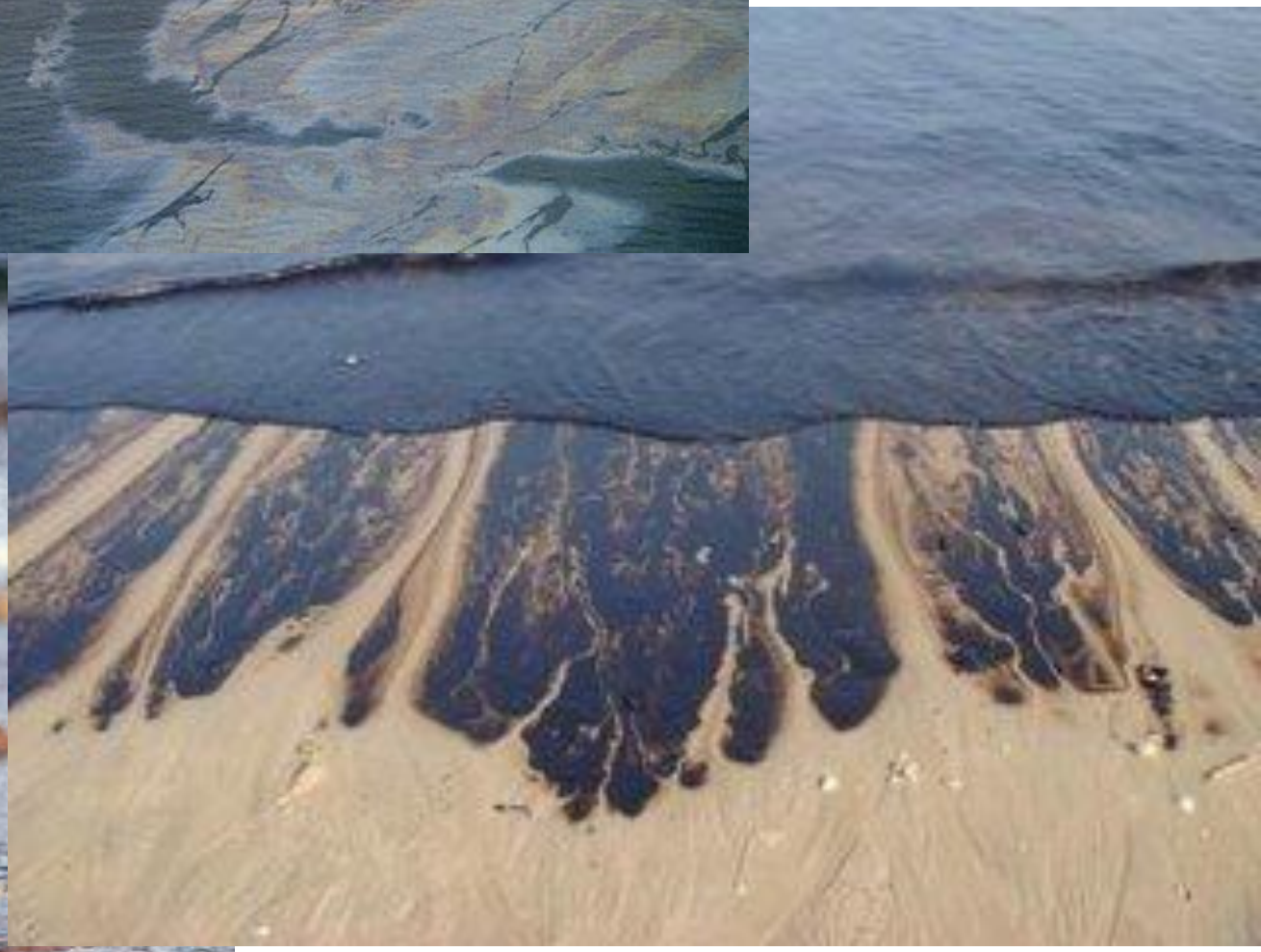
Loading errors

UNIVERSITY OF
Southampton
School of Engineering Sciences

Piper Alpha

www.news.bbc.co.uk

Oil spills



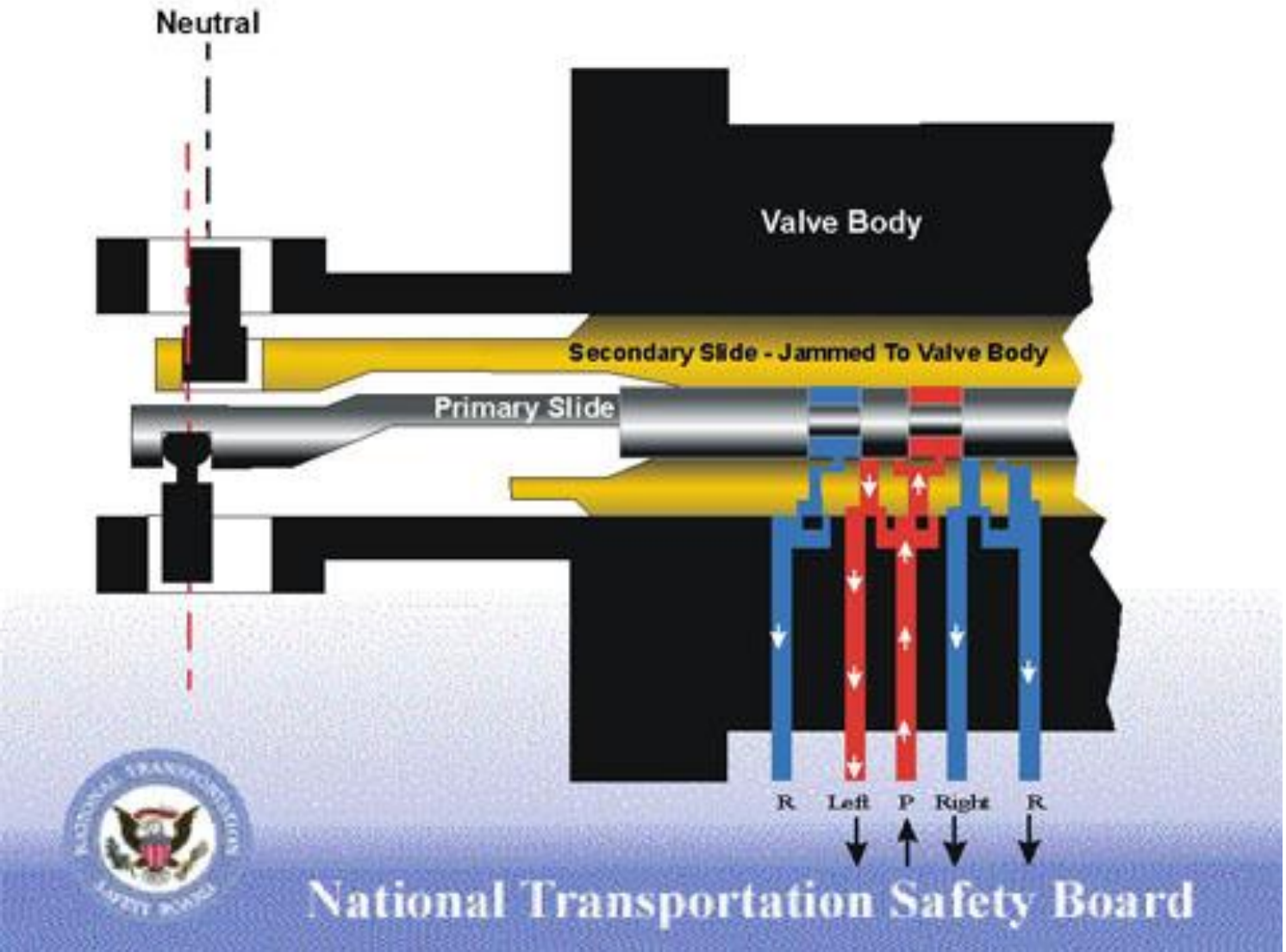
UNIVERSITY OF Southampton
School of Engineering Sciences

Latent defects

Boeing 737 rudder power control actuator

- Two unexplained crashes
  - United 585 at Colorado Springs on 3 March 1991
  - USAir 427 at Pittsburg on 8 September 1994
- Other near misses, notably Eastwind 517 near Richmond on 9 June 1996
- Consistent with a rudder reversal scenario – an uncommanded hard-over opposite rudder evolution

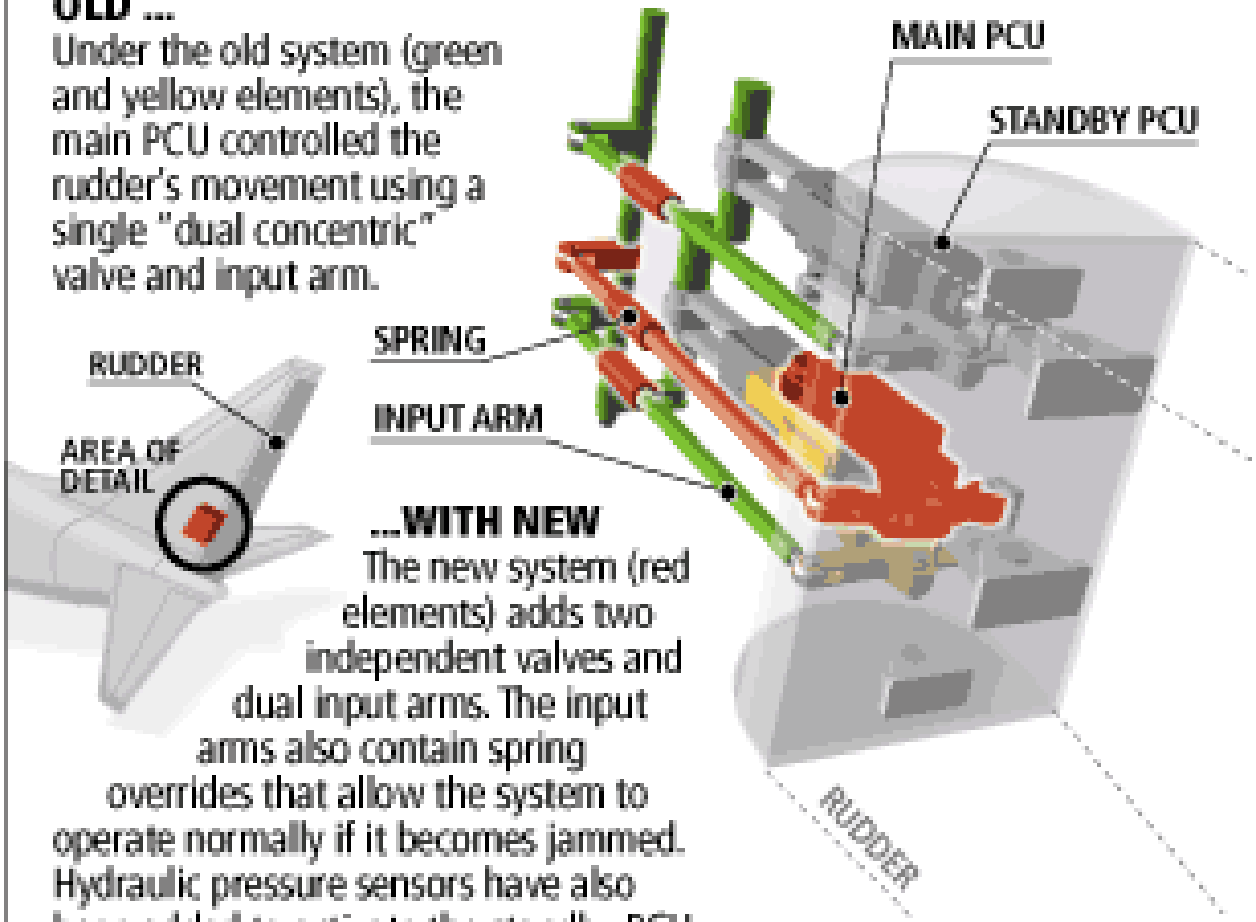
Dual concentric servo valve



CHANGES TO 737 RUDDER SYSTEM

All Boeing 737s will be modified so that the power control unit (PCU) in the rudder control system has multiple backups in the event of a mechanical failure.

OLD ...
Under the old system (green and yellow elements), the main PCU controlled the rudder's movement using a single "dual concentric" valve and input arm.



...WITH NEW
The new system (red elements) adds two independent valves and dual input arms. The input arms also contain spring overrides that allow the system to operate normally if it becomes jammed. Hydraulic pressure sensors have also been added to activate the standby PCU if abnormal readings are detected.

Source: The Boeing Co.

Earlier FAA required increased checks

FDAU to be installed by 1 August 2001

Modification of 2800 aircraft at $150m

Which is the anomaly?

Many years of accident free operation

Crash in Paris

Which is the anomaly?

Many years of accident free service

Hazard was always present

Crash in Paris

UNIVERSITY OF Southampton
School of Engineering Sciences

Methodologies

Principles of risk assessment

- What can go wrong?
- How likely is it to go wrong?
- What happens if it does go wrong?
- Does it matter?
- If it does, what can we do to:
  a) prevent it from going wrong in the first place?
  b) reduce the frequency of its occurrence?
  c) mitigate the consequences of its occurrence?

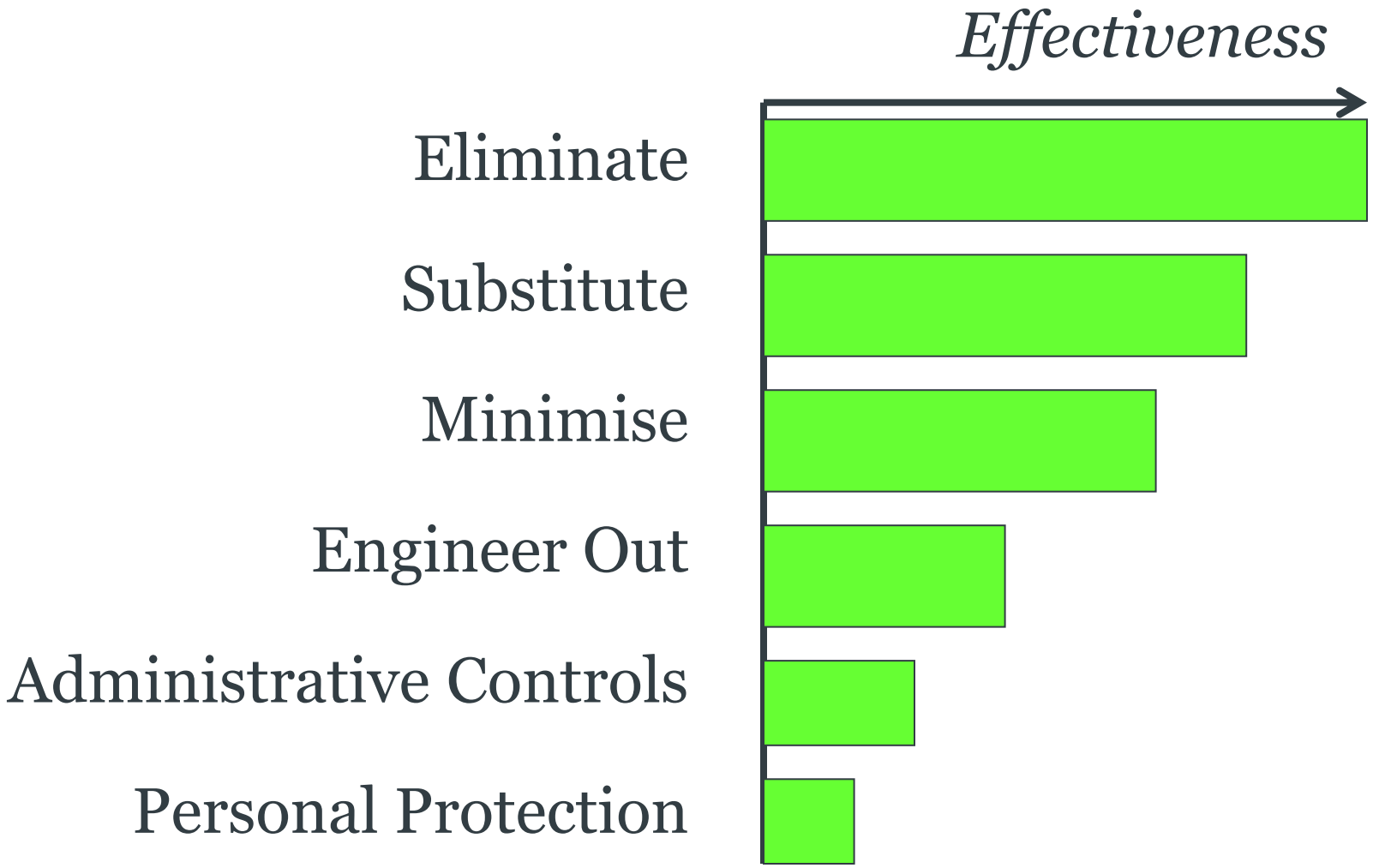
Process

- Hazard Identification
- Hazard Analysis
- Consequence Analysis
- Risk Evaluation
- Development of hazard avoidance, risk reduction and mitigation strategies.

Forms of corrective actions/risk control

- Eliminate hazard
- Substitute with lower hazard solution
- Minimise hazard
- Engineer out hazard
- Procedures and administrative controls
- Protect individuals

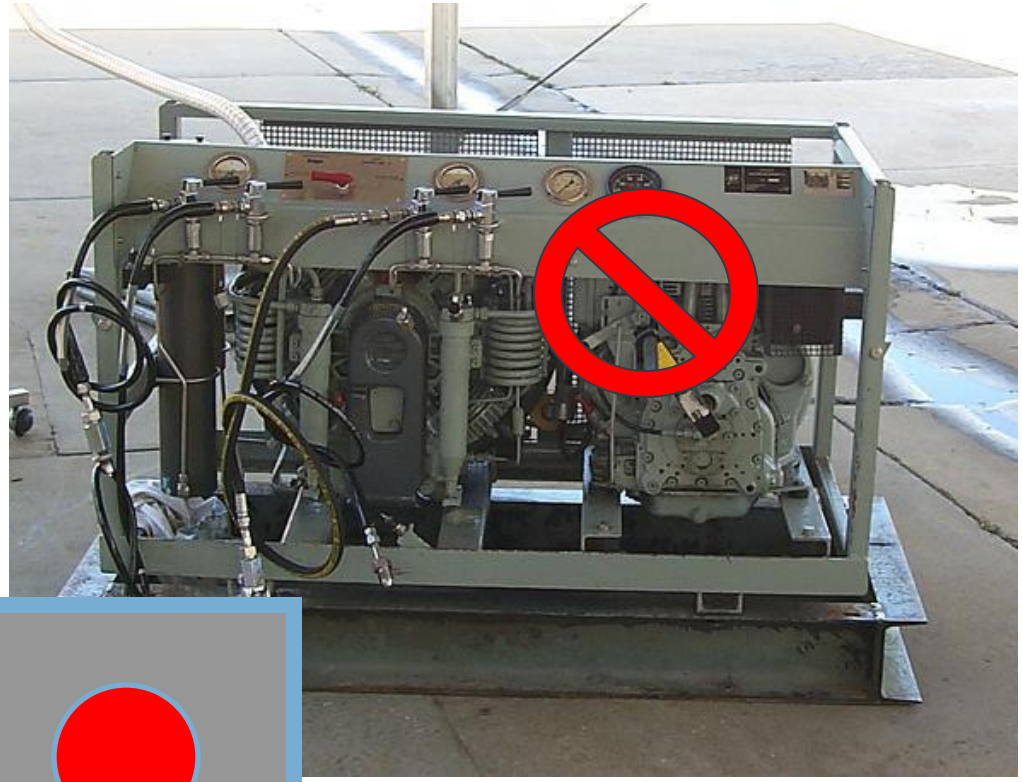
UNIVERSITY OF Southampton
School of Engineering Sciences

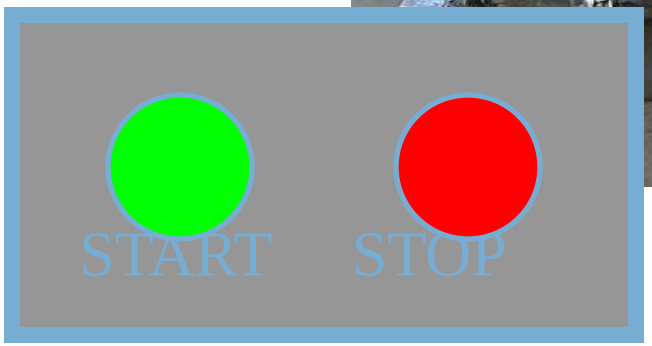


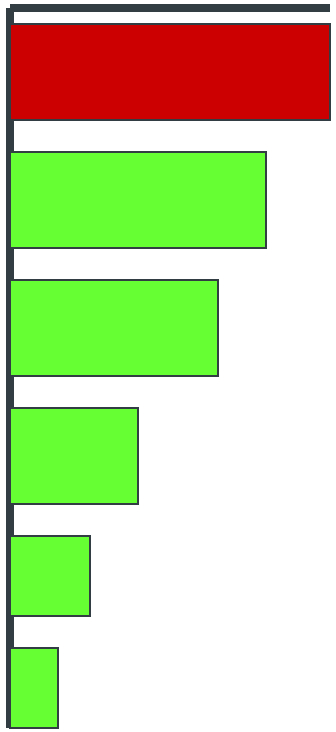
Eliminate the Hazard

UNIVERSITY OF Southampton
School of Engineering Sciences

Eliminate the Hazard







Effectiveness

Engineered solutions

- Duplication of critical items
  - Redundancy
  - Separation
  - Diversity
  - Voting arrangements
- Beware of
  - Common mode failures (Millennium bug)
  - Common cause failures (flooding of compartments)

UNIVERSITY OF Southampton
School of Engineering Sciences

Redundancy

- Characteristic
- Common causes and common modes
- Series and parallel systems
- Diversity and voting systems
- How good is redundancy?
- Do redundant systems still fail?

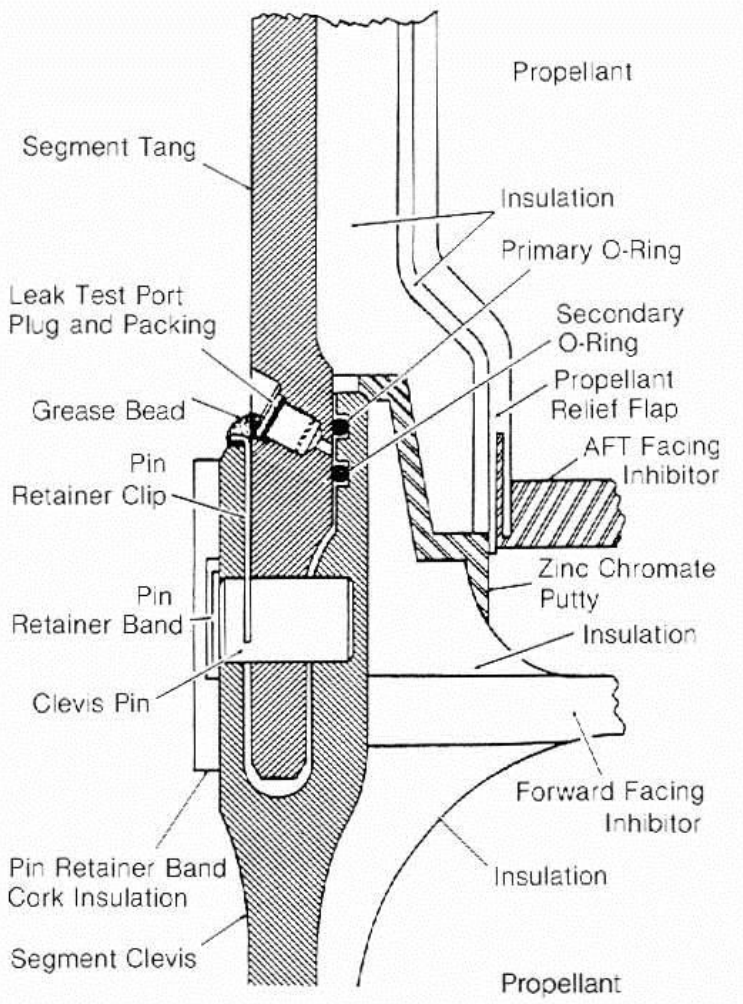


Figure 14
Solid Rocket Motor cross section shows positions of tang, clevis and O-rings. Putty lines the joint on the side toward the propellant.

UNIVERSITY OF
Southampton
School of Engineering Sciences

Reliance on administrative controls

Reliance on administrative controls

Protection of individuals

UNIVERSITY OF
Southampton
School of Engineering Sciences

UNIVERSITY OF Southampton
School of Engineering Sciences

Imagining the unthinkable

Everything that happens was once infinitely improbable

Therefore, nothing that happens should be surprising

All swans are white.....

Except those that are black!

Open minds

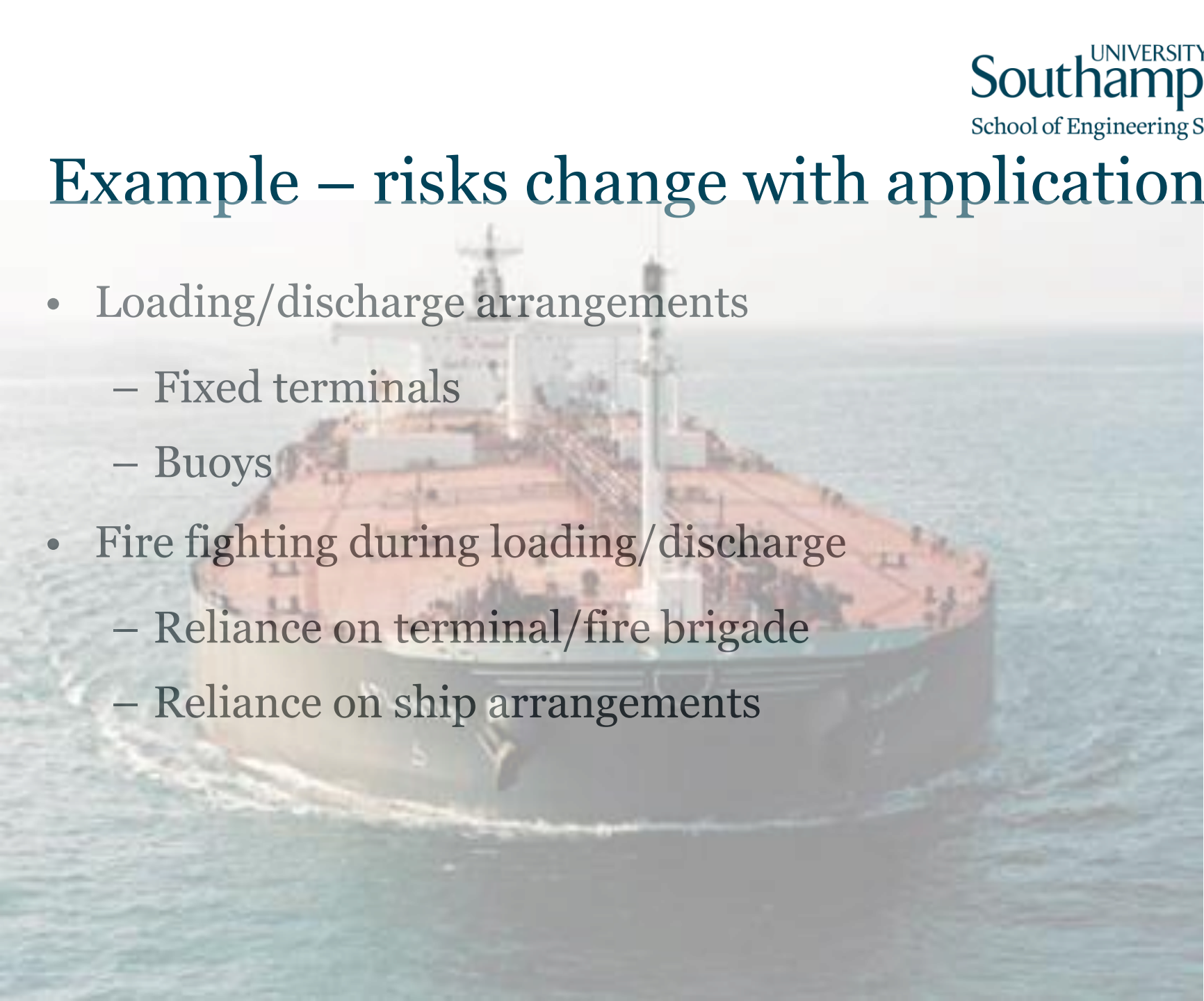
- Try to identify all possible failure modes
- Evaluate all possible consequences
- Look for all possible interactions between elements

- Do not initially censor the lists
  - Because it doesn't happen
  - Because people don't do that
  - Because it only happens when people behave badly

Concept of Operations

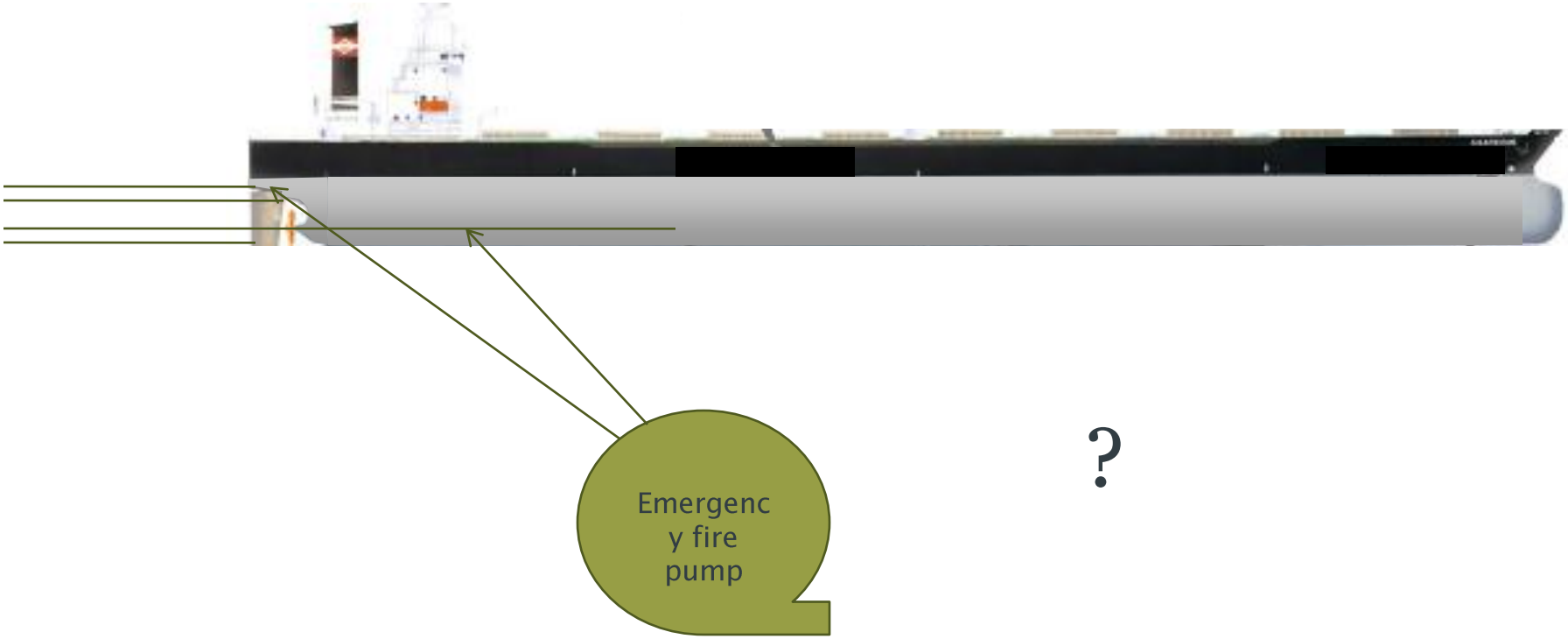
- What is the purpose of the asset?
- Who will use it?
- How will it be used?
- Where will it be used?
- How will the asset REALLY be used
  - Change of operating area?
  - Change of operational mode?
  - Change of operators?

Example – risks change with application



- Loading/discharge arrangements
  - Fixed terminals
  - Buoys
- Fire fighting during loading/discharge
  - Reliance on terminal/fire brigade
  - Reliance on ship arrangements

Emergency fire pump



Viewpoints

- Regulator assumed EFP only required in sea going conditions
- Shipbuilder assumed regulatory compliance was enough
  - Location of EFP and emergency generator on steering flat provided compliant and cost-effective solution
- Owner intended to load at buoys with no shore fire support
- EFP suction above lightest operational draught
- Safety compromised, unintentionally
- SOLUTION – relocate EFP in pump room

How can we make sure that we think?

- Do not stop at thinking when you know how things will perform the required tasks
- Challenge the standard practices and solutions – will they do what is required?
- Think about how things might fail

Unintended consequences

- Good intentions miss possible outcomes
- Result of not thinking out the problem completely
- Happen at all levels
  - Regulations that drive inappropriate but compliant solutions
  - Enhanced functionality which confuses the operator
  - Notices that are unclear and can be misinterpreted

UNIVERSITY OF Southampton
School of Engineering Sciences

Professor Vaughan Pomeroy
r.v.pomeroy@soton.ac.uk