SAFETYWISE

Design failures and faults contributing to incidents

Plant Safety in the Mining Industry Seminar

Gerry Gibb

Panthers Club
May 1st 2007

Bottom Line of Safety

SAFETY WISE

"Safety is NOT an intellectual exercise.
Safety is truly a matter of life and death, and is the sum and quality of all our individual contributions that determines whether our colleagues LIVE or DIE…on July 7, 1987, 167 people died."

Brian Appleton (ICI)
Opening Statement as Technical Advisor to the Cullen Inquiry (Piper Alpha)

Efficiency

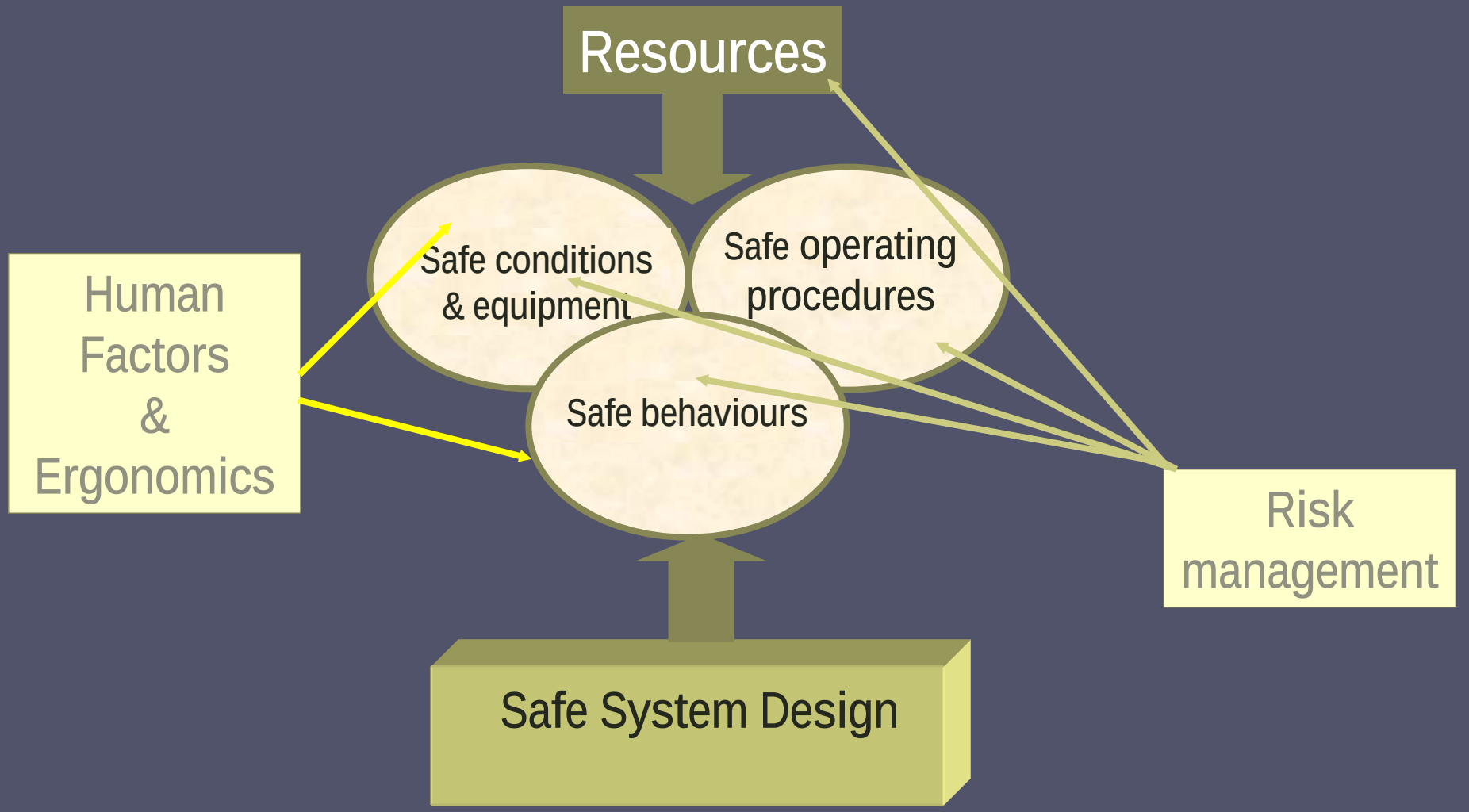
SAFETY WISE

In our endeavour to increase production efficiency,

we must never lose sight of the end user

Safe System - Prerequisites

Tools for a safe system



How does equipment design impact safety?

- The way in which equipment is constructed makes certain operations difficult
- Equipment design allows unexpected/unplanned usage.
- Poor design may require extra effort and unusual maintenance.
- Inadequate design capacity may lead to extending the equipment beyond limits.
- Many design failures result from the physical and professional separation of the designer and end user

What causes inadequate design

- no standardisation of equipment or usage
- not adapting to human needs and limitations
- poor designer - user communication
- time or financial constraints
- no indication of system status provided by design (on / off, working or not etc)
- inadequate design premise data

What can inadequate design lead to?

- extra effort to do the job
- unexpected performance of equipment
- inability to operate equipment properly
- inability/difficulty in controlling processes
- long or repeated training requirements
- equipment is unused or improvised usage

Design failure or end user error ?

SAFETYWISE

Design failure or end user error ?

SAFETY WISE

MCA Mobile Equipment Incident Causation Survey 2005 - 2006

Some findings

There is a need to increase the layers of protection from fatal injury in the design, construction and operation of mobile equipment used in the mining industry

The survey showed that the equipment type with the most opportunity to yield improvement is in Off-Highway Haul Trucks

The MCA should consider establishing a Minerals Industry Mobile Equipment Round table with the mandate to identify and prioritize the key issues for the industry and Equipment Suppliers

Case Study 1
A340 Switch Design Incident

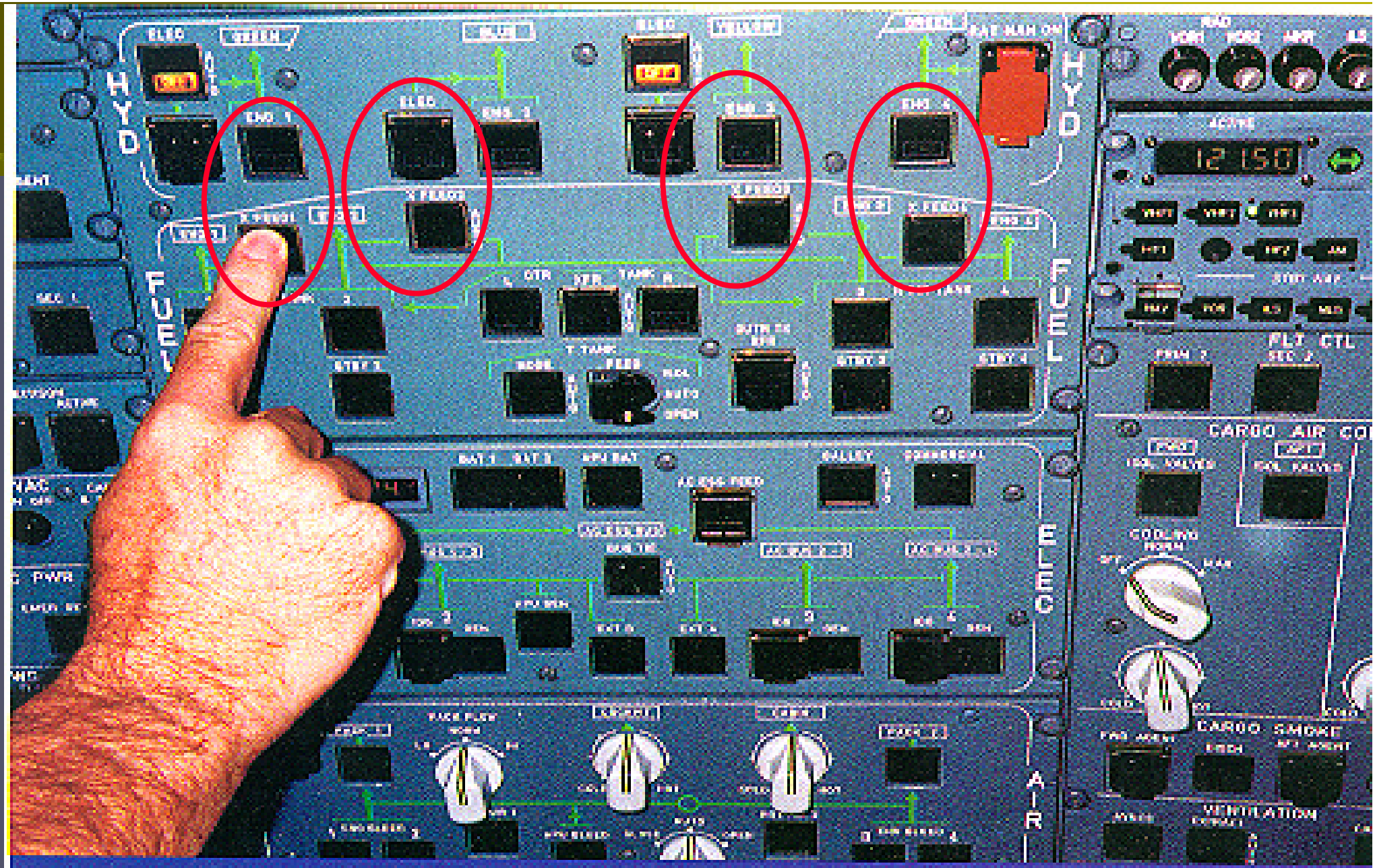
SAFETYWISE

- 10 minor injuries, 1 serious injury
- Circumstances:
  - fuel imbalance (common)
  - solution: open the 4 crossfeed fuel valves
  - procedure: depress the fuel crossfeed valve switches on centre overhead panel

Event Sequence

- Pilot (PNF) initially placed his finger on the fuel crossfeed switch,
- Pilot was distracted, with attention drawn to the ECAM (engine condition and monitoring) instrument panel
- Whilst pilot was observing the panel, his finger moved slightly, repositioning itself over the hydraulics switch
- Pilot continued with the crossfeed - looked up to his finger, and then pressed the (incorrect) switch. He then depressed the remaining 3 switches, believing them to be the fuel switches.
- The pilots noticed the problem before complete control was lost. But positive and negative accelerations did result in large pitch changes .
- The aircraft pitched up and then during recovery severe pitch up in the rear of the aircraft resulted in 1 serious injury (neck injuries) to cabin crew member


ENG 1
ENG 2
ENG 3
ENG 4
APU



A340 centre overhead panel. Finger is on number 1 crossfeed valve switch. Number 1 engine driven-hydraulic pump switch is about 3 cm immediately above.

Design issues

- The switches were not guarded
- They were of very similar appearance as fuel crossfeed switches
- Activated by the same push button switching action (Design/HF Issue - same action/feedback)
- Use same white illumination to indicate activation (Design/HF Issue - same feedback)
- Located immediately above the fuel crossfeed switches (Design/HF Issue - almost aligned)

Case Study 2
Bunga Teratai Satu
Sudbury Reef, Great Barrier Reef
2 November 2000

SAFETYWISE

Sequence of events - 1

The Malaysian flag container ship Bunga Teratai Satu sailed from Singapore on 26 October 2000, bound for Sydney via the inner route of the Great Barrier Reef with a cargo of 857 containers. A licensed pilot was embarked to conduct the navigation through the inner route between Goods Island and Cairns.

At 0554 AEST on 2 November 2000, *Bunga Teratai Satu* disembarked the pilot at Yorkeys Knob, off Cairns, at the southern limit of the compulsory pilotage area.

At 0600, 'full away' was rung and the vessel resumed its passage to Sydney on a course of 120° (true). A programmed way-point, at position 16° 52.8' S, 146° 02.3' E, was reached at 0700. At this way-point, the course was supposed to be altered to 164° (true) to round Fitzroy Island and take the vessel to the west of Sudbury Reef. However, no course alteration was made.

Sequence of events - 2

The ship was reporting under the Great Barrier Reef Ship Reporting System, REEFREP, administered from Reefcentre, Hay Point. This system requires ships transiting the inner route to report at certain positions within the inner route. To help enforce compliance with pilotage and reporting requirements the normal entry points to the inner route are monitored by radar. In the limited areas covered by radar, the system fulfils a secondary, monitoring role, to improve safe navigation.

Bunga Teratai Satu had been acquired as a target at Reefcentre when it entered the area covered by the Green Island radar system at about 0430. From about 0715 to 0725, the Reefcentre operator was attempting to re-establish lost targets on the Hammond Island radar display covering the western area of Torres Strait. Just before 0716 *Bunga Teratai Satu* entered the restricted zone (2 miles off Sudbury Reef) but the Reefcentre operator did not notice the alarm message as he worked on other tasks.

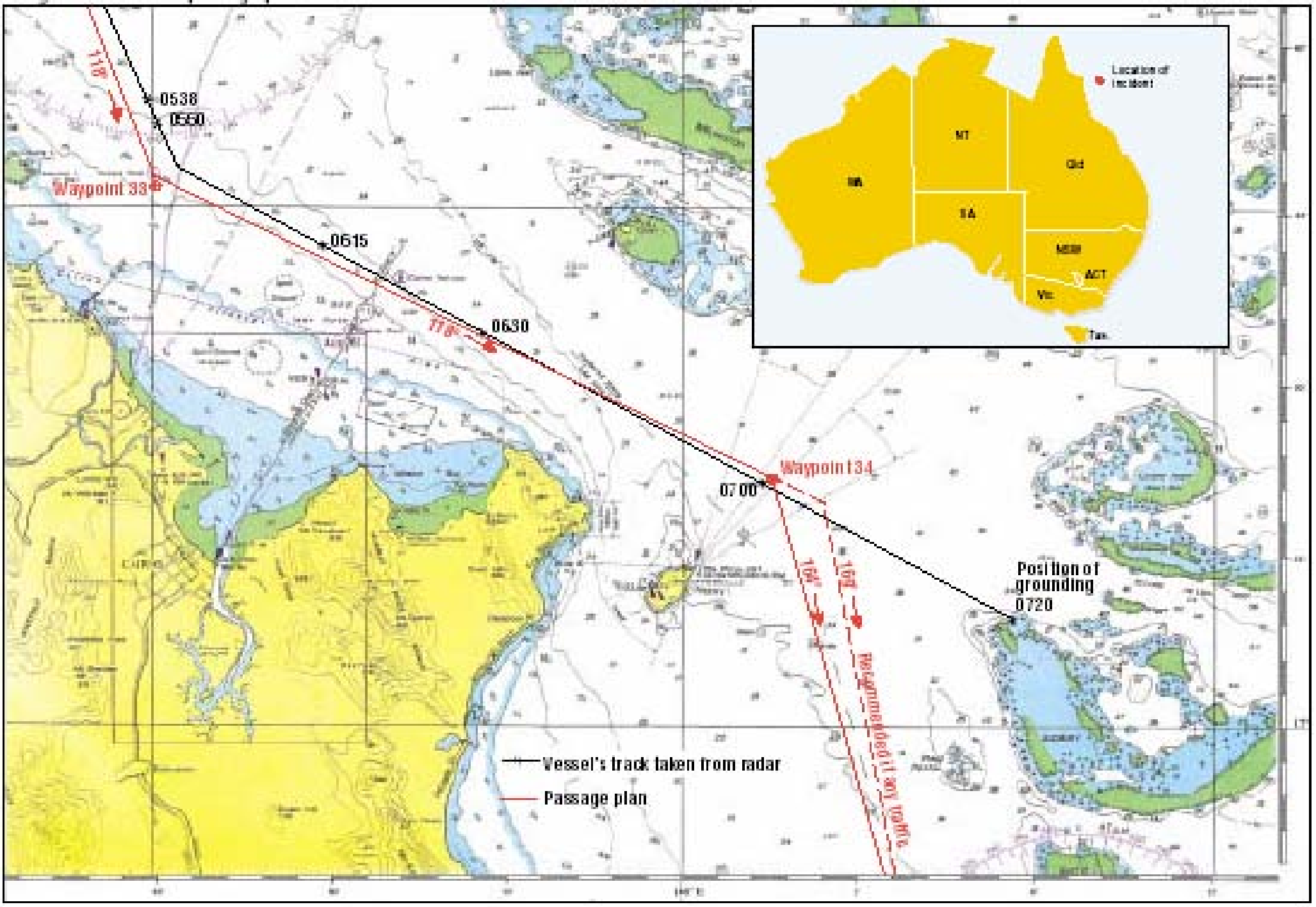
Incident Description

At about 0723, the ship struck the north end of Sudbury Reef at a speed of over 20 knots on a heading of 120°. It was about 1 3/4 hours after low water and the vessel's bow rode some 100 metres onto the reef leaving the stern in approximately 12 metres of water.

Nobody was hurt as a result of the grounding and no oil or other pollutant escaped from the ship. The grounding resulted in mechanical damage to the reef and the yet-to-be assessed effects of the ship's anti-fouling paint.

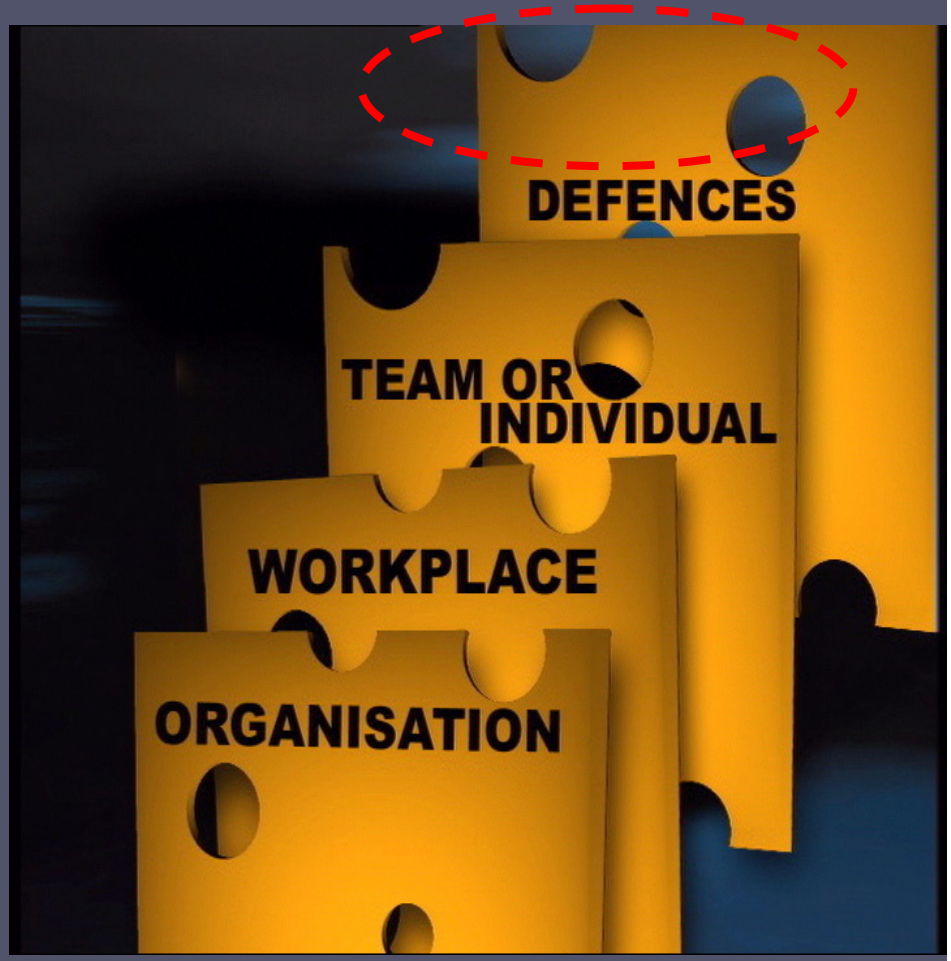
The Australian authorities issued detention orders while the ship's situation was being assessed. *Bunga Teratai Satu* remained fast on the reef until it was eventually refloated with the aid of tugs at about 0930 on 14 November 2000.

Bunga Teratai Satu's passage plan and track



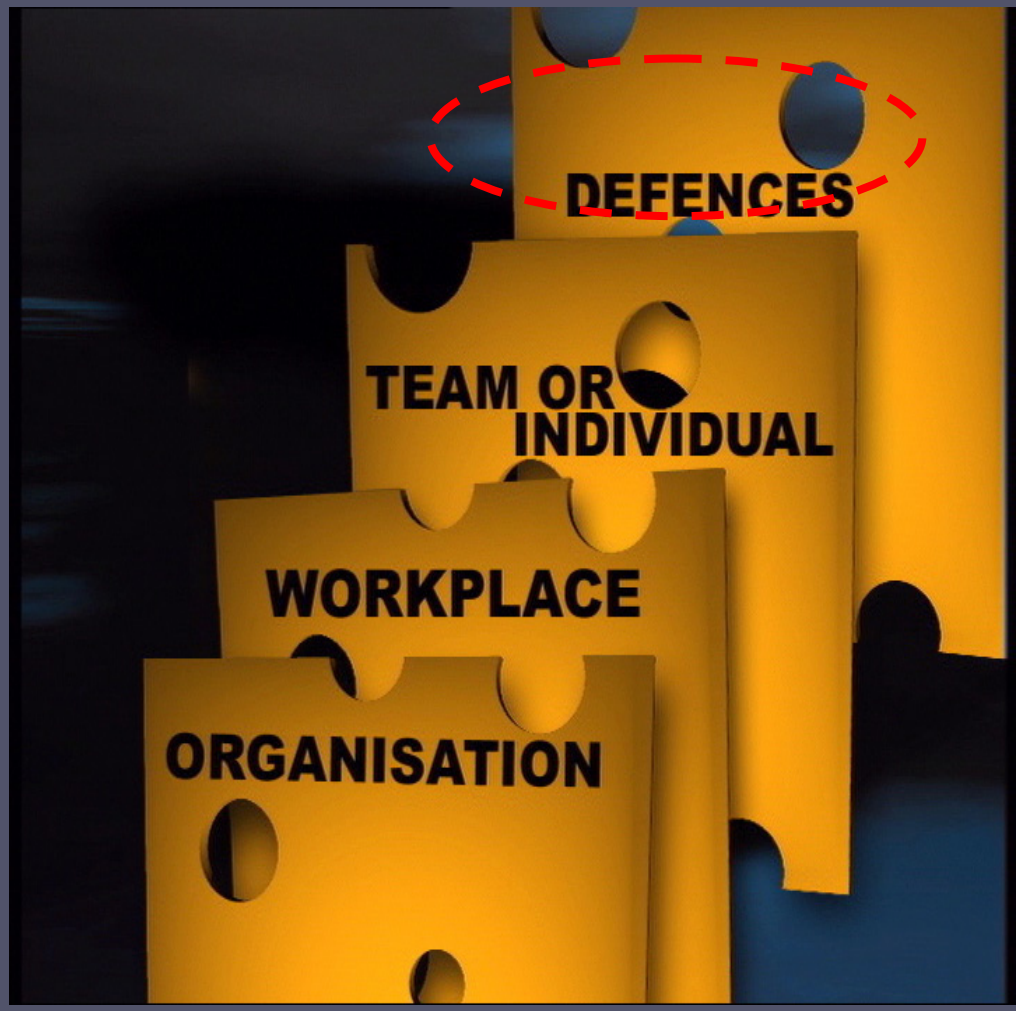
Absent / failed defences - Ship

- Ineffective bridge watch procedures
- Poor Bridge Resource Management on the vessel allowed a basic error by one person to result in a serious accident
- The ship's GPS cross-track error alarm was neither loud enough nor strident enough to attract urgent attention. Design issue



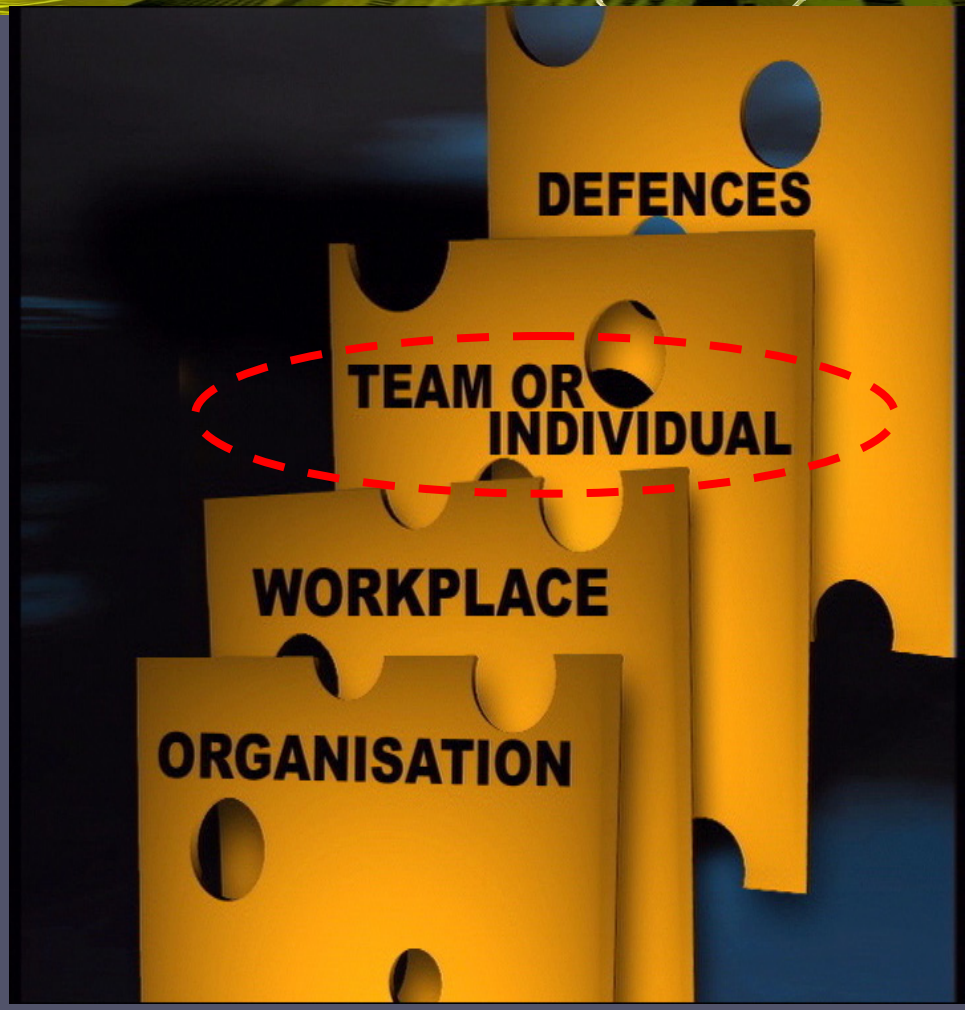
Absent / failed defences - Reefcentre

- Reefcentre monitoring of 4 radar displays
  Poor user interface
- The frequency of annunciation of Traffic Information Module alarms and associated radar system alarms had led to the desensitising of Reefcentre operators to the whole TIM alerting system
  Design issue



Team / individual actions

- The manner in which the mate maintained his watch on 2 November 2000 lacked appropriate motivation and fell well below proper professional standards
- Reefcentre did not detect ship entering resistricted zone or acknowledge TIM alarms
  Poor user interface



Task / environmental conditions - Ship

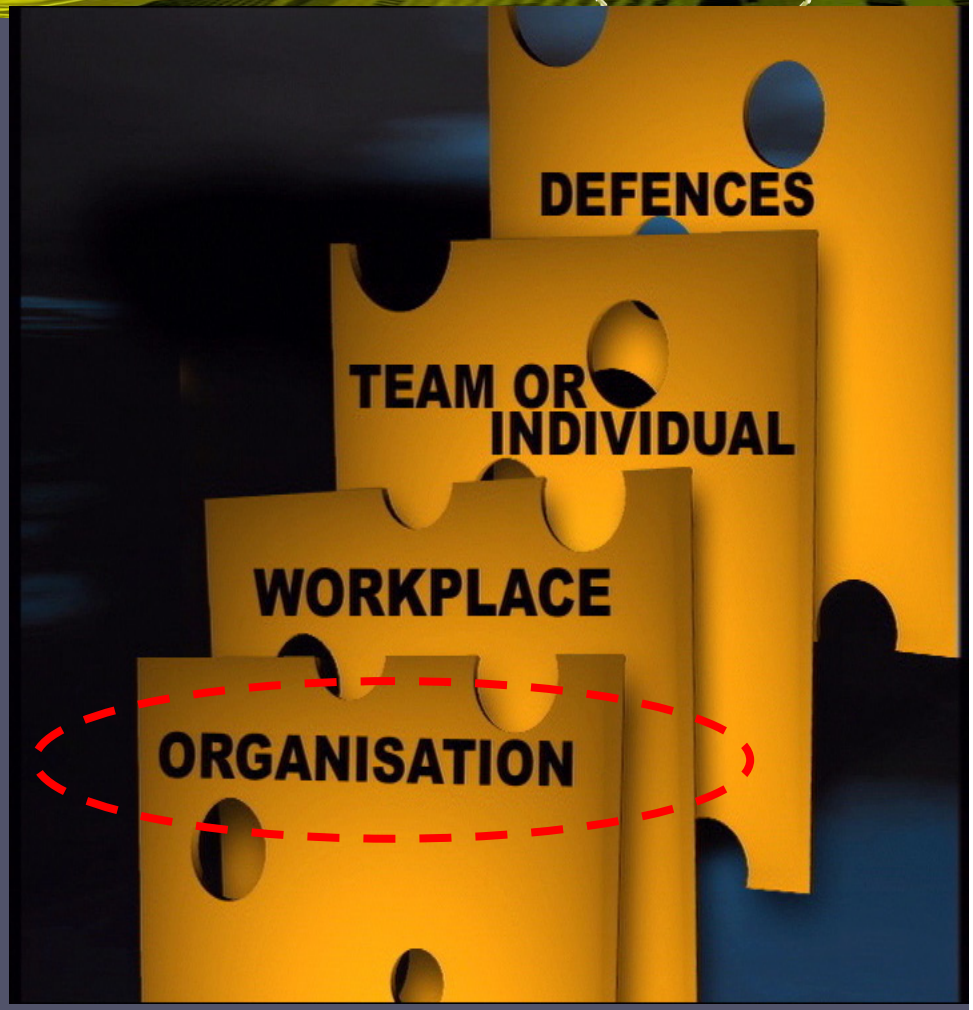
- Featureless horizon
- Mate's wife on the bridge
- Mate and his wife talking to Mother-in Law by mobile from wing of the bridge
- Cultural norms – AB plotting track
- AB assumed Mate knew they had passed waypoint
- Confusion over actual position and track to steer Poor user interface

Task / environmental conditions - Reefcentre

- High workload – 4 radar screens to monitor Poor user interface
- Desensitization to TIM alarms Poor user interface

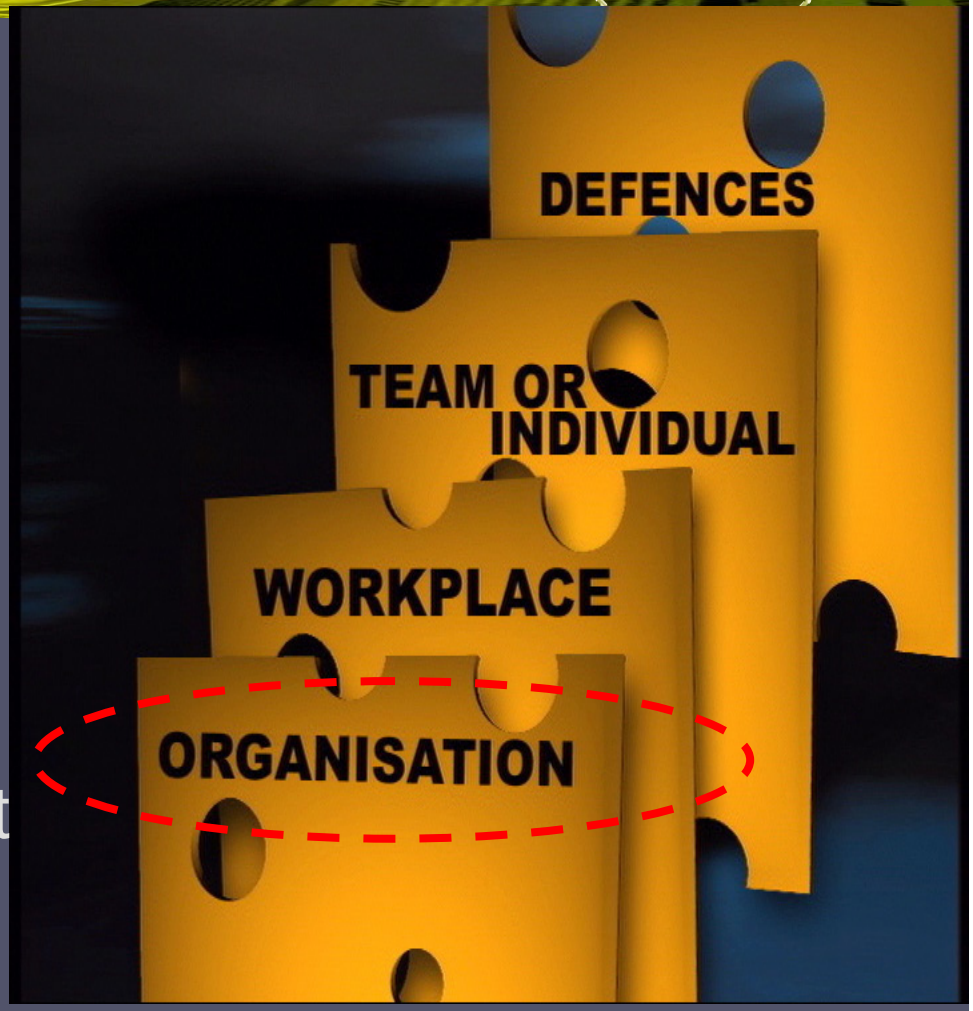
Organisational factors - Ship

- DE GPS cross track error alarm position and audability Design issue
- PR Did not comply to MISC and Chamber of Shipping Guide (1998)
- TR Inadequate Bridge Resource Management
- PR Use of mobile phones on the bridge

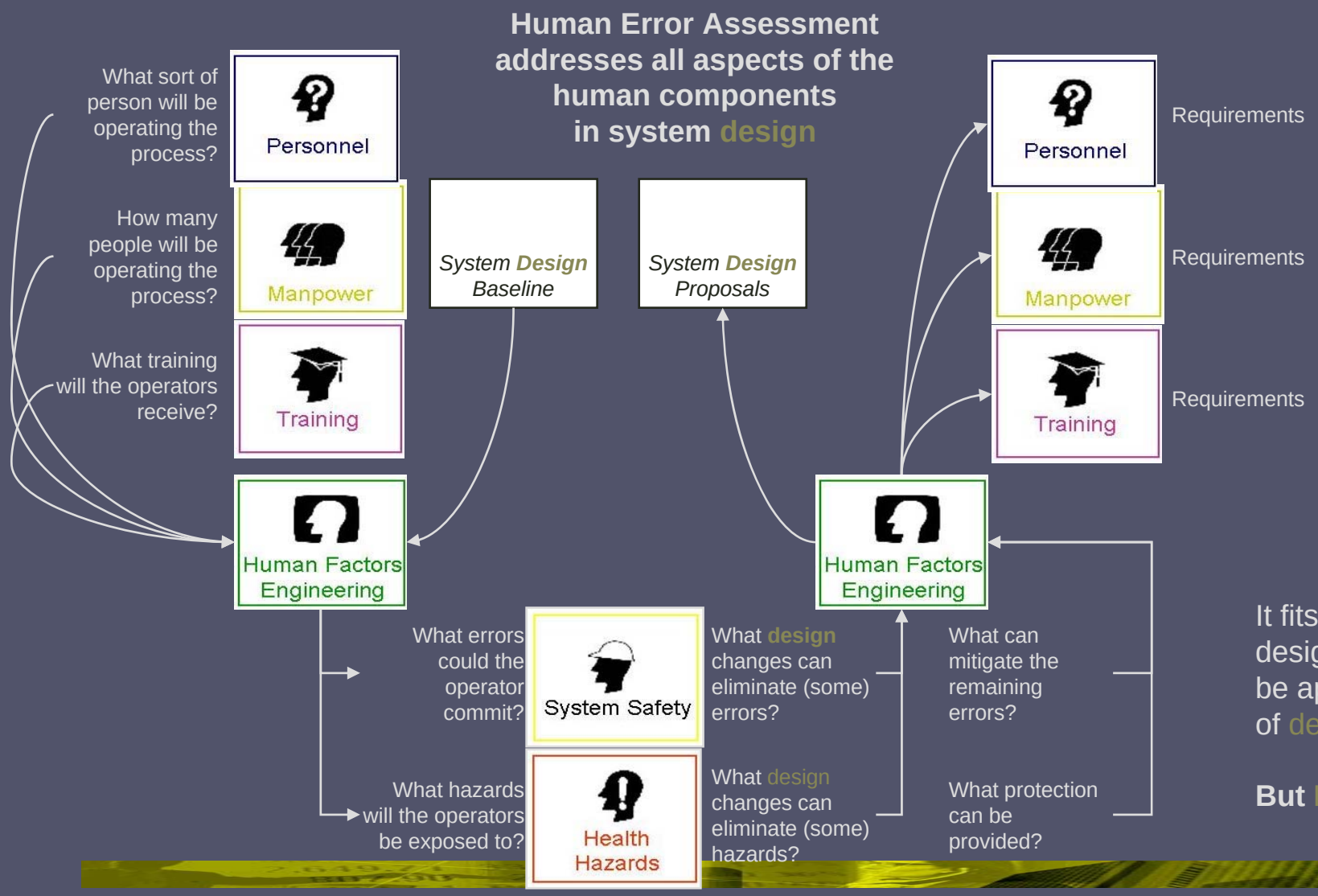


Organisational factors - Reefcentre

- DE The ‘alert’ message system, the prioritising of messages
  Design issue
- DE The extent of restricted areas south of the compulsory pilotage zone
  Design issue
- OR The role of Reefcentre and the current ship reporting system does not provide a full advisory service.



Human Error Assessment



It fits in with an iterative design process and can be applied at any stage of design maturity.

But HOW is it done?

Human Error Assessment Tools

Some Human Error Assessment techniques:

- THERP (Technique for Human Error Rate Prediction)
- Human HAZOP (A human factors version of the chemical engineering HAZOP)
- GEMS (Generic Error Modelling System)
- SHERPA (Systematic Human Error Reduction & Prediction Approach)

…but there are many others.

Conclusion

Safe Processes Need Humans

Operators need to be involved systematically with design. In this way they continue the work of the design team when they, the operators, “finish the design of the system”

Design Must Accommodate Human Performance…

It specifies safe operational limits for human work and design interfaces with other components.

Human Factors throughout the design

Principles and guidelines at conceptual stage
Design solutions at the design stage
Modelling, testing and validation throughout to support safety assurance.

Thank You

SAFETY WISE

Any Questions ?

Gerry.Gibb@safetywisesolutions.com

www.safetywisesolutions.com