An Introduction to Human Factors and System Safety


Dr. Carl Sandom, iSys Integrity Ltd

ASSC 2017
31 May 2017, Sydney, Australia.

iSys Integrity

- Safety Management
  - SMS development
- Systems Safety Engineering
  - Safety assurance
  - Safety auditor
- Safety Training:
  - Software Systems Safety
  - Human Factors for Safety
  - Safety Management Systems

iSys Integrity

- Current Contracts:
  - NATO AirC2 — Safety Advisor
  - NATO BMD — Safety Advisor
- Some Past Contracts:
  - Lockheed Martin — Safety Training
  - Westland Helicopters — Software Safety
  - EUROCONTROL — Safety Instructor
  - Watchkeeper UAV — Systems Safety

Tutorial Aim

- To provide an appreciation of human factors and ergonomics issues relating to safe systems design.

Tutorial Scope

- Human Factors and Safety
- Human (Cognitive) Limitations
- Human Systems
- Human Error
- Human Systems Exercise

Human Factors and Safety

Significant Factors?

Kegworth

Challenger

Paddington

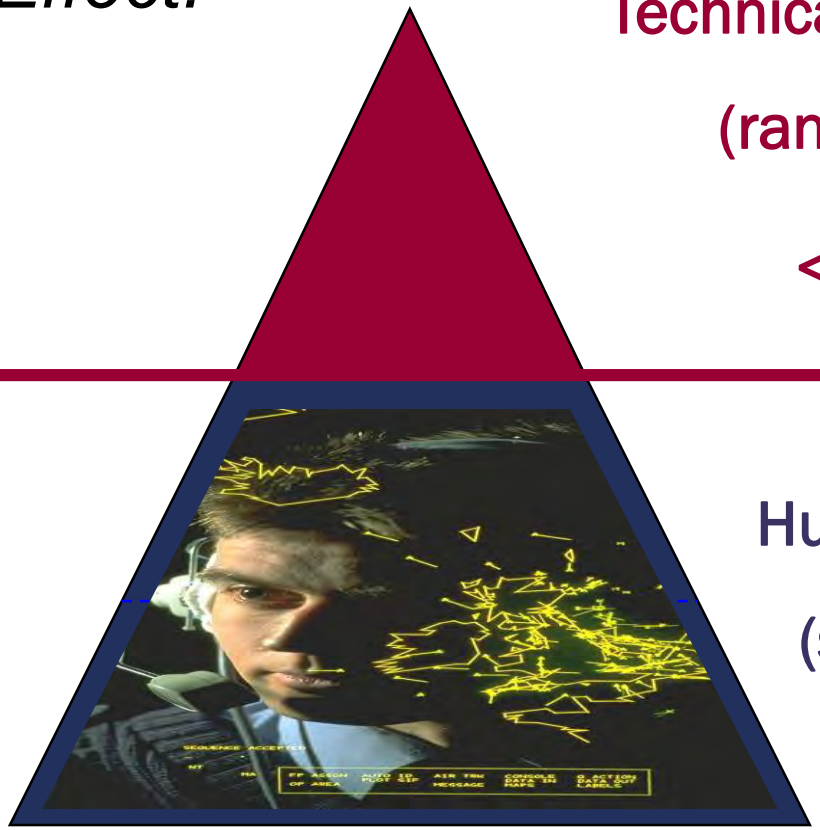
Herald of Free Enterprise

Herald of Free Enterprise

- Bow doors open because:
  - Bosun sleeping
  - First-officer not on deck
  - Captain assumed closed
- Water entered deck and ship capsized
- Public enquiry blamed Bosun, First-officer and Captain.
- “Disease of sloppiness and negligence at every level of the corporation's hierarchy”

Accident Causal Factors

The 'Iceberg' Effect:



Technical Factors

(random)

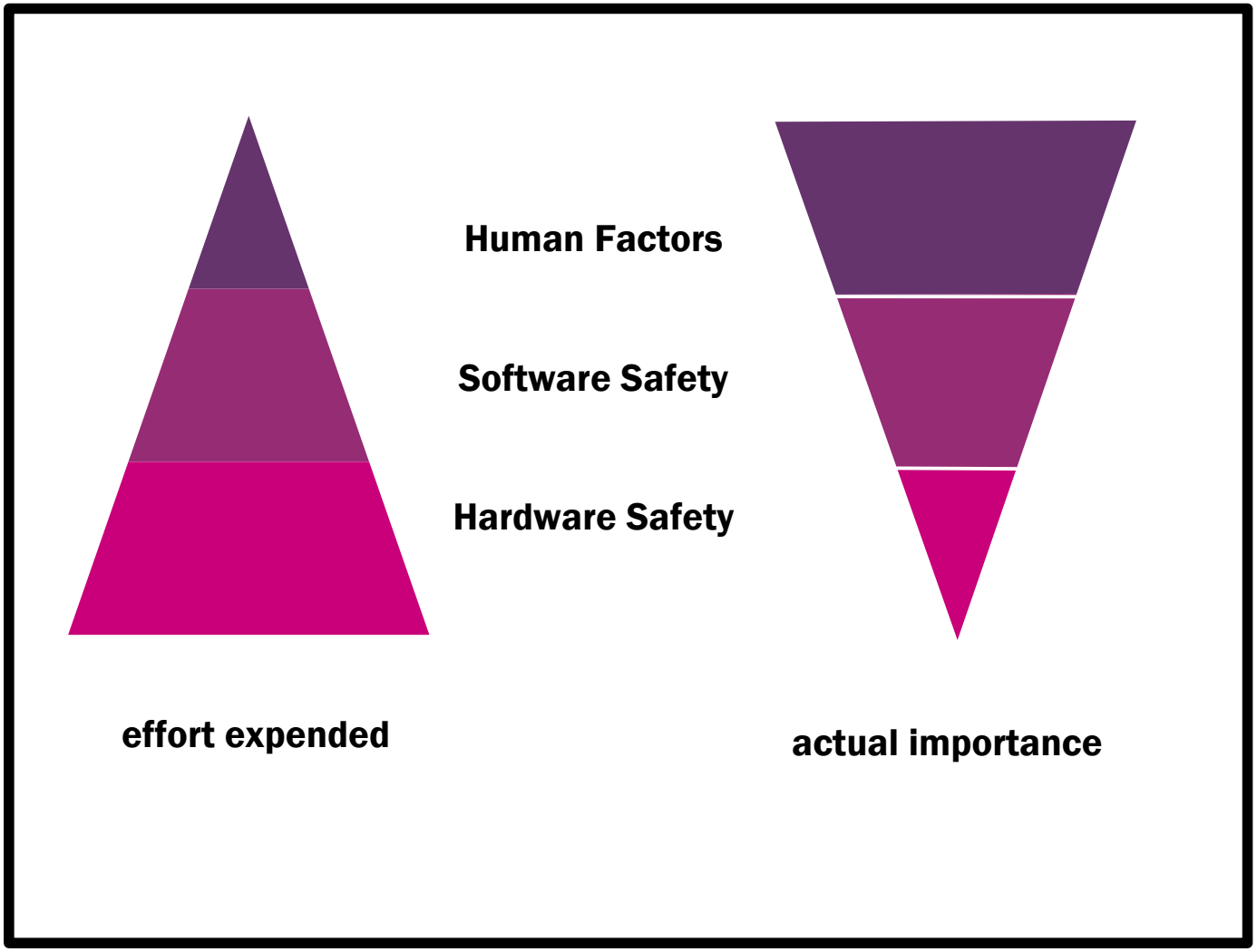
<10%

Human Factors

(systematic)

>90%

Some Disciplines Are More Equal…..



Why Ignore Human Factors?

Human Factors are hard:

- Complexity of human actions
- Accounting for context
- Quantitative nightmare!
  - Setting human safety targets
  - Demonstrate human integrity

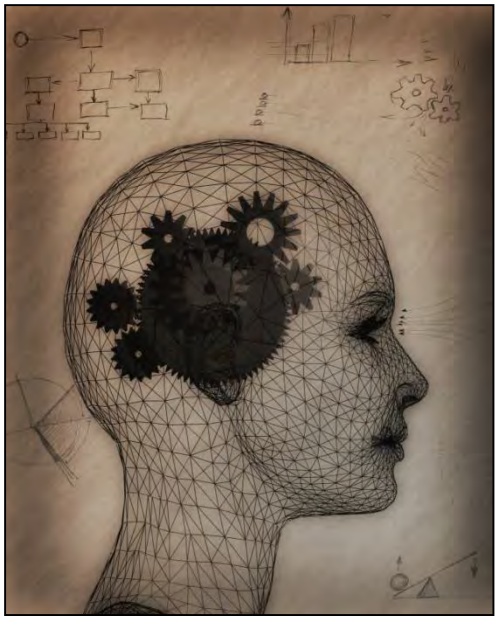
Result?

The Ostrich Approach….

HF - A Tale of Two Topics:

Anthropometric

Relatively easy



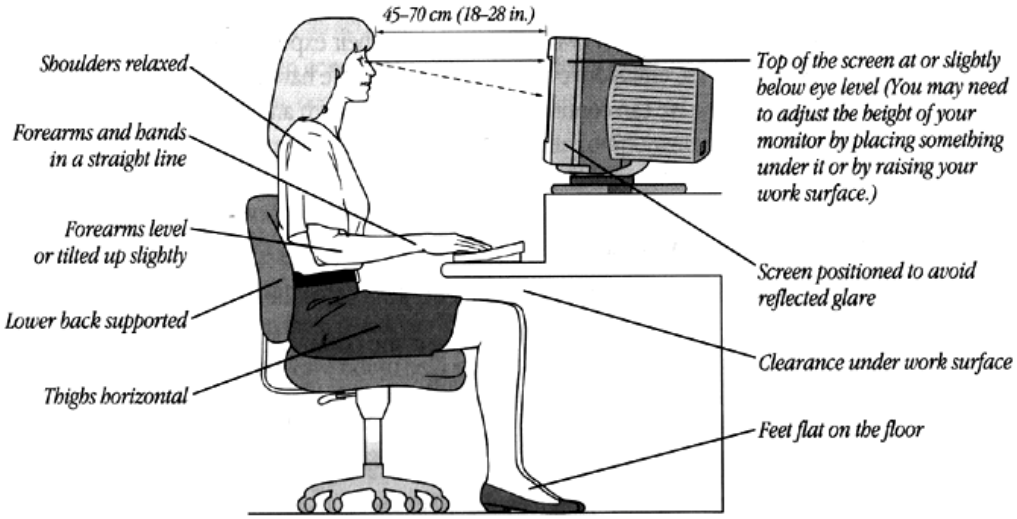
Cognitive

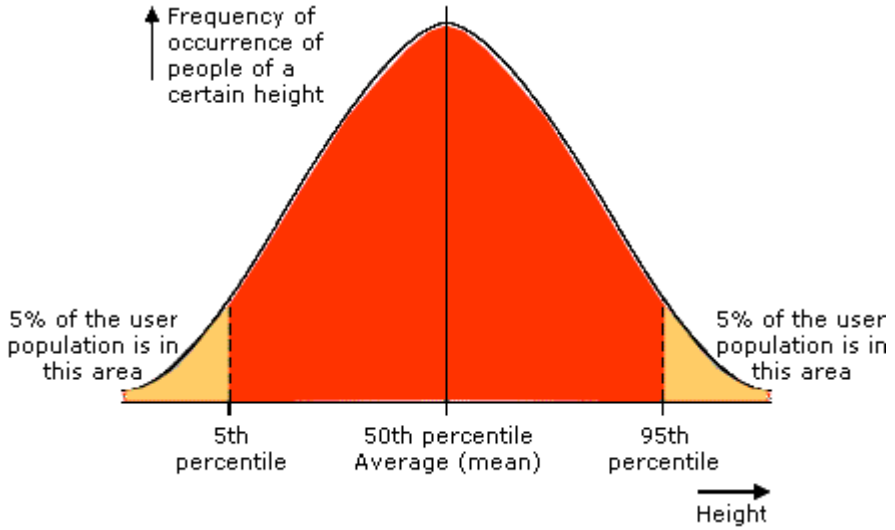
Can't be directly measured

Extrapolate from behaviour?

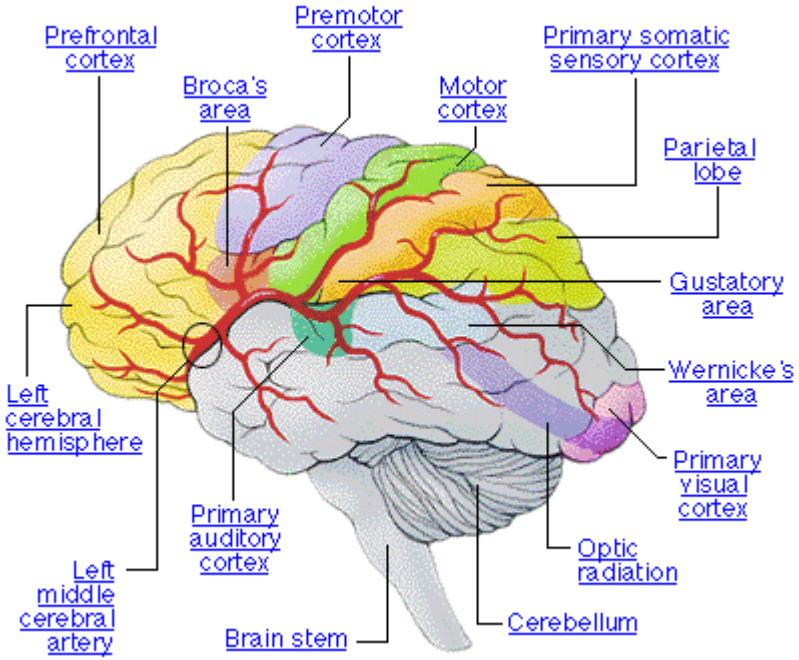
Relatively hard

Anthropmetric Factors

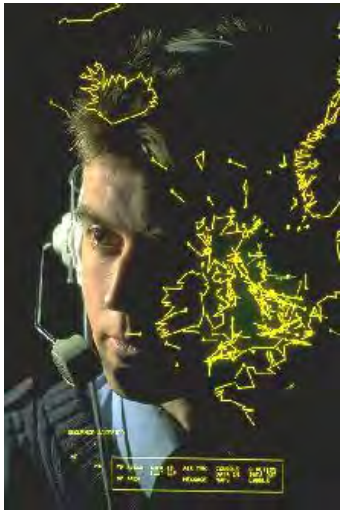




Cognitive Factors



Cognitive Factors



Situation → Through the Interactions → Awareness

Human Factors Definition

"…an interdisciplinary science concerned with influencing the design of manned systems, equipment and operational environments so as to promote safe, efficient and reliable total system performance"

(UK Defence Standard 00-25/12, 1989)

Human Factors Definition

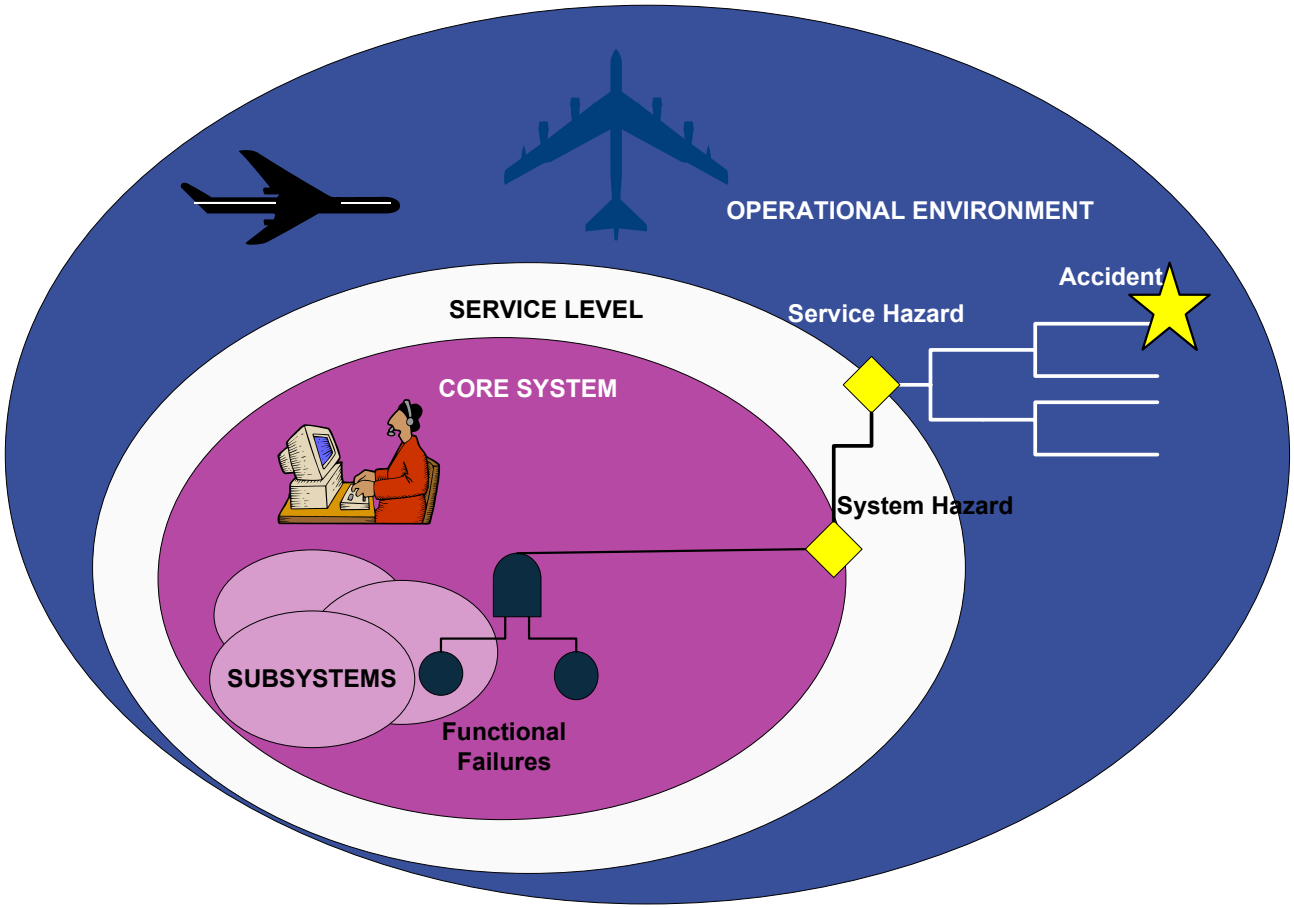
"Designing human systems within a specified context to maximize human **Physical** and **Mental** performance and minimize errors."

HF is just another Systems Engineering Discipline!

What things are assessed?

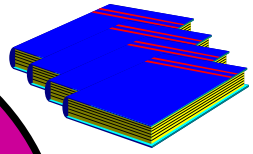
HFI DOMAINS	DESCRIPTION
Health Hazard Assessment	Identification and consideration of conditions inherent in the operation or use of a product (e.g. vibration, fumes, radiation, noise, shock, recoil etc) which can cause death, injury, illness, disability or reduce the performance of personnel.
Human Factors Engineering	The comprehensive integration of human characteristics into product design, including all aspects of workstation and workspace design including accommodation / habitability issues.
Manpower	The number of men and women required and available to operate and maintain the product / system.
Personnel	The aptitudes, experience and other human characteristics (including body size & strength) necessary to achieve optimum performance.
System Safety	Application of Human Factors expertise to minimise safety risks occurring as a result of the system being operated or functioning in a normal or abnormal manner. The objective is to minimise to as low a level as reasonably practicable the risk of injury to personnel and damage to equipment.
Training	Specification and evaluation of the optimum combination of instructional systems, education, on job training required to develop the knowledge, skills and attitudes needed by the available personnel to operate and maintain the product to the specified level of effectiveness under the full range of operating conditions.

Human Factors Scope

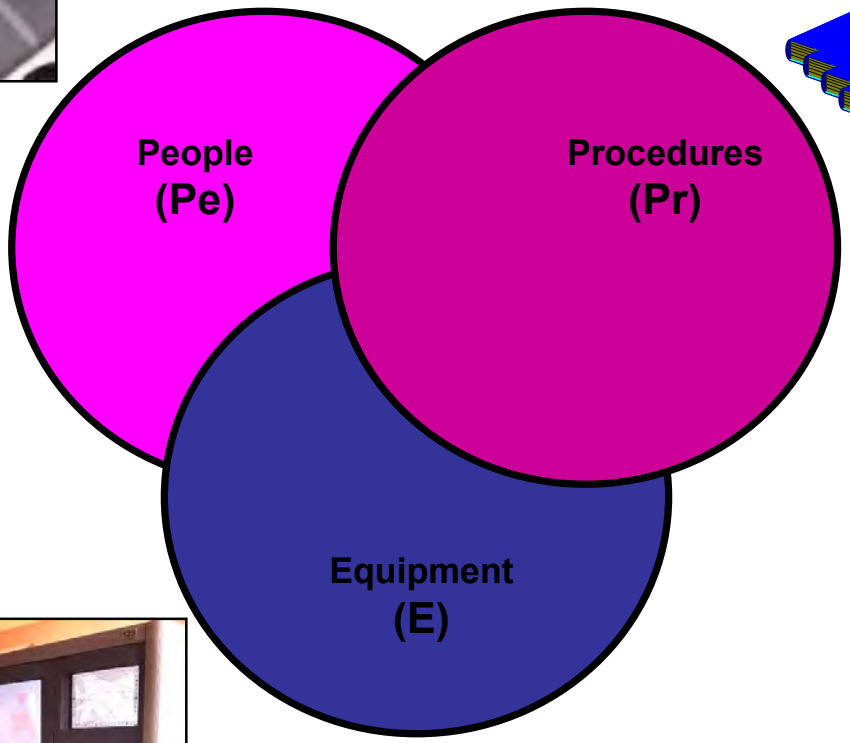


System Levels

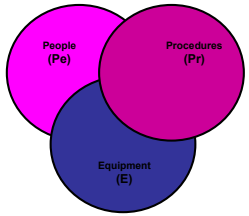
Human Factors Scope



HF Attributes

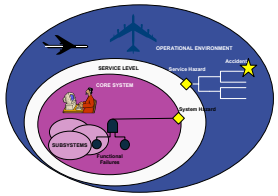


Human Factors Scope



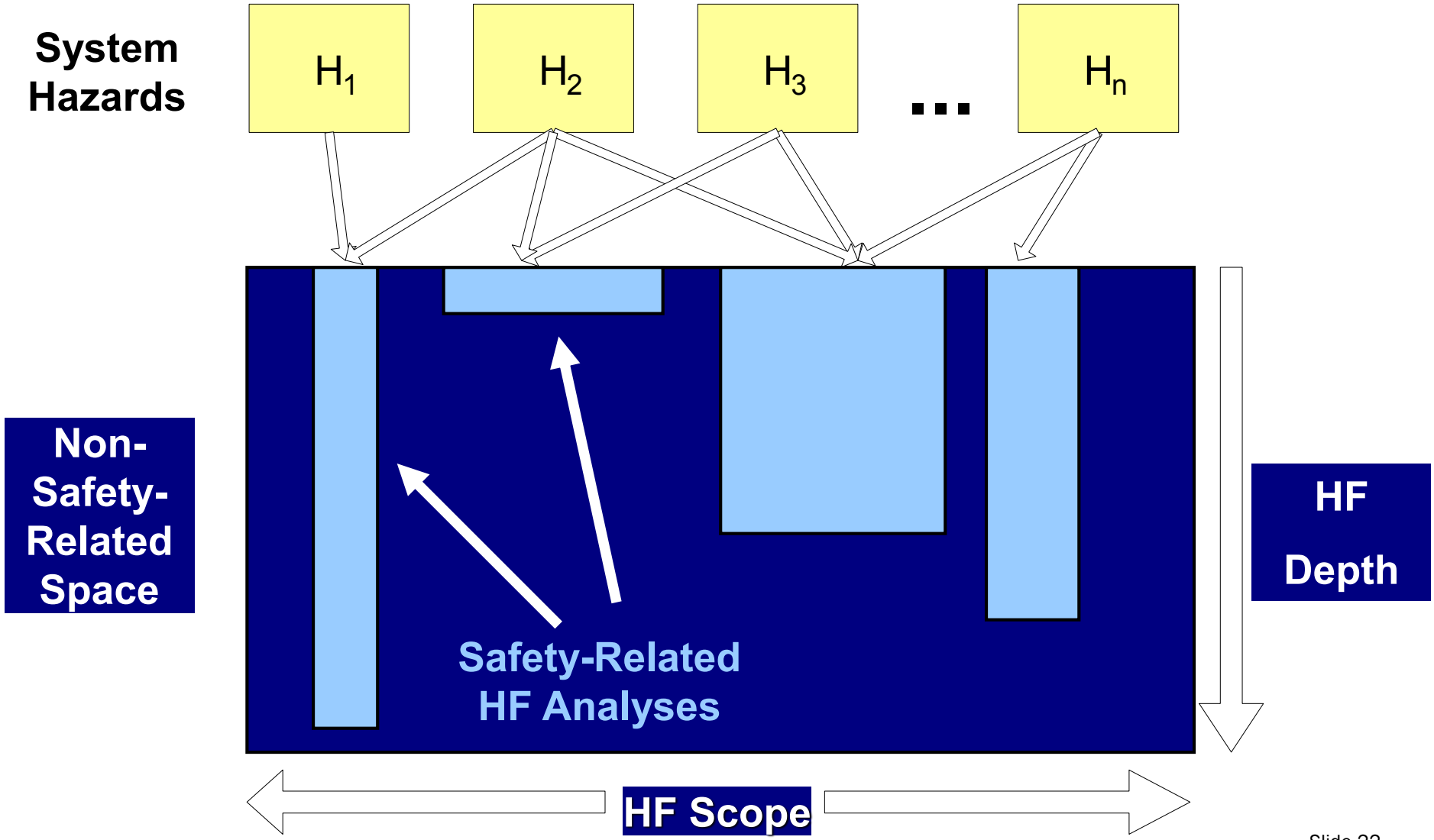
HF scope is massive….

Each **HF attribute** must be considered at every **system level** to a depth of analysis commensurate with the human integrity requirements.”



Human Factors Scope

Safety-Related Scope



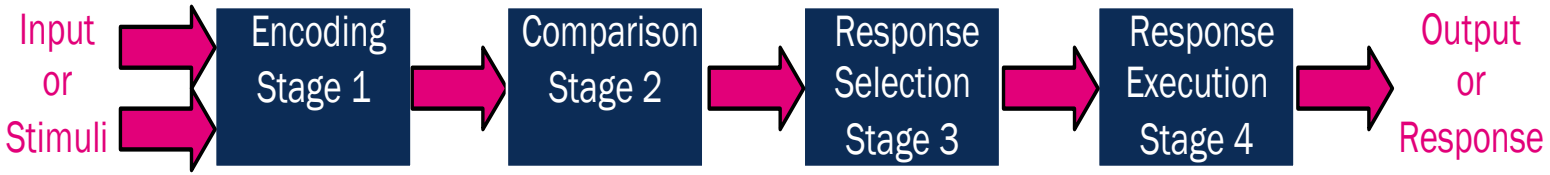
Human (Cognitive) Limitations

Human (Cognitive) Limitations

Cognitive Workload and Driver Performance?

Human (Cognitive) Limitations

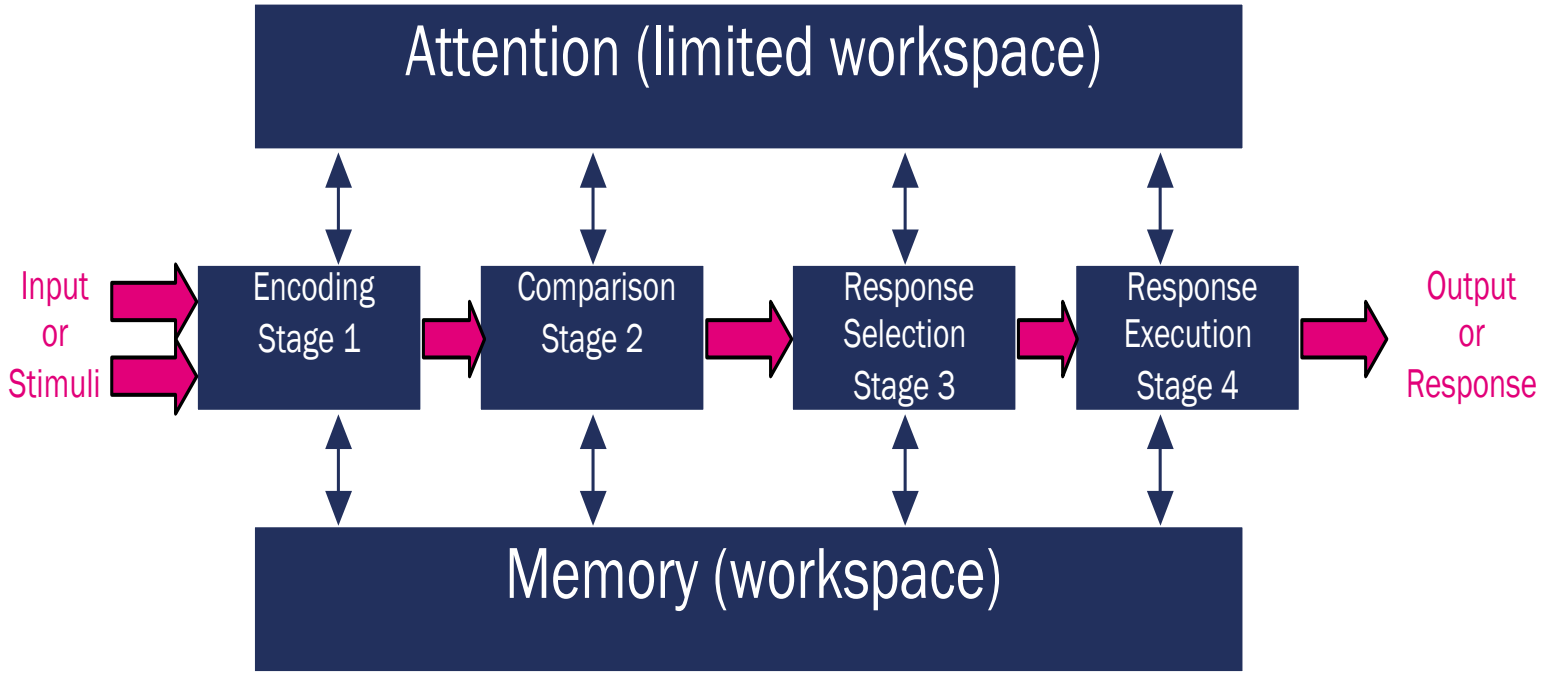
Human Information Processor (Card *et.al. 1983)*



- **Stage 1** – Encode information from environment into internal representation
- **Stage 2** – Internal representation compared with memorized representation
- **Stage 3** – decide on response to encoded stimulus
- **Stage 4** – organize response and necessary action

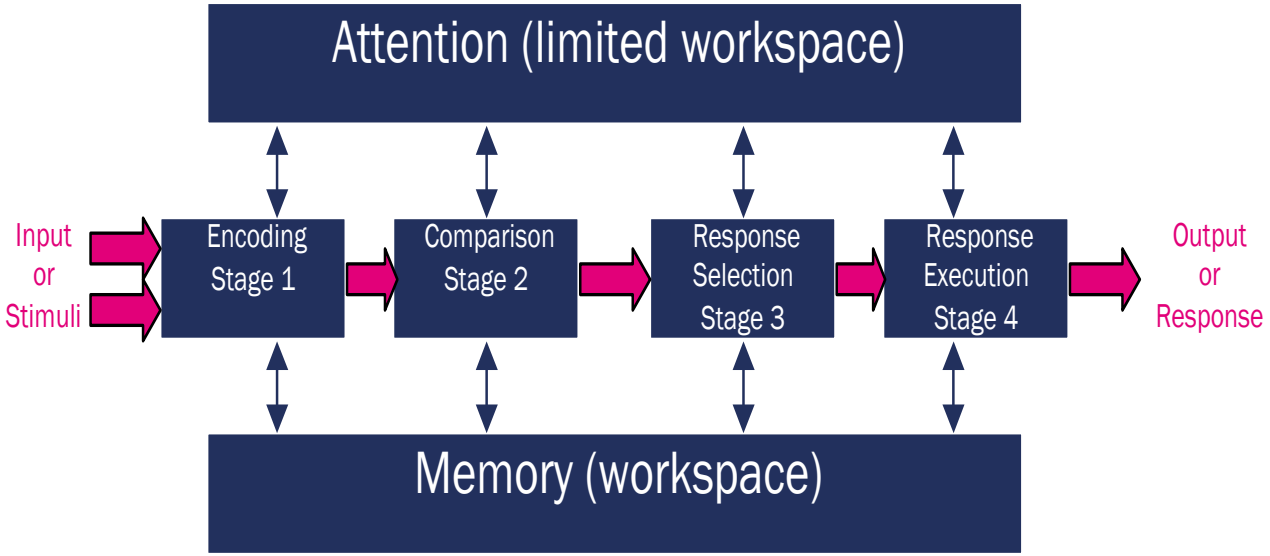
Human (Cognitive) Limitations

Human Information Processor



Human (Cognitive) Limitations

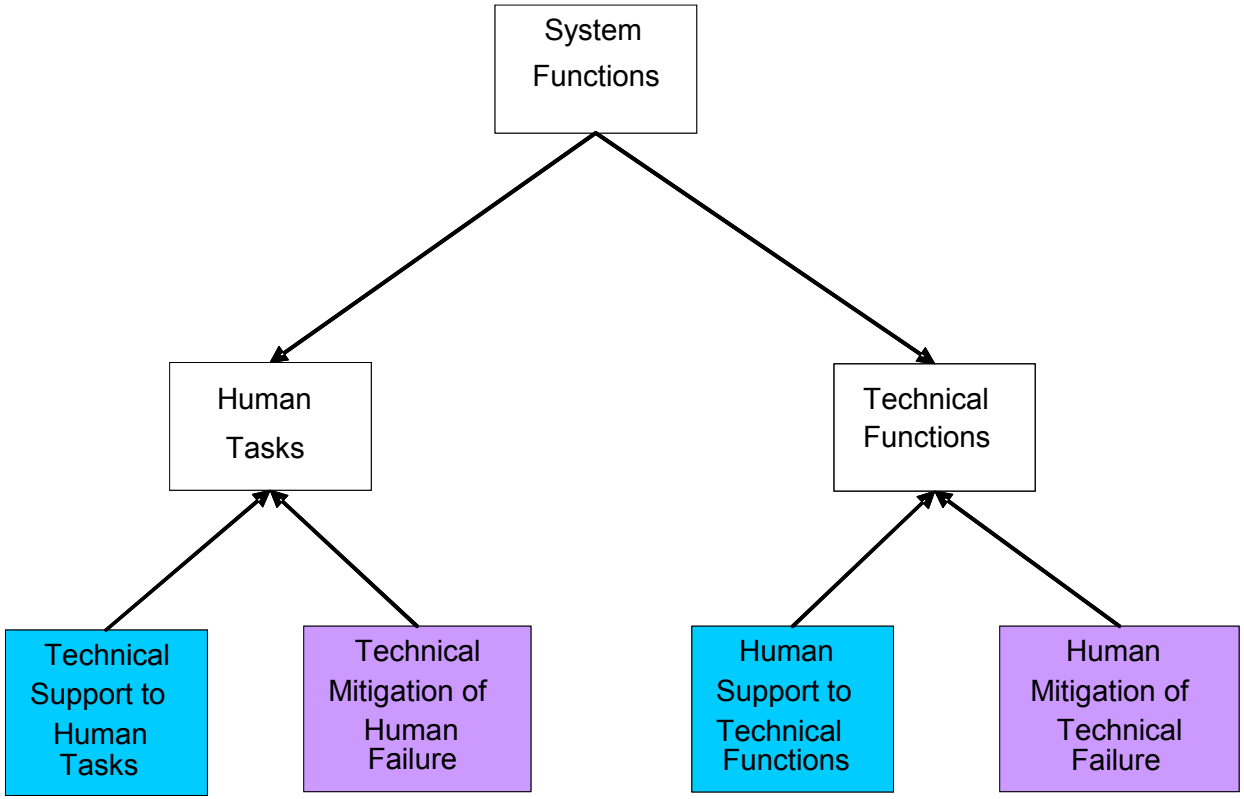
- Human Information Processor
  - Error and interaction failure occurs because of cognitive limitations
  - What are the constraints on attention and memory?
  - How can we design interaction to overcome this?



Allocation of Function

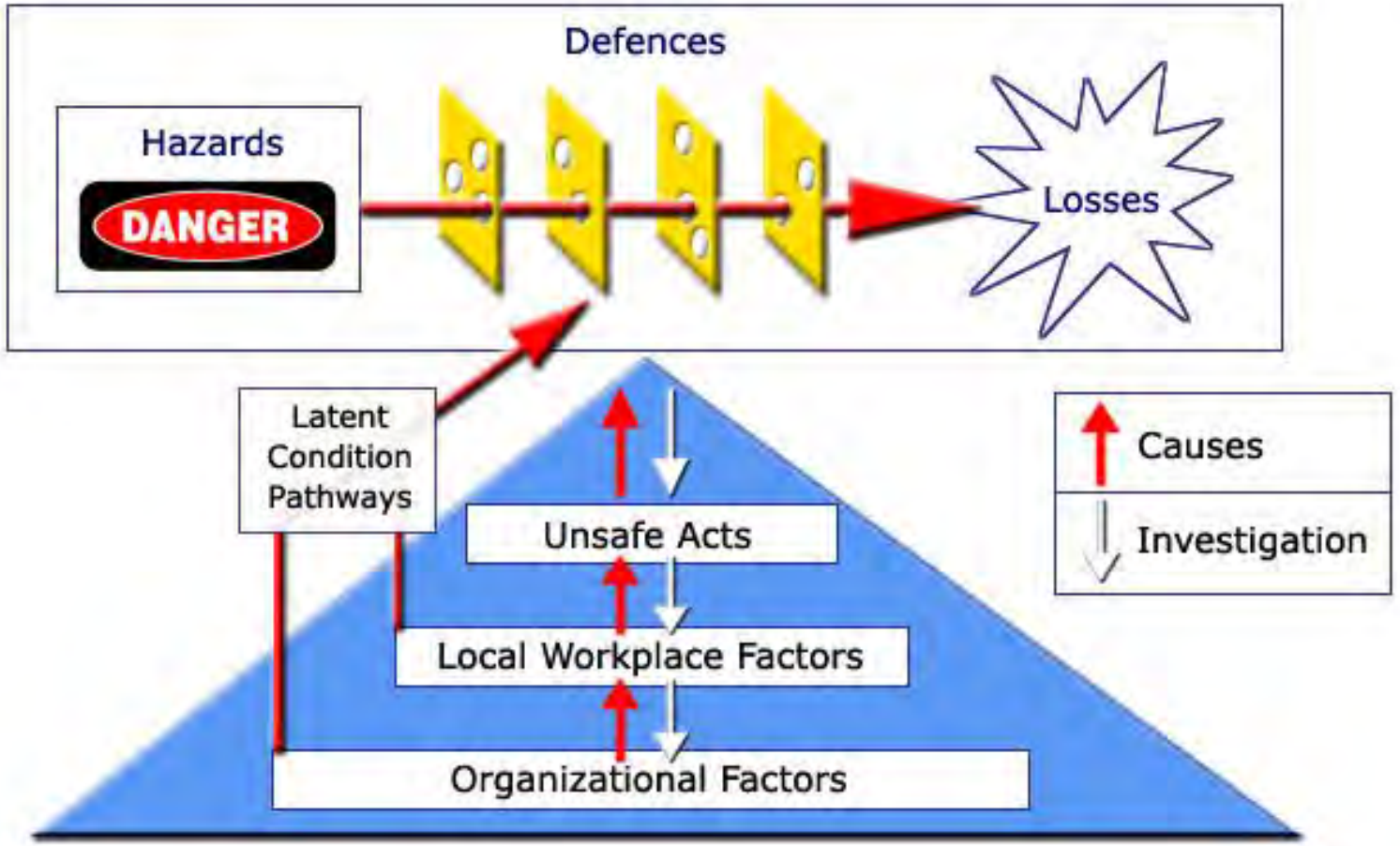
- Human tasks must consider:
  - Physical (anthropometric) constraints
  - Cognitive limitations
- Functions can allocated to:
  - Man
  - Machine
  - Man and Machine
  - Machine and Man

Safety-Related Functions



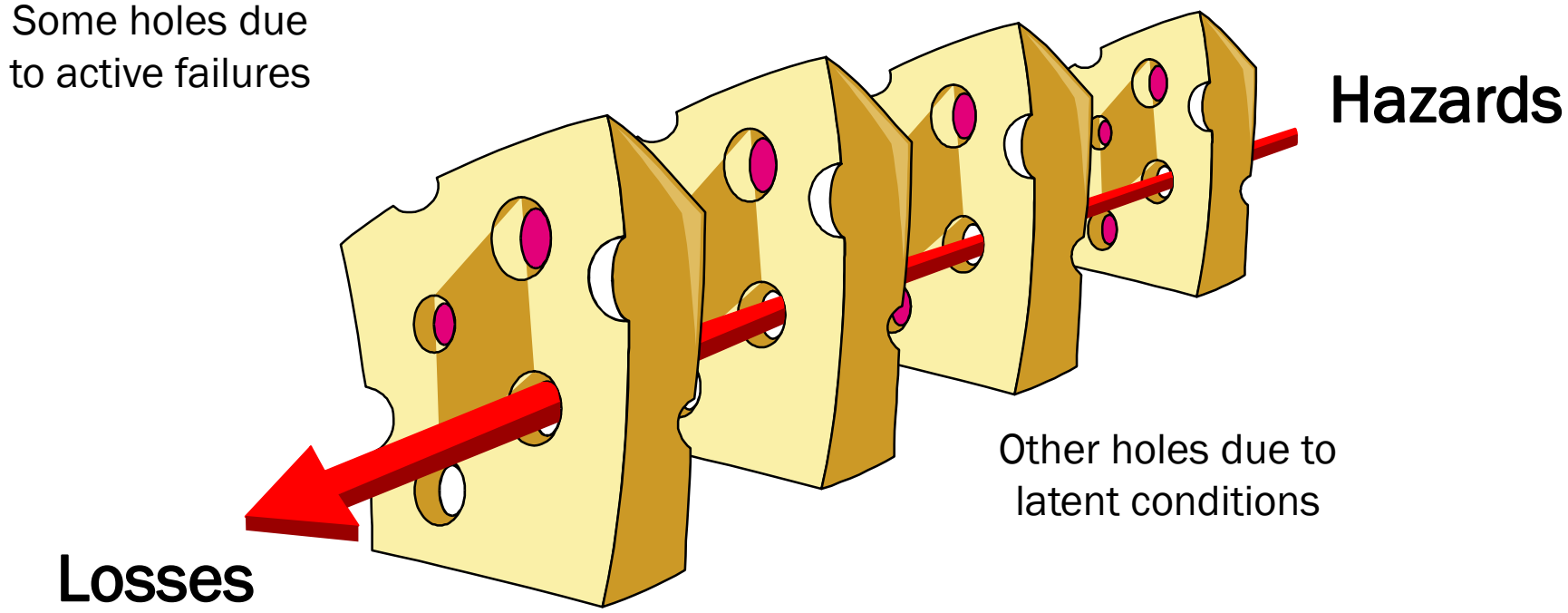
Human Systems

Accident Causation Model



(Reason, Managing the Risks of Organisational Accidents,1997)

Swiss Cheese Model



Successive layers of defences, barriers, & safeguards

Organisational Factors

Organizational Factors

- Start of Causal Chain
- Typical Org Factors:
  - Strategic decisions;
  - Org processes;
  - Corporate safety culture;
- Latent conditions initiated
- Corporate manslaughter?

Local Workplace Factors

Local Workplace Factors

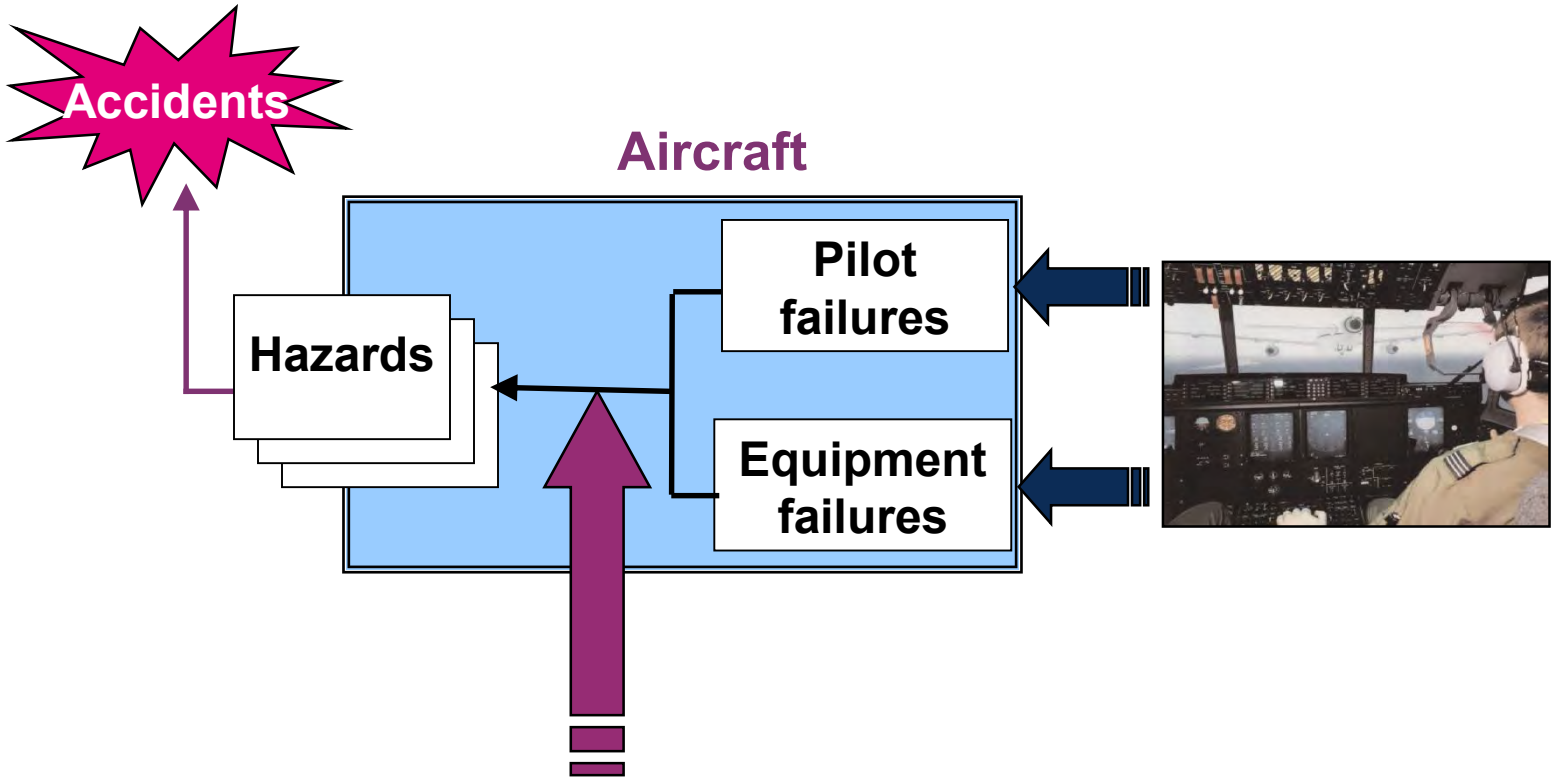
- Workplaces:
  - Control room
  - Flight deck
  - Engineering facilities
- Factors promoting unsafe acts:
  - Time pressure
  - Tools and equipment
  - Training
  - Supervision
  - Poor equipment design……..

Local Workplace Factors

Unsafe Acts

Human Input

- Human as error source
- Human as mitigator



Herald of Free Enterprise

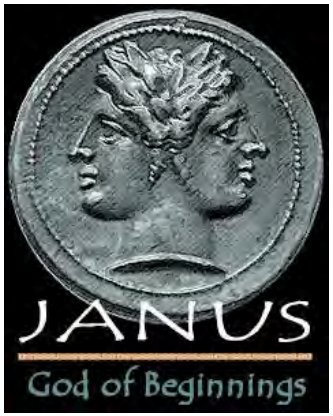
- No Technical Failures involved
- Human Factors only:
  - Unsafe Acts
  - Workplace design (indicators)
  - Organisational Safety Culture

Human Error

Two faces of the Human Factor

Human as hazard

- Slips
- Lapses
- Mistakes
- Violations



Human as hero

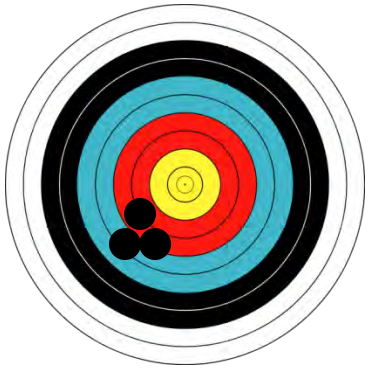
- Adjustments
- Compensations
- Recoveries
- Improvisations

Human Error Quantification

- Human failures often most prevalent
- HRA underpinned by simplistic assumptions
- Human Error Probability = Number of Errors made/Number of Error *Opportunities*

Random or Systematic

- Common misconceptions:
  - Errors are not always meaningless events
  - Errors may be random
    - The novice shooter
  - Errors may have a pattern
    - Rifle with defective sights
    - Precision v Accuracy!
  - Errors and intent are intimately linked
    - Spelling mistakes
    - Precision v Accuracy!



Human Error Source

- Behavioural account v Cognitive account
  - Behavioural => What happened?
  - Cognitive => Why it happened?
  - Implies a need to model Human Action and Human Error to form framework for analysis

Analysing Human Error

- James Reason's slips, lapses, mistakes:

Behavioural Error Type (What Happened)	Erroneous Cognitive Process (Why it Happened)
Mistakes	Planning
Lapses	Memory Storage
Slips	Execution

Human Slips

- Example slip:

  "There can be no doubt I raised the flaps instead of the U/C after take off. I had no memory at all of doing this. Why would I do this potentially dangerous thing on an aircraft with which I was completely familiar? I have no idea: no sickness, no stress, nothing dramatic personally."

  CHIRP incident database

Mistakes

- Example mistake:

  “Approximately 13 minutes into the flight the turbofan on the left engine fractured causing a series of compressor stalls in that engine. The pilots did not know what had happened, the indications were excessive vibration felt throughout the airframe, noise and a smell of fire in the cockpit. The crew throttled back the right engine when it was the left engine that was faulty; the first officer had identified the wrong engine”.

  AAIB Kegworth accident report

Question of Intent

- Slips or mistakes?
  - "I intended to stop on the way home to buy a paper but 'woke up' to find that I had driven right past"
  - "All the signs were that interest rates would drop so we took on the mortgage"
  - "I meant to take off only my shoes but took off my socks as well"
  - "I was so busy that I failed to notice the other aircraft within the vicinity so I continued on regardless"

Errors and Cognition

- Rasmussen's Skill-Rules-Knowledge model

Performance Level	Cognitive Characteristics
Skill-Based	Automatic, unconscious, parallel activities
Rule-Based	Recognising situations and following associated procedures
Knowledge-Based	Conscious problem solving

Analysing Human Error

- Consider changing gear in a car:
  - Wait until engine ready for a change
  - Depress leftmost pedal with left foot while at same time taking right foot of rightmost pedal
  - Once leftmost pedal fully depressed work out what the new position of the gear lever should be
  - Move gear level to new position
  - Gently depress rightmost pedal with right foot while simultaneously releasing leftmost pedal with left foot until leftmost pedal fully released and engine sounds about right.

Analysing Human Error

- Skill-based behaviour disrupted when:
  - Unexpected external cues detected
  - Unexpected actions detected
  - Outcome not as planned
- Rule-based behaviour disrupted when:
  - Situation cannot be interpreted adequately
  - No appropriate procedures can be found
  - Procedures are remembered incorrectly
  - Outcome not as planned

Analysing Human Error

- Generic Error Modelling System (GEMS)

Performance Level	Behavioural Error Type
Skill-Based	Slips and Lapses
Rule-Based	Rule-Based Mistakes
Knowledge Based	Knowledge-Based Mistakes

(from James Reason, Human Error, 1990)

Analysing Human Error

- Rule-based mistakes
  - Information presented is underspecified
  - Familiar but wrong procedures are used
  - Procedures are misremembered or combined

Analysing Human Error

- Knowledge-based mistakes
  - **Availability bias:** recently presented information, information currently visible or emotive information given undue weight in decision making
  - **Confirmation bias:** People interpret ambiguous scenes to reach an explanatory model. They then seek confirmation and disregard discomforting information.
  - **Selectivity:** Problem solver's attention directed to psychologically salient aspects of a problem in preference to logically important aspects

Analyzing Human Error

Is opening door: Skill, Rule or Knowledge based?

GEMS Design Example

Flight Deck Crew Immediate Actions

GEMS Design Example

- Flight Deck Crew Immediate Actions:
  - Assess emergency:
    - Consider Vibration & Smoke
    - Check Flight Instruments & Warnings
    - Refer ac checklists
  - Take emergency action:
    - Disengage Auto-throttle
    - Throttle Back No. 2 Engine
  - Review emergency:
    - Reconsider Vibration & Smoke
    - Recheck Flight Instruments & Warnings
    - Review ac checklists

GEMS Design Example

Task	Description	GEMS Error Type (Skill-Based Slip, Rule-Based Mistake, Knowledge-Based Mistake)	System Design Mitigation
1.1	Consider vibration and smoke	Knowledge	Training
1.2	Check flight instruments and warnings	Knowledge	•Vibration Gauge trigger CWP Alert •Auto-throttle indication
1.3	Refer ac checklists	Rule	Vibration & smoke action
2.1	Disengage auto-throttle	Skill	
2.2	Throttle back engine No. 2	Skill	
3.1	Reconsider vibration and smoke	Knowledge	Training
3.2	Recheck flight instruments and warnings	Knowledge	•Vibration Gauge trigger CWP Alert •Auto-throttle indication
3.3	Review ac checklists	Rule	Stress post-action checks (vibration gauge etc.)

Analysing Human Error

- Summary:
  - Errors can be described at a behavioural level
  - To understand human error need to look at cognitive processes involved in human action
  - Slips,lapses and mistakes are the result of different cognitive processes
  - RB & KB Mistakes are result of erroneous Situation Awareness
  - Slips & mistakes have different implications for system design

Human Systems Exercise

Aim

- The aim of this exercise is to gain an appreciation of the important relationship between people and procedures and equipment (hardware, software, firmware) in system safety analyses

Background

- The avionics system of a new commercial airliner is to be implemented in a modular fashion, i.e. it will consist of a number of independent hardware units which can be replaced quickly and easily for maintenance or after failure.
- The units will be physically identical, and fit in a common rack, but each will be pre-loaded with a particular system (such as radar, navigation, etc.) in firmware (i.e. in ROM).
- Each rack will include a module known as the Configuration Management Unit (CMU), which will provide a number of "housekeeping" functions. These include:
  - Recording basic operational parameters, such as flight hours
  - Storing the *master configuration list,* which contains information about all the modules currently fitted in the rack
  - Monitoring communications between modules in the rack, and on the external buses linking the racks to other equipment and systems
  - Providing the main interface between the avionics system and the Ground-crew Data Panel (GDP)
- The GDP is a portable computer used by the ground crew to download recorded data from the CMU, to initiate test routines, and to upload new configuration information after modules have been changed. The GDP is also capable of exchanging data with the Main Maintenance Computer (MMC) used by the aircraft operator, which holds details of the complete maintenance history of every aircraft.
- Some functions of the CMU have already been classified as safety-critical after a Preliminary Hazard Analysis; these include the **built-in test facilities** and **data down-loading facilities**.

Module Change Procedure (1)

- To exchange a system module, a maintenance engineer must perform the following actions:
  1. Identify the unit to be replaced
  2. Use configuration information held on the MMC to select an appropriate replacement unit. It is important that the correct module is fitted, as some combinations of modules will not operate correctly together.
  3. Obtain a replacement module from engineering stores
  4. Exchange the units
  5. Enter details of the new unit (type, revision, ID etc.) into his GDP and upload them to the CMU, which updates the master configuration list
- After changing the module, the engineer should check that the system is correctly recognising the new module, and it is the one expected. To do this, he should:
  6. Request a configuration check (**see slide 68**)
  7. If no errors are reported on the GDP, the replacement is OK, otherwise further tests must be carried out to determine the problem

Module Change Procedure (2)

CMU

5 & 6

GDP

MMC

1 & 4

5 & 6

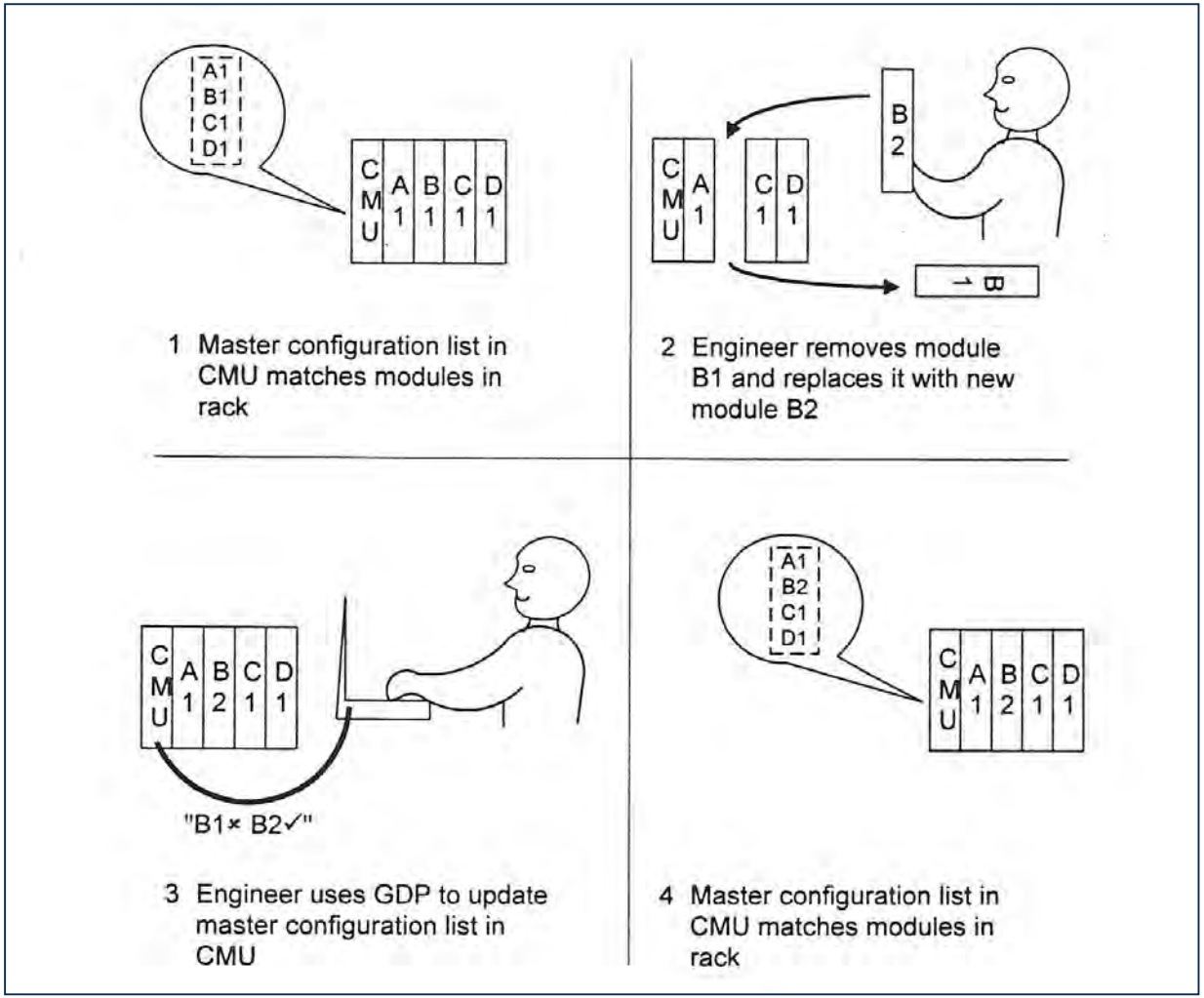
2

Engineering Stores

3

Technician

Module Change Procedure (3)



Configuration Check Software

- Configuration check software validates avionics system modules
- It can be requested by the pilot or from the GDP during maintenance
- Configuration check algorithm is:
  - Broadcast a message to all modules, instructing them to respond with identification information
  - Wait a pre-set time during which modules are expected to respond
  - Compare responses received with the expected responses (from master configuration list held in CMU)
  - If no data has been received from a module by the time-out it is assumed to be missing or failed
  - If responses received:
    - Match the expected responses do nothing
    - DO NOT match the expected responses send message to the originator identifying module whose response does not match

System Hazard Analysis (Q1 & Q2)

Consider the module change procedure and configuration check function. The most obvious hazard is if an attempt is made to fly the aircraft with a set of avionics modules which will not operate correctly together.

Q1. Can you identify any other hazardous situations which may arise?

People, procedures and equipment whose actions may impact the safety of the aircraft include:

1. Configuration check software
2. Other avionics modules
3. Ground-crew Data Panel (GDP)
4. Maintenance Engineer

Q2. What/who else do you think might contribute to a hazard and how would that contribution be made?

System Hazard Analysis (Q1 Answer)

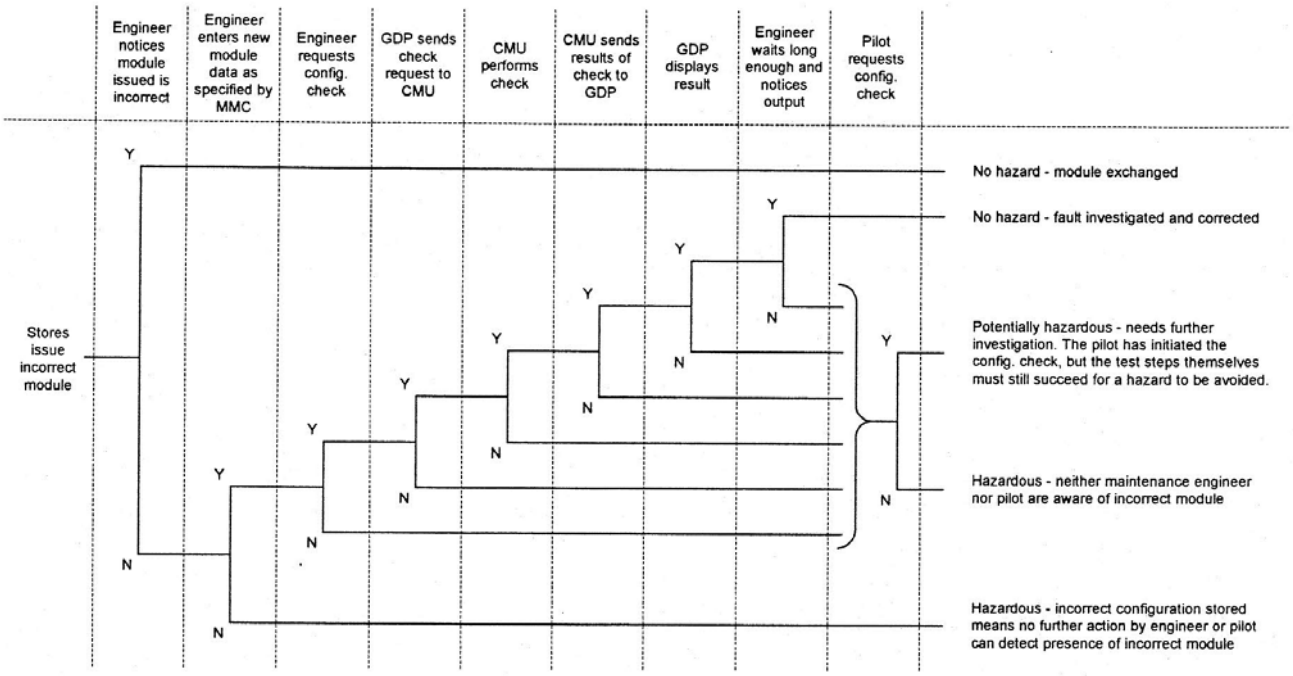
answer to be revealed

System Hazard Analysis (Q2 Answer)

answer to be revealed

Event Tree Analysis (Q3)

The event tree shown below was developed to investigate the effects of the event **"stores issue incorrect module to maintenance engineer"**.



Event Tree for the event "stores issue incorrect module to maintenance engineer"

Q3. Study the event tree and comment on it. Identify potential human errors and any possible design changes to mitigate them.

Event Tree Analysis (Q3 Answer)

answer to be revealed

Event Tree Analysis (Q4)

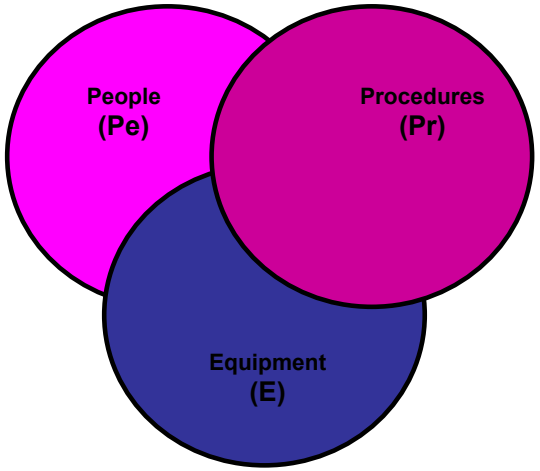
Q4. From the revised event tree, can you suggest any simple modifications to either the module change procedure or the configuration check software which you think would improve the safety of the system?

Event Tree Analysis (Q4 Answer)

answer to be revealed

Exercise Summary

- Functionality cannot be analysed alone without taking into account:
  - Equipment
    - Hardware
    - Software
  - People
  - Procedures



- Safety cannot be analysed ‘bottom-up’ or in isolation from the systems context

Tutorial Summary

Take home messages ...

- Human Factors are important for safety
  - Main accident causal factor
  - Physical (Anthropometrics)
  - Mental (Cognitive)
- Human Systems
  - People, procedures and equipment
- Human Errors not inevitable
  - Design to mitigate
  - People also provide mitigation!

Any Questions?

carl@isys-integrity.com www.isys-integrity.com