Slips or mistakes, human factors or human actors

Michael Harrison
Newcastle University, UK

Software reliability vs. hardware reliability

- Hardware failures: ageing, random shocks, design failure, manufacture failure, misuse
- "software is more a reflection of the design of the system than it is a component of the system"*
- "Reliability should also be regarded as a system property"*
- Example:
  - US ATC system bought by the UK, not designed to account for Greenwich meridian, folded its map at 0.
- *Context and software assessment, Garrett & Apostolakis HESSD'98

Software failures

- Occur because of:
  - Poor design
  - Poor context, which includes
    - Inappropriate use in an application for which it was not designed
    - Context might include: plant conditions such as sensor management, working conditions, human-system interface, availability of procedures, time available for action
  - Key to assessing risk associated with a particular piece of software is to identify which situations are "incorrect" and then evaluate the probability in one of these situations
  - The error forcing context, confluence of unexpected conditions and latent software faults which result in failure

The unit of analysis?

- Focus of human factors
  - Physical device
  - Human cognition
- Focus on action?
  - The opportunity for error
  - The characteristics of the interaction
  - The potential for recovery
- Focus on activity?
  - Often action is implicit, triggered by some change of context and the error comes later

Where does human factors fit?

- Architectural design
  - function allocation
  - job design/crew complement
  - human capabilities analysis
- Detailed Design
  - task/procedure design
  - dialogue design
  - interface design and evaluation
  - human error and reliability analysis

How to express the human context

- Defining the task environment.
- Defining scenarios, narratives in which the people are part of the system. The narrative describes the context in which the tasks are carried out.
- Expressing user constraints rather than prescribing precise user behaviours.

The problem of automation

- Move from thinking human or machine to allocate functions amongst the human and machine roles
- So that:
  - A coherent set of roles are produced
  - Does not interfere with the person's ability but supports the performance of the role
  - Creates an experience that contributes to safety
  - There are acceptable levels of technical risk satisfying functional constraints

When automation breaks

- Disruptive to unconscious behaviour:
  - unexpected external cues and actions are detected
  - outcome is not as planned
- Disruptive to rule based behaviour:
  - Situation cannot be interpreted adequately
  - No appropriate procedures can be found for the situation
  - procedures are misremembered
  - outcome is not as planned
- Technology can be brittle

The Narita incident

- From an internal airline report on an in-flight pylon/wing fire incident in which “there was no indication of fire presented to the crew when a fire actually existed”.

"...numerous EICAS messages began to appear, indicating a deteriorating mechanical condition of the aircraft. The first was OVHT ENG 1 NAC, closely followed by BLEED DUCT LEAK L, ENG 1 OIL PRESSURE, FLAPS PRIMARY, FMC L, STARTER CUTOUT 1 and others. [In total] the crew received and had to sort out 42 EICAS messages, 12 caution/warning indications, repeated stick shaker activation and abnormal speed reference information. An electronic system 'nightmare’”.

resist

Newcastle University

Human error analysis (chronology)

- Observable errors
  - Omissions, commissions, …
    expertise of the team to interpret whether worth investigating
- What causes the error? What are the mitigating factors?
  - Cognitive factors
  - Design factors
  - Interaction factors
- Would it be a good thing to eliminate human error? We learn from our mistakes.

Causes of human error?

- Slips and lapses

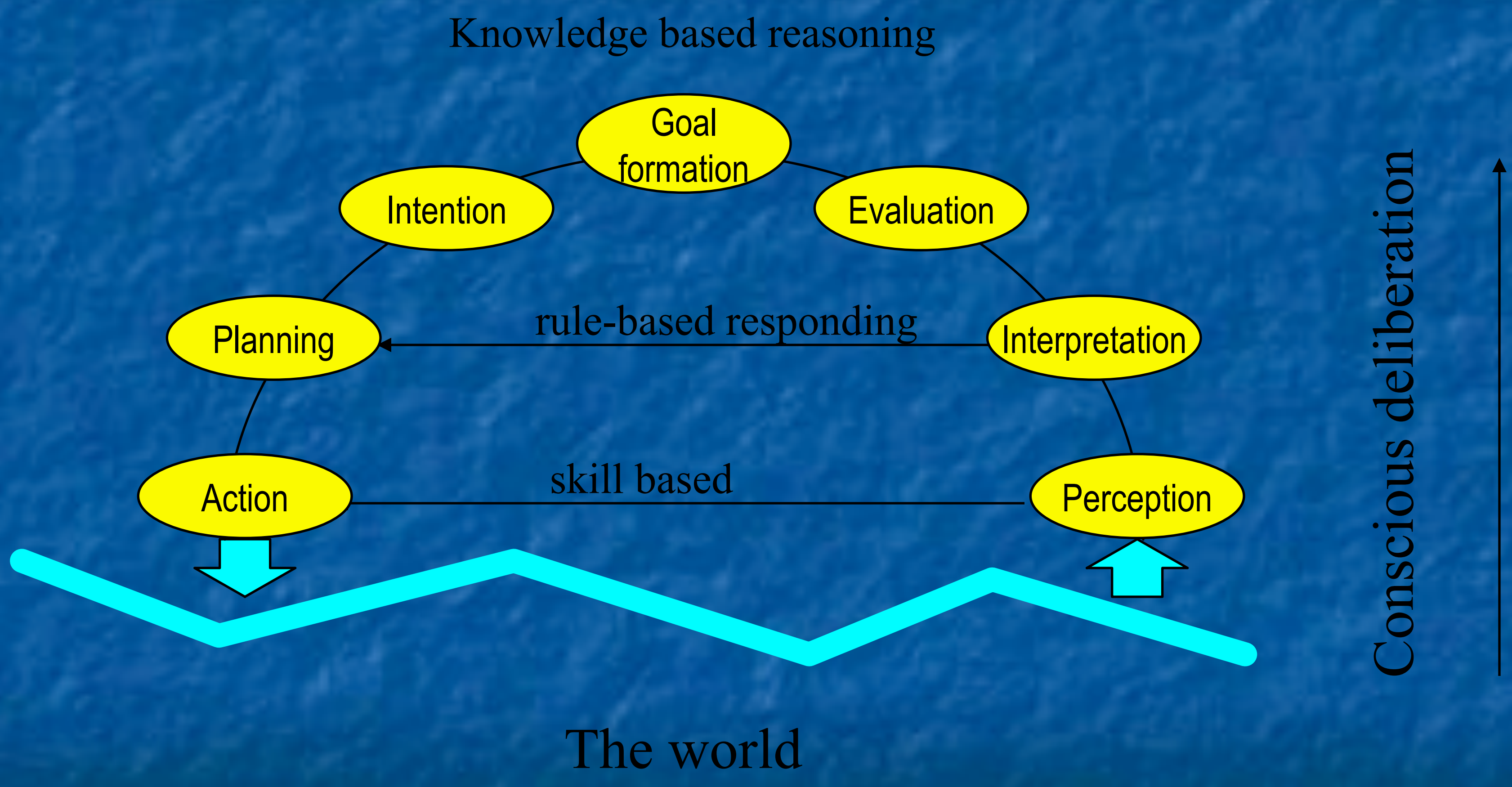
  action that occurs is not what was intended

  involves failure of execution/storage.

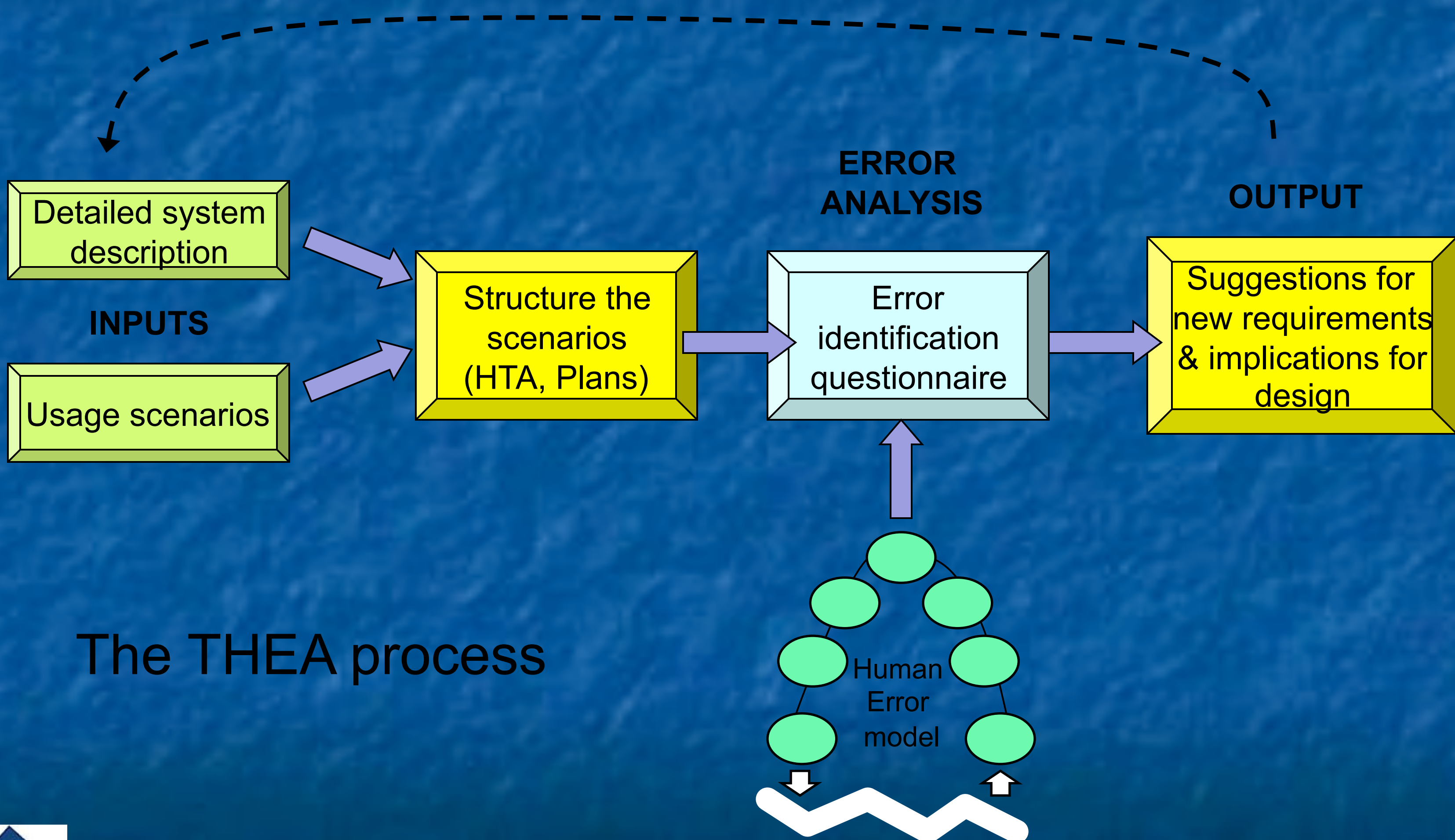
- Mistakes

  Action that occurs was as intended but did not succeed in meeting goal.

Human action is not always deliberate and plan based



Identifying design issues



The THEA process

Focus on action

- Deals with mitigation and implicitly recovery

THEA Question	Causal Issues	Consequences
G1 (Triggers, Task initiation)	Some goals are poorly triggered, especially if there are several goals with only a single trigger on the display e.g. “Engine 4 shutdown” or “Engine 3 cleanup”	It is also possible that “Engine 4 shutdown” or “Engine 3 cleanup” might be omitted or delayed
G3 (Goal conflicts)	Goals to increase power and Engine 3 shutdown are in conflict (although inevitable here)	Resolving the conflict satisfactorily requires negotiation between pilot and co-pilot. The time required for this may lead to a non-optimal (too late) decision

Error analysis

Action	Action Type	Human Error
L FIRE	Alert acknowledge	- not read (pilot unaware of warning - misread (pilot aware of warning but mistakes it for another
Both Throttles to MAX RHT	Control operation	- incorrect op not possible (cannot confuse throttles for other control) - inadvertent op (at any time) - non operation (pilot misses step in written procedure)

Human Error	*Applicable design f eatures*
Not reading L FIRE	- Highlight (flashing red caption head-down) - Audio (attention and voice message) - Attention getters (flashing amber head-up) - Size (easily readable) - Position (handed correctly on warning panel)
Misreading L FIRE	- Labelling (consistent, unambiguous) - Colour (red caption) - Graphics (n/a) - Size (easily readable) - Tradition (similar to existing warning system)

Assign HEPs from lookup tables:

1×10^{-4} per action

1×10^{-3} per action

Resist

Newcastle University

But action is within an organisation

- Typical to analyse actions in the context of a fault tree
- But factors shape performance of the action
  - Performance shaping factors
  - Failed action may be seen in the context of a cascade of failures, human and otherwise
    - The cascade may increase workload and therefore the likelihood of error
  - Activity within systems may be goal oriented, but may be triggered or implicit
    - Different types of error associated with these different modes

Dimensions of analysis techniques

Surface analysis: use team to provide interpretation	Explicit model of causes applied by individual or team
Qualitative techniques for identifying error	Quantification techniques
Analytic action based techniques	Holistic analyses

Traditionally quantification:

- Assigns numbers to events identified in the human error identification phase
- Issues
  - Separable actions unique causes?
  - No interaction between events?
  - Aggregation of parts?
  - Failures usually result from a cascade of actions. Probability assessments view each action in isolation.

Approaches to quantification

- Based on database of human error probabilities
- Based on comparison: data about existing system
- Based on simulation

Methods based on database

- Human Error Probabilities (HEPs) derived from military and nuclear industries
- Represent probability estimates of general (failure) characteristics of human performance
- Modified by actual situations, Performance Shaping Factors (PSFs) devised. Represent specific context or task characteristics, and serve to:
  - Compensate for lack of appropriate empirical data and lack of context

Quantification techniques

- HEART: a human performance model-based technique utilising some standard probabilities
  - A data-based method for assessing and reducing human error to improve operational performance.

  J.C. Williams (1988) IEEE Fourth Conference on Human Factors and Power Plants (pp.436-450)
- SLIM: a utility-based technique using team based judgements
- THERP: earliest method

HEART

Generic Task (F): **Shift system to new state using procedures:** **0.003**

Task 1: **Operator removes lifeboat tarpaulin and safety anchoring bolts**

Error Producing Conditions	Total HEART effect **(E)**	Assessed proportion **(P)** (Σ ≠ 1)	Assessed Effect = ((E-1)*P)+1
2. Shortage of time	11.00	0.10	2.00
13. Poor feedback	4.00	0.10	1.30
17. No independent check	3.00	0.20	1.40
27. Physical capabilities exceeded	1.40	0.05	1.02
29. Emotional stress	1.30	0.40	1.12
33. Hostile environment	1.15	0.50	1.08
35. Disruption of sleep	1.10	0.10	1.01

Assessed probability of failure = 0.003 * 2.00 * 1.30 * 1.40 * 1.02 * 1.12 * 1.08 * 1.01 = **0.014**

Task 2: Stow bolts in pre-designated central location; **Assessed probability of failure = 0.378**

Task 3: Check bolts are stowed prior to pressing detonator button; **Assessed probability of failure = 0.397**

resist

Newcastle University

SLIM: Success Likelihood Index Method

- not based on tables of human performance, based on
  - Calibration against similar situations.
  - meeting involving expert panel (for example, two operators with “minimum 10 years experience”; one human factors analyst; one reliability analyst);
  - calculates “success likelihood index” from performance shaping factors ratings
  - converts SLIs into probabilities

Newcastle University

CREAM claims to be more holistic

- Measures organisational factors using subjective assessment of descriptors
- Provides overall assessment of control mode
- Assigns values depending on control mode

CREAM calculate control mode

- scrambled control
  - choice of next action is unpredictable or haphazard, no thinking
- opportunistic control
  - choice of next action determined by salient features of current context rather than stable intentions or goals
- tactical control
  - performance based on planning hence more or less follows a known procedure or rule
- strategic control
  - considers global context, thus using a wider time horizon.

CREAM works at organisational level

Table 3: CPCs and performance reliability.

CPC name	Level / descriptors	Expected effect on performance reliability
Adequacy of organisation	Very efficient	Improved
	Efficient	Not significant
	Inefficient	Reduced
	Deficient	Reduced
Working conditions	Advantageous	Improved
	Compatible	Not significant
	Incompatible	Reduced
Adequacy of MMI and operational support	Supportive	Improved
	Adequate	Not significant
	Tolerable	Not significant
	Inappropriate	Reduced
Availability of procedures / plans	Appropriate	Improved
	Acceptable	Not significant
	Inappropriate	Reduced
Number of simultaneous goals	Fewer than capacity	Not significant
	Matching current capacity	Not significant
	More than capacity	Reduced
Available time	Adequate	Improved
	Temporarily inadequate	Not significant
	Continuously inadequate	Reduced
Time of day (circadian rhythm)	Day-time (adjusted)	Not significant
	Night-time (unadjusted)	Reduced
Adequacy of training and experience	Adequate, high experience.	Improved
	Adequate, limited experience.	Not significant
	Inadequate.	Reduced
Crew collaboration quality	Very efficient	Improved
	Efficient	Not significant
	Inefficient	Not significant
	Deficient	Reduced

Calculating screening probabilities

- Is it worth continuing the analysis or is there nothing to worry about?

Control Mode	**Reliability interval (probability of action failure)**
Strategic	0.5 x 10**-5 < p < 1.0 x 10**-2
Tactical	1.0 x 10**-3 < p < 1.0 x 10**-1
Opportunistic	1.0 x 10**-2 < p < 0.5
Scrambled	1.0 x 10**-1 < p < 1

For those aspects that are problematic

- what are the cognitive demands of the task?
  - Transform the event sequence into cognitive activities
  - Consider the cognitive functions that are required by the cognitive activities
  - Perform error analysis on cognitive functions
  - Identify possible errors

Quantification through simulation

- MIDAS
- Use of modelling and simulation system with virtual representation of humans to determine situations that may challenge human performance in space systems
- Stochastic modelling to predict
- We are exploring gross behaviours of groupware and smart environments

Stochastic models in groupware and smart environments

- M. Massink, D. Latella, M.H. ter Beek, M. Harrison, and M. Loreti (2008) A Fluid Flow Approach to Usability Analysis of Multi-user Systems. In Engineering Interactive Systems 2008 - Proceedings of the 2nd Conference on Human-Centered Software Engineering (HCSE'08), Pisa, Italy (P. Forbrig and F. Paternò, eds.), Lecture Notes in Computer Science 5247, Springer-Verlag, Berlin, 166–180

Resilience engineering

- Presupposes that human errors and human failures are likely to occur
- More useful effort should be placed on the means to anticipate disturbances and the ability to remove and restore the system to the original state
- Complementary with existing techniques
- Assertion that the most serious incidents cannot be anticipated in the system design
- Systems are dynamic and complex

Resilience

- What is a resilient system from a human point of view?
- Ability of an individual or team to:
  - Detect drift towards unsafe operating boundaries
  - Accept and respond to unexpected situations and to mitigate any consequences
  - Continue imagining and worrying about safety implications of system behaviour
- System is flexible and absorbs the effects, the concern is to brittleness when the system cannot cope

How to achieve resilience

- Management responsibilities
  - Encouragement of anticipation
- Identifying key system variables and checking whether they are close to the edge
- Climate of openness
- Encourage mutual respect and recognition regardless of states

Challenges

- Methods systematic but highly sensitive to individual differences
- Lack of plausible data, how can data be used to predict behaviour in new contexts
- Resilience agenda important, these are complex systems, but not leading to methods and techniques, currently an empty critique of practice
- Resilience approach focussed on qualitative not quantitative issues
- Validation, see Halden study for example

Bibliography

- Context and software assessment Garrett & Apostolakis HESSD'98
- Hollnagel, E. (1998) Cognitive Reliability and Error Analysis Method. Elsevier.
- Swain, A. and Guttman, H. (1983) Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications. Technical Report NUREG/CR-1278 SAND80-0200 RX, AN, U.S. Nuclear Regulatory Commission. Final Report.
- Resilience engineering: concepts and principles, ed Hollnagel, Woods, Leveson. Ashgate 2007
- An Introduction to Complexity in Social Science Bernard Pavard & Julie Dugdale http://www.irit.fr/COSI/training/complexity-tutorial/complexity-tutorial.htm