Analytical Usability Evaluation for Safety-Critical Systems

Safety Critical Systems

Systems which can cause loss of life, and/or damage to the environment, infrastructure and equipment.

- Medical Systems
- Chemical plants
- Space crafts
- Airplanes
- Trains
- Air traffic-control

How important is human factors?

- Nuclear power plant significant events 1983/1984, USA (180 events):
  human performance problems 51%
- Petrochemical industry 1986-1991 (450 incidents):
  human error 55%
- Chemical process industry 100 largest losses 1955-1984: operational error $600 million
- Boeing: "*Human error has been documented as a primary contributor to more than 70 percent of commercial airplane hull-loss accidents*"

Human error???

- “The pilot pushed the wrong button”
- “The cleaner unplugged the life support” (myth)
- “The driver missed a red signal”

Yes, human error,

but not of the user!

Hazard Analysis

- Think about the most terrible things that can happen
- Determine what could cause them
- Determine how you can prevent them (or reduce their effect)

Hazard Analysis: Template

Hazard	Causes	Effects	Hazard Category	Actions

Hazard Category

The "Hazard Category" says something about the nature of the hazard

- For example, a numbered scheme from the US Dept. of Energy:
  - Hazard Category 1 - potential for significant off-site consequences
  - Hazard Category 2 - potential for significant on-site consequences
  - Hazard Category 3 - potential for significant but localized consequences

Another example:

- Physical
- Chemical
- Biological

Example: Alarm button

Hazard	Causes	Effects	Hazard Category	Actions

Example: Alarm button

Hazard	Causes	Effects	Hazard Category	Actions
User falls and no alarm	Battery dead Alarm falls away	Death, Injury	Severe	Beep for battery low Add cord

Hazard and Operability Analysis (HAZOP)

- Bottom-up, designed for chemical plants
- Focus on process parameters
- **Primary Keywords** which focus attention upon a particular aspect of the design intent or an associated process condition or parameter.
- **Secondary Keywords** which, *when combined with a primary keyword*, suggest possible deviations.
- Deviation =

  Primary keyword + Secondary keyword

Primary keywords

- These reflect both the process design intent and operational aspects of the plant being studied.
- Depend on the plant being studied
- Examples: Flow,Temperature, Pressure, Level, Separate (settle, filter, centrifuge), Composition, React, Mix, Reduce (grind, crush, etc.) Absorb, Corrode, Erode

Secondary keywords

- No - The design intent does not occur (e.g. Flow/No), or the operational aspect is not achievable (Isolate/No)
- Less - A quantitative decrease in the design intent occurs (e.g. Pressure/Less)
- More - A quantitative increase in the design intent occurs (e.g. Temperature/More)
- Reverse - The opposite of the design intent occurs (e.g. Flow/Reverse)
- Also - The design intent is completely fulfilled, but some other related activity also occurs (e.g. Flow/Also)
- Other - The activity occurs, but not in the way intended
- Fluctuation - The design intent is achieved only part of the time
- Early, Late - A step is started at the wrong time or done out of sequence

Doing a HAZOP analysis

- For each part of the plant,
  - For each pair of primary and secondary keywords which makes sense,
    - Is there a possible cause for this deviation?
    - If so, record all possible causes, with relevant consequences, safeguards and actions to be done

HAZOP: Template

Deviation	Causes	Detection	Consequences	Actions

Example: Alarm Button

Deviation	Causes	Detection	Consequences	Actions

Example: Alarm Button

Deviation	Causes	Detection	Consequences	Actions
No alarm	Empty battery	None	Potential death, injury	Beep at low battery
False alarm	Button pressed by accident	None	Effort for alarm people, cost	Produce noise when pressed; Cancel
No response	Wrong address	When arrive at wrong place	Potential death, injury	Check details regularly

Predictive Human Error Analysis (PHEA)

- Attempt at a human focussed form of HAZOP.
- Predict where errors will occur on basis a list of error types.

PHEA: Error Classification

- Action Errors (A)
- Checking Errors (C)
- Information Retrieval Errors (R)
- Communication Errors (I)
- Errors in Selection between alternatives (S)

PHEA: Example Errors

- Action:
  - too late / early
  - too fast / slow
  - omitted, too little / incomplete
  - in wrong direction
  - Right action on wrong object
- Check:
  - omitted
  - incomplete
  - Right check on wrong object
  - too late / early

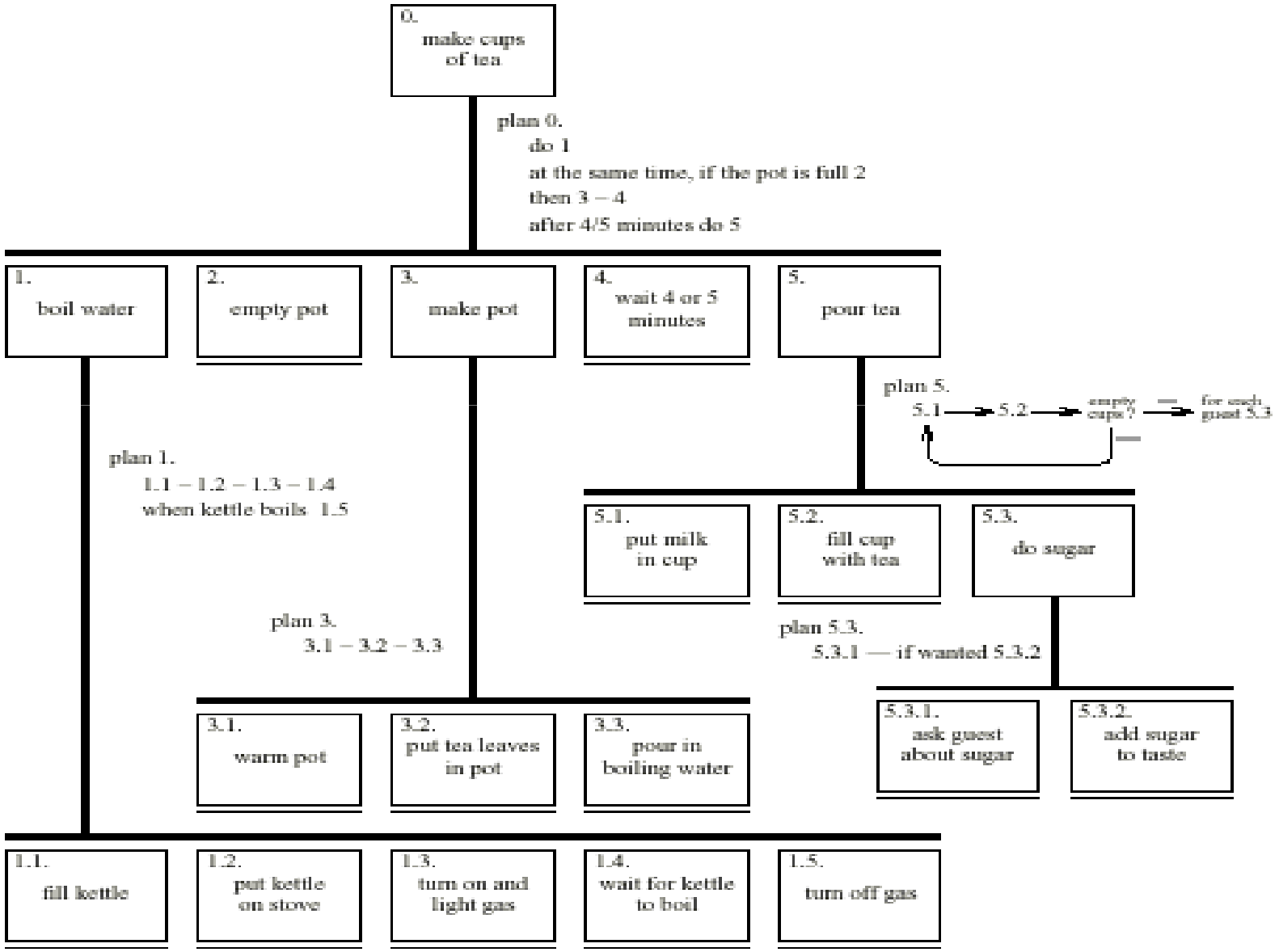
PHEA: Steps

- Decompose task into individual step using Hierarchical Task Analysis
- Use PHEA error categories to specify possible error types for each bottom level activity
- Identify possible recovery
- Specify error prevention (reduction) strategies

PHEA: Template

Task Step	Error Type	Description	Consequences	Recovery	Error Reduction

Example: Making tea - HTA



Example: Making Tea - PHEA

Task Step	Error Type	Description	Consequences	Recovery	Error Reduction
1.1 Fill kettle	Action: omitted	Forgets to put water in kettle and puts on stove	Kettle overheats	Switch heat off at max temp.	Warn when no water Warn when temp. too high
	Action: too much	Fills kettle completely	Kettle overflows when water boils	Switch heat off when water overflows	Show maximum water level Warn when too much water

PHEA: How effective is it? (1)

- Example in water storage power station
- Errors predicted using PHEA
- Actual occurrence of errors over a five year period inferred from de-brief of inspectors
- 92% of errors predicted

PHEA: How effective is it? (2)

- 18 steps analysed by two analysts
- 60 credible errors identified
- 42 (70%) by both analysts
  - 11 differences due to different knowledge of equipment
  - 5 differences due to different interpretation of procedures
  - 2 differences due to different understanding of PHEA

Safety-Critical Systems only?

- You can apply these methods to other systems as well!
- Even when an error can not kill people, it may still be vital that it does not occur!
- Your company's revenue may depend on it!

- Risk = Probability of occurrence x
  Severity of consequence

Summary

- Safety-Critical systems are increasingly controlled by software
- A range of analytical techniques can be applied to evaluate designs for robustness
- The techniques are also applicable on other systems
- Advisable to approach systems from a holistic design perspective at the outset