TACTIC

Targeted Action for Curing Trauma Induced Coagulopathy

chi+med

making medical devices safer

Rigour, rules and regulation in safety critical interactive systems

Michael Harrison

Newcastle University and Queen Mary University London

My background

- Formal methods and interactive systems
- Focus on aviation until 2004
- More recent work related to medical systems
  - IV infusion
  - Dialysis
  - App to aid prediction of trauma induced coagulopathy

Structure of talk

- Designing autonomous systems for role
- Other criteria that relate to safety?
  - Etiquette
  - Teamwork
- Proving requirements
- Requirements for autonomous systems?

Function allocation

Autonomy and Role

- Systems are becoming more autonomous but are they safe
  - Compatible with user roles?
    - What are the roles?
  - Can they be trusted?
    - Assessing trust

Appropriate and safe use of autonomy

- Who should do what?
- Fitts’ (MABA-MABA) lists
- Levels of automation
- Relating to role / analysing function
- IDA-S technique: result of funding from [dstl] and BAE Systems
- Harrison, M., Johnson, P., and Wright, P. (2003). Relating the automation of functions in multi-agent control systems to a system engineering representation. In *Handbook of Cognitive Task Design.* Lawrence Erlbaum Associates. pp. 503-524.

IDA-S method

- Scenarios, functions and roles
- Analysis of function
  - Information, Decision, Action and Supervision
  - Assessing function in the context of scenario
  - Assessment against performance shaping factors and role

Function for allocation
(F1: Plan Route)

Function	**F1 Plan Route**
Solution	Sol6 Plot way-points
Design Solution	The navigator plots a number of way-points describing the destination and route required The electronic chart evaluates the proposed route based upon its knowledge of navigation and sailing, proposing any changes or conflicts it identifies The navigator can modify the route as required and approve the route The electronic chart then calculates the distances and bearing between the points The navigation officer supervises the entire process

IDA-S (F1: Plan Route)

	Information		Decision		Action	
Planning the response	Collect	N	Propose	N	Approve	
	Integrate	N	Evaluate	E		
	Configure	N	Modify	N		
	Initiate Response	N	Select	N		
Supervise ongoing execution	Monitor progress	C	Identify exceptions	C	Revoke Authority	C
Supervise termination	Determine output content	E	Identify completion	N	Stop process	C
Action	Execute actions	N				

- N Navigator, C navigation officer or command and control, E electronic chart

Trade offs

- Is the proposed solution technically feasible – what are the risks associated with implementing it?
- Rating different performance shaping factors
- Considerations that lead to dynamic function allocation

But there is more than function allocation

- Is allocation static or should it change due to circumstances?
- What qualities engender trust?
- Who has the initiative?
  - Collaborative interaction?

Engendering trust: issues of etiquette

- Adapting Grice’s maxims (Miller)
  - M1: Make it easy to override and correct errors
  - M2: System should be capable of being informed that it has taken a wrong step
  - M3: System should learn from mistakes
  - M4: Should communicate clearly what it is doing and why
  - M5: Should use multiple modalities and information channels redundantly
  - M6: Should not assume every user is the same and be aware of what each user knows

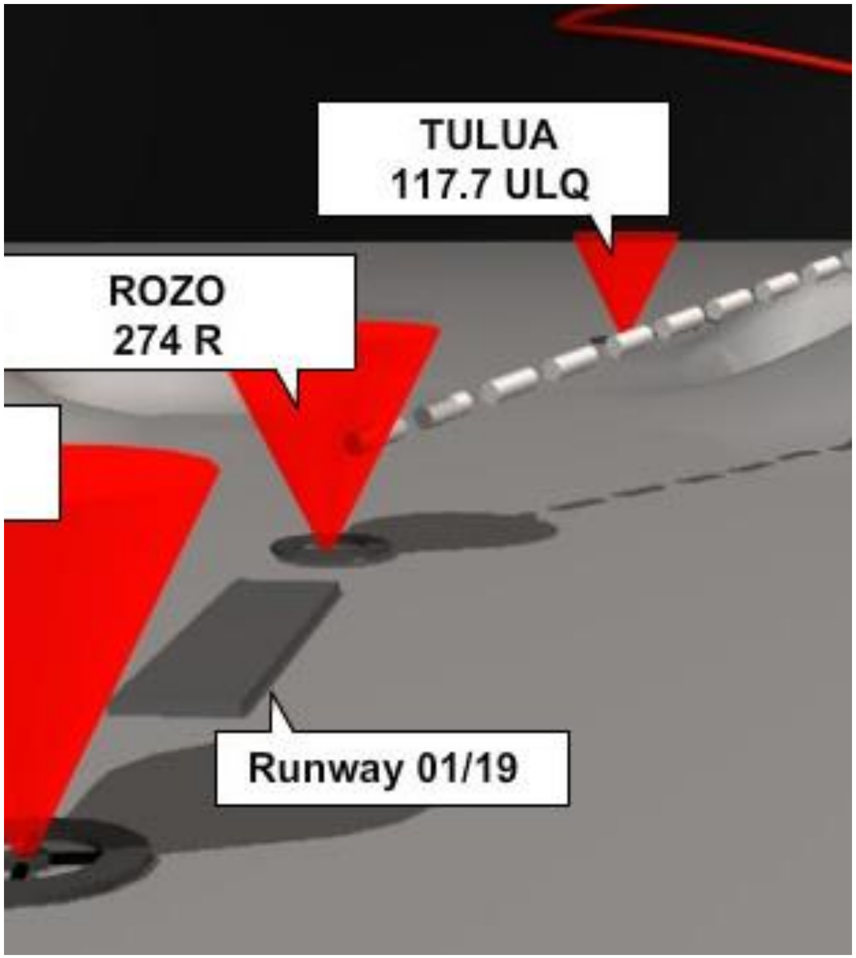
Simple stuff but …

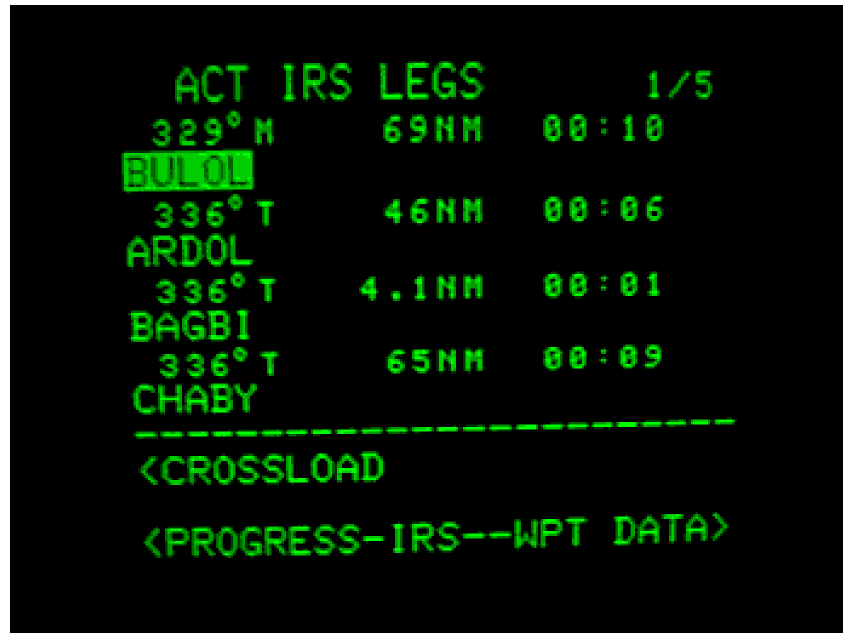
- M2: System recalculating when you know the short cut
- M3: Next time it should take the short cut
- M4: Easy review of proposed route
- M5: Speech and text interchangeable
- M6: My wife and I see the system very differently

And the consequences can be catastrophic …

- Aircraft accident at Cali, Columbia 1995 (described on the WBA web site, and Leveson, 2004)
- The minimum details:
  - Pilot asked for clearance to take a particular approach (Rozo) – Rozo is the name of a beacon
  - Pilot types R into the flight management system (should have typed ROZO)
  - R was the symbol for another beacon – the aircraft flew into mountainous terrain

R -> ROZO


TULUA
117.7 ULQ
ROZO
274 R
Runway 01/19


ACT IRS LEGS 1/5
329° M 69NM 00:10
BULOL
336° T 46NM 00:06
ARDOL
336° T 4.1NM 00:01
BAGBI
336° T 65NM 00:09
CHABY
<CROSSLOAD
<PROGRESS-IRS--WPT DATA>

How could the link between these events be explained (Leveson)?

- Crew procedure error
  - In the rush to start descent, the captain entered the waypoint without verification from the pilot
- Pilot error
  - Pilot executed a change of course without verifying its effect on the flightpath
- Approach chart and FMS inconsistencies
  - The identifier used to identify Rozo on the approach chart was R which did not match the identifier in the FMS
- FMS design deficiency
  - FMS did not provide the pilot with feedback – choosing the first identifier listed on the display was not the closest beacon with that identifier

Adaptation and mixed initiative

Automation as team player (Klein et al)

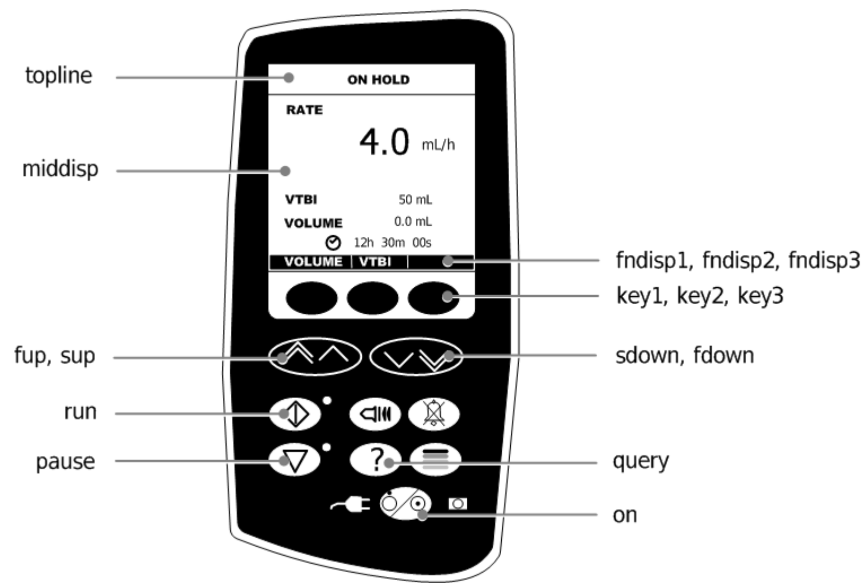
- “basic compact” fulfil the requirements of a set of common grounded agreements
- Rules? Agent must
  - Fulfil the basic compact
  - Model other participants
  - Trust other agents
  - Agents must be directable
  - Make relevant signals of status
  - Be able to negotiate goals

But how do we prove that automation can be trusted?

Example: IV infusion

Infusion pump

- IV infusion – commonly used in intensive care and oncology
- Focus on modes and number entry
- Proving safety requirements



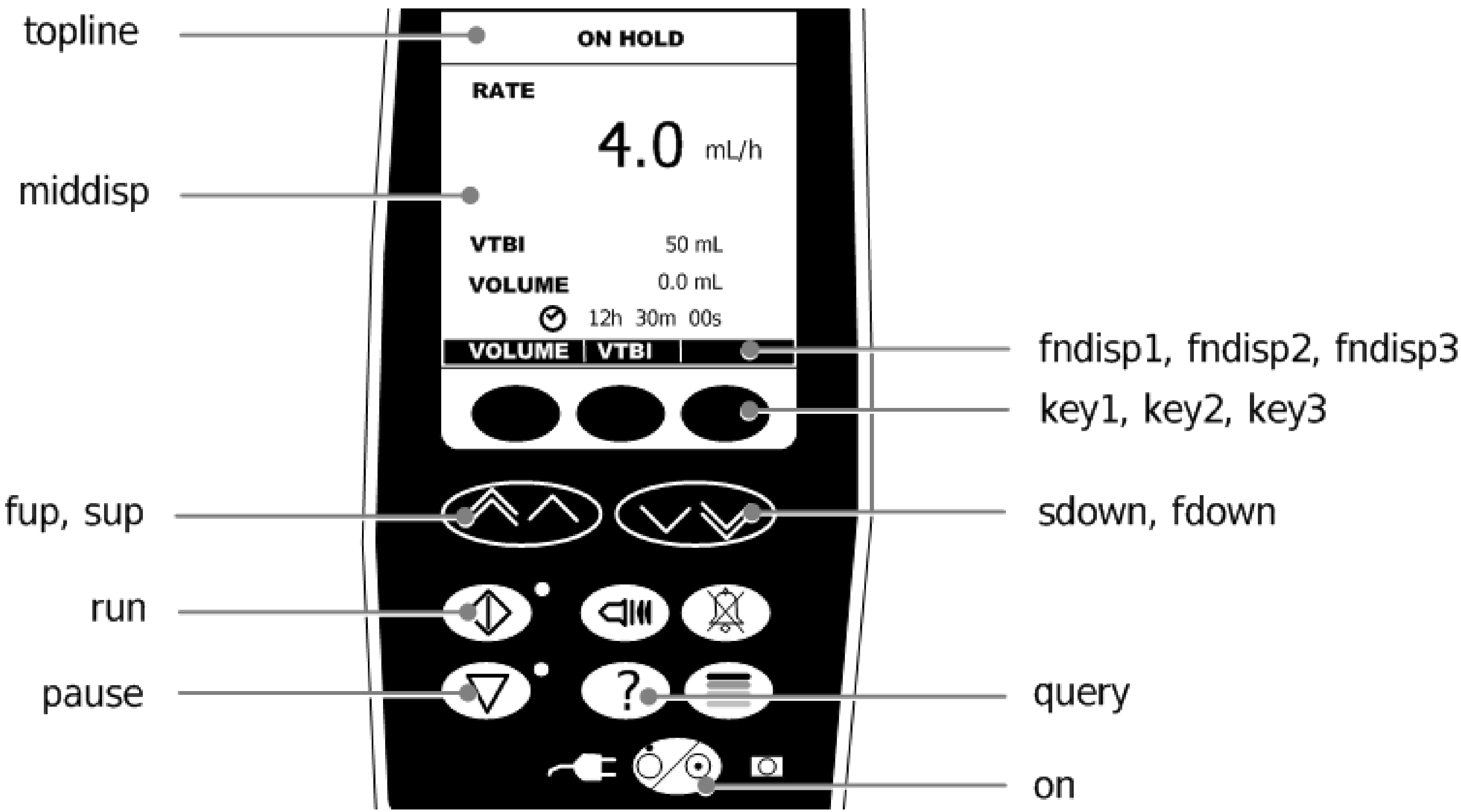
Safety requirements

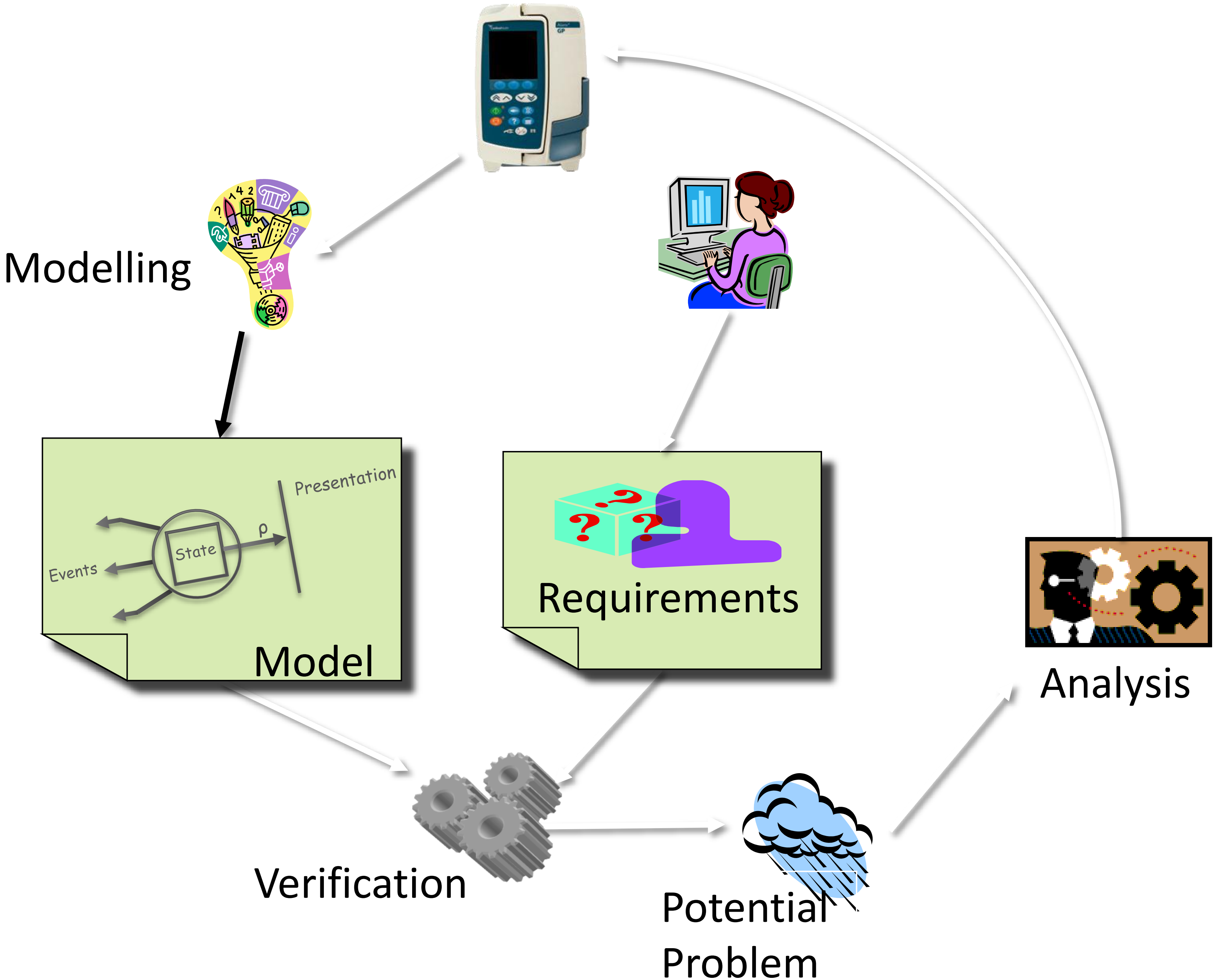
- Demonstrating that a risk is mitigated
  - "***Clearing the pump settings and resetting of the pump shall require confirmation*** "
  - Mitigates the risk that the device will be reset inadvertently
  - Developed by the FDA

What do we want?

- Systematic analysis of a device either formative or summative
- Base the analysis on a precise description of a device
- Tools to ease the development and analysis of these descriptions
- MAL and PVS models, combining model checking with theorem proving

Model attributes





Modelling
Presentation
ρ
State
Events
Model
Requirements
Analysis
Verification
Potential
Problem

Making requirements precise

Clearing the pump settings and resetting of the pump shall require confirmation

- vtbi_ready_to_clear(st, x) => clear_setting_vtbi(st)`vtbi = x AND confirm_action(clear_setting(st))`vtbi = 0 AND no_confirm(clear_setting(st))`vtbi = x)

Proving requirements using theorem proving

- ***Clearing the pump settings and resetting of the pump shall require confirmation***

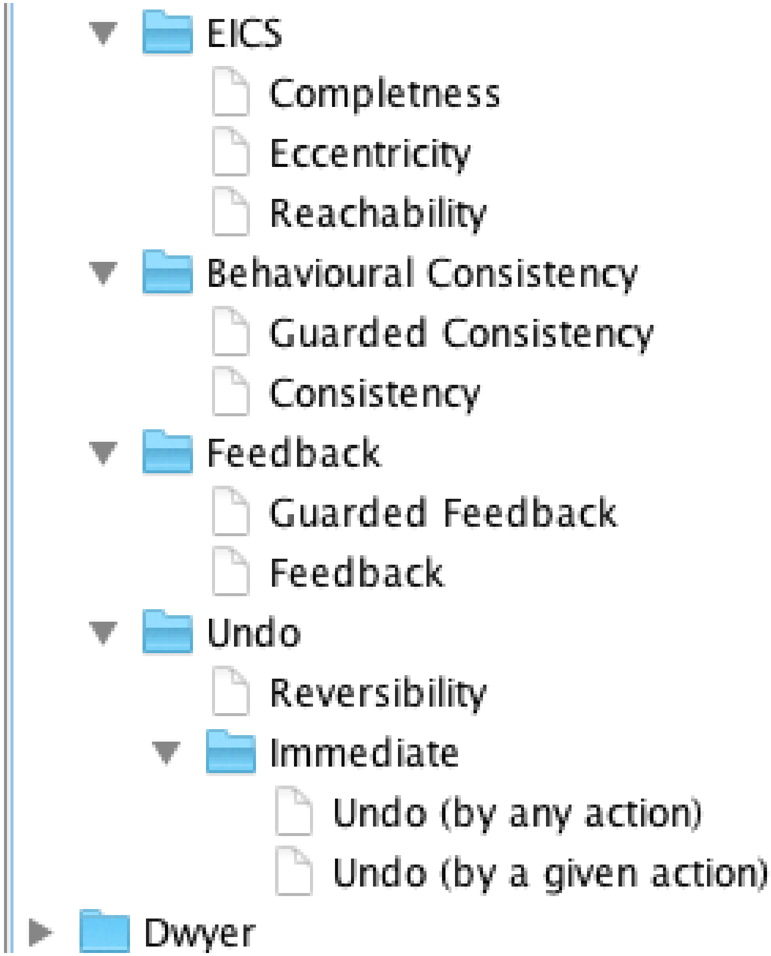
```
R1vtbi: THEOREM
FORALL (st: alaris, x: ivols):
LET stprime=clear_setting(st) IN
(vtbi_ready_to_clear(st,x) IMPLIES
(topline(stprime) = clearsetup AND
device(stprime)`vtbi=x AND no_confirm(stprime)
AND device(key1(stprime))`vtbi=0 AND
device(key3(stprime))`vtbi=x))
```

FDA User Input Requirements

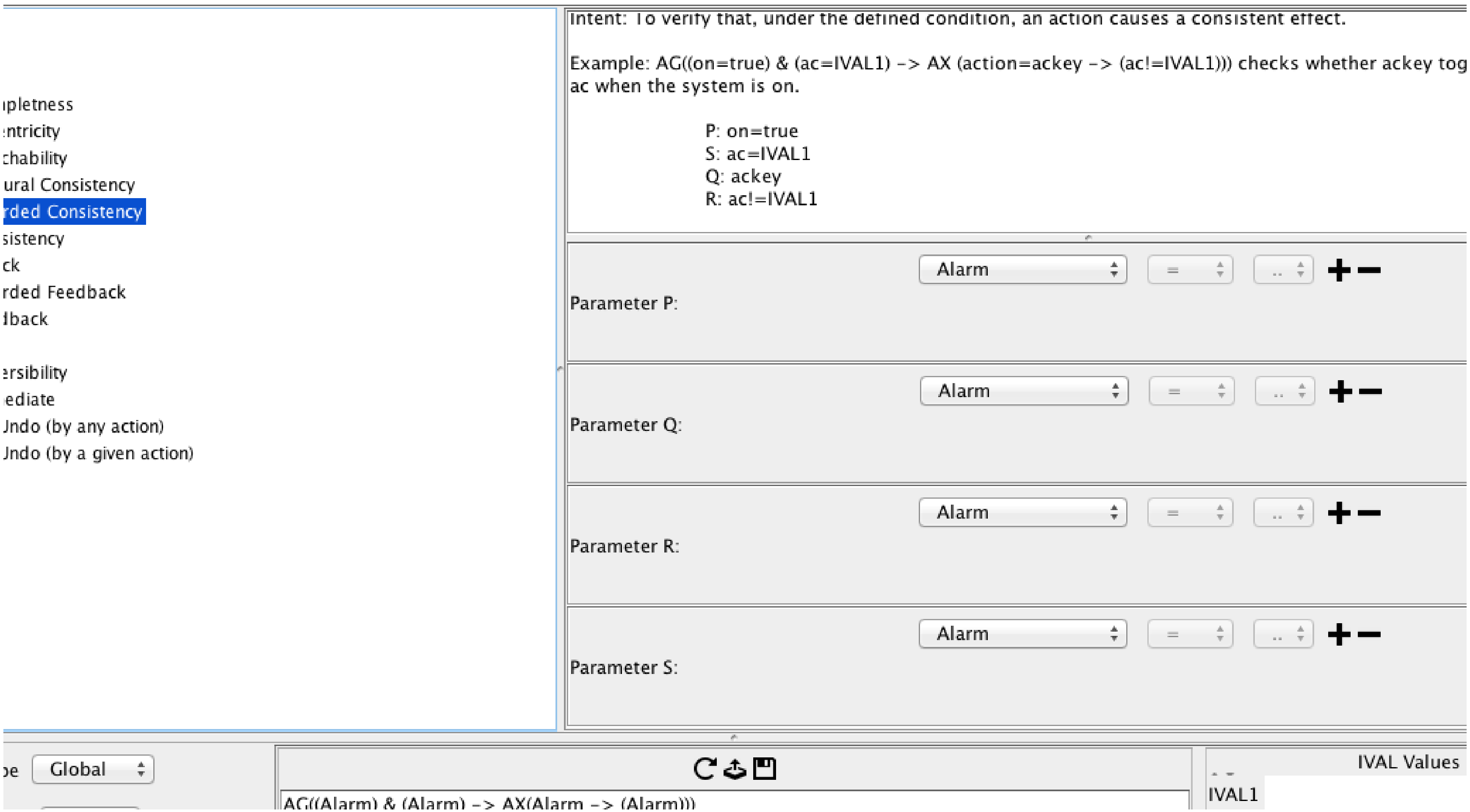
- If the pump is in a state where user input is required, the pump shall issue periodic alerts/indications every *t minutes* till the required input is provided.
- The pump shall issue an alert if paused for more than *t* minutes
- Clearing of the pump settings and resetting of the pump shall require confirmation.
- If the pump is idle for *t minutes* while programming a dose setting, the pump shall issue an alert to indicate that the user needs to finish programming/start infusion
- If the pump is idle for more than *t minutes* while programming a dose setting, the pump shall issue an alarm and clear the dose parameters defined.
- Each change in the dose settings must be confirmed before it is applied.

Using generic property templates as heuristics

- Completeness
- Feedback
- Consistency
- Visibility
- Reversibility



Templates as heuristics



Refinement of templates

- Iterative process
- Recognising counter-examples
- Exploring the consequences of a property or failure of a property
  - Is the assumption about the salience of feedback valid?
  - Role of human factors

Requirements for automation?

- M1: Make it easy to override and correct errors
- M2: System should be capable of being informed that it has taken a wrong step
- M3: System should learn from mistakes
- M4: Should communicate clearly what it is doing and why
- M5: Should use multiple modalities and information channels redundantly
- M6: Should not assume every user is the same and be aware of what each user knows

Modelling etiquette properties

- Plans
- Assumed intentions
- Multiple modalities

Issues and opportunities

- Checking the model is of the device
- Roles for alternative proof technologies: PVS, MAL-IVY, ALLOY?
- Supporting the technology
- Active involvement of FDA: working with them on user-related safety requirements

Summary

- How can we demonstrate interaction with autonomous systems is safe?
- There are properties of these systems that relate to trust, for example
- A formal process can assess whether a system has these properties
- The challenge is to develop a process that can be used routinely

References

- C. A. Miller. Human-computer etiquette. Communications of the ACM, 37(4):31–34, 2004.
- Gary Klein, David D. Woods, Jeffrey M. Bradshaw, Robert R. Hoffman, and Paul J. Feltovich. Ten challenges for making automation a ”team player” in joint human-agent activity. IEEE Intelligent Systems, 19(6):91–95, 2004.
- T. B. Sheridan. Function allocation: algorithm, alchemy or apostasy? International Journal of Human-Computer Studies, 52:203–216, 2000.
- Harrison, M., Johnson, P., and Wright, P. (2003). Relating the automation of functions in multi-agent control systems to a system engineering representation. In *Handbook of Cognitive Task Design.* Lawrence Erlbaum Associates. pp. 503-524.
- Masci P, Ayoud A, Curzon P, Harrison MD, Lee I, Thimbleby H. Verification of interactive software for medical devices: PCA infusion pumps and FDA regulation as an example. In: Proceedings of the 5th ACM SIGCHI symposium on Engineering interactive computing systems. 2013, London, UK: ACM Press.