IMPROVING DIAGNOSIS IN COMPLEX PROCESS SYSTEMS: WHY IT'S A CHALLENGE

Ian Cameron[1], Erzsébet Németh[1], Benjamin Seligmann[1], Maureen Hassall[1], Penelope Sanderson[1], Katalin M. Hangos[2], Kim Hockings[3], John Lee[4]

[1]Faculty of Engineering, Architecture and Information Technology, The University of Queensland, Brisbane, QLD, Australia 4072 (itc@uq.edu.au, 07 33654261)

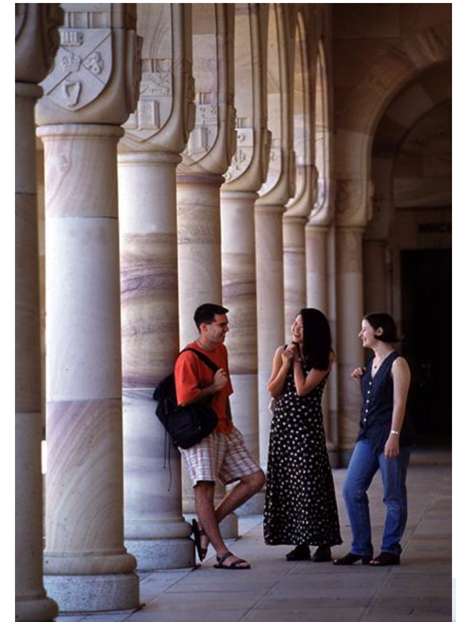
[2]Computer and Automation Research Institute, Hungarian Academy of Sciences, Budapest, Hungary 1111

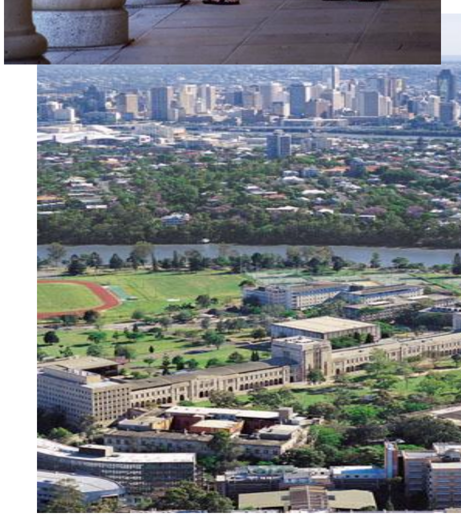
[3]BlueScope Steel Ltd Port Kembla Steelworks Wollongong, NSW Australia 2500

[4]BP Refinery (Bulwer Island) Tingira Street, Pinkenba, QLD Australia 4008

Where this work is done …

THE UNIVERSITY OF QUEENSLAND
AUSTRALIA





100 YEARS AHEAD

Why we need to do this.

"A complex and interlinked series of mechanical failures, human judgments, engineering design, operational implementation and team interfaces came together to allow the initiation and escalation of the accident."
(BP Internal Investigation Report, 2010, p. 5)

… and another $50BN or more per year!

Motivation and aims

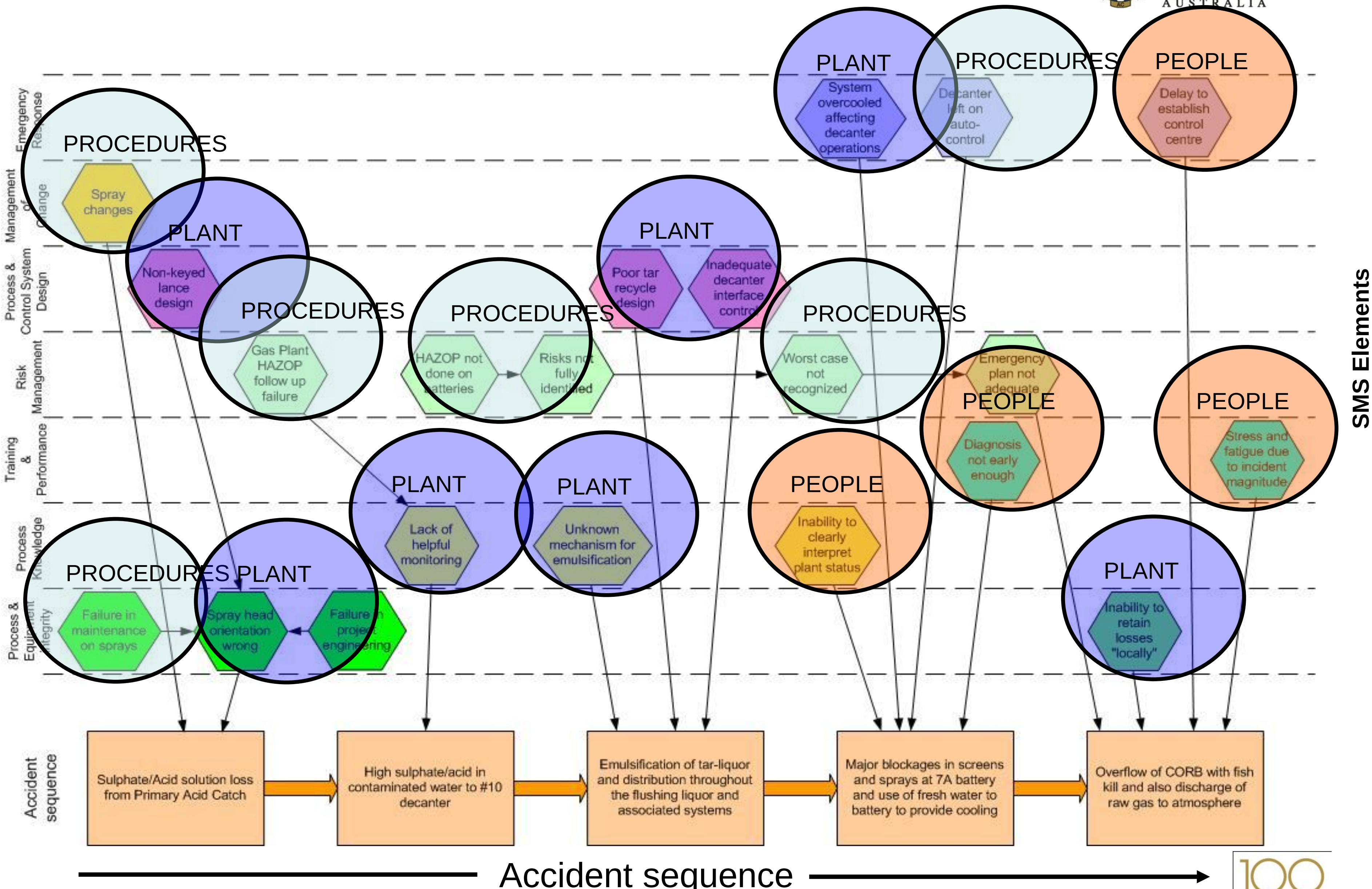
Motivation

Diagnosis still remains a major challenge, especially during abnormal conditions. We need new insights and system based approaches to address such issues.

Aims

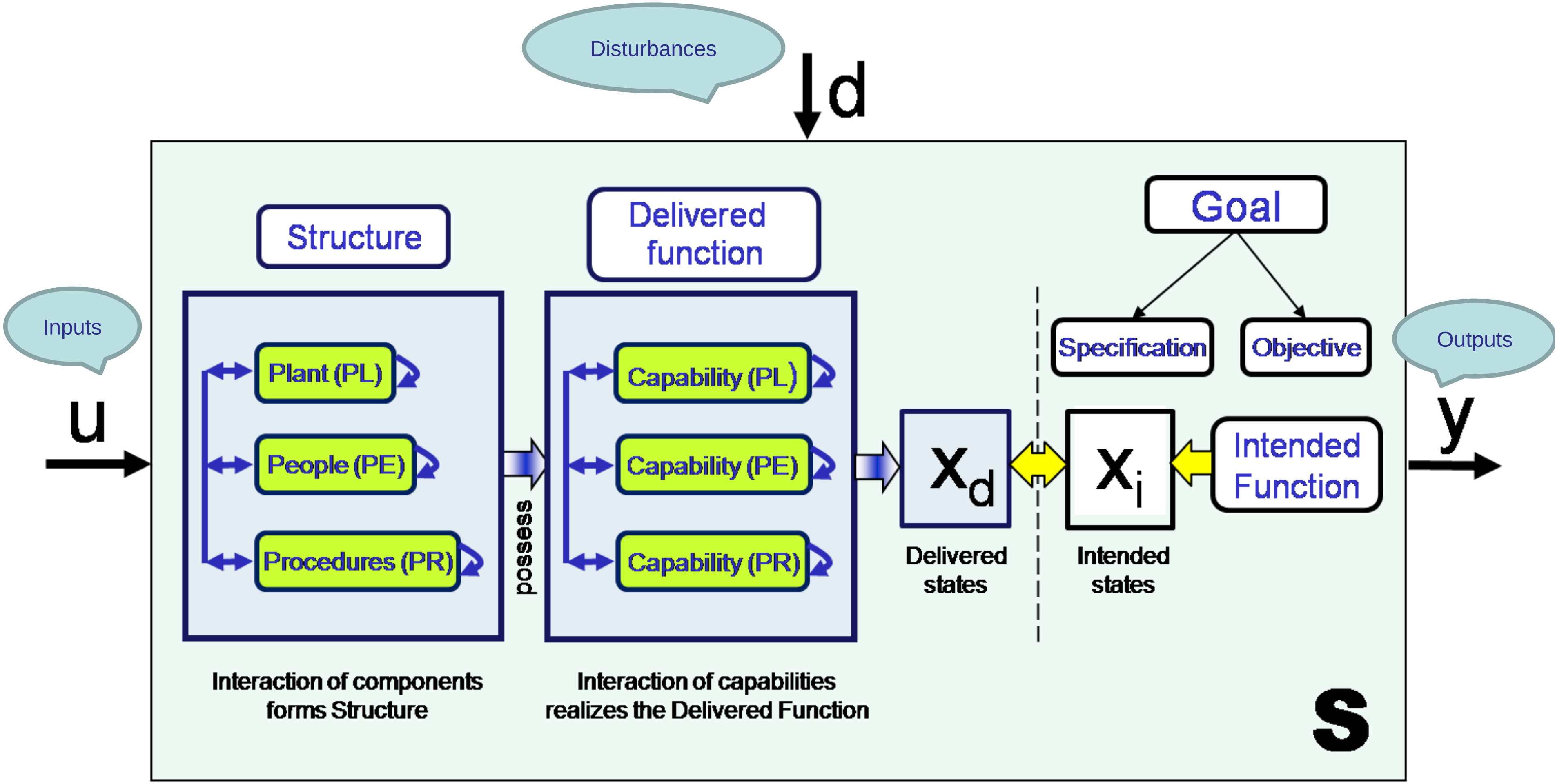
- Develop a new, integrated framework for thinking about systems that encompass PLANT, PROCEDURES and PEOPLE
- Apply a suite of intelligent methodologies and tools that form an integrated approach to considering PLANT, PROCEDURES and PEOPLE during design and operation.
- Provide insights and tools to explicitly understand how *function* arises and how it is lost or degraded through *failure* to improve design, training and operational performance.

Accident causation & latent factors



The functional systems framework (FSF)

The University of Queensland
AUSTRALIA



All systems deliver functions through components and capabilities due to their connections or structure

100 YEARS AHEAD

Capabilities, Functions, Goals

- Capability: "The ability of a component or combination of components to affect the states of a system"
  - Conditional nature of capabilities and their activation.
- Function: "The intended effects of the capabilities"
- Formal language descriptions:
  - Structured, flexible, extensible, transferable, searchable, understandable.

Capability Sets

$$C_i = \{C^P_{i,j} : j = 1 \ldots m \, | C^S_{i,k} : k = 1 \ldots n\}$$

- Capabilities syntax for plant:
  - <action><property>
    - e.g. <hold><mass>, <transfer><mass>, <permit><flow> etc.
  - Failure mode causes (break, rupture, …) are actions that negate or degrade capabilities, e.g.
    - FMC: break ⇒ <¬ hold><mass>
    - FMC: plugged ⇒ <¬ transfer><mass>
  - Can be extended to people and procedures

Formal language: syntax + semantics

THE UNIVERSITY OF QUEENSLAND AUSTRALIA

Major concepts

- State
- State condition
- Deviation
- Component
- Capability
- Failure mode

...

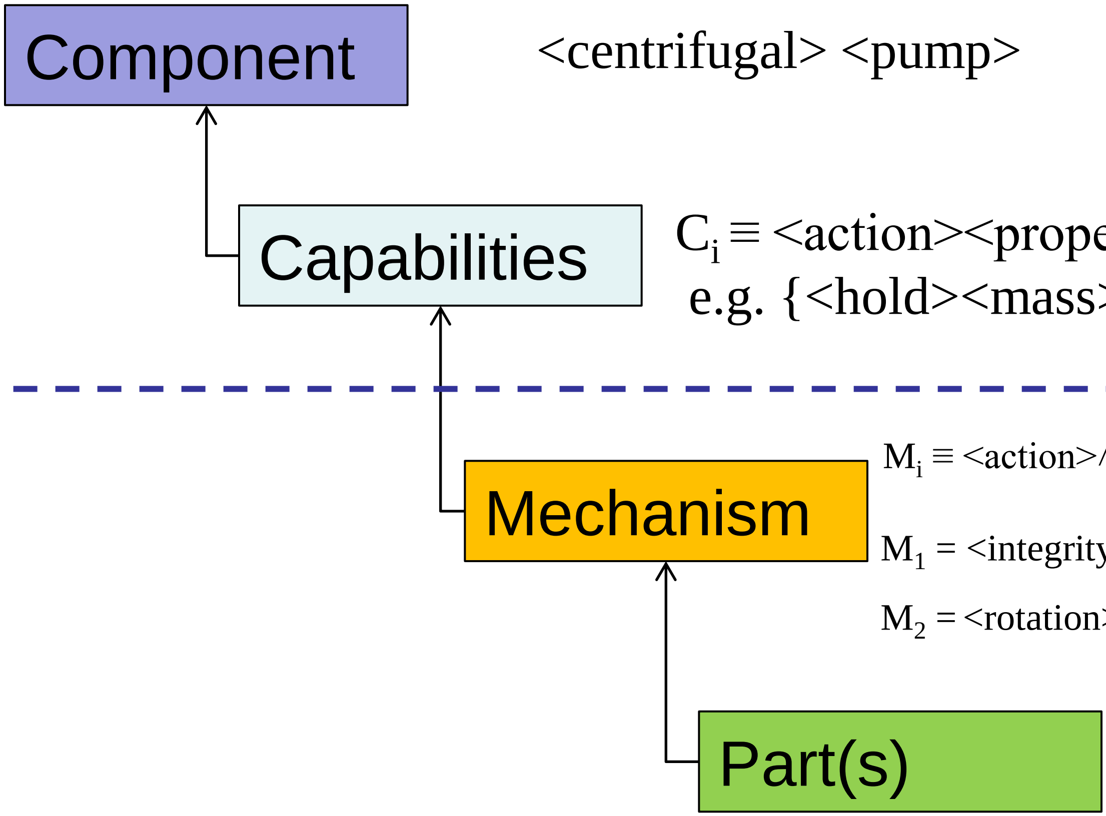
- Implication

...

Language use (pairs, triplets)

- {<flow>, <pressure>, …} ≡ {<state>}
- {<no>, <high>, …} ≡ {<s_condition>}
- {<no><flow>} ≡ {<s_condition><state>}
- {<valve>, <line>, …} ≡ {<PL_com>}
- {<permit><flow>} ≡ {<action><state>}
- {<valve><fails><open>} ≡ {<PL_com><action><state>}
- {<vessel><pressure><high>} ≡ {<PL_com><state><s_condition>}

Plant components



<centrifugal> <pump>

$C_i \equiv$ <action><property>:
e.g. {<hold><mass>; <increase><pressure>; ...}

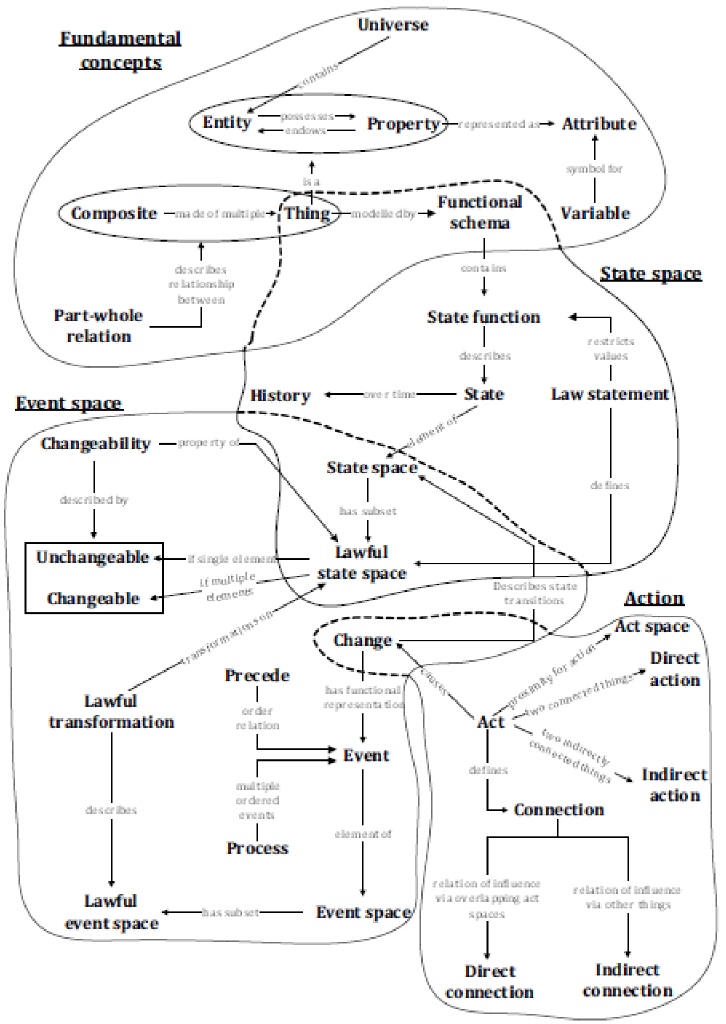
$M_i \equiv$ <action>^<status> of a <part> or <parts in combination>

M_1 = <integrity><{casing, seal}>

M_2 = <rotation><{drive, drive_shaft, gearbox, impeller}>

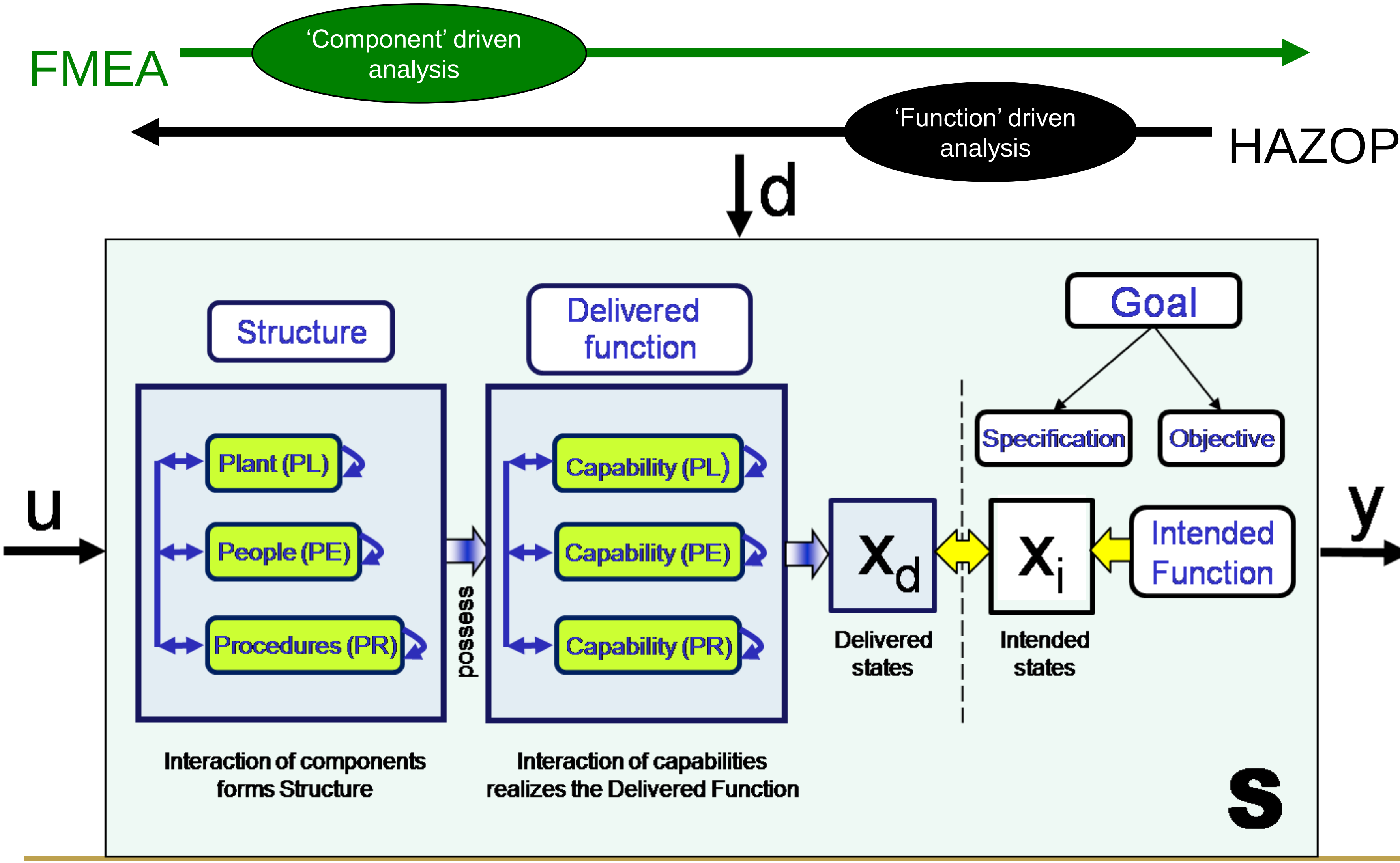
{casing, impeller, seal, drive_shaft, drive, coupling, gearbox, flange ...}

Systems concepts formalised



ANALYSING PLANT ISSUES USING FUNCTIONAL APPROACHES

The functional systems framework (FSF)



Blended HAZID (BLHAZID) method

THE UNIVERSITY OF QUEENSLAND AUSTRALIA

Focus

- systematically analysing ***components*** and ***streams***
- ***blending*** two fundamentally different types of HAZID methods:
  - a *goal-driven method* such as HAZOP where the focus is on the cause of the loss or degradation of system function
  - a *component-driven* method such as FMEA
- based on Functional systems framework (FSF)

Workflow

System selection and decomposition

1. Select the system to be analysed
2. Decompose the system into subsystems

Hazard identification

3. For each subsystem:
   - a) Identify characterizing variables
   - b) For each characterizing variable:
     - i) Generate deviations
   - c) For each deviation:
     - i) Elicit possible causes
     - ii) For each possible cause:
       - Elicit its implications

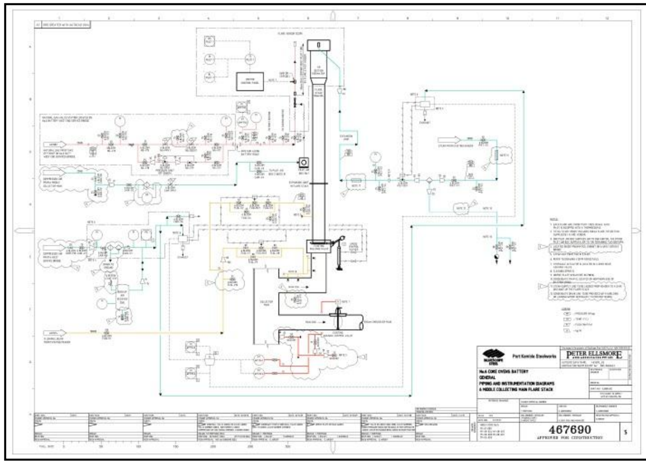
   (a–c: **stream failure analysis**)

   - d) For each component:
     - i) Elicit failure modes
     - ii) For each failure mode:
       - Elicit its implications

   (d: **component failure analysis**)

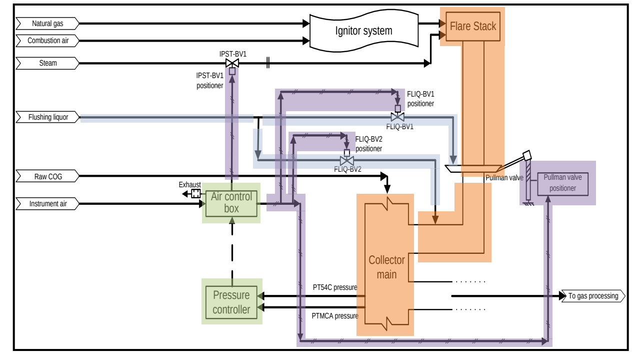
   - e) Collate consequence list
   - f) Collect new characterising variables from possible causes and implications and add them to initial char. variable list. Go back to step b)

The University of Queensland
AUSTRALIA

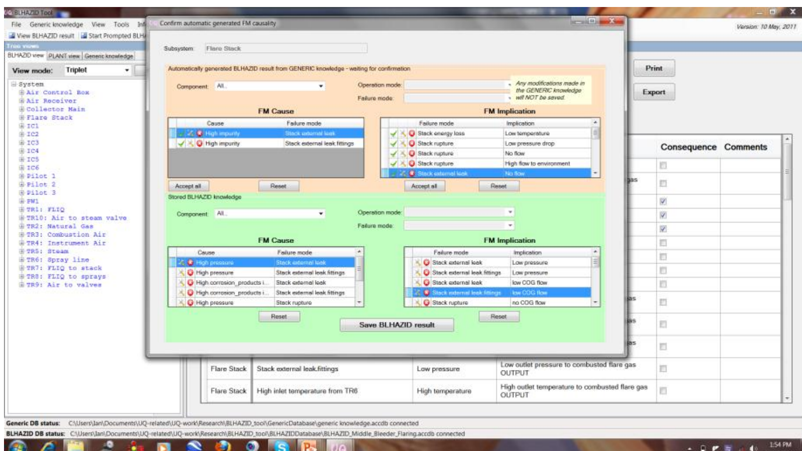


Piping & Instrumentation diagrams

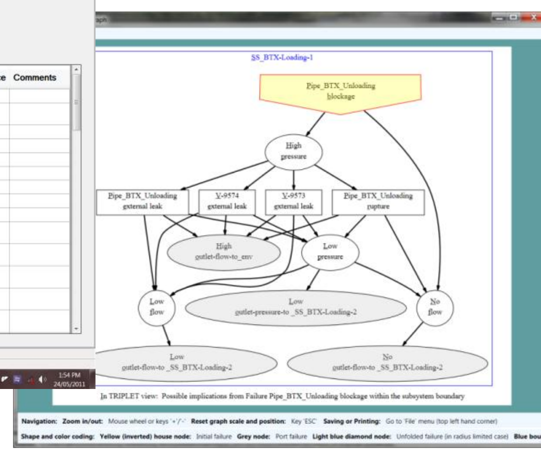
Information extraction



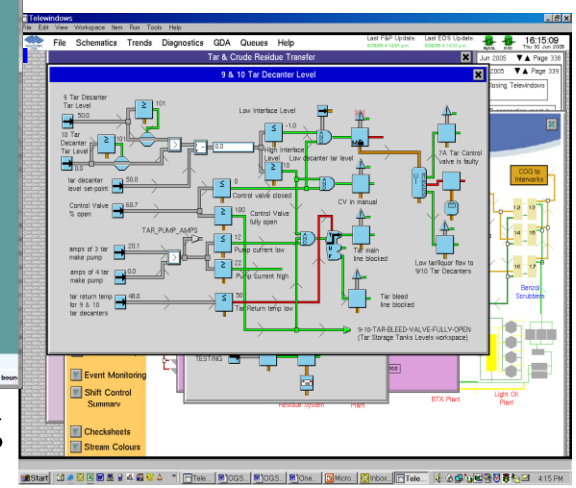
Decomposition into sub-systems



BLHAZID knowledge generation



Generate CIGs via questioning

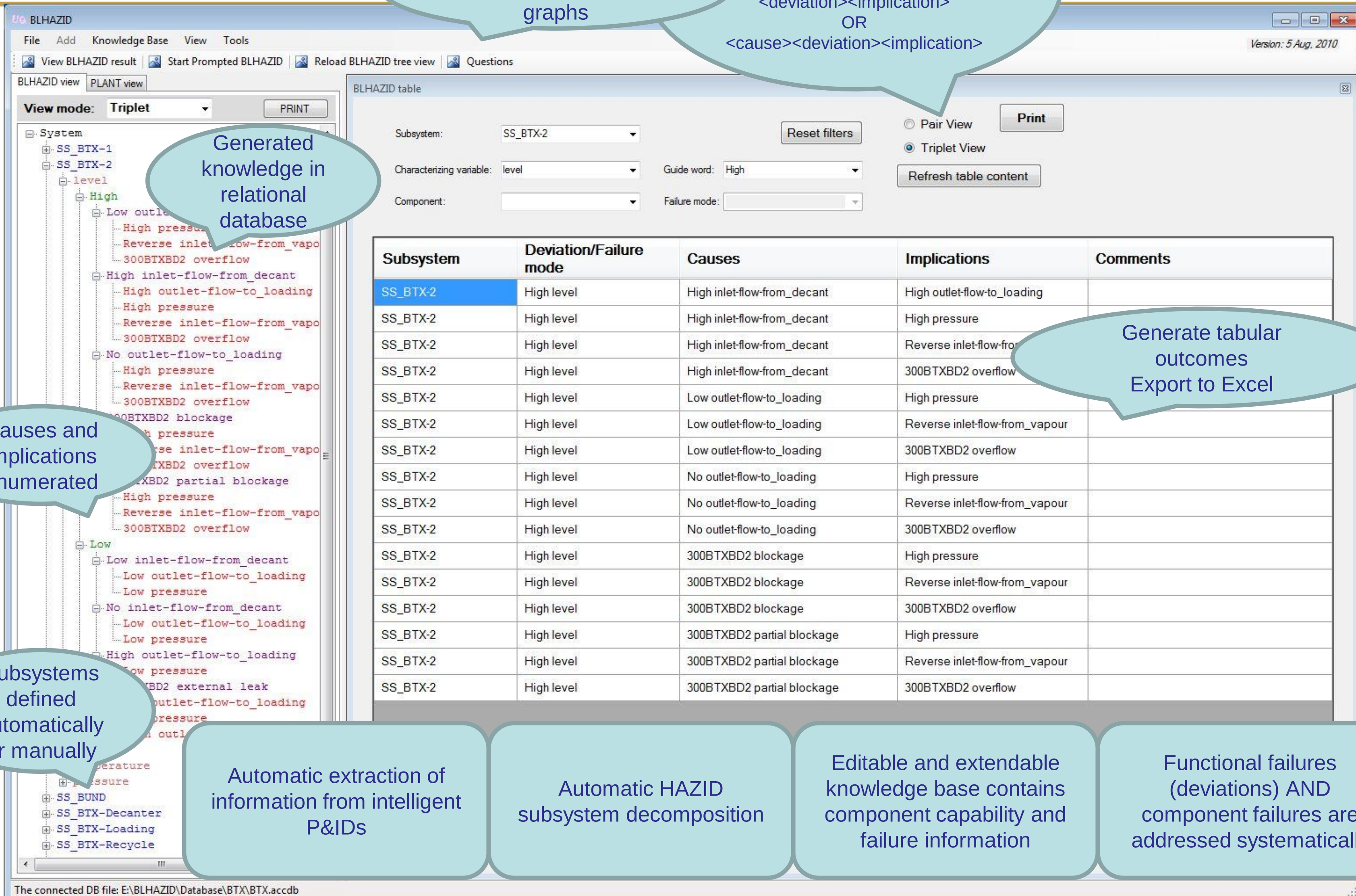


RT deployment systems

100 YEARS AHEAD

BLHAZID

THE UNIVERSITY OF QUEENSLAND
AUSTRALIA



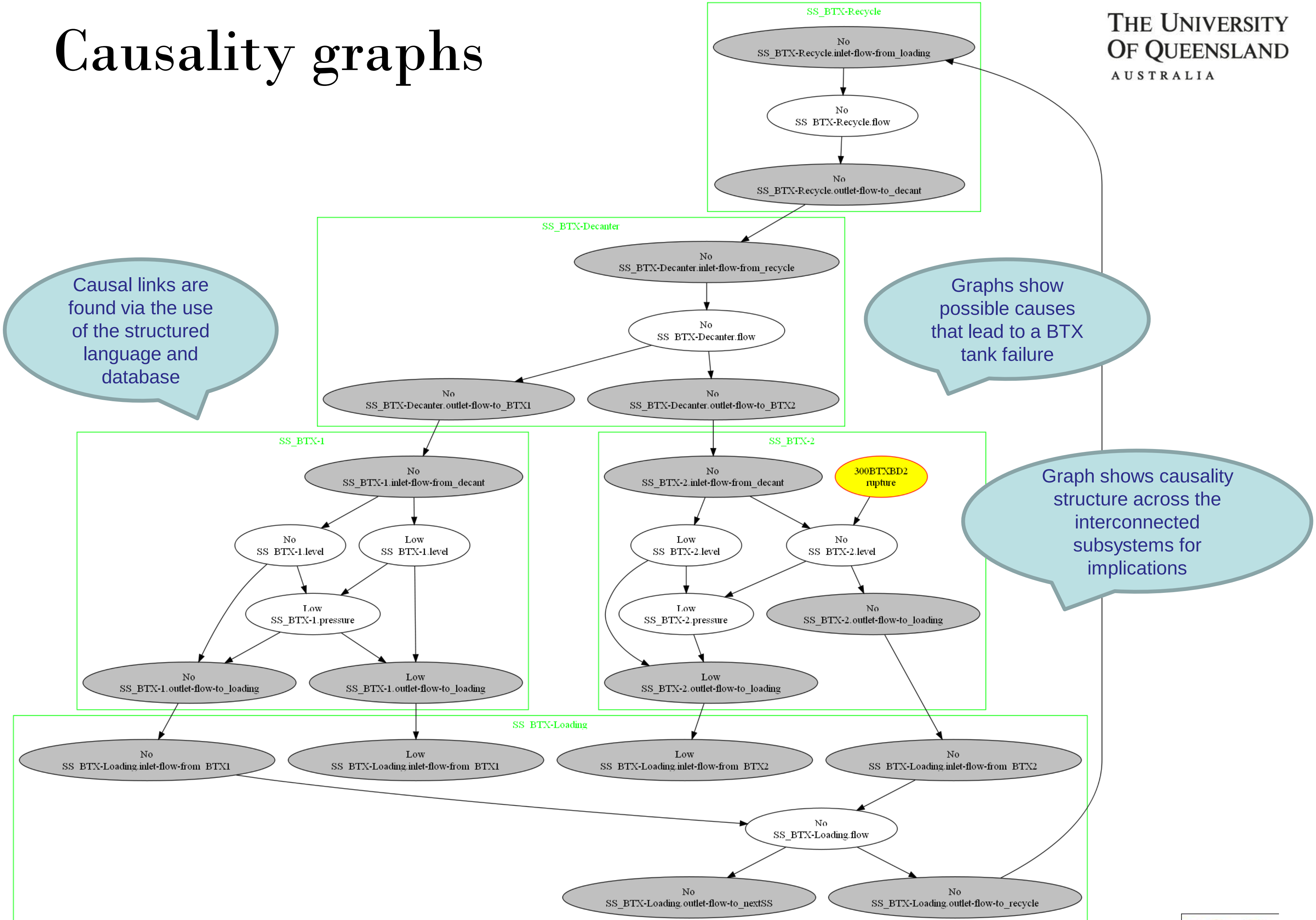
Subsystem	Deviation/Failure mode	Causes	Implications	Comments
SS_BTX-2	High level	High inlet-flow-from_decant	High outlet-flow-to_loading	
SS_BTX-2	High level	High inlet-flow-from_decant	High pressure	
SS_BTX-2	High level	High inlet-flow-from_decant	Reverse inlet-flow-fro	
SS_BTX-2	High level	High inlet-flow-from_decant	300BTXBD2 overflow	
SS_BTX-2	High level	Low outlet-flow-to_loading	High pressure	
SS_BTX-2	High level	Low outlet-flow-to_loading	Reverse inlet-flow-from_vapour	
SS_BTX-2	High level	Low outlet-flow-to_loading	300BTXBD2 overflow	
SS_BTX-2	High level	No outlet-flow-to_loading	High pressure	
SS_BTX-2	High level	No outlet-flow-to_loading	Reverse inlet-flow-from_vapour	
SS_BTX-2	High level	No outlet-flow-to_loading	300BTXBD2 overflow	
SS_BTX-2	High level	300BTXBD2 blockage	High pressure	
SS_BTX-2	High level	300BTXBD2 blockage	Reverse inlet-flow-from_vapour	
SS_BTX-2	High level	300BTXBD2 blockage	300BTXBD2 overflow	
SS_BTX-2	High level	300BTXBD2 partial blockage	High pressure	
SS_BTX-2	High level	300BTXBD2 partial blockage	Reverse inlet-flow-from_vapour	
SS_BTX-2	High level	300BTXBD2 partial blockage	300BTXBD2 overflow	

- Automatic extraction of information from intelligent P&IDs
- Automatic HAZID subsystem decomposition
- Editable and extendable knowledge base contains component capability and failure information
- Functional failures (deviations) AND component failures are addressed systematically

100 YEARS AHEAD

Causality graphs

THE UNIVERSITY OF QUEENSLAND
AUSTRALIA



In TRIPLET view: Possible implications from Failure 300BTXBD2 rupture

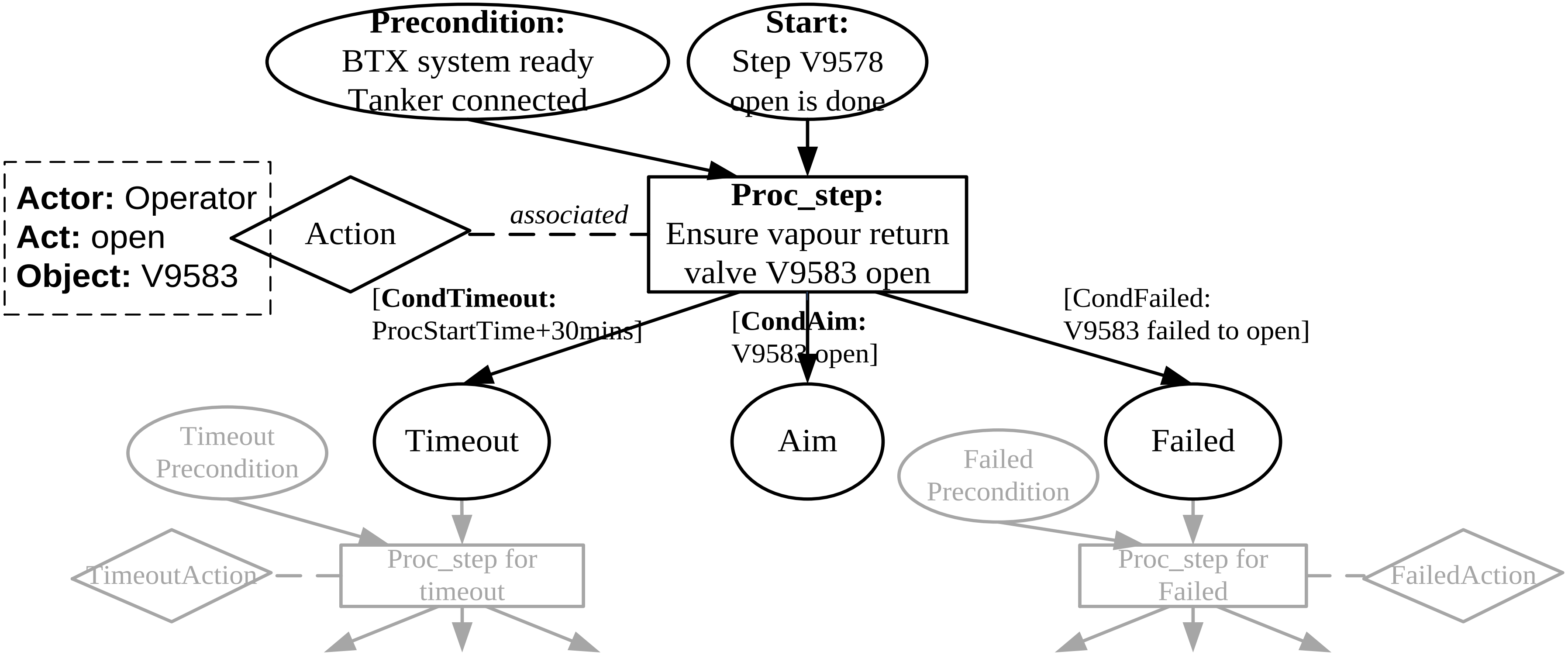
Significance of the work and outcomes

- Improve HAZID coverage
- Exploit growing use of intelligent design tools
- Semi-automation seeks to improve outcomes and reduce tedium and overall costs
- Generate re-usable knowledge for life cycle purposes, e.g. improved real-time diagnosis, operator training, ACM etc.
- Internal checks on causality pathways for completeness
- Incorporate into DCS operator guidance systems, live fault tree and event tree analysis
- Provide basis for auditing and periodic revision
- Potential integration with hazard and risk registers for live, up-to-date causality understanding.

ANALYSING PROCEDURE ISSUES USING FUNCTIONAL APPROACHES

Formal representation of procedures

- *Procedures* (PR) — sequences of instructions for operators or a control system that should be executed to manage a process plant.
- Coloured Petri net model of a single procedure step and its logical environment for a step



Syntactical elements of BLHAZID for procedures

- *Nominal "functional behaviour"* of the PLANT controlled by a procedure:
  - given in terms of a nominal *input-output trace*:

    fixes the events both in the input and output signals of the system as a consequence of the actions (also events) directed by the procedure
- *Procedure deviation*: any kind of deviation from the nominal traces
- *Functional failure* for Procedures: guideword – variable pair
  - applicable guide words:
    earlier, ***later***, ***smaller***, ***greater***, ***never happened***, ***wrong order***
  - variable: given by a nominal event or a pair of events in the case of ***wrong order***

Blended HAZID analysis of procedures

THE UNIVERSITY OF QUEENSLAND AUSTRALIA

Any members of the causality triplet (cause – deviation – implication) in the BLHAZID result can be given in a form of:

(i) a procedure functional failure

(ii) a plant functional or component failure

(iii) a people functional failure

Cause	PR Deviation	Implication
PE: (*Step skipped*, procedure execution**)**	(***later***, 'Ensure vapour return valve V9583 open')	**PE:** (***to do***, TimeoutAction)
PE: (*Right action wrong object*, open**)**	(***never happened***, 'Ensure vapour return valve V9583 open')	**PL:** (***High***, flow to environment)
PL: (*failed to open*, V9583**)**	(***smaller***, 'Ensure vapour return valve V9583 open')	**PR:** (***incomplete termination***, procedure step)

100 YEARS AHEAD

ANALYSING PEOPLE ISSUES USING FUNCTIONAL APPROACHES

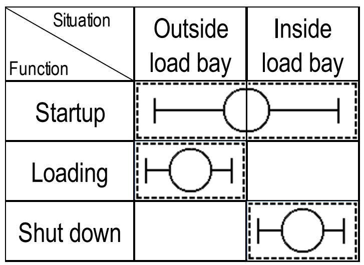
Human hazard identification (HumHID)

Theoretical basis: Cognitive work analysis (CWA)

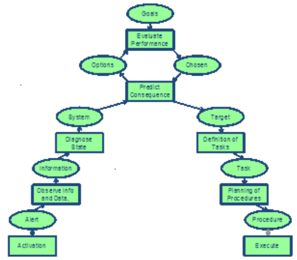
- identifies technological and organizational functions and constraints that shape human activity within the system
- CWA phases most suited to eliciting insights into human activity within an engineering system:
  - ***control task analysis***:
    - determines *what* needs to be done within the work domain in order to achieve the system goal
  - ***strategies analysis***:
    - identifies *how* the control tasks might be executed
    - the output can be matched with relevant people related *characterising variable – guideword – cause* triplets from the People framework to reveal deviations in human behaviour and an understanding into the causality behind them

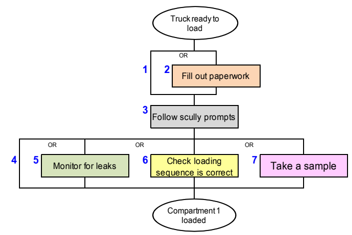
OVERVIEW

CONTROL TASK ANALYSIS → STRATEGIES ANALYSIS → HF HAZID

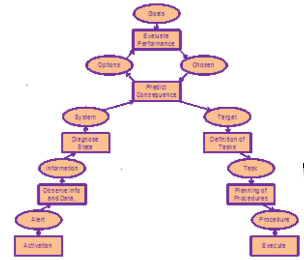


Likelihood	Consequences: Negligible	Low	Medium	High
High	Med	High	Extreme	Extreme
Medium	Low	Med	High	Extreme
Low	Low	Low	Med	High
Negligible	Low	Low	Med	Med





Likelihood	Consequences: Negligible	Low	Medium	High
High	Med	High	Extreme	Extreme
Medium	Low	Med	High	Extreme
Low	Low	Low	Med	High
Negligible	Low	Low	Med	Med



Characterising Variables
- Sensing
- Data processing
- Decision making
- Procedure execution
- Communication
- Social interaction
- Physical action

Deviation Guidewords
- None
- Incorrect/Inaccurate
- Incomplete
- Not at right time
- Not right duration
- Not right area
- Not too right detail

Possible Causes
- Insufficient resources
- Inaccurate knowledge
- Concealed signal
- Confusing signal
- Lapse of attention
- Forgotten meaning
- Violation

Decision Ladder Element	Description	C_Var	Guide-word	Cause	Implication
Activation	Determining that plant and tanker are ready for BTX transfer	Sense	None	No resource allocated	Loading delayed or not started
				Failure to search for information	
				Insufficient knowledge	
				Slips/lapses of attention/concentration	
				Forgotten meaning/ importance	
				Violation or noncompliance	
			Inaccurate	Wrong item percieved as right one	Loading started before plant ready
				Concealed signal	
				Confusing signal	Loading started before tanker ready
				Mismatch b/n actor & requirements	

100 YEARS AHEAD

CATs and IO diagrams

The University of Queensland
AUSTRALIA

Contextual Activity Templates

Situation / Function	Away from bleeder	At bleeder	Away from bleeder
Prepare			
Test pilots			
Test bleeder			
Return to normal			

Add column
Delete column
Delete row
Add row

Situation / Function	Away from bleeder	At bleeder	Away from bleeder
Prepare			
Test pilots			
Test bleeder			
Return to normal			

Input Output Diagrams

Links to Decision Ladder Diagrams

Click to Create/ Refresh Links

1. Function: Prepare; Situation: Away from bleeder.

Time to do weekly bleeder test → Prepare equipment and tools & do notifications → Ready to go to battery

Go To

2. Function: Prepare; Situation: At bleeder.

Ready to go to battery → Access bleeder → At bleeder control panel

Go To

3. Function: Test pilots; Situation: At bleeder.

At bleeder control panel → Test natural gas pilots → Natural gas test completed

Go To

4. Function: Test bleeder; Situation: At bleeder.

Natural gas test completed → Test bleeder → Bleeder test completed

Go To

5. Function: Return to normal; Situation: At bleeder.

Bleeder test completed → Return controls to normal → Leave the battery

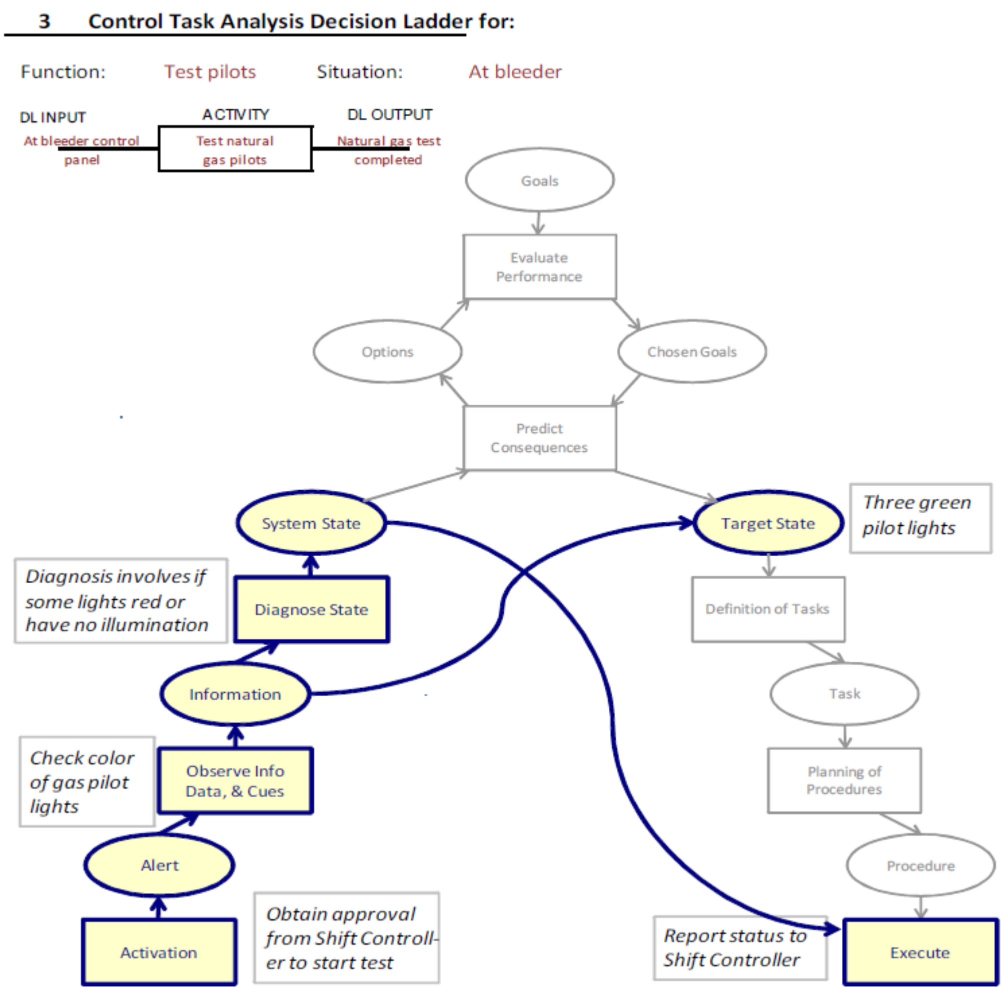
Go To

6. Function: Return to normal; Situation: Away from bleeder.

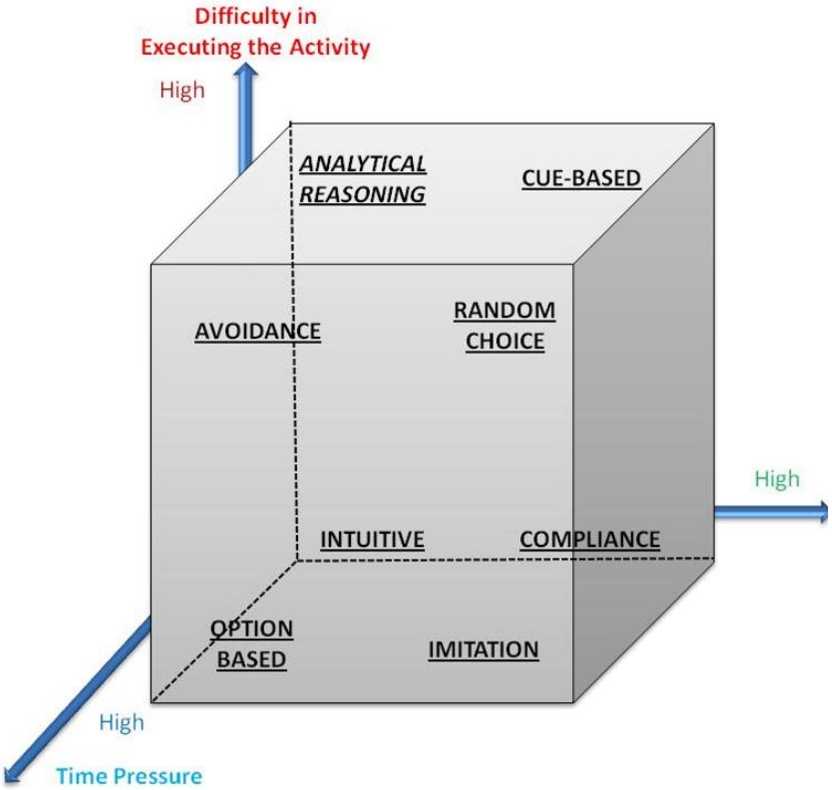
Leave the battery → Complete paperwork → Weekly bleeder test complete

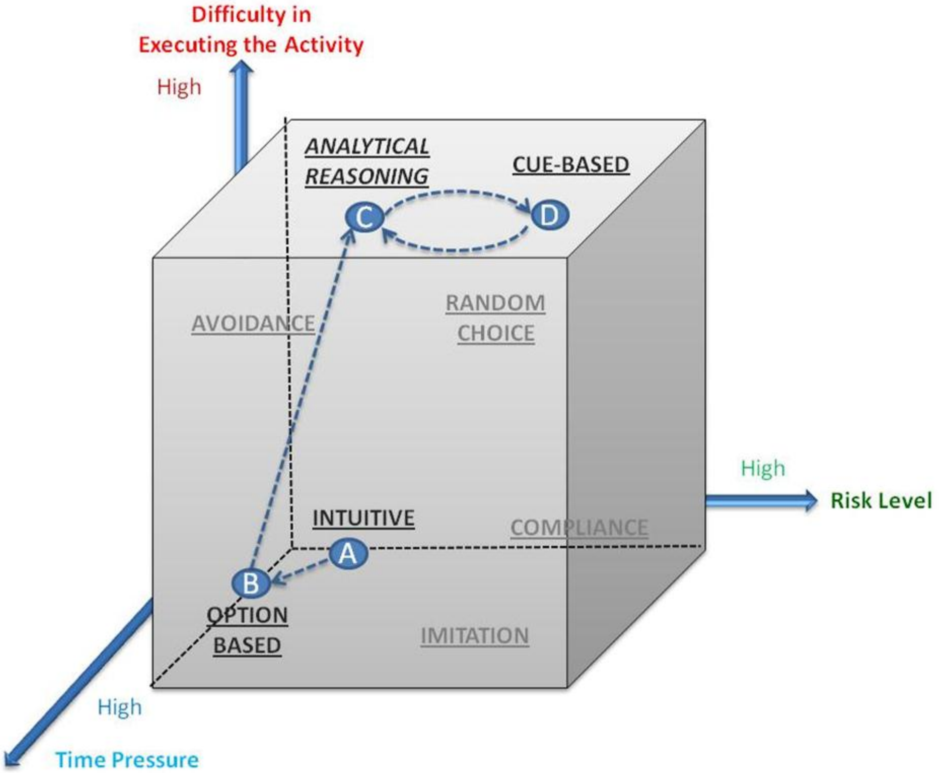
Go To

Control task decision ladder



Strategies options





HumHID outcomes table

C-var	Description	Deviation Guideword	HAZARDS	Causes	Actions
Whole activity	Test natural gas pilots				
		Not done	Likelihood of deviation:	3 Medium	Consequence Severity: 4 High
		Done in adhoc way	Likelihood of deviation:	2 Low	Consequence Severity: 3 Medium
		Done by copying others	Likelihood of deviation:	4 High	Consequence Severity: 2 Low
		Easiest way (meets min stds)	Likelihood of deviation:	4 High	Consequence Severity: 2 Low
		Match approach to situation cues	Likelihood of deviation:	3 Medium	Consequence Severity: 3 Medium
		Automated/ habitual approach	Likelihood of deviation:	4 High	Consequence Severity: 3 Medium
		Follow procedures exactly	Likelihood of deviation:	2 Low	Consequence Severity: 2 Low
		Thorough logical/ analytical approach	Likelihood of deviation:	2 Low	Consequence Severity: 2 Low
Observe situation	Check color of gas pilot lights				
		No observation	Likelihood of deviation:	2 Low	Consequence Severity: 4 High
			Describe implications in terms of hazards and consequences. Assess severity of consequences in grey row above.	Concealed/confusing/incorrect observation information/tools	
				Situation seen as simple and straight-forward requiring no observation	
				Slips/lapses of attention/concentration or forget right way to do it	
				Insufficient resources available at right time	
				Actors have incorrect knowledge of requirements	
				Too complex for current capability of actors	
				Insufficient time available	
				Situation/Observation not seen as important so given no/low priority	
				Situation seen as very risky so rush to address rather than observe state	
				…other…	

Conclusions

The University of Queensland
Australia

- Systems framework for addressing interconnected components in process systems: PLANT, PEOPLE and PROCEDURES
- Approaches based on the underlying principle of *function*, formalised by the Functional Systems Framework (FSF)
- Techniques improve industrial understanding of the systems that are designed and built through better knowledge generation and capture.
- Knowledge reuse can help build improved diagnostic tools to address abnormal condition management
- Application areas include improved operator, engineer training regimes to enhance decision making and address staff turn-over
- Integration of existing event and risk registers to enhance process understanding,
- Address improved process systems resilience