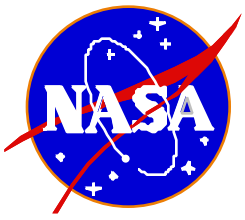
NEXTOR Annual Research Symposium
November 14, 1997

Session III
Issues for the Future of ATM

CTAS Verification

Darren Cofer, Honeywell

Formal Specification and Analysis of the Center-TRACON Automation System



National Center of Excellence for Aviation Operations Research
Annual Research Symposium - 14 November 1997
Project sponsor: NASA Langley Research Center

Honeywell Technology Center
3660 Technology Dr.
Minneapolis MN 55418

Point of contact: Dr. Darren Cofer
(612) 951-7279

Honeywell

Team

- Honeywell Technology Center

  Darren Cofer, Rosa Weber, John Maloney

- University of California at Berkeley

  George Pappas, Shankar Sastry

- Massachusetts Institute of Technology

  John Lygeros, Nancy Lynch

Unique capabilities and emphasis

- Modeling/analysis of complex systems

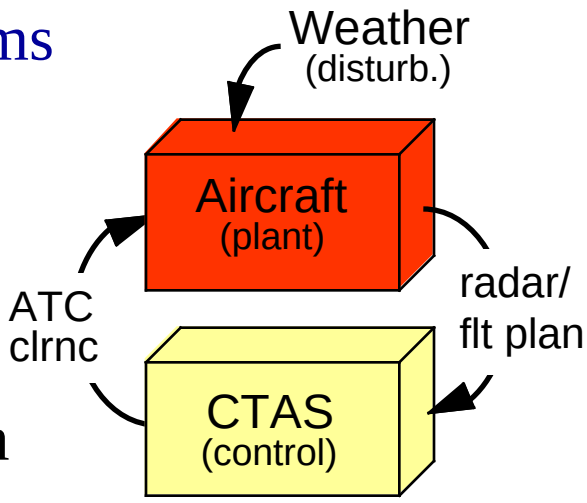
  HW + SW architecture issues, tools

- Control-theoretic viewpoint

  CTAS as input/output control system

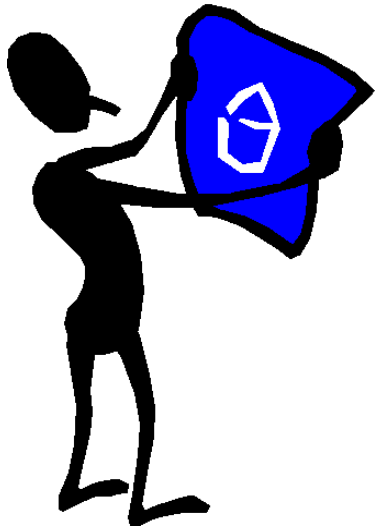
- Hybrid systems

  Discrete-event and continuous dynamics



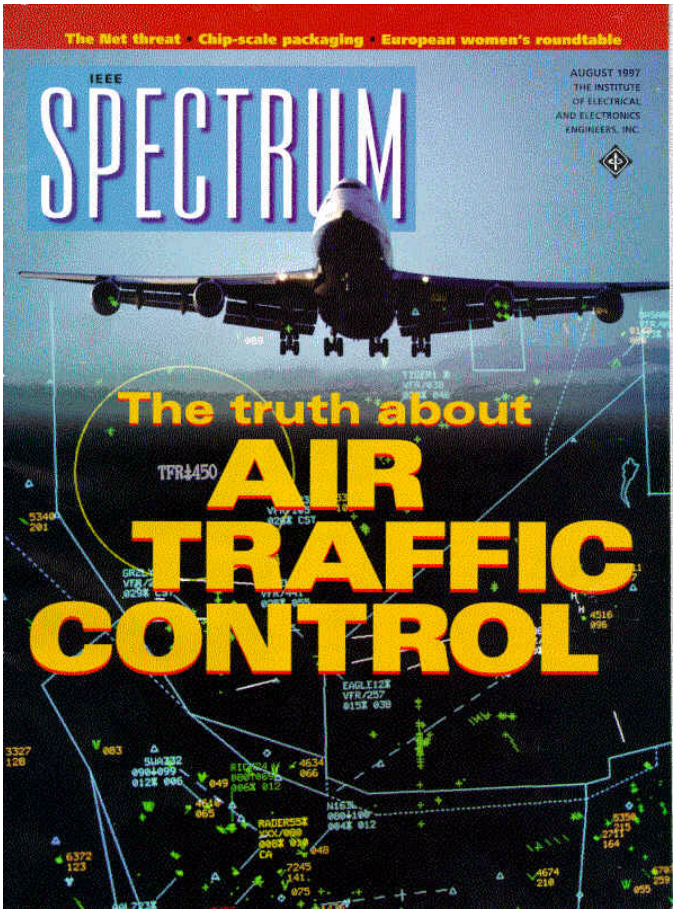
Roadmap for presentation

- What CTAS means to me…
- Changes in ATM/NAS
- Safety Issues and Technologies
- Requirements Specification: *HOPTs*
- System Architecture: *MetaH*
- Formal Systems Analysis: *Hybrid Systems*



Honeywell

Assessing changes in NAS



- Increasing demands on system
- New technologies
- New procedures

Impact on system?

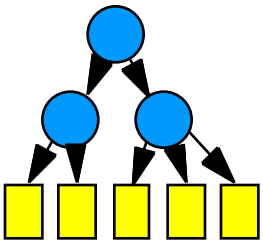
Affected components?

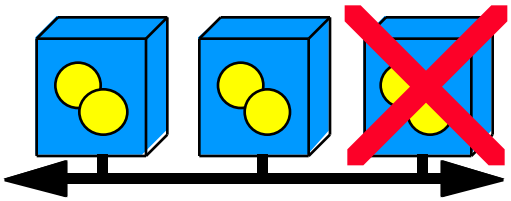
Safety?

Honeywell

Safety issues

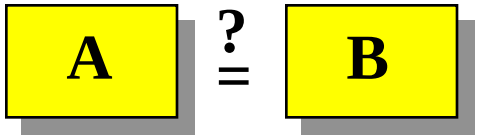
Logical correctness of requirements and implementation



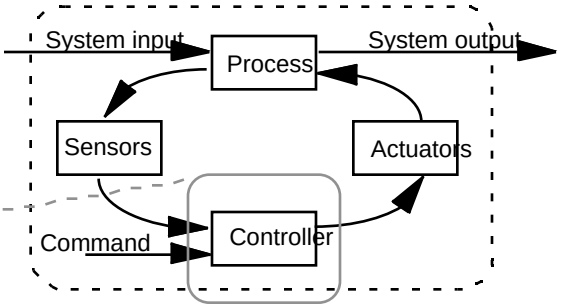


System architecture and timing, degraded modes of operation

Formal equivalence of systems, preservation of properties



Operationally embedded reactive systems



Scenario inputs

Behavior inputs

Title:
Creator: DoME by Honeywell Technology Center, Honeywell Inc.
CreationDate:

Behavior outputs

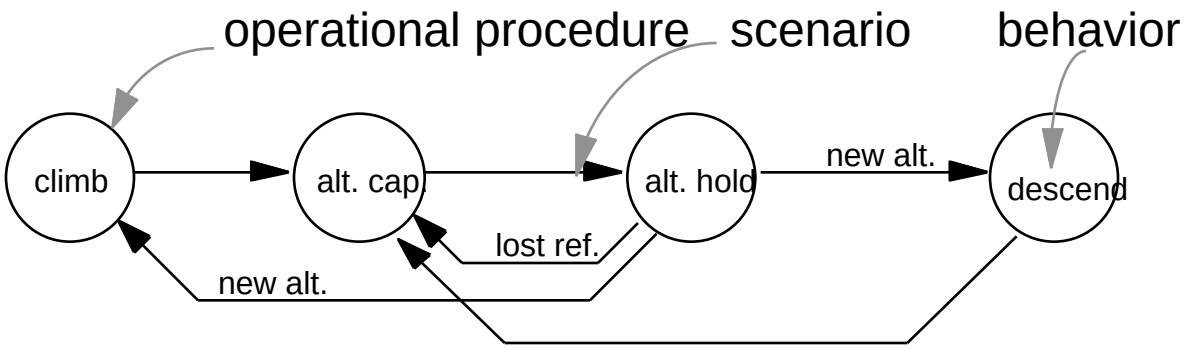
Modes / Procedures
- Ascent
- Descent
- Level Cruise
- Emerg. procedures
- Conflict res. mode

- Altitude target
- Speed target
- Vertical speed target
- Pitch/thrust control mode

Honeywell

Operational procedure table

```
Title:
Creator:  DoME by Honeywell Technology Center, Honeywell Inc.
CreationDate:
```



Semantics

1. Get input state

Inputs	States
Prev Op Proc	climb
	altitude capture
	altitude hold
	descend
new_ref_altitude	yes
	no
altitude	greater_than_ref
	within_ref
	less_than_ref

climb	altitude capture		altitude hold	descend
	lost ref altitude	new altitude		
		X		
			X	
X	X			X
		X		
		X		
	X			
	X	X		X
			X	
X	X	X		

2. Compute scen
and select ope
procedure

X			X
	X	X	
X	X	X	
			X

Outputs	Functions
thrust	altitude_control
	speed_control
elevator	altitude_control
	AOA_control

3. Collect associated behavior
output functions

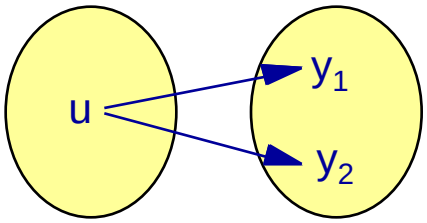
4. Execute

Completeness and Consistency

$$f : U \rightarrow Y$$

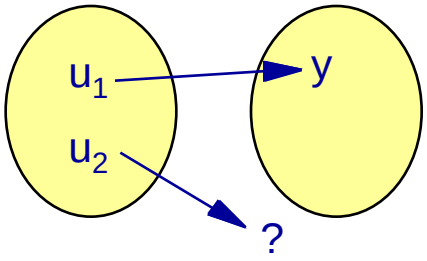
- Consistent: f(u) is unique.

  (a *function* vs. a relation)



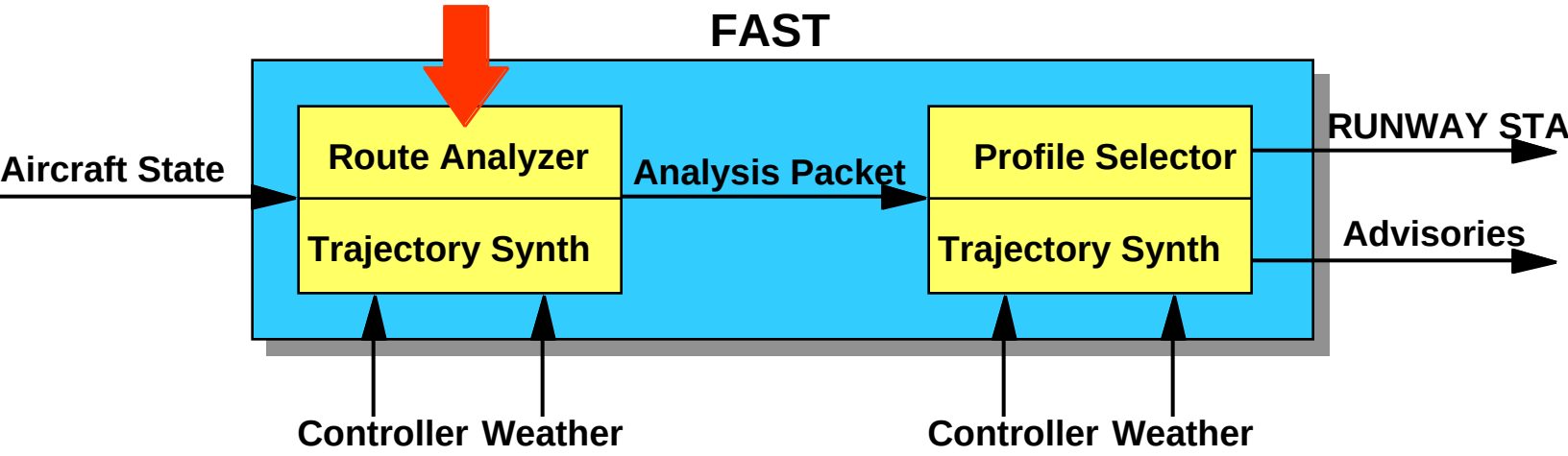
- Complete: f(u) defined u U.

  (a *total* function)



CTAS decision logic

Focus on algorithms
in Route Analyzer



Route Analyzer

Contains many decision logic elements

```
Title:
Creator:  DoME by Honeywell Technology Center, Honeywell Inc.
CreationDate:
```

Update heading (OPT)

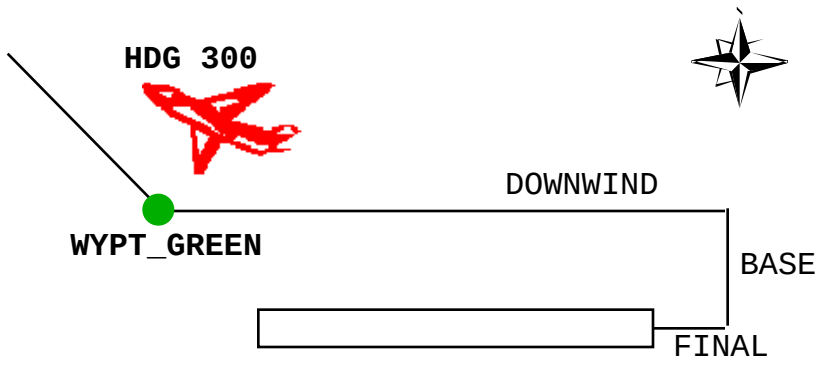
```
Title:
Creator:  DoME by Honeywell Technology Center, Honeywell Inc
CreationDate:
```

Findings

- Consistent
- Some incomplete

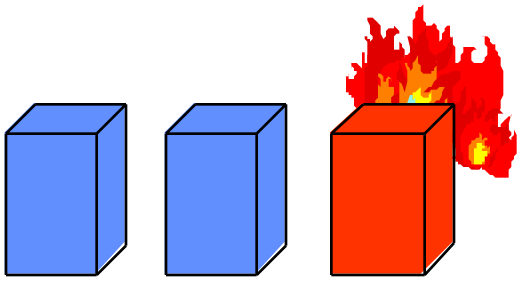
  May rely on context:

Heading = 300 **AND**
Waypoint = WYPT_GREEN
not possible

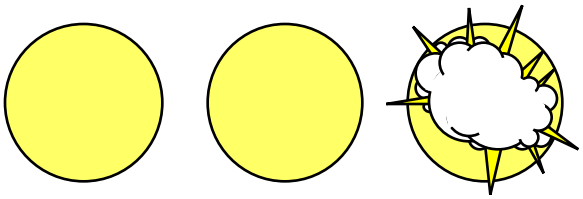


Assess performance in degraded operational modes

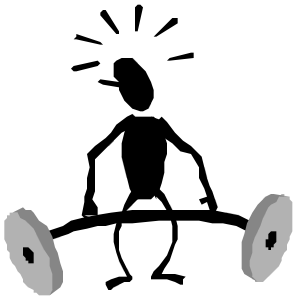
- Hardware node failure



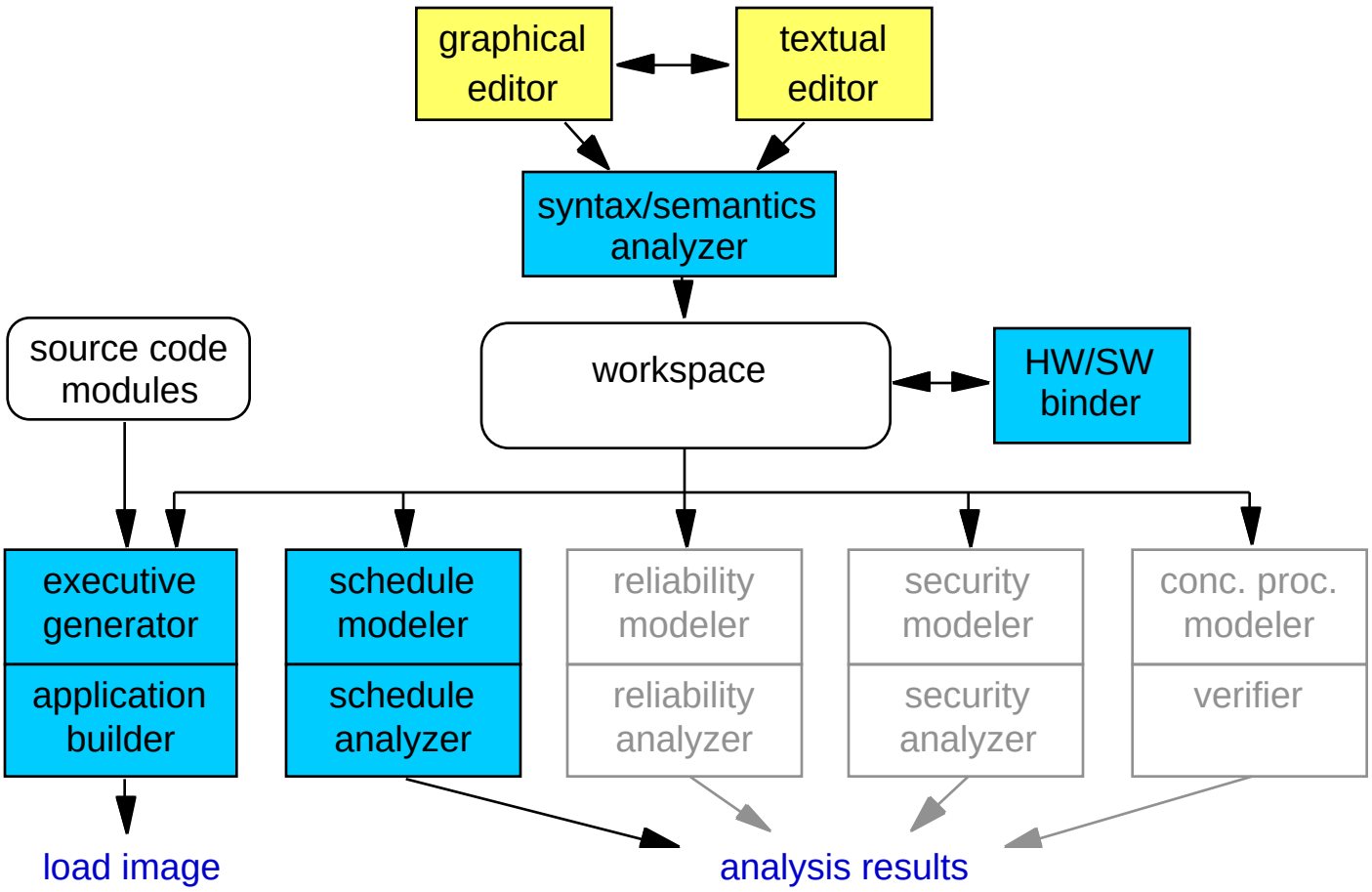
- Software failure



- Excess computational load

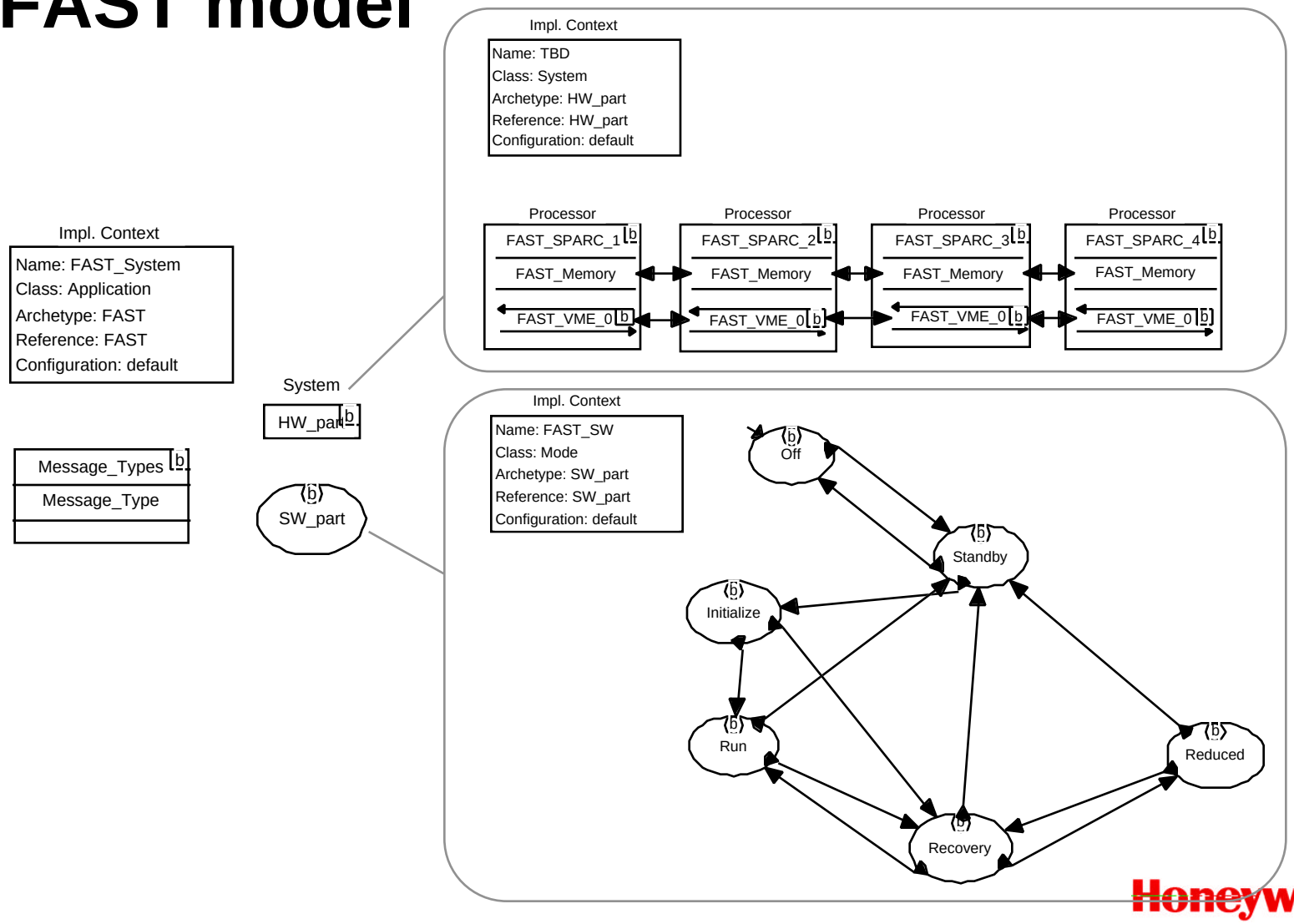


What is MetaH?



Honeywell

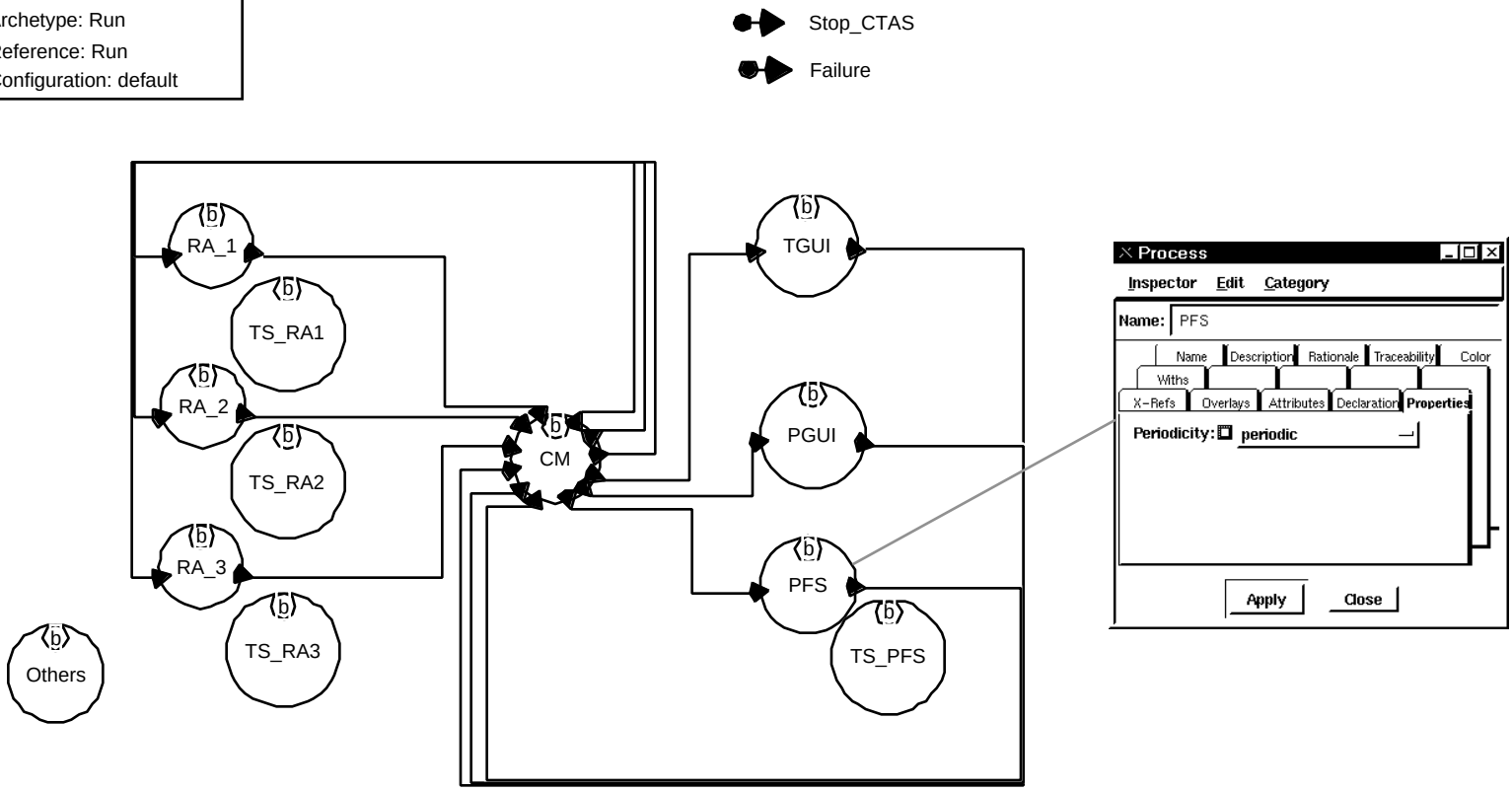
FAST model


Impl. Context
Name: FAST_System
Class: Application
Archetype: FAST
Reference: FAST
Configuration: default
Message_Types
Message_Type
System
HW_part
SW_part
Impl. Context
Name: TBD
Class: System
Archetype: HW_part
Reference: HW_part
Configuration: default
Processor
FAST_SPARC_1
FAST_Memory
FAST_VME_0
Processor
FAST_SPARC_2
FAST_Memory
FAST_VME_0
Processor
FAST_SPARC_3
FAST_Memory
FAST_VME_0
Processor
FAST_SPARC_4
FAST_Memory
FAST_VME_0
Impl. Context
Name: FAST_SW
Class: Mode
Archetype: SW_part
Reference: SW_part
Configuration: default
Off
Standby
Initialize
Run
Reduced
Recovery

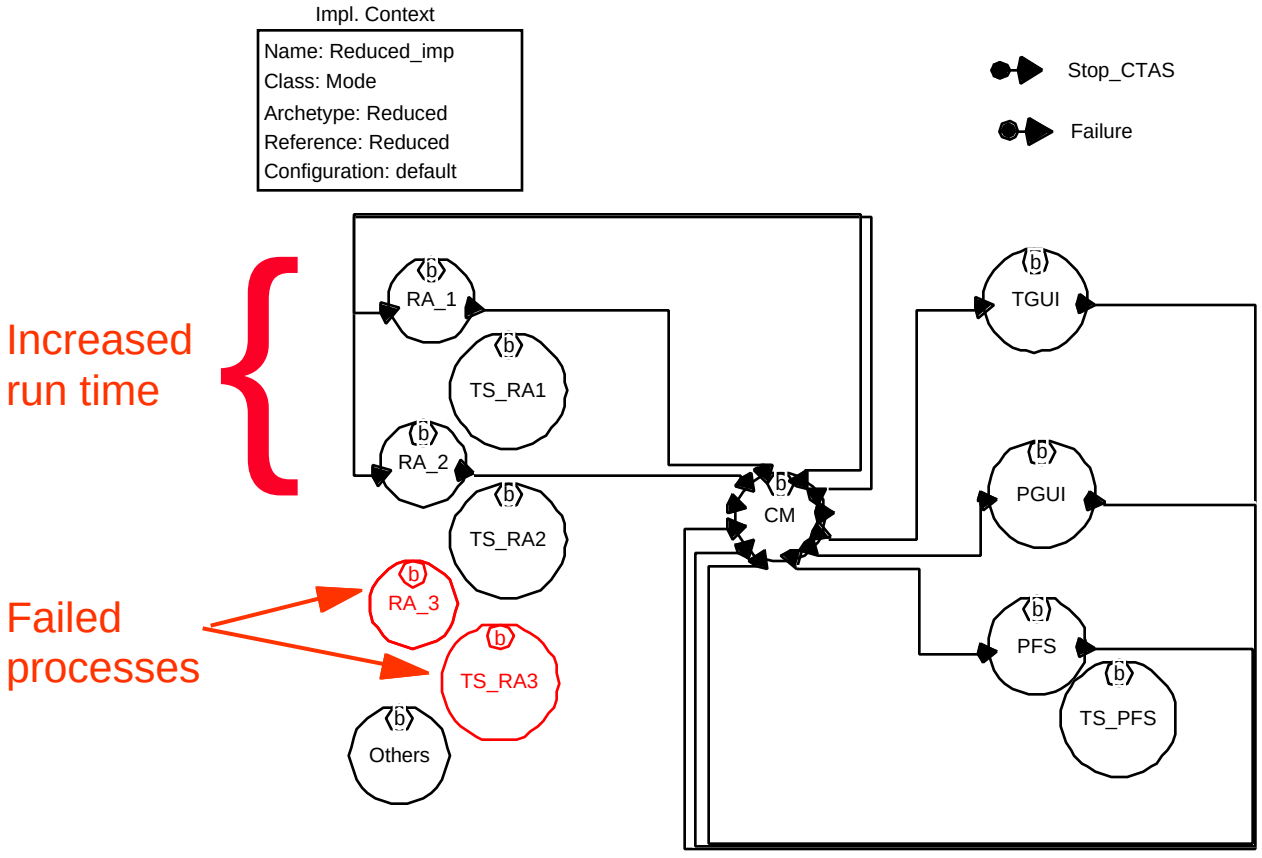
FAST model: Run mode

Impl. Context

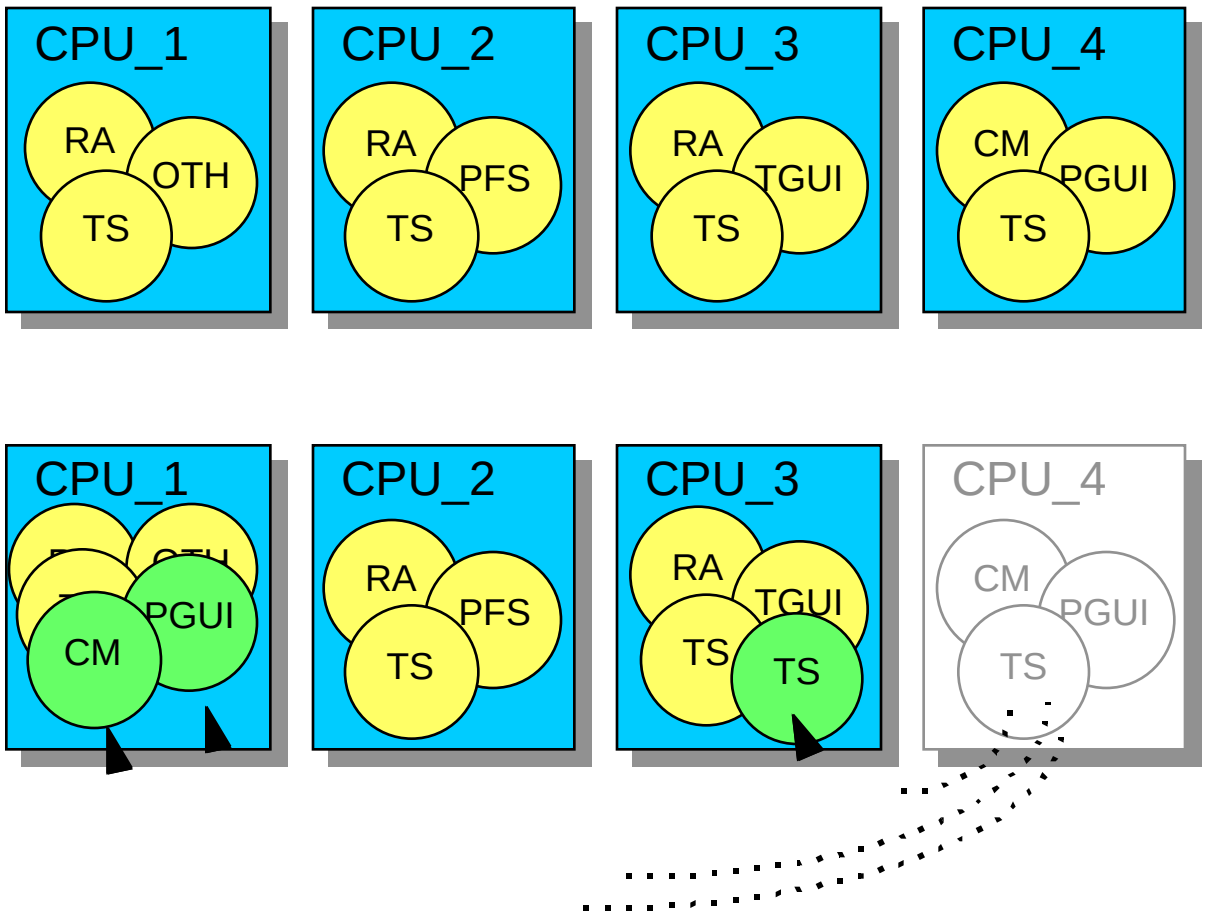
Name: Run_imp
Class: Mode
Archetype: Run
Reference: Run
Configuration: default



FAST Model: Reduced mode

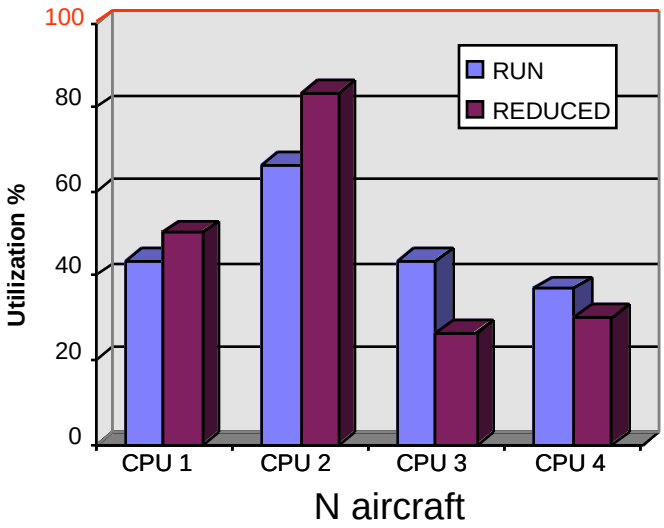


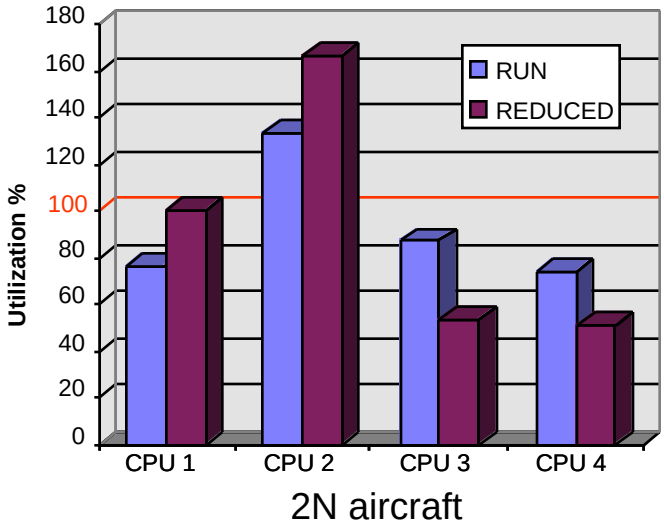
FAST model: HW-SW binding



Honeywell

Performance: Nominal Hardware

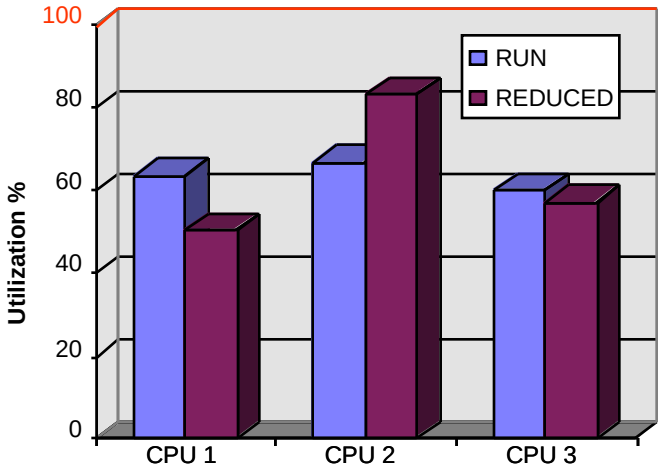




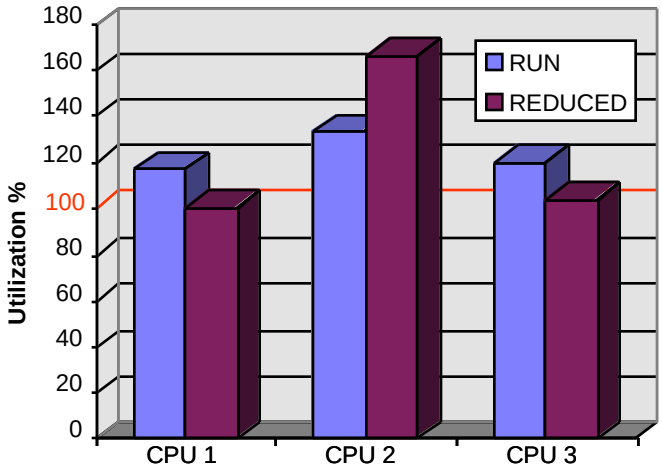
- In Reduced mode, processor load becomes more unbalanced.
  Reduces margin to schedulability
- Doubling number of aircraft results causes scheduling failure
  Unable to meet deadline for updates.

Honeywell

Performance: One node failure



N aircraft



2N aircraft

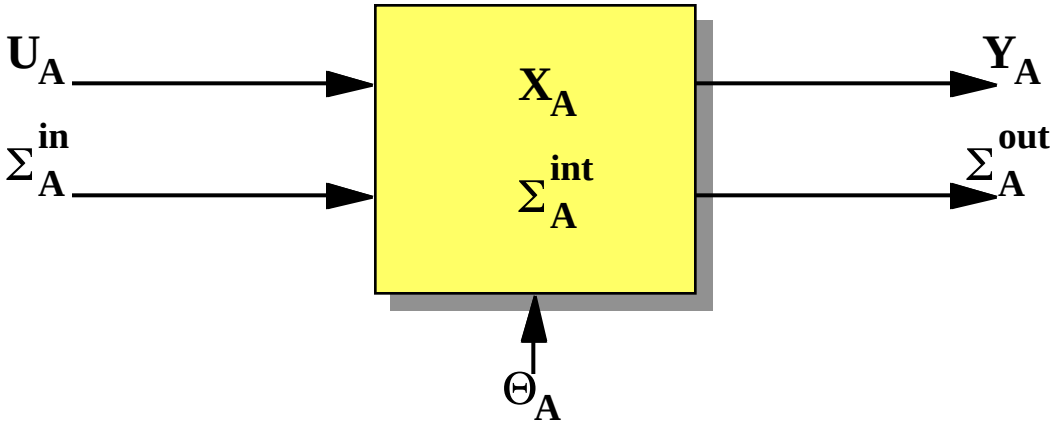
- Load from failed CPU transferred to less busy nodes.
  Reduces margin to schedulability on those nodes.
- Doubling number of aircraft results in scheduling failure.
  Unable to meet deadline for updates.

Honeywell

Other analyses...

- New processs added to system
  - Departure automation
- New capabilities added to existing processes
  - Weather data in route analysis
- Faster cycle times required
  - Fast radar updates or GPS data

Hybrid Input/Output Automata



A hybrid input/output automaton A is defined by

- Input, output and internal typed variables
- Input, output and internal actions
- State space is set of all possible variable values
- Initial conditions
- A set W of trajectories of variables and D of discrete transitions

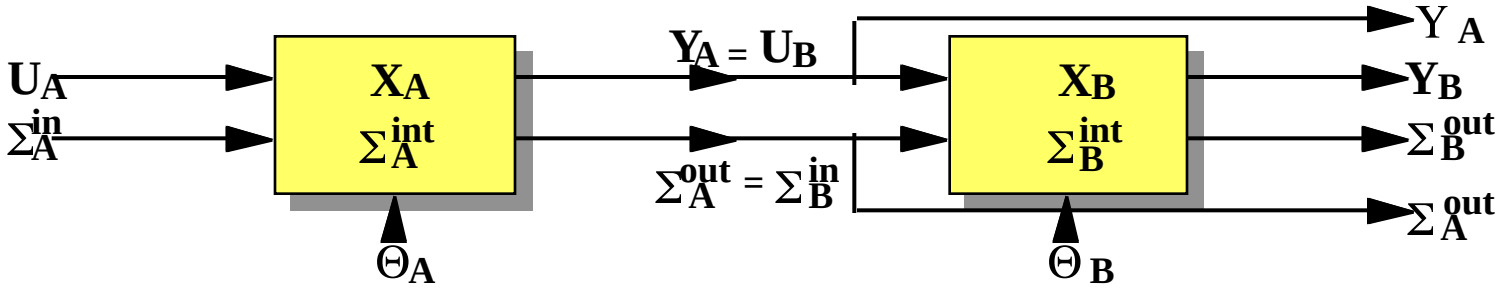
Each action has an associated precondition and effect

An execution of the automaton is α = w1 a1 w2 a2 w3 a3.....

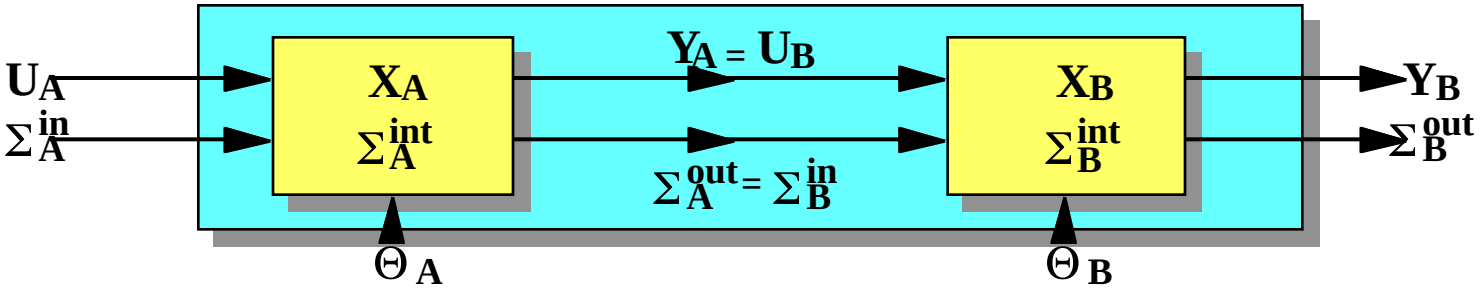
Honeywell

Hybrid Input/Output Automata

Compositions of compatible hybrid automata are hybrid automata



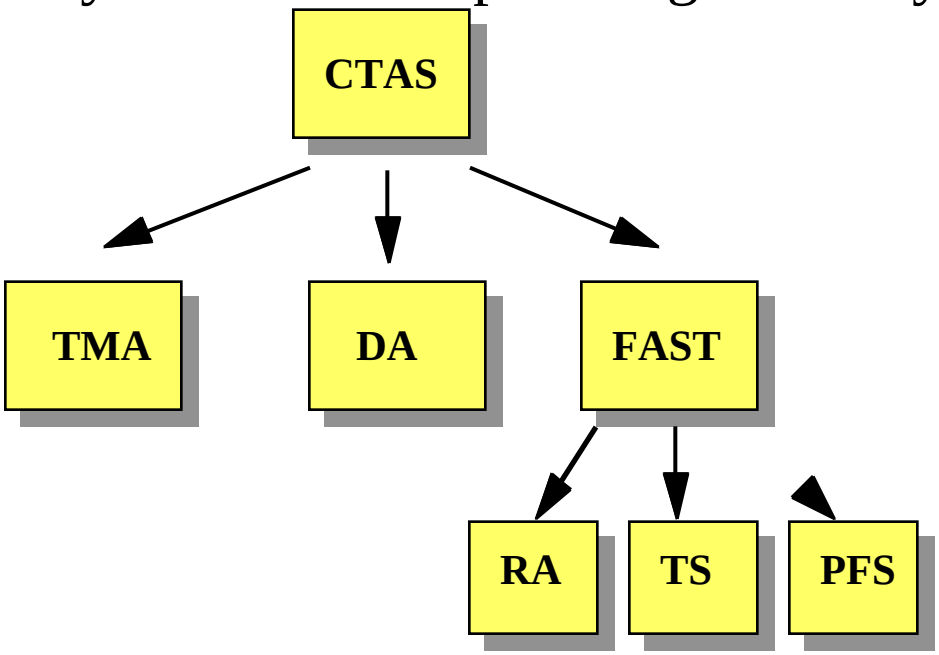
- Variable and action hiding allows building macrocomponents



- Composite system satisfies composite specification

Safety Analysis

How can one analyze such a complex large scale system?



- Step 1 : Top down specification refinement
- Step 2 : Verify that low level systems meet specification
- Step 3 : Abstract behavior of composite system

Honeywell

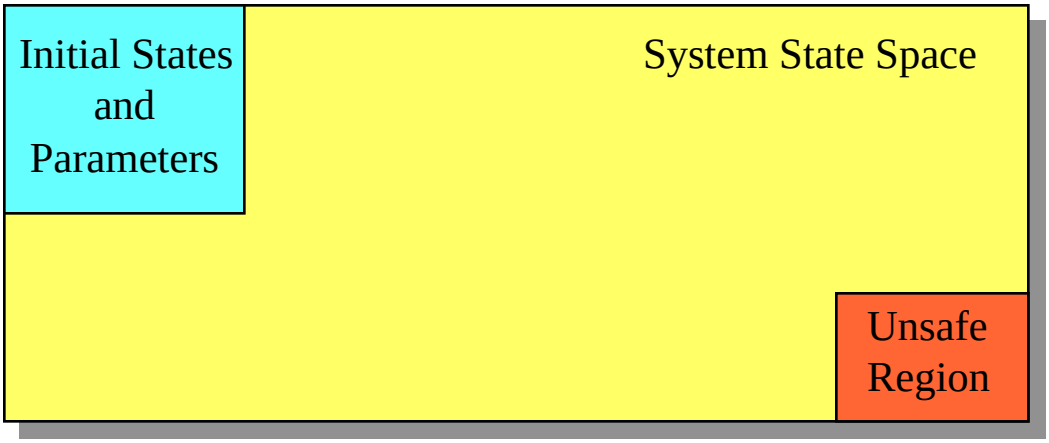
Safety Analysis

Safety specs can be expressed as undesirable state regions

Will aircraft lose separation? Is TRACON capacity exceeded?

Specs can also be formulated using performance monitors

The analysis approach: Forward & Backward Reachability



- Forward : *Verify safety given parameters and initial states or generate trajectory leading to unsafe operation*
- Backward : *Determine which initial states and parameters are reachable from the unsafe region*

Honeywell

Safety Tools

Discrete Systems

- COSPAN (Correctness of communication protocols)
- VIS (Correctness of hardware/software systems)

Timed Systems

- KRONOS (real-time properties of communication networks)
- Timed COSPAN

Hybrid Systems

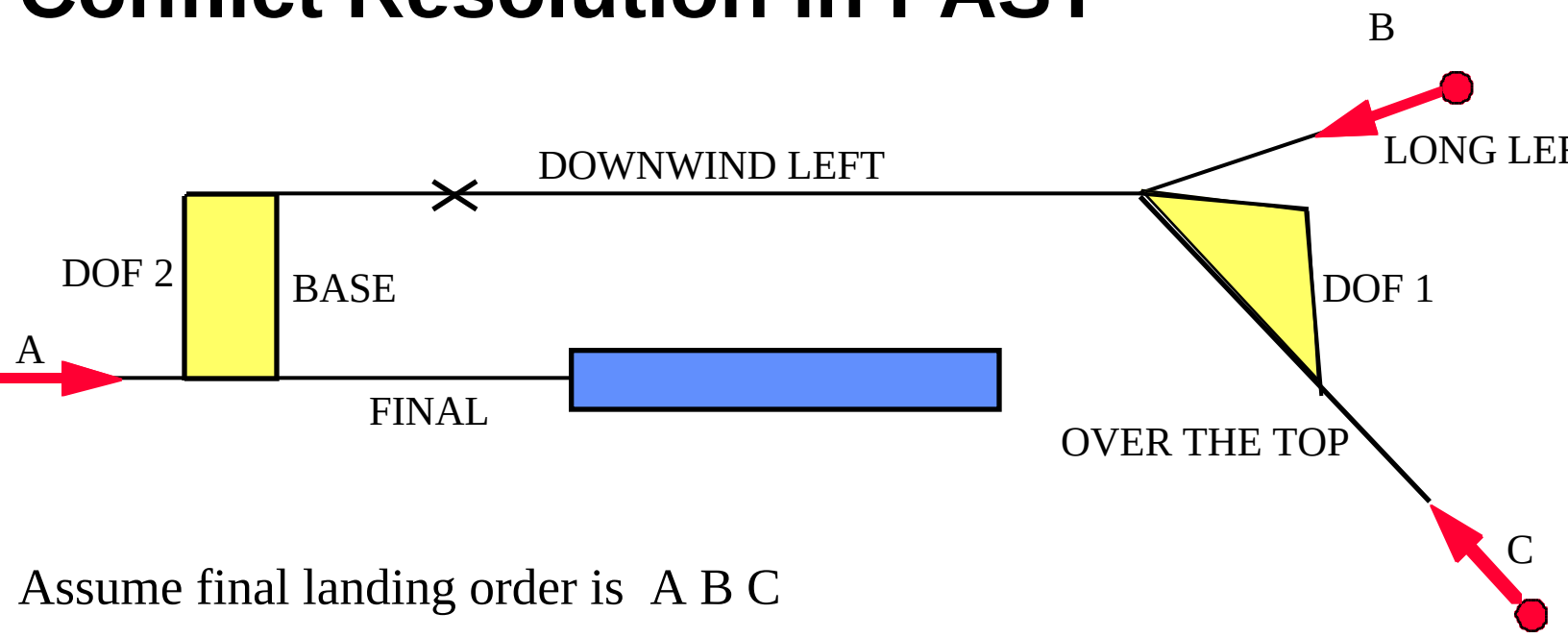
- HyTech (Rectangular Hybrid Systems)

Various Mathematical Tools from

- Systems Theory
- Probability Theory
- Computer Science and Logic

Honeywell

Conflict Resolution in FAST



Assume final landing order is A B C

Potential conflict between B and C on downwind left

Aircraft C must be delayed using 2 degrees of freedom

Speed and altitude profiles dictated by TRACON procedures

Question: For what initial configurations (horizontal and vertical coordinates) of Aircraft C is conflict avoided?

Honeywell

Conclusions

System perspective of safety analysis

Formal Methods Approach

- Modeling, specification and analysis

Safety assessment of NAS is similar conceptually

- Methodology does not depend on CTAS details

Questions are challenging, but are the right ones!