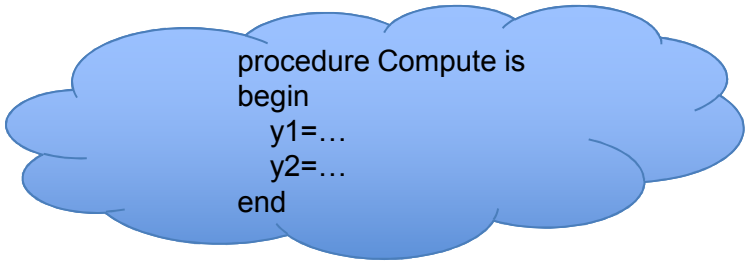
TOWARDS A FORMALLY VERIFIED MODEL-BASED DEVELOPMENT

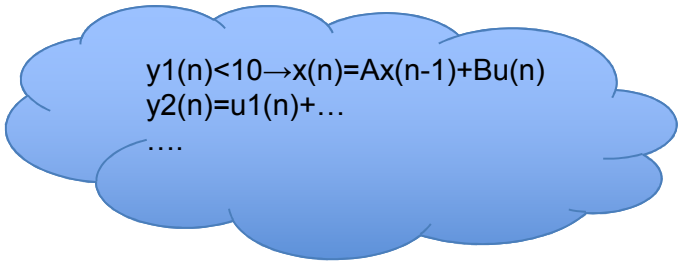
An Industrial Experience

LEONARDO HELICOPTERS

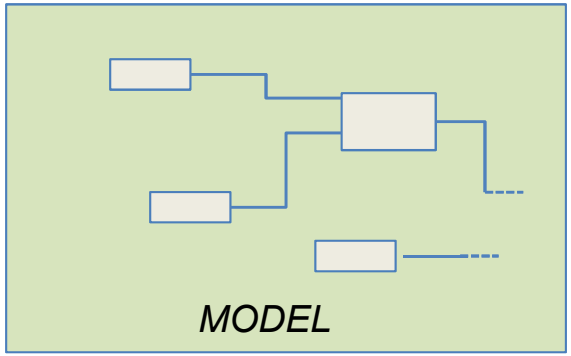
AgustaWestland Products

THE MODEL DUALITY
A Question Of Gestalt-psychologie
What are you seeing looking at the model?





CODE PRODUCTION and TEST



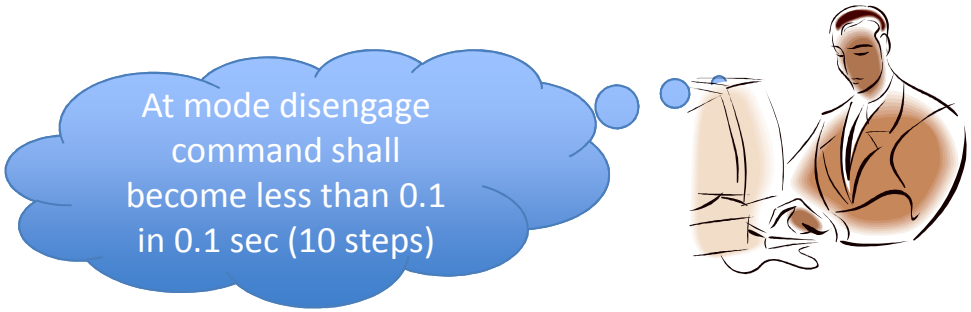
ALGORITHMS DEFINITION and VALIDATION

GOODBYE SOFTWARE

Code Generators allow you to **Shift your focus**

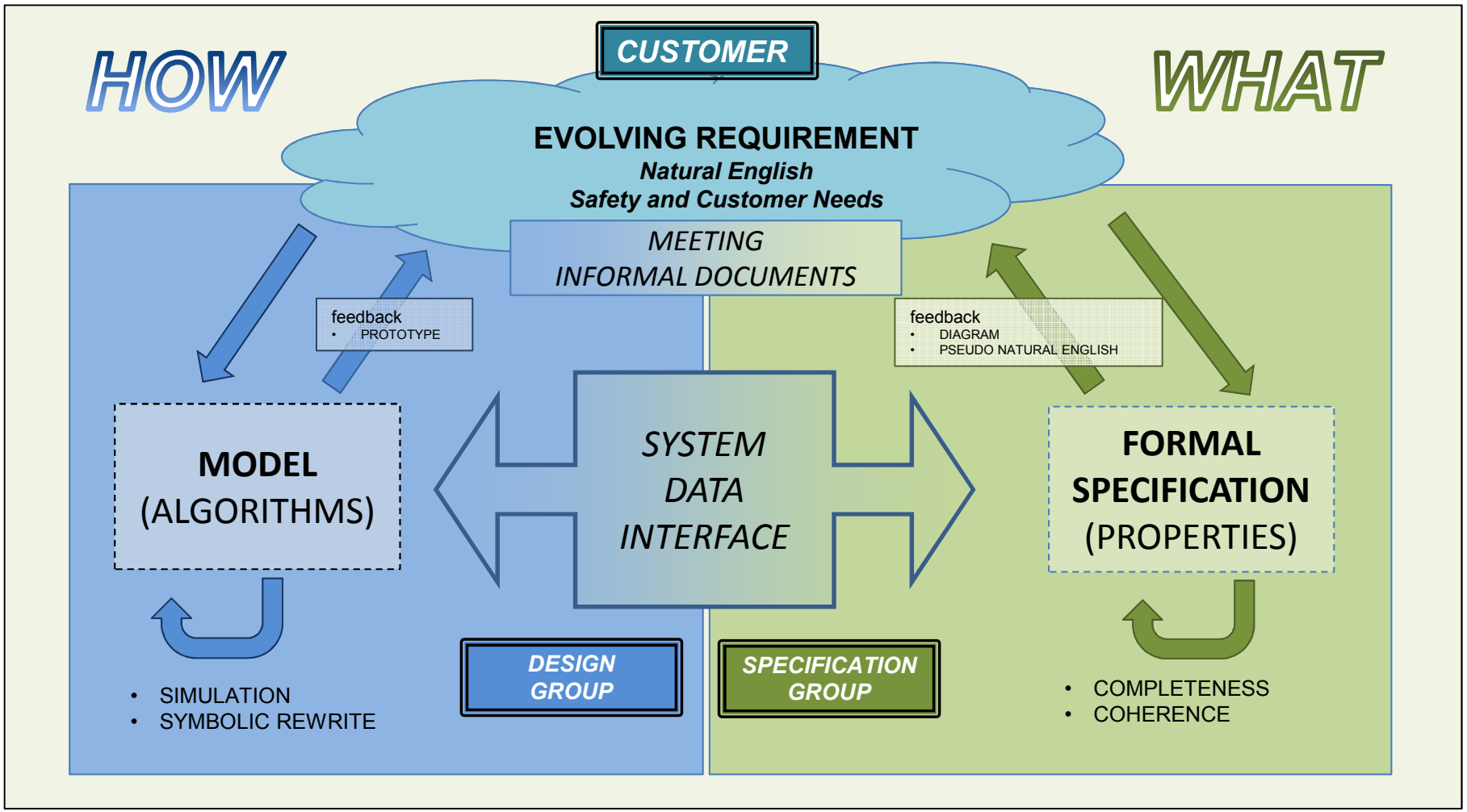
WELCOME MATH

METRIC TEMPORAL LOGIC AS SPECIFICATION LANGUAGE FOR MONITORING AND MODEL CHECKING

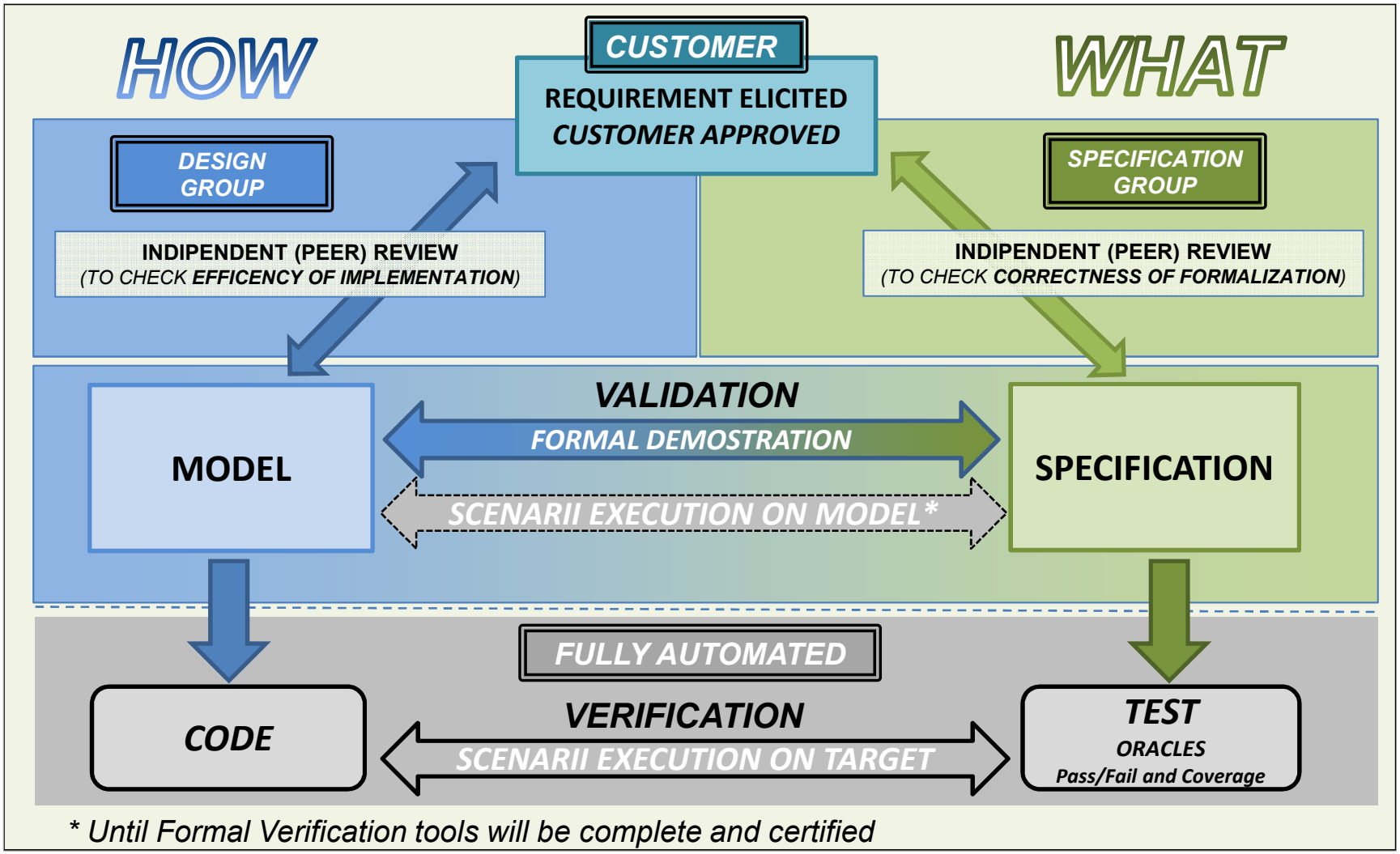


Falling(Mode)=>
Eventually$_{<10}$ (Command<0.1)

PROPOSED METHODOLOGY
DEVELOPMENT



PROPOSED METHODOLOGY
VALIDATION & VERIFICATION



FIRST SUCCESSES WITH LOGIC

SAT SOLVER FOR

- *BOUNDED MODEL CHECKING*
- *UNBOUNDED MODEL CHECKING*
  - *DIAMETER COMPUTATION*
  - *K-INDUCTION*

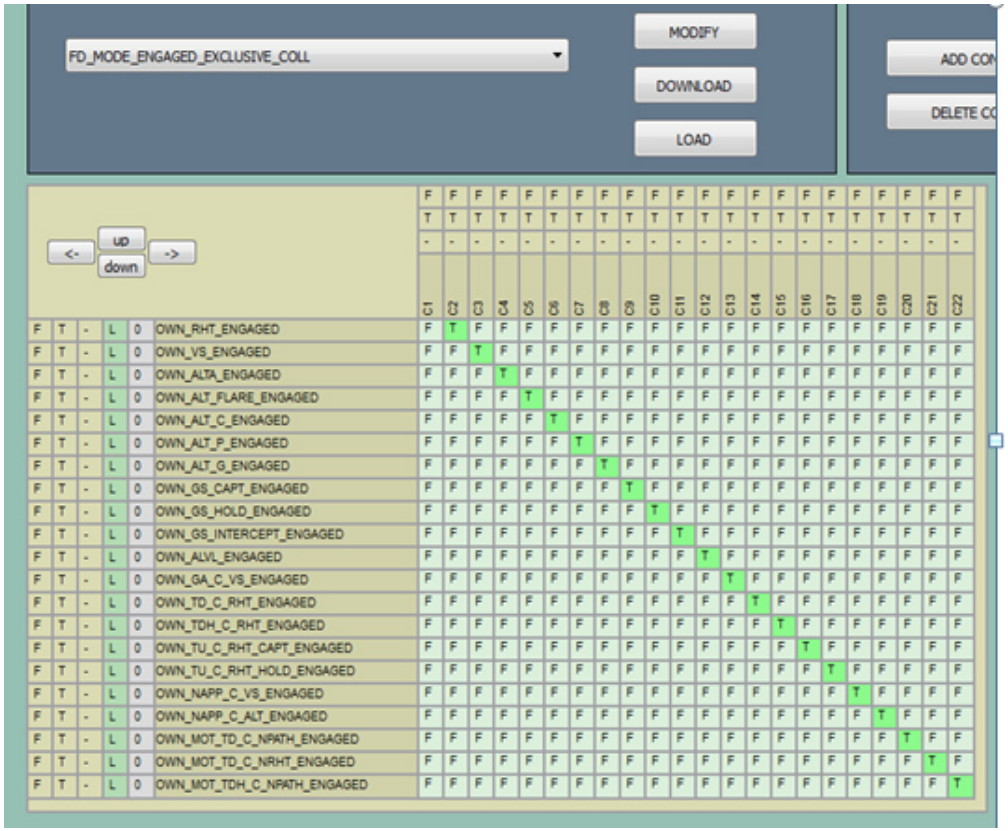
This model implement *Upper Model Logic for AW 101 Autopilot*

This is a very ***complex logic sequential*** circuit involving

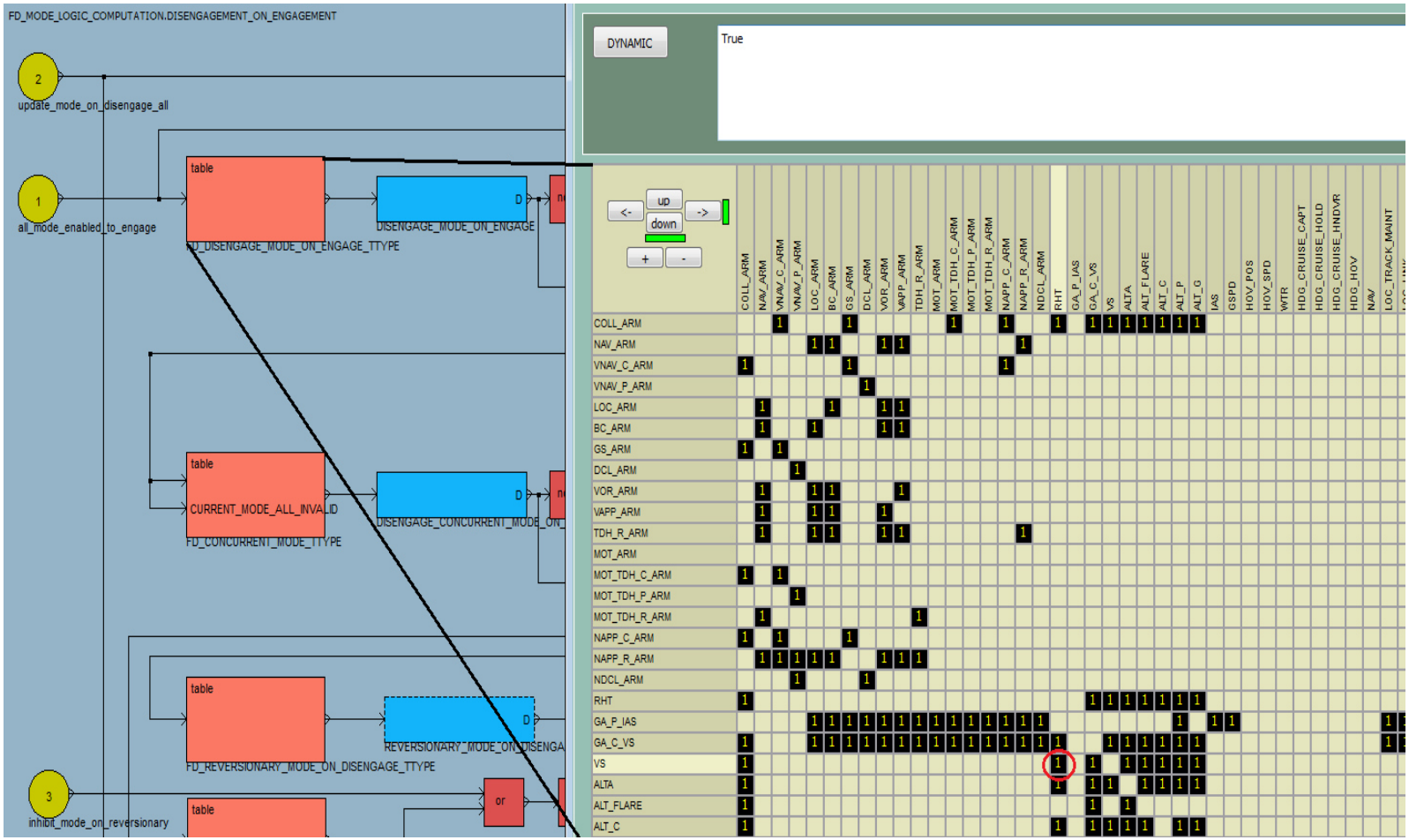
353 Inputs
181 Memories
876 Outputs

Note: states are interconnected *i.e*. is not possible to create more than one indipendent and separate state spaces.
Automaton ***specification*** of each mode involves other modes ***previous and current value*** making it highly implicit.
This makes model synthesis (and verification) a very challenging activity.

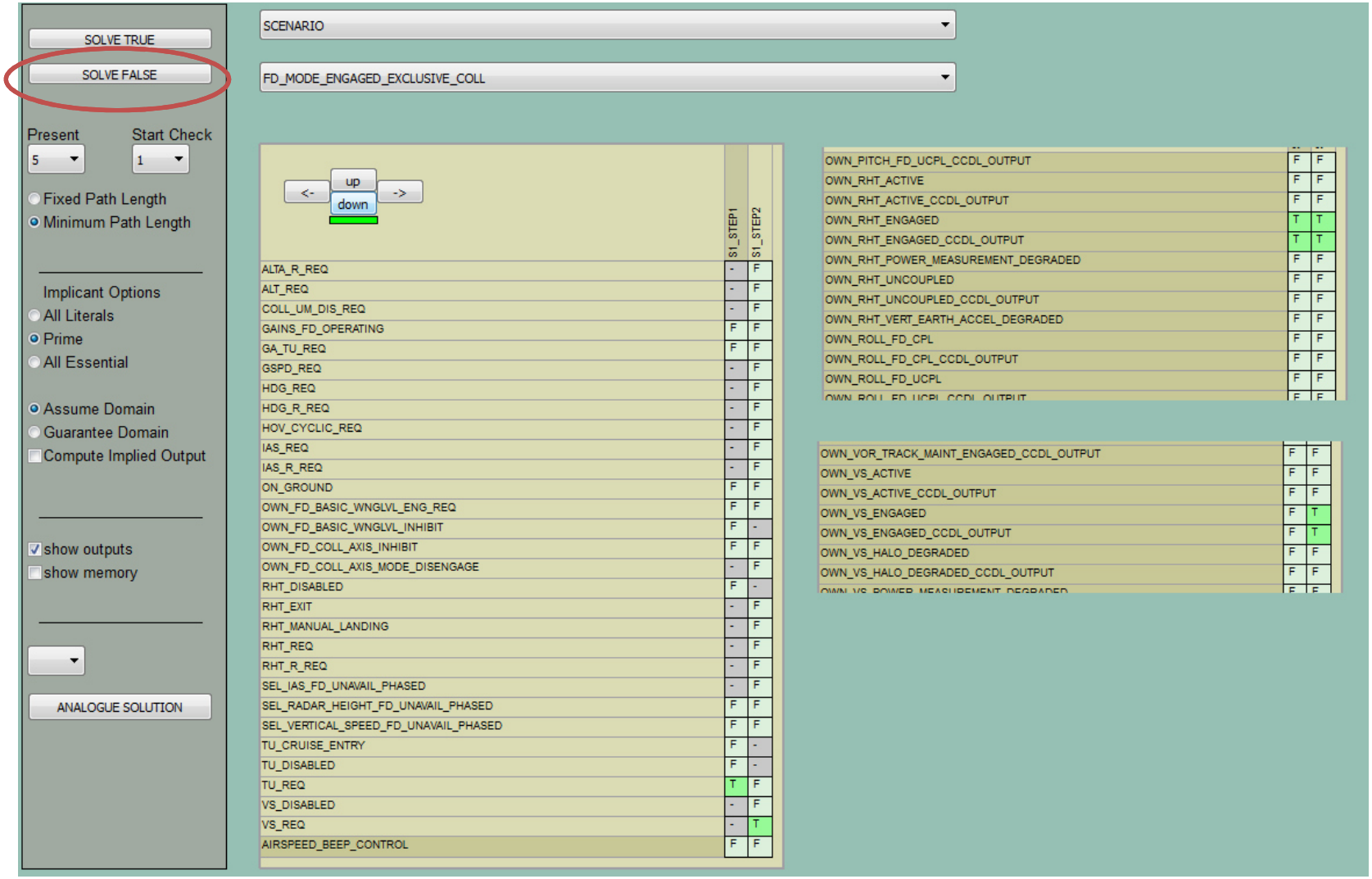
CHECK FOR EXCLUSIVE MODE ENGAGEMENT ON COLLECTIVE AXIS PROPERTY



LOOKING FOR AN ERROR (ad hoc inserted)
(removed automatic disengage of RHT at VS engagement)



COUNTEREXAMPLE FOUND IN JUST FEW SECONDS

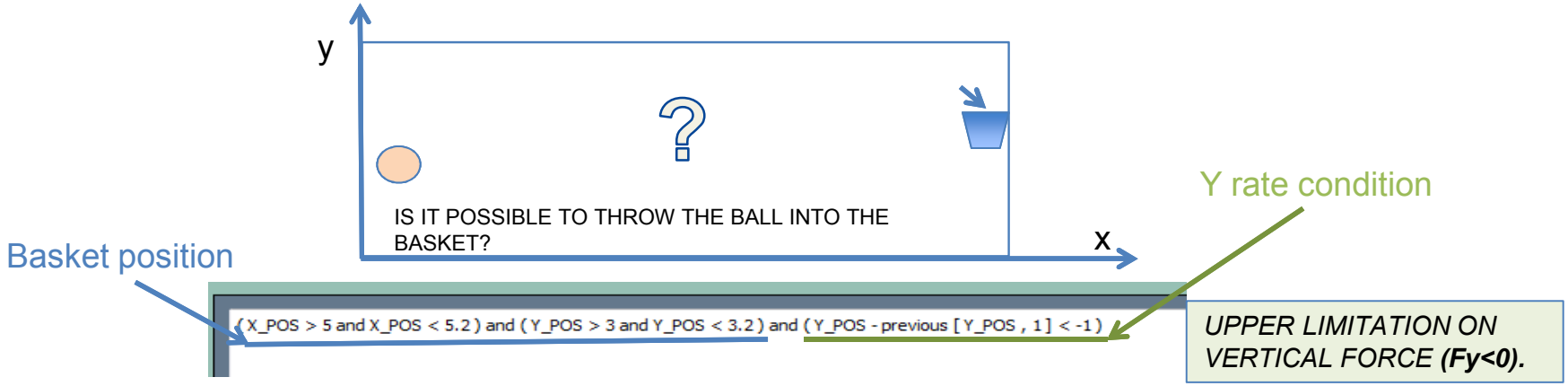


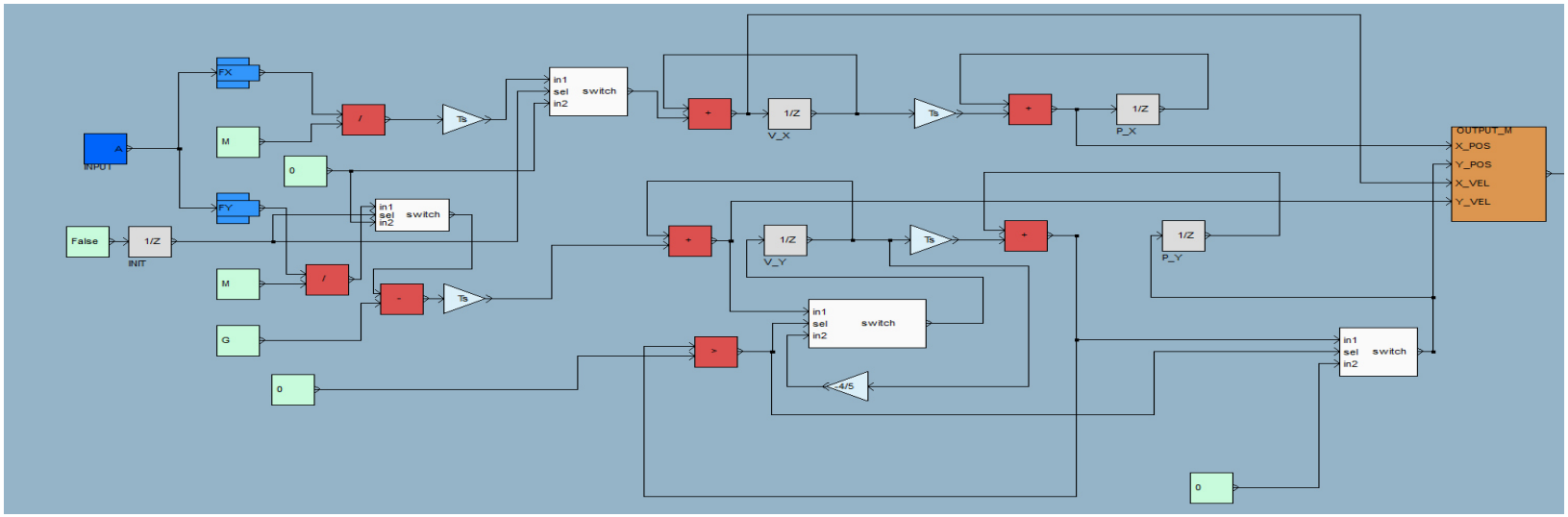
TROUBLE WITH DYNAMIC (PWA)

SMT SOLVER (or MILP) FOR

- ***BOUNDED MODEL CHECKING*** *(Computational Limitation On Steps Number)*
- ***UNBOUNDED MODEL CHECKING***
  - ***DIAMETER COMPUTATION*** *(Infinite)*
  - ***K-INDUCTION*** *(No Termination Guarantee)*

MODEL VALIDATION
A TOY EXAMPLE



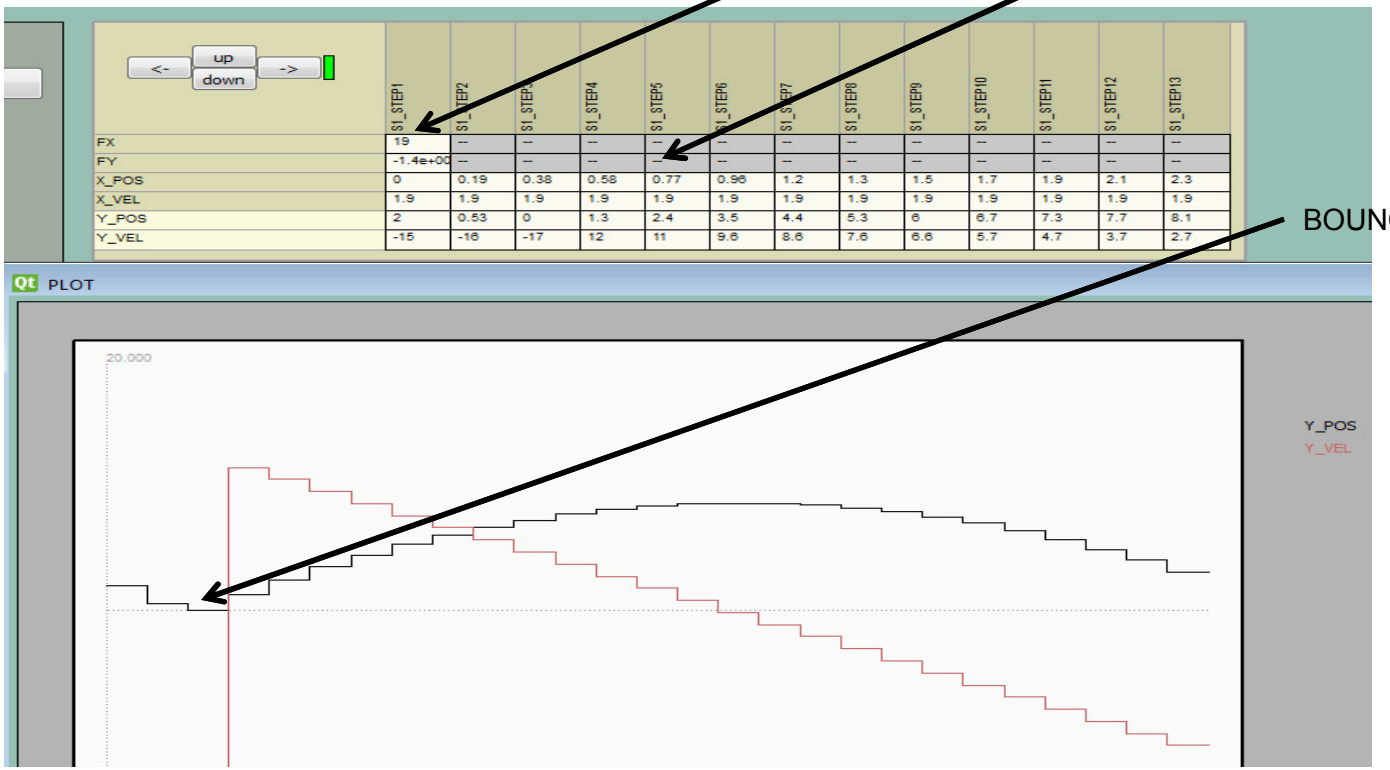


MODEL VALIDATION
A TOY EXAMPLE

FORCE TO APPLY

AFTER BALL IS THROWN
FORCE IS ININFLUENT

BOUNCING ON FLOOR



	S1_STEP1	S1_STEP2	S1_STEP3	S1_STEP4	S1_STEP5	S1_STEP6	S1_STEP7	S1_STEP8	S1_STEP9	S1_STEP10	S1_STEP11	S1_STEP12	S1_STEP13
FX	19	--	--	--	--	--	--	--	--	--	--	--	--
FY	-1.4e+00	--	--	--	--	--	--	--	--	--	--	--	--
X_POS	0	0.19	0.38	0.58	0.77	0.96	1.2	1.3	1.5	1.7	1.9	2.1	2.3
X_VEL	1.9	1.9	1.9	1.9	1.9	1.9	1.9	1.9	1.9	1.9	1.9	1.9	1.9
Y_POS	2	0.53	0	1.3	2.4	3.5	4.4	5.3	6	6.7	7.3	7.7	8.1
Y_VEL	-15	-16	-17	12	11	9.6	8.6	7.6	6.6	5.7	4.7	3.7	2.7

HOW TO EXTEND BOUNDED MODEL CHECKING HORIZON?
HOW TO DEMONSTRATE THAT PROPERTY ALWAYS HOLDS?

REACHABILITY IS THE SOLUTION?

Current Collaboration with POLIMI

THANK **YOU** FOR YOUR ATTENTION

LEONARDO HELICOPTERS

AgustaWestland Products