

TOWARDS A FORMALLY VERIFIED MODEL-BASED DEVELOPMENT

An Industrial Experience





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



Company General Use







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

										I	MODIFY							ı		P								
	5	0_1	100	E_B	VGAGED_EXCLUSIVE_COLL						•			P					٠			L		Ŀ		4	00	C
														L	DX	JWN	LOA	0				L		r				
														r					1							DE	LET	
														L		LO	AD		4			L						
	-		-	-		F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	T
						т	Т	т	т	T	т	т	т	T	т	Т	т	Т	т	т	т	Т	Т	т	т	т	T	1
	_		u			-	-	•	-	-	-	-	-	-	•	-	-	-	-	-	•	-	-	-	-	-	-	1
	<	-	dor	vn.	->	C1	8	8	3	8	8	C1	8	8	C10	C11	C12	C13	C14	C15	C16	C17	C18	C19	C20	8	C23	
F	т		L	0	OWN_RHT_ENGAGED	F	т	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	
F	т	-	L	0	OWN_VS_ENGAGED	F	F	т	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	
F	т	-	L	0	OWN_ALTA_ENGAGED	F	F	F	т	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	
F	т	-	L	0	OWN_ALT_FLARE_ENGAGED	F	F	F	F	т	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	
F	т	-	L	0	OWN_ALT_C_ENGAGED	F	F	F	F	F	т	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	
F	т	-	L	0	OWN_ALT_P_ENGAGED	F	F	F	F	F	F	т	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	
F	т	-	L	0	OWN_ALT_G_ENGAGED	F	F	F	F	F	F	F	т	F	F	F	F	F	F	F	F	F	F	F	F	F	F	
F	т	-	L	0	OWN_GS_CAPT_ENGAGED	F	F	F	F	F	F	F	F	т	F	F	F	F	F	F	F	F	F	F	F	F	F	
F	т	-	L	0	OWN_GS_HOLD_ENGAGED	F	F	F	F	F	F	F	F	F	т	F	F	F	F	F	F	F	F	F	F	F	F	
F	т		L	0	OWN_GS_INTERCEPT_ENGAGED	F	F	F	F	F	F	F	F	F	F	Т	F	F	F	F	F	F	F	F	F	F	F	
F	т	-	L	0	OWN_ALVL_ENGAGED	F	F	F	F	F	F	F	F	F	F	F	т	F	F	F	F	F	F	F	F	F	F	
F	т	-	L	0	OWN_GA_C_VS_ENGAGED	F	F	F	F	F	F	F	F	F	F	F	F	т	F	F	F	F	F	F	F	F	F	J
F	т	-	L	0	OWN_TD_C_RHT_ENGAGED	F	F	F	F	F	F	F	F	F	F	F	F	F	т	F	F	F	F	F	F	F	F	
F	т	-	L	0	OWN_TDH_C_RHT_ENGAGED	F	F	F	F	F	F	F	F	F	F	F	F	F	F	т	F	F	F	F	F	F	F	j
F	т	-	L	0	OWN_TU_C_RHT_CAPT_ENGAGED	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	т	F	F	F	F	F	F	j
F	т	-	L	0	OWN_TU_C_RHT_HOLD_ENGAGED	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	т	F	F	F	F	F	
F	т	-	L	0	OWN_NAPP_C_VS_ENGAGED	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	т	F	F	F	F	
F	т	-	L	0	OWN_NAPP_C_ALT_ENGAGED	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	т	F	F	F	
F	Т	•	L	0	OWN_MOT_TD_C_NPATH_ENGAGED	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	Т	F	F	J
F	Т	-	L	0	OWN_MOT_TD_C_NRHT_ENGAGED	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	Т	F	J
F	Т	-	L	0	OWN_MOT_TDH_C_NPATH_ENGAGED	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	Т	1



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



Agusta Westland Products .



COUNTEREXAMPLE FOUND IN JUST FEW SECONDS

SOLVE TRUE	SCENARIO		•								
SOLVE FALSE	FD_MODE_ENGAGED_EXCLUSIVE_COLL										
Present Start Check 5 • 1 • Fixed Path Length • Minimum Path Length	<- up down ->	81_STEP1 S1_STEP2	OWN_PITCH_FD_UCPL_CCDL_OUTPUT OWN_RHT_ACTIVE OWN_RHT_ACTIVE_CCDL_OUTPUT OWN_RHT_ENGAGED OWN_RHT_ENGAGED_CCDL_OUTPUT OWN_RHT_ENGAGED_CCDL_OUTPUT	F F F F F F T T T T F F							
Implicant Options All Literals Prime	ALTA_R_REQ ALT_REQ COLL_UM_DIS_REQ GAINS_FD_OPERATING GA_TU_REQ	- F - F - F - F - F	OWN_RHT_UNCOUPLED OWN_RHT_UNCOUPLED_CCDL_OUTPUT OWN_RHT_VERT_EARTH_ACCEL_DEGRADED OWN_ROLL_FD_CPL								
All Essential Assume Domain Guarantee Domain Compute Implied Output	GSPD_REQ HDG_REQ HDG_R_REQ HOV_CYCLIC_REQ IAS_REQ	- F - F - F - F - F	OWN_ROLL_FD_UCPL								
	IAS_R_REQ ON_GROUND OWN_FD_BASIC_WNGLVL_ENG_REQ OWN_FD_BASIC_WNGLVL_INHIBIT OWN_FD_COLL_AXIS_INHIBIT	- F F F F F F - F F	OWN_VS_ACTIVE OWN_VS_ACTIVE_CCDL_OUTPUT OWN_VS_ENGAGED OWN_VS_ENGAGED_CCDL_OUTPUT OWN_VS_HALO_DEGRADED	F F F F F T F T F T							
show memory	OWN_FD_COLL_AXIS_MODE_DISENGAGE RHT_DISABLED RHT_EXIT RHT_MANUAL_LANDING RHT_REQ	- F F - - F - F - F	OWN_VS_HALO_DEGRADED_CCDL_OUTPUT	F F							
ANALOGUE SOLUTION	RHT_R_REQ SEL_IAS_FD_UNAVAIL_PHASED SEL_RADAR_HEIGHT_FD_UNAVAIL_PHASED SEL_VERTICAL_SPEED_FD_UNAVAIL_PHASED	- F - F F F F F									
	TU_CRUISE_ENTRY TU_DISABLED TU_REQ VS_DISABLED VS_REQ ANDRESD BEER CONTROL	F - F - F - F - F F F F									
	AIRSPEED_BEEP_CONTROL	F F									



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









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

REACHABILITY IS THE SOLUTION?

Current Collaboration with POLIMI

14





AgustaWestland Products

Ċ.

Company General Use