Formal Design and Safety Analysis of AIR6110 Wheel Brake System

Revisiting AIR6110 with formal methods

M. Bozzano[1] , A. Cimatti[1] , **A. Fernandes Pires[1]** , D. Jones[2] ,
G. Kimberly[2] , T. Petri[2] , R. Robinson[2] , and S. Tonetta[1]

[1]Fondazione Bruno Kessler (FBK), Italy
[2]The Boeing Company,USA

July 23rd, 2015

Table of contents

Table of contents

AIR 6110 Wheel Brake System

- Aerospace Information Report 6110
  - Contiguous Aircraft/System Development Process Example
- Hypothetical dual-engine aircraft
  - 300-350 passengers
  - 5 hours of flight max
- Focus on the Wheel Brake System (WBS)
  - Braking function for the two main landing gears
    - 4-wheels landing gear
    - Independently controlled

AIR 6110 Wheel Brake System

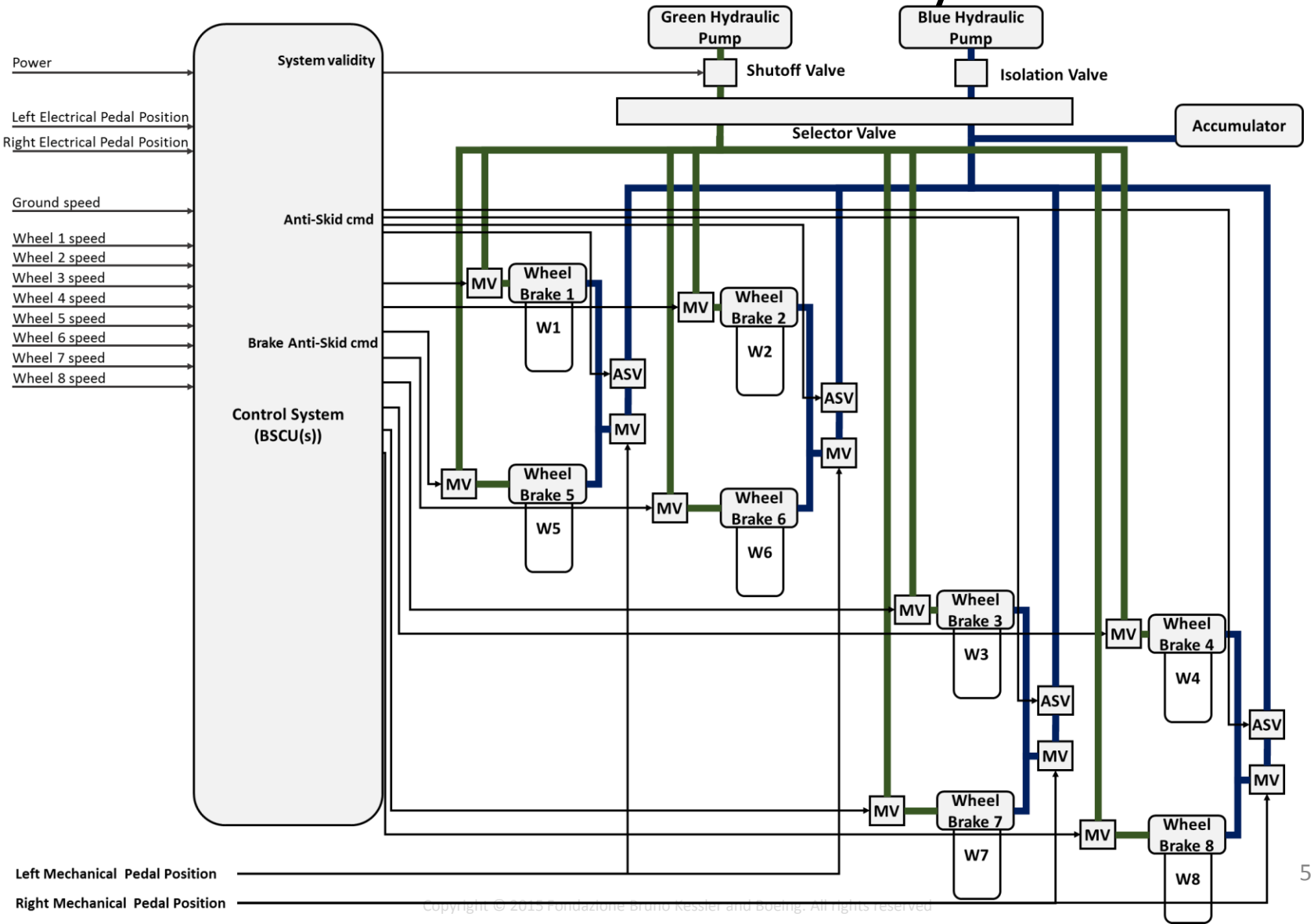
- Main features
  - Hydraulic brake electrically or mechanically controlled braking
  - Anti-skid function
  - Redundancy in the hydraulic and control system

AIR 6110 Wheel Brake System

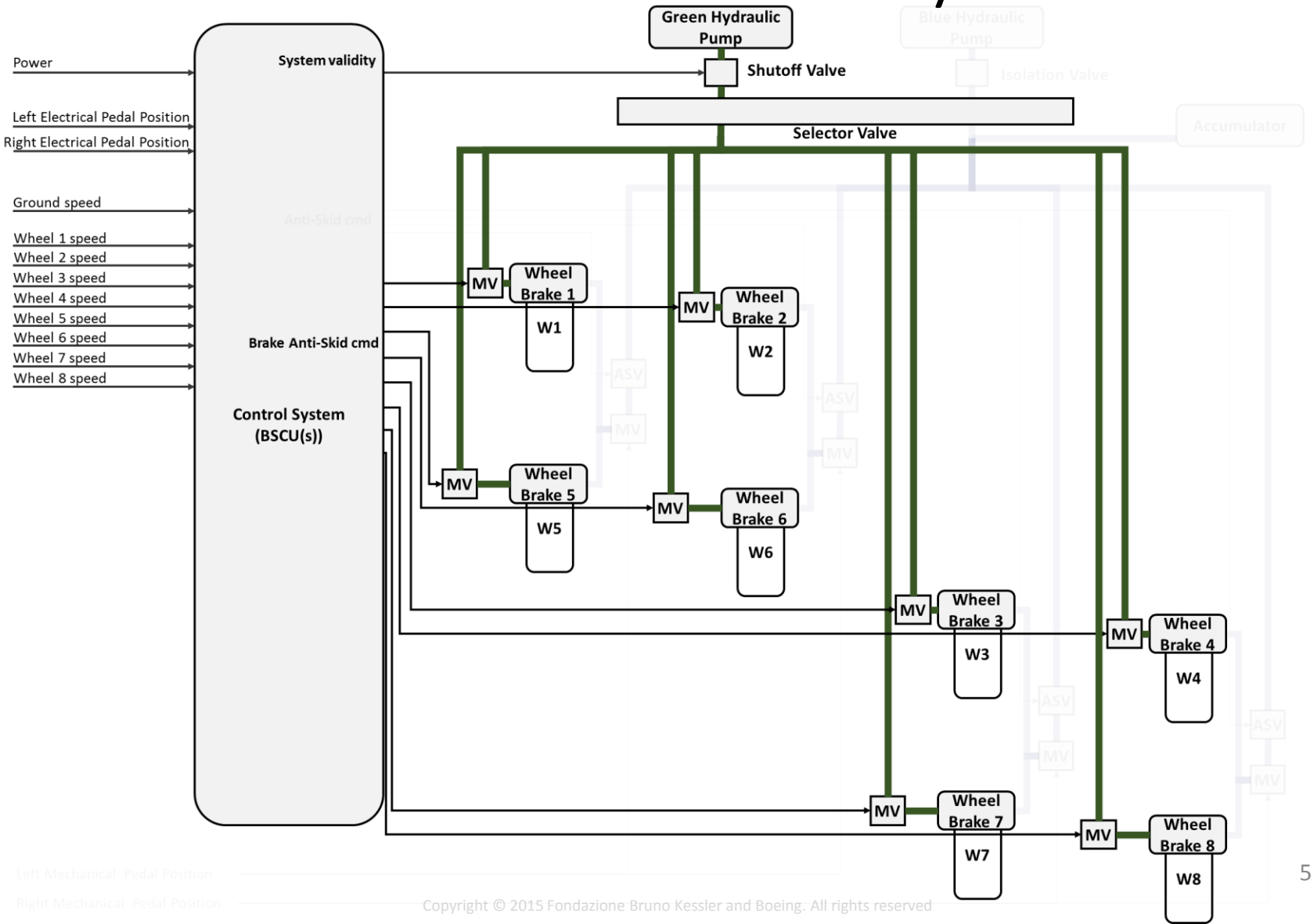
- Main features
  - Hydraulic brake electrically or mechanically controlled braking
  - Anti-skid function
  - Redundancy in the hydraulic and control system

		Wheel Brake System		
		Normal Mode *(Primary pressure source)*	**Alternate Mode** *(Secondary pressure source)*	**Emergency Mode** *(Finite-reserve accumulator)*
Control system	**Valid**	• $Brake_{Elec}$ • Individual AntiSkid	• $Brake_{Mech}$ • Paired-AntiSkid	• $Brake_{Mech}$ • Paired-AntiSkid
	Invalid	N/A	$Brake_{Mech}$	$Brake_{Mech}$

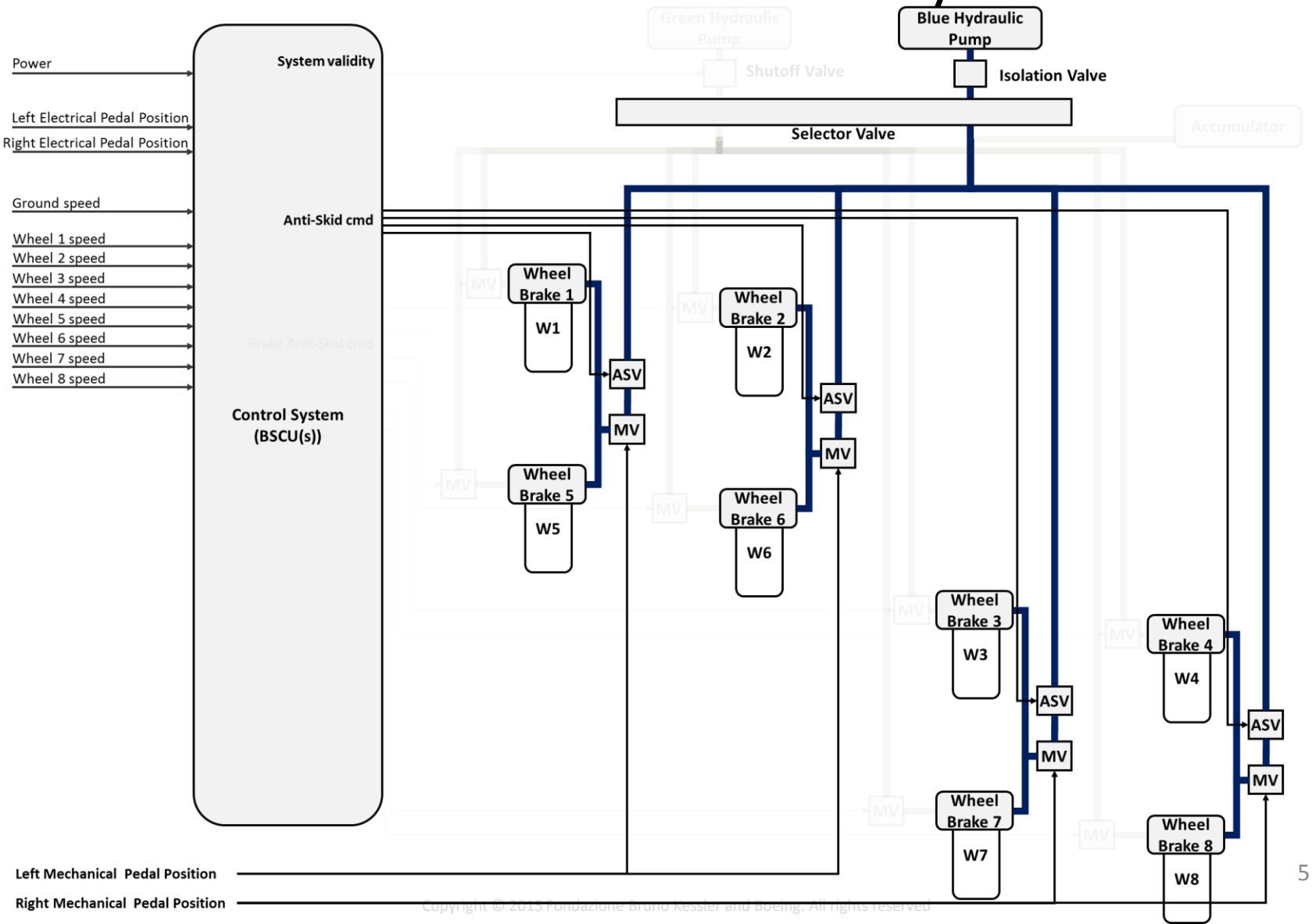
AIR 6110 Wheel Brake System



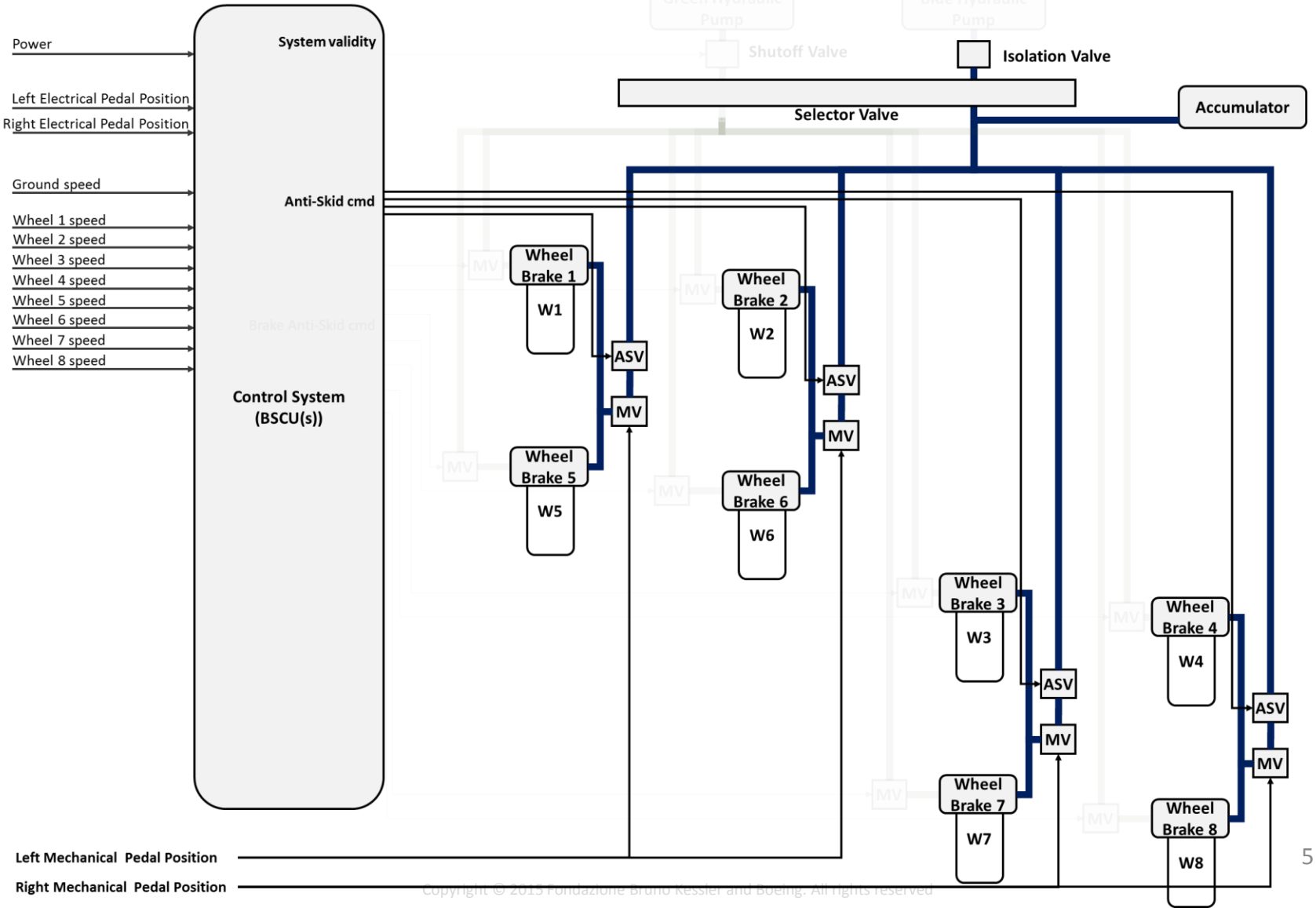
AIR 6110 Wheel Brake System



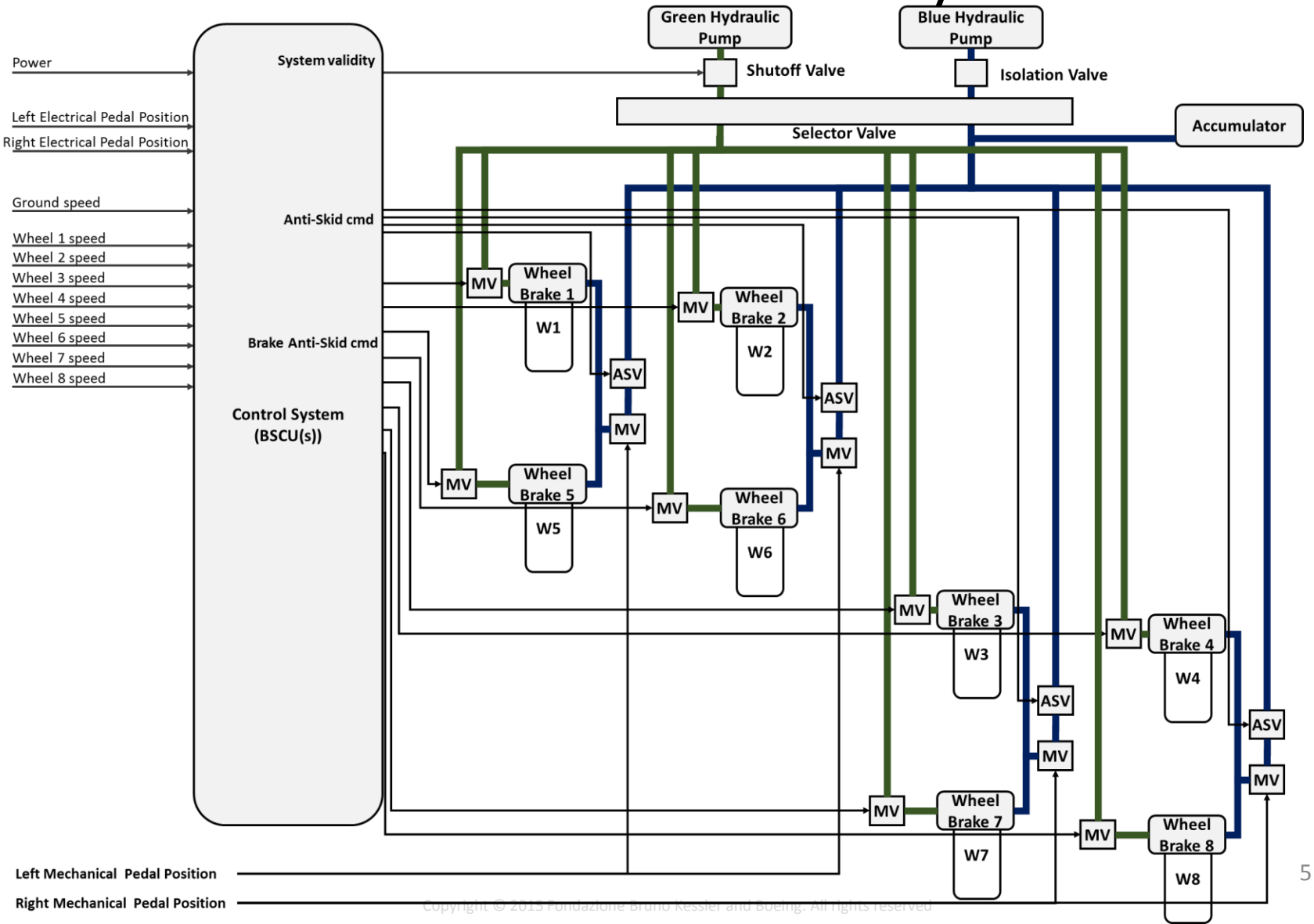
AIR 6110 Wheel Brake System



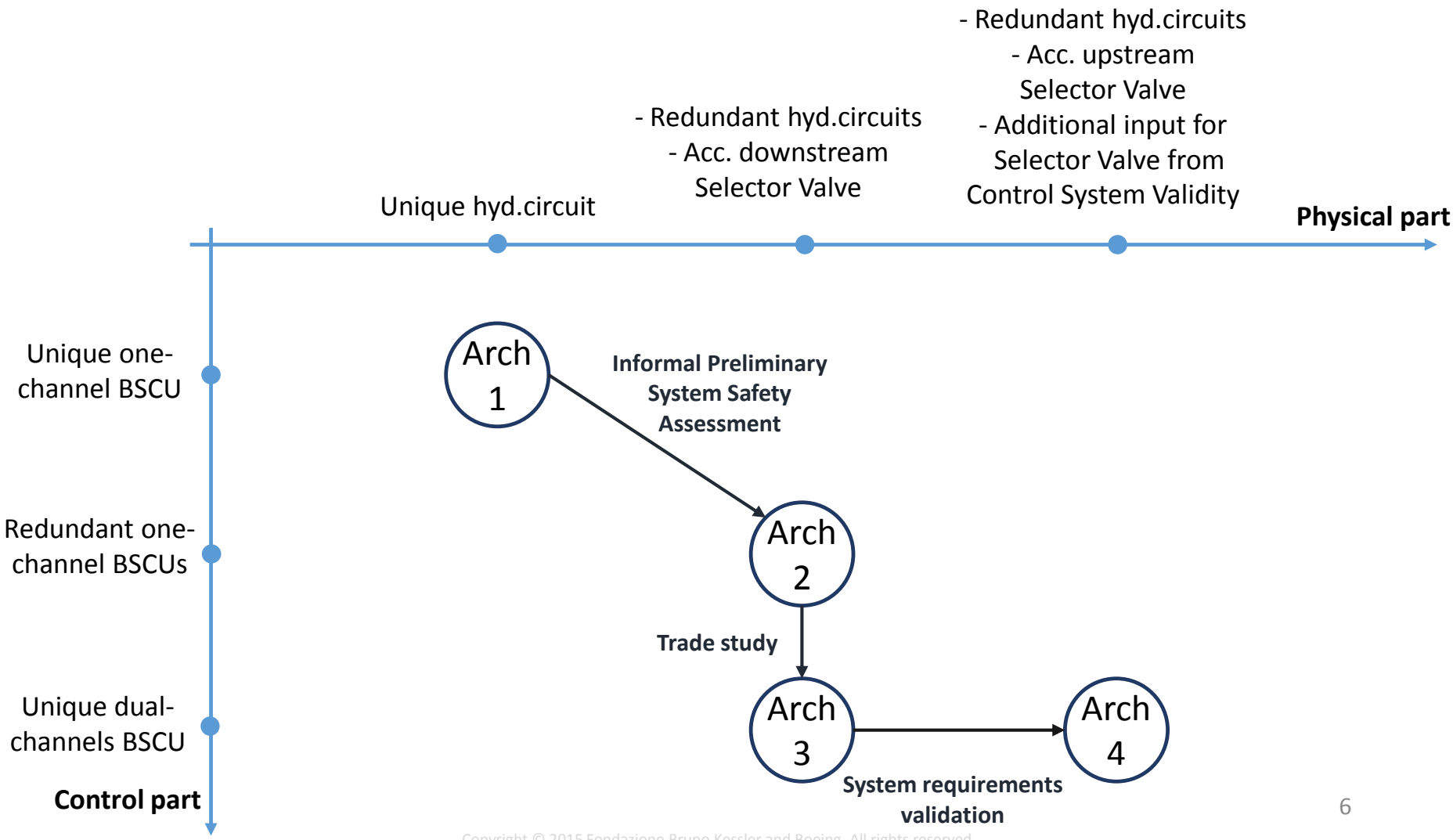
AIR 6110 Wheel Brake System



AIR 6110 Wheel Brake System



AIR 6110 Process



AIR 6110 WBS requirements

- Requirements sample:
- **S18-WBS-R-0321:** Loss of all wheel braking (unannunciated or annunciated) during landing or RTO shall be extremely remote
- **S18-WBS-R-0322:** Asymmetrical loss of wheel braking coupled with loss of rudder or nose wheel steering during landing or RTO shall be extremely remote
- **S18-WBS-0323:** Inadvertent wheel braking with all wheels locked during takeoff roll before V1 shall be extremely remote
- **S18-WBS-R-0324:** Inadvertent wheel braking of all wheels during takeoff roll after V1 shall be extremely improbable
- **S18-WBS-R-0325:** Undetected inadvertent wheel braking on one wheel w/o locking during takeoff shall be extremely improbable

Table of contents

Beyond Model Checking

- Application of formal methods
  - ensuring the design is correct
    - Model-checking

$$M \models \varphi$$

Beyond Model Checking

- Application of formal methods
  - ensuring the design is correct
    - Model-checking

$$M \models \varphi$$

NOT SUFFICIENT HERE

NEED TO ENSURE THE ROBUSTNESS AGAINST FAILURE CONDITIONS

Safety Assessment

- Safety Assessment
  - *"The safety assessment process provides a methodology to evaluate the design of systems, and to determine that the associated hazards have been properly addressed."*
  - Process described in:
    - ARP4754A: Guidelines for Development of Civil Aircraft and Systems
    - ARP4761: Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment

Safety Assessment

- Used in AIR6110 by means of analyses and reviews
- If applied with formal methods
  1. Fault extension

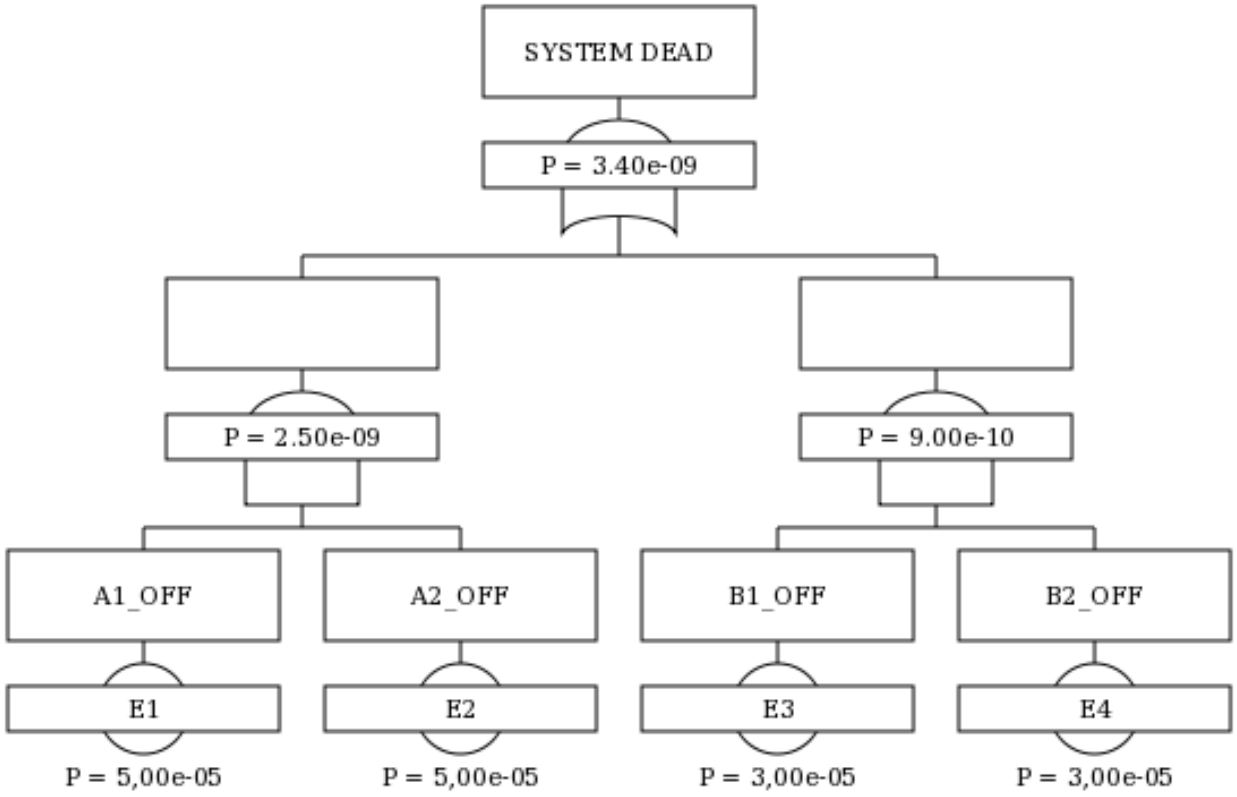
$$M \rightsquigarrow M_{[F]}$$

  2. Model-Based Safety Assessment

$$\delta(F) : M_{[F]} \not\models \varphi$$

Safety Assessment

$\delta(F)$:



Contributions

- Review of the AIR6110 with:
  - Formal modeling
  - Formal Verification & Validation
  - Formal Safety Assessment

- Use of tools developed in FBK
  - OCRA, contract-based design tool
  - nuXmv, model-checker
  - xSAP, model-based safety analysis tool

Adopted approach

Adopted approach

MODELING \ ANALYSIS	
Architecture decomposition & Contracts	
Behavioral Implementation (Leaf components & System)	

Adopted approach

ANALYSIS / MODELING	V & V	Safety Assessment	
		Fault extension	**Fault trees computation**
Architecture decomposition & Contracts			
Behavioral Implementation (Leaf components & System)			

Adopted approach

ANALYSIS / MODELING	V & V	Safety Assessment	
		Fault extension	Fault trees computation
Architecture decomposition & Contracts			
Behavioral Implementation (Leaf components & System)			

Adopted approach

ANALYSIS / MODELING	V & V	Safety Assessment	
		Fault extension	Fault trees computation
Architecture decomposition & Contracts	• Automatic contract refinement verification **OCRA**		
Behavioral Implementation (Leaf components & System)			

Adopted approach

ANALYSIS / MODELING	V & V	Safety Assessment	
		Fault extension	Fault trees computation
Architecture decomposition & Contracts	• Automatic contract refinement verification **OCRA**		
Semi-automatic Generation			
Behavioral Implementation (Leaf components & System) M			

Adopted approach

ANALYSIS / MODELING	V & V	Safety Assessment	
		Fault extension	Fault trees computation
Architecture decomposition & Contracts	• Automatic contract refinement verification **OCRA**		
Semi-automatic Generation			
Behavioral Implementation (Leaf components & System) M	• Automatic compositional verification **OCRA** • Automatic monolithic verification **nuXmv** $M \models \varphi$		

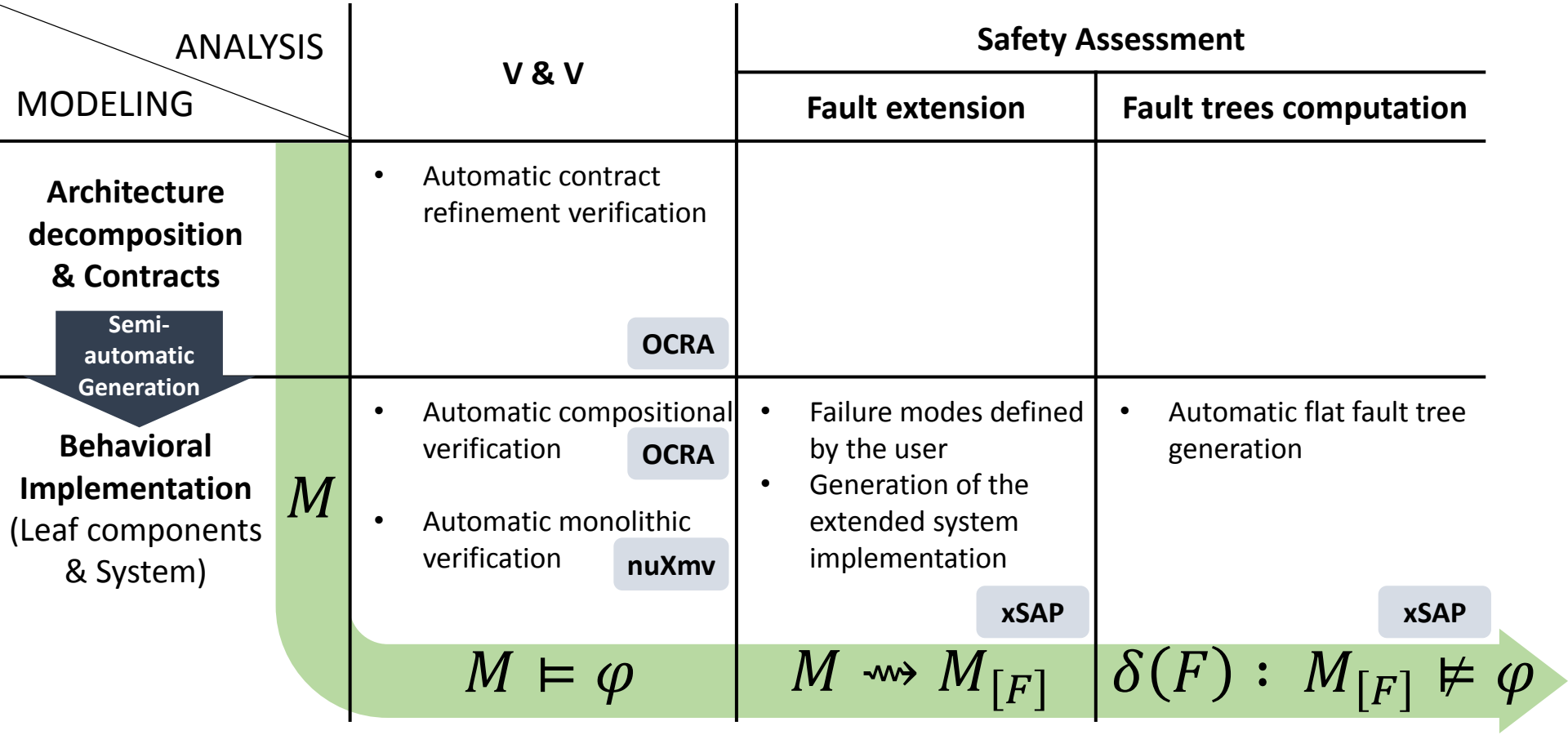
Adopted approach

ANALYSIS / MODELING	V & V	Safety Assessment	
		Fault extension	Fault trees computation
Architecture decomposition & Contracts	• Automatic contract refinement verification **OCRA**		
Semi-automatic Generation			
Behavioral Implementation (Leaf components & System) M	• Automatic compositional verification **OCRA** • Automatic monolithic verification **nuXmv** $M \models \varphi$	• Failure modes defined by the user • Generation of the extended system implementation **xSAP** $M \rightsquigarrow M_{[F]}$	

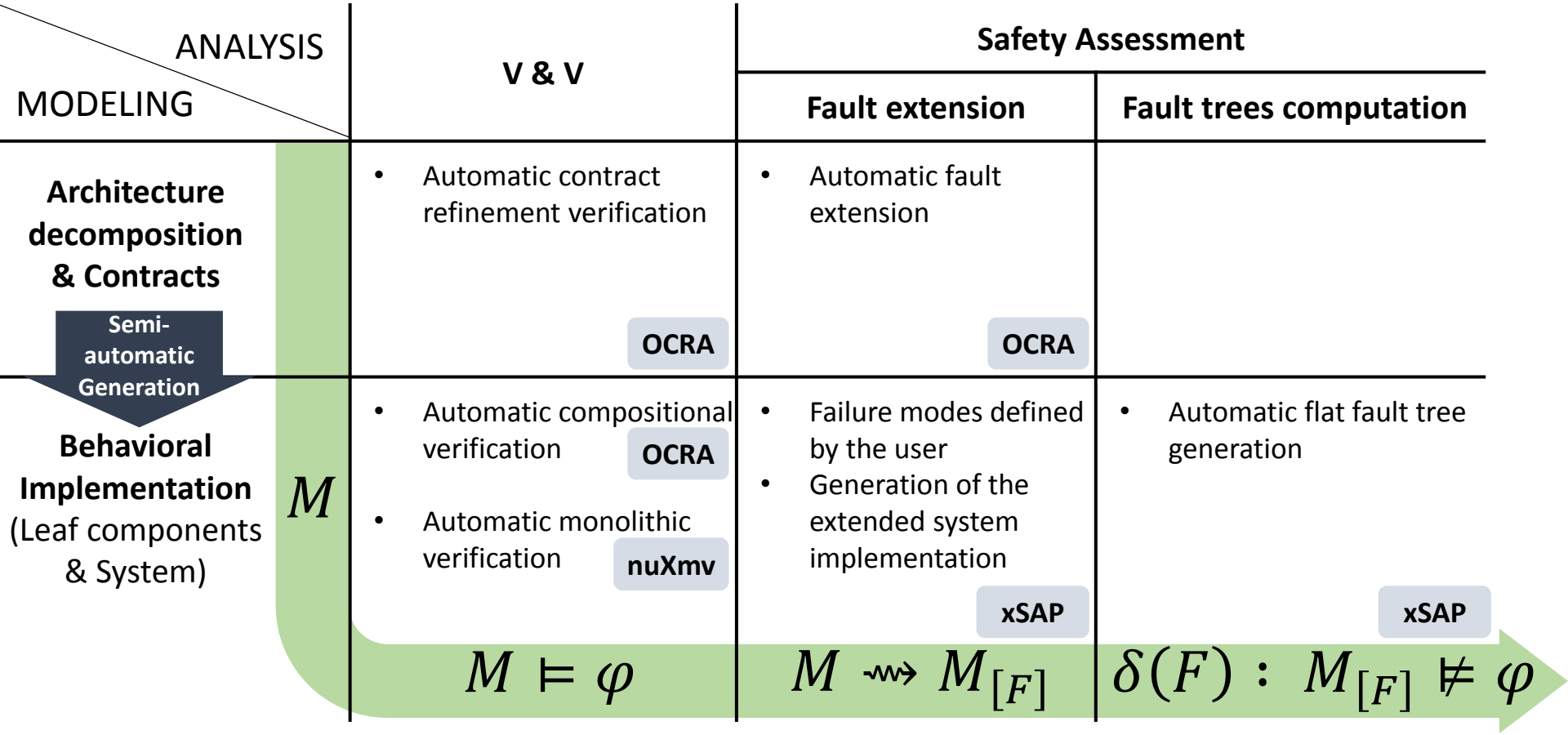
Adopted approach

ANALYSIS / MODELING	V & V	Safety Assessment	
		Fault extension	**Fault trees computation**
Architecture decomposition & Contracts	• Automatic contract refinement verification **OCRA**		
Semi-automatic Generation			
Behavioral Implementation (Leaf components & System) M	• Automatic compositional verification **OCRA** • Automatic monolithic verification **nuXmv** $M \models \varphi$	• Failure modes defined by the user • Generation of the extended system implementation **xSAP** $M \rightsquigarrow M_{[F]}$	• Automatic flat fault tree generation **xSAP** $\delta(F) : M_{[F]} \not\models \varphi$

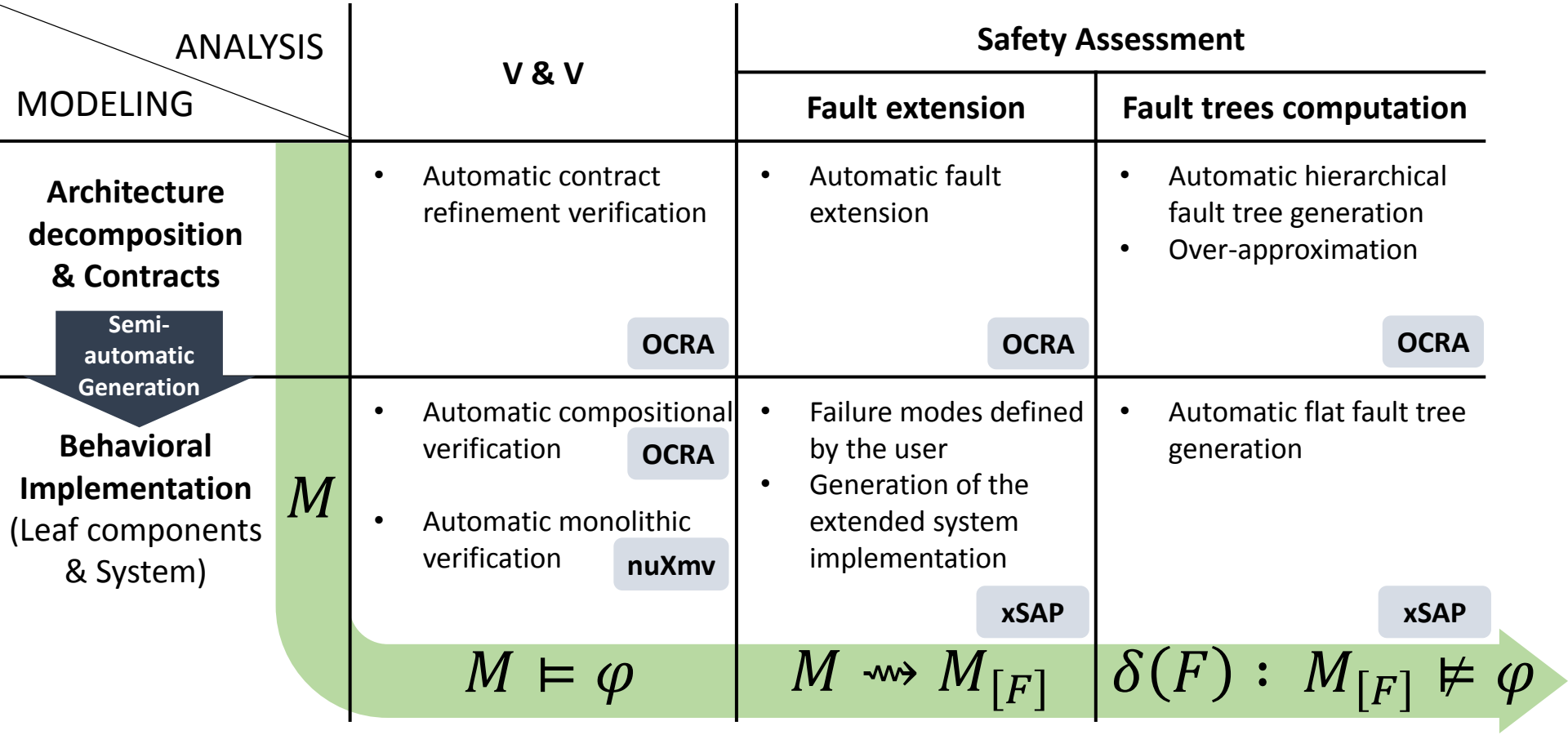
Adopted approach



Adopted approach



Adopted approach



Adopted approach

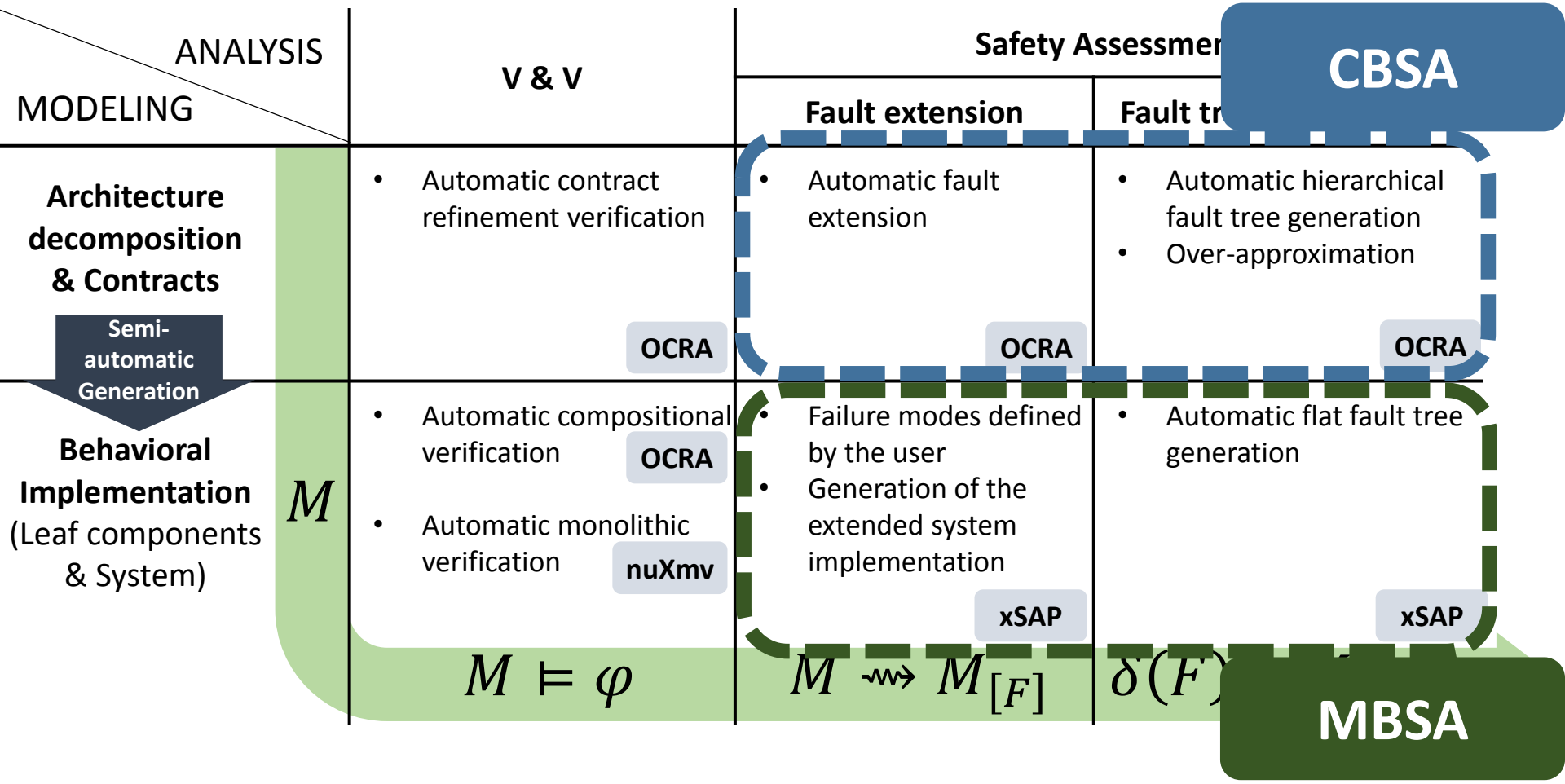
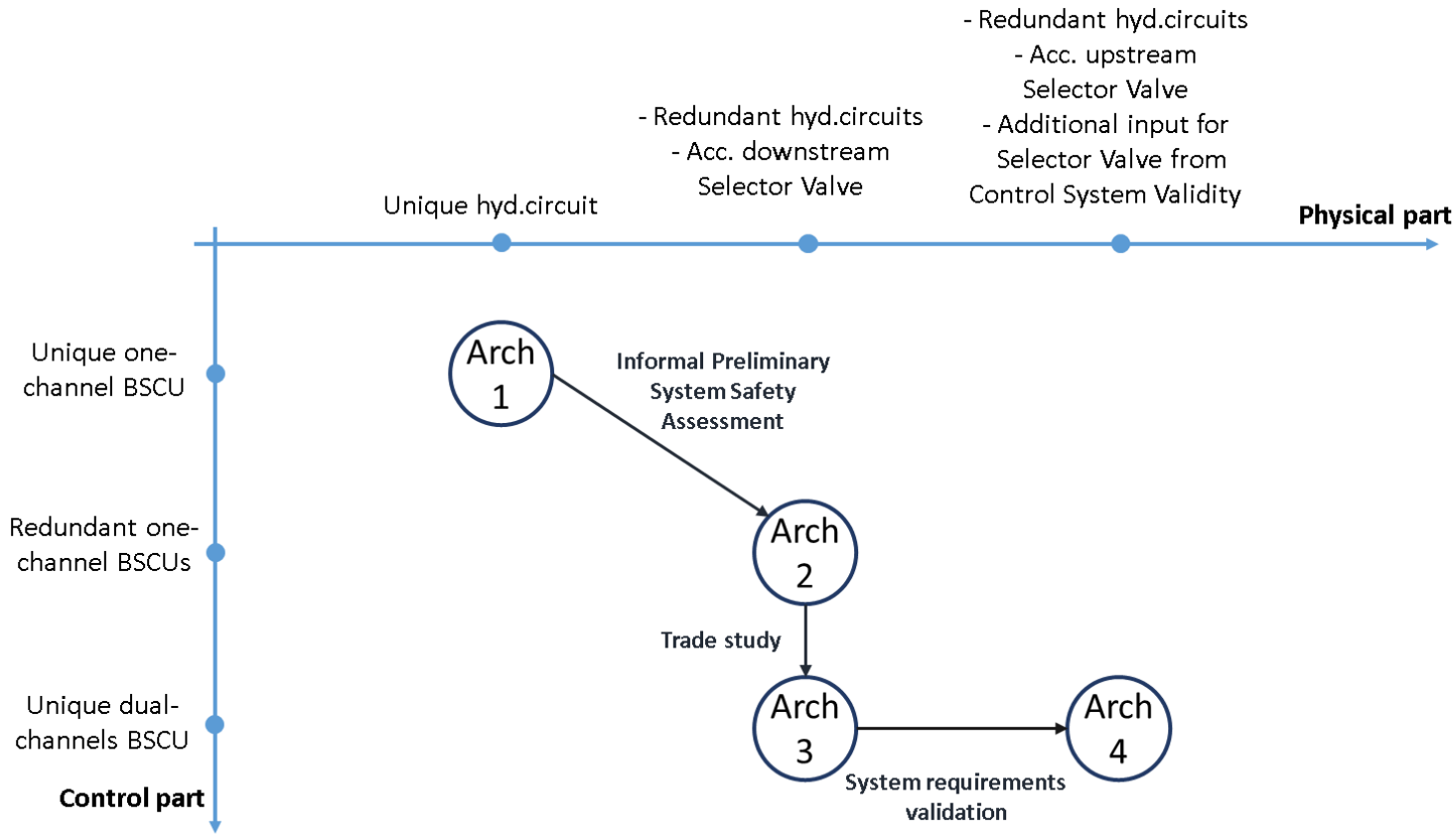


Table of contents

- AIR6110 WBS case study
- Approach
- Results
- Lessons learned and conclusion

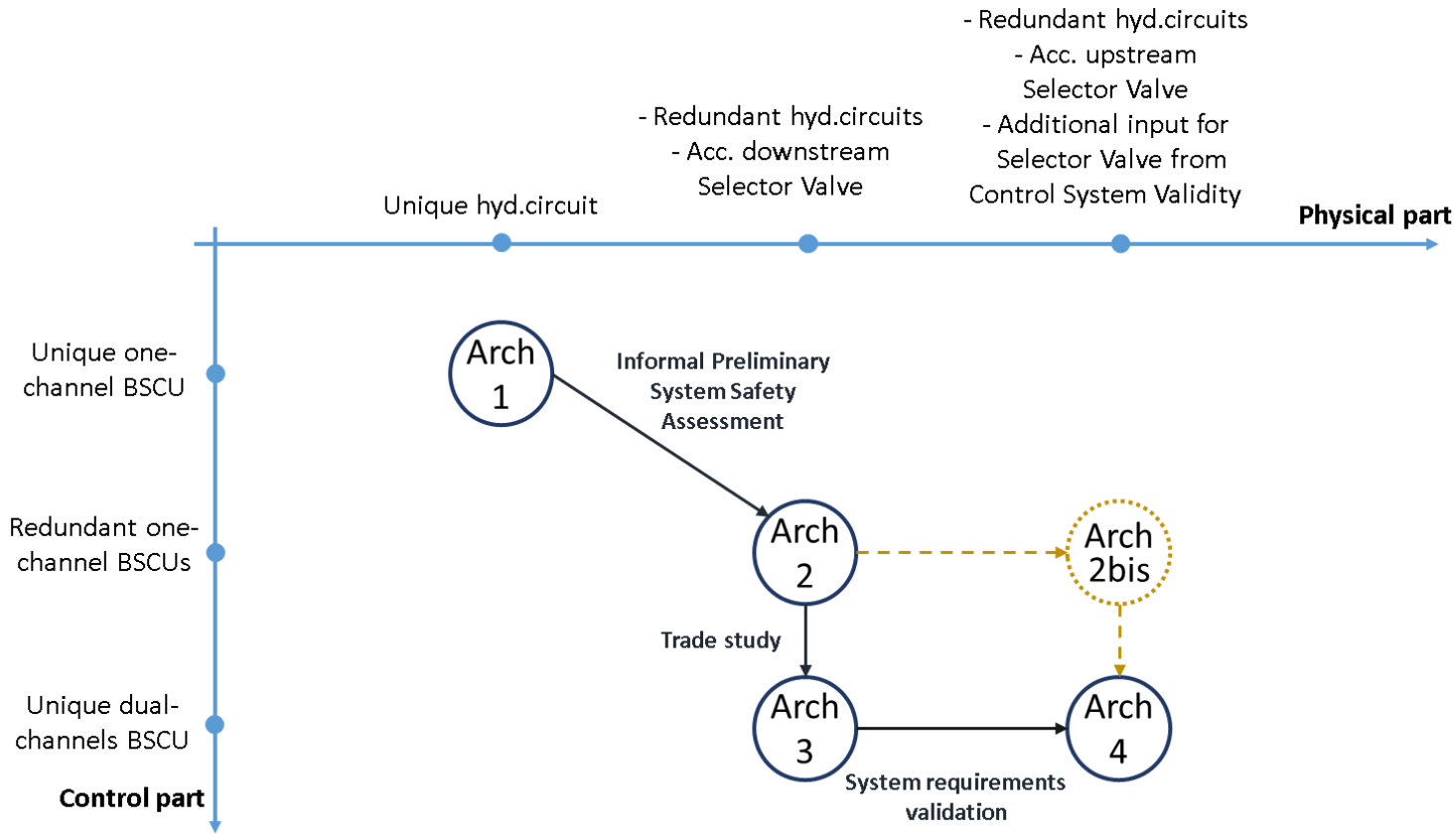
Application on AIR6110 WBS

- Application on 5 WBS architectures versions



Application on AIR6110 WBS

- Application on 5 WBS architectures versions



Formal modeling

- Size of the formal models:
  - 30 component types for 169 instances
  - Max depth of 6 levels
  - 149 contracts for 304 property instances
  - 33 failure modes for 261 fault variables

- Translation of requirements:
  - Example:
    - **S18-WBS-R-0321: "***Loss of all wheel braking (unannunciated or annunciated) during landing or RTO shall be extremely remote***"**
    - **Becomes**: "*never loss of all wheel braking"*
    - *"Shall be extremely remote"* will be used for evaluating the reliability during MBSA

V & V: Compositional approach

- Contracts refinement (BDD algorithm) checked in 30-100s
- Detection of an unexpected flaw in Arch2
  - Preclusion of the operation modes: Normal VS Alternate
  - Arch2: the alternate circuit can be supplied by the accumulator while the normal circuit is operating
    - Detection of the problem in Arch3 which leads to Arch4! (AIR6110, p.67)
  - If application of the modification of Arch 4 concerning the placement of the accumulator
    - Creation of architecture Arch2bis
    - The previous property is verified

V & V: Monolithic approach

- BDD algorithm:
  - Build of the BDD model out of reach => Simplification needed
  - After simplification: All properties checked in ≈3000s
- IC3 algorithm:
  - No need of simplification
  - All properties checked in ≈150s

Safety Assessment

- MBSA
  - Conducted with xSAP
  - Safety requirements chosen as Top Level Events (TLE)
  - **3150 Analyses launched: 3089 succeeded, 61 timed out (10h)**
- CBSA
  - Conducted with OCRA
  - Same safety requirements chosen as TLE
  - Fault trees for all TLEs for each architecture computed in few minutes
  - For each property, the hierarchical fault tree produced is an over-approximation of the one produced with MBSA
    - Formally checked for the case study

Safety Assessment

- Arch1 is weaker than the other architectures
- Arch2 and Arch3 have the same results
  - it confirms the results of AIR6110: Modification due to trade study has no impact on the safety objectives.
- Arch4 is better than Arch3
  - same observation for Arch2bis and Arch2
- The computed probabilities for Arch2, Arch2bis, Arch3 and Arch4 are consistent with the expectations

Table of contents

- AIR6110 Wheel Brake System
- Approach
- Results
- Lessons learned and conclusion

Conclusion

- Cover the process described in AIR6110 with formal methods
- Production of modular descriptions of 5 architectures
  - Analysis of their characteristics in terms of a set of requirements expressed as properties
  - Production of more than 3000 fault trees
  - Production of reliability measures
- Detection of an unexpected flaw in the process
  - Detection of the wrong position of the accumulator earlier in the process

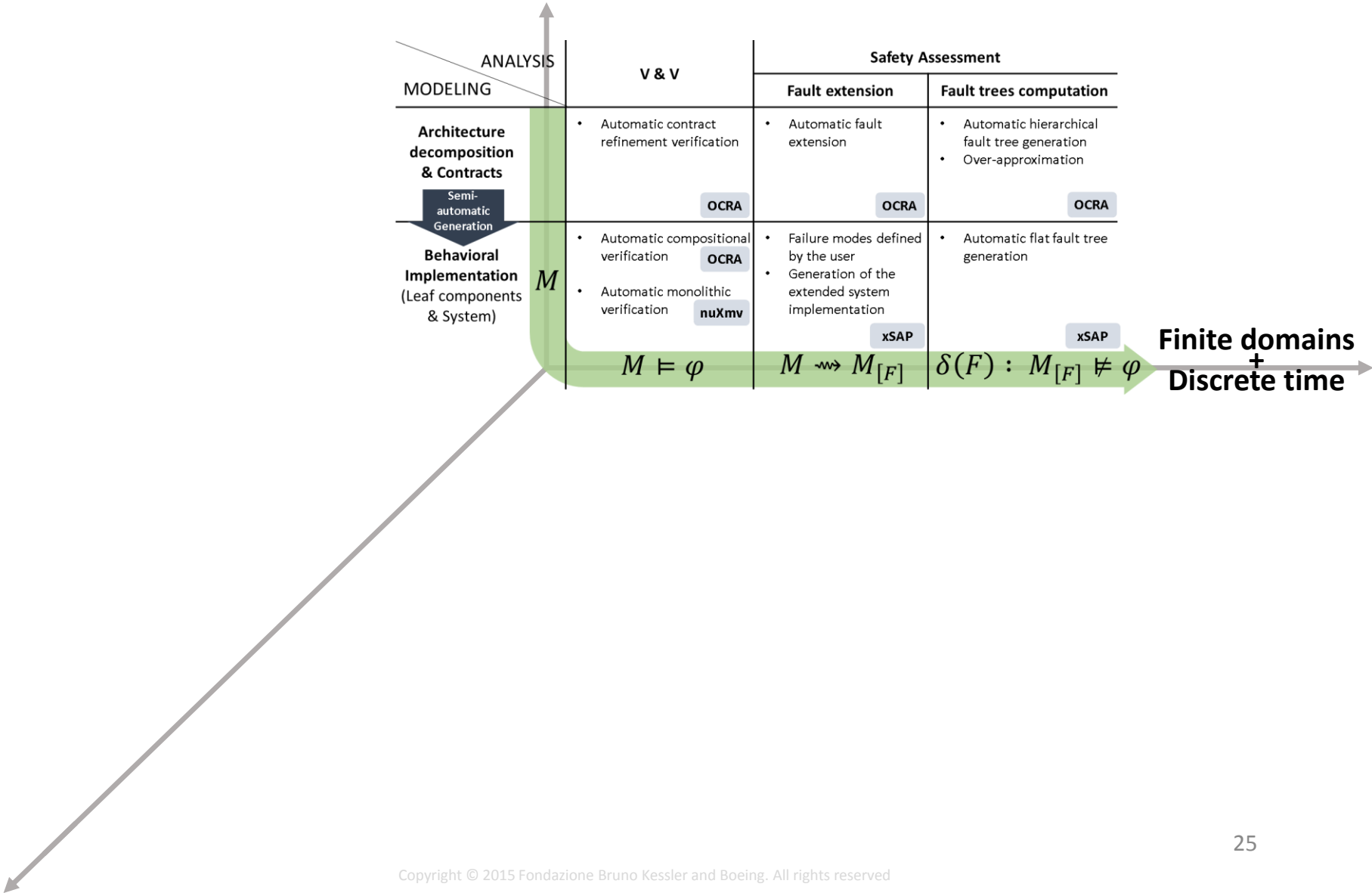
Lessons learned

- Going from informal to formal allows highlighting the missing information of the AIR6110 to reproduce the process
- OCRA modular modeling allows a massive reuse of the design through architectures variant
- Automated and efficient engines as IC3 is a key factor
- MBSA is crucial in this context:
  - Automatic extension of the nominal model with faults
  - Automatic generation of artifacts eases the analysis and the architecture comparison in terms of safety

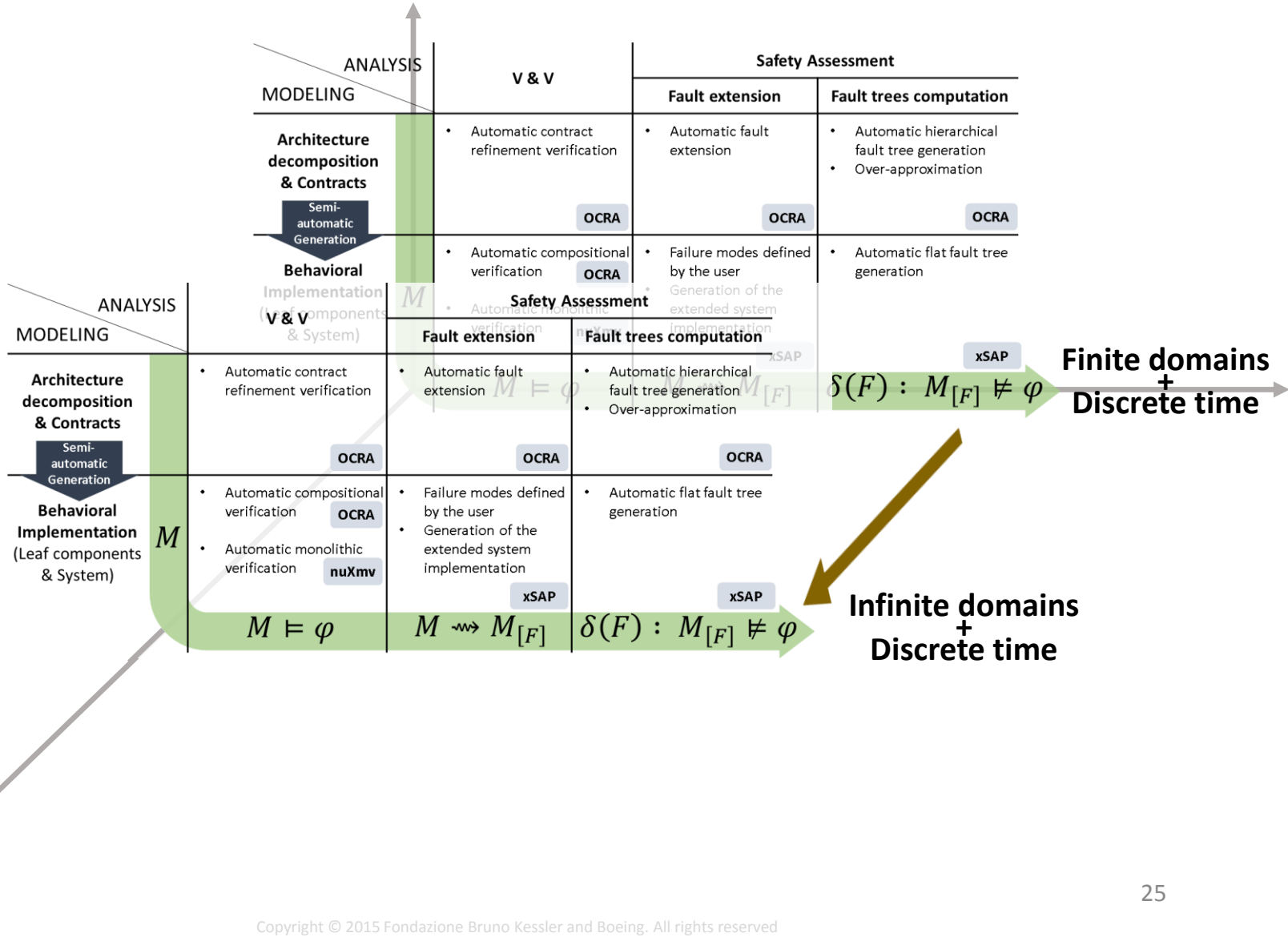
Future work

- Improvement of contract-based design in terms of debugging
- Improvement of scalability of MBSA
- Making the modeling more realistic

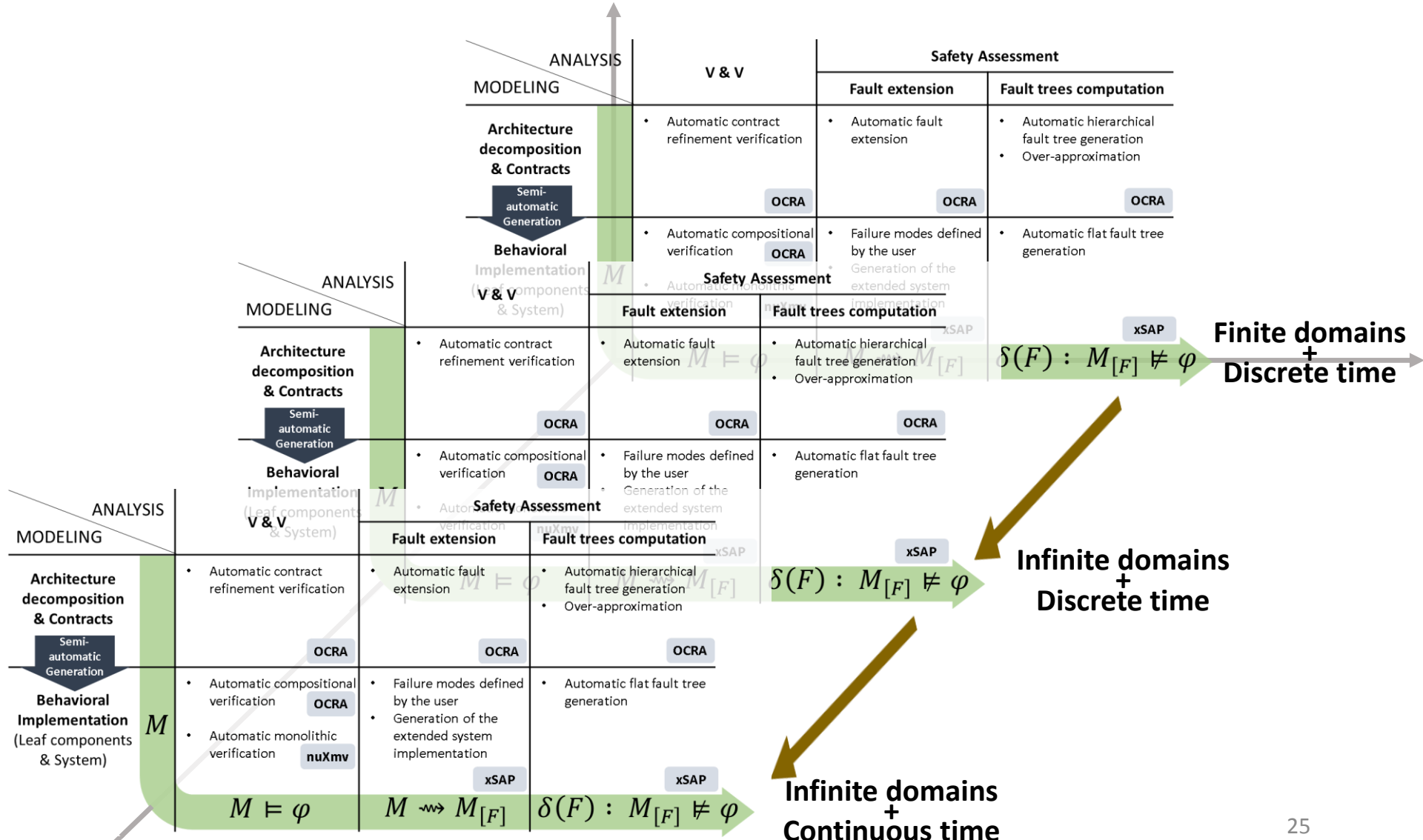
Future work



Future work



Future work



Thank you for your attention

Technical report and all artifacts available at:

https://es.fbk.eu/projects/air6110

Architecture decomposition

Architecture	Total component types	Leaf component types	Total component instances	Leaf component instances	Max depth	Contracts
Arch1	22	15	100	79	5	121
Arch2	29	20	168	143	5	129
Arch2bis	29	20	168	143	5	129
Arch3	30	20	169	143	6	142
Arch4	30	20	169	143	6	142

System implementation

Architecture	Properties	State variables	
		Boolean	Enumerative
Arch1	199	31	55
Arch2	291	79	88
Arch2bis	291	79	88
Arch3	304	79	88
Arch4	304	79	88

Extended system implementation

Architecture	Failure modes	Fault variables	State variables	
			Boolean	Enumerative
Arch1	28	170	74	184
Arch2	33	261	156	311
Arch2bis	33	261	156	311
Arch3	33	261	156	311
Arch4	33	261	156	311

Formal verification

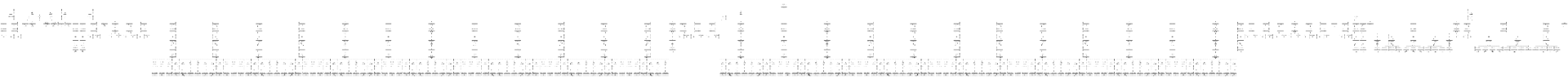
	System implementation			Architecture decomposition			
Arch	**BDD** *after simplification*	**IC3** *after simplification*	**IC3**	**Refinement check**	**Leaf component impl check**	**Total**	**Virtual parallelization**
Arch1	38.32	53.30	56.62	1422.24	6.07	1428.31	439.62
Arch2	2700.64	599.02	153.28	102.04	1.26	103.30	24.12
Arch2bis	3069.82	628.09	153.19	32.38	1.26	33.64	1.39
Arch3	2935.88	671.29	159.01	72.87	1.29	74.16	10.74
Arch4	3429.59	652.50	158.51	29.74	1.29	31.03	1.78

(All times are in seconds)

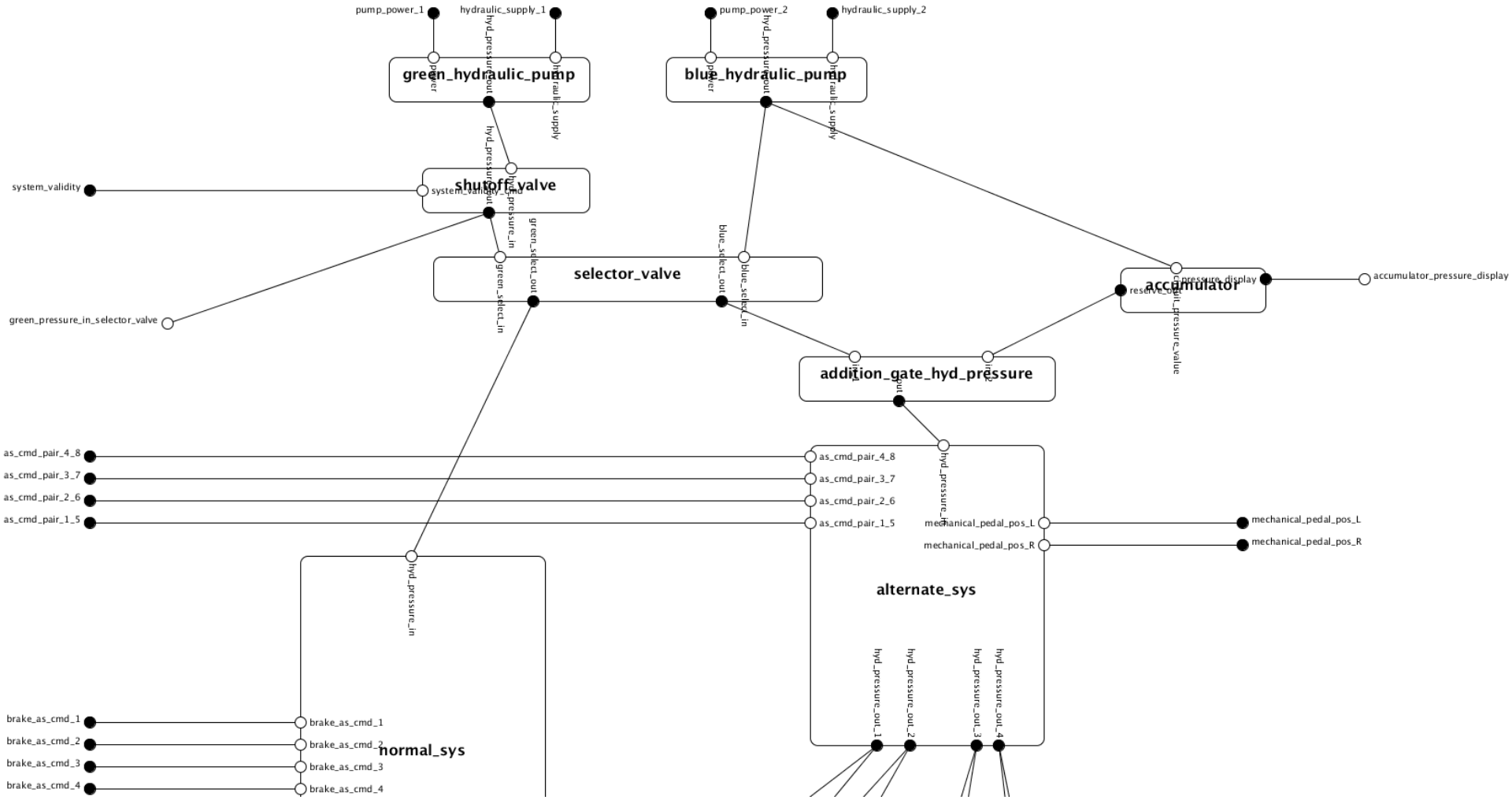
Arch/Prop		Prob.	$\|mcs\| = 1$	$\|mcs\| = 2$	$\|mcs\| = 3$	$\|mcs\| = 4$	$\|mcs\| = 5$	Full
arch2	S18-WBS-R-0321	4.51e-10	0	6	1252	629	-	N
	S18-WBS-R-0322-left	1.00e-05	2	2	732	47583	-	N
	S18-WBS-R-0322-right	1.00e-05	2	2	732	47583	-	N
	S18-WBS-R-0323	0.00e+00	0	0	0	0	0	N
	S18-WBS-R-0324	2.50e-11	0	1	0	38	10859	N
	S18-WBS-R-0325-wheel1	1.20e-04	9	19	2597	0	0	Y
	S18-WBS-R-0325-wheel2	1.20e-04	9	19	2597	0	0	Y
	S18-WBS-R-0325-wheel3	1.20e-04	9	19	2597	0	0	Y
	S18-WBS-R-0325-wheel4	1.20e-04	9	19	2597	0	0	Y
	S18-WBS-R-0325-wheel5	1.20e-04	9	19	2597	0	0	Y
	S18-WBS-R-0325-wheel6	1.20e-04	9	19	2597	0	0	Y
	S18-WBS-R-0325-wheel7	1.20e-04	9	19	2597	0	0	Y
	S18-WBS-R-0325-wheel8	1.20e-04	9	19	2597	0	0	Y
	braking_implies_cmd_w1	1.25e-04	10	40	2651	7395	9636	Y
	cmd_implies_braking_w1	1.13e-04	13	30	8053	3815	2873	Y

Arch/Prop		Prob.	$\|mcs\| = 1$	$\|mcs\| = 2$	$\|mcs\| = 3$	$\|mcs\| = 4$	$\|mcs\| = 5$	Full
arch2bis	S18-WBS-R-0321	4.51e-10	0	6	627	629	-	N
	S18-WBS-R-0322-left	1.00e-05	2	2	203	46287	-	N
	S18-WBS-R-0322-right	1.00e-05	2	2	203	46287	-	N
	S18-WBS-R-0323	0.00e+00	0	0	0	0	0	N
	S18-WBS-R-0324	2.50e-11	0	1	0	2	8729	N
	S18-WBS-R-0325-wheel1	1.20e-04	9	12	2596	0	0	Y
	S18-WBS-R-0325-wheel2	1.20e-04	9	12	2596	0	0	Y
	S18-WBS-R-0325-wheel3	1.20e-04	9	12	2596	0	0	Y
	S18-WBS-R-0325-wheel4	1.20e-04	9	12	2596	0	0	Y
	S18-WBS-R-0325-wheel5	1.20e-04	9	12	2596	0	0	Y
	S18-WBS-R-0325-wheel6	1.20e-04	9	12	2596	0	0	Y
	S18-WBS-R-0325-wheel7	1.20e-04	9	12	2596	0	0	Y
	S18-WBS-R-0325-wheel8	1.20e-04	9	12	2596	0	0	Y
	braking_implies_cmd_w1	1.25e-04	10	24	2647	4530	59	Y
	cmd_implies_braking_w1	1.13e-04	13	30	7428	3815	1768	Y

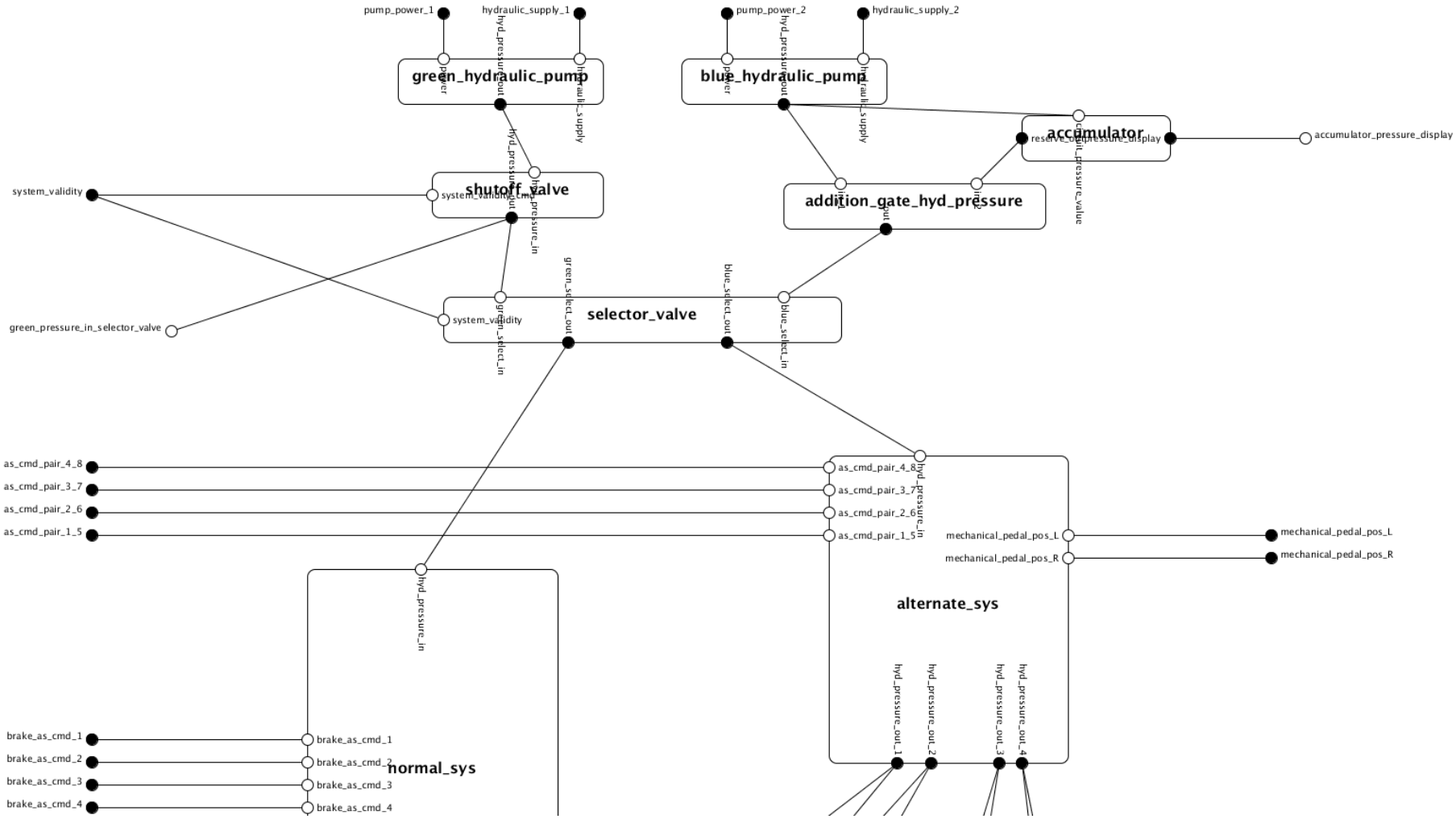
Contract-Based Safety Analysis (CBSA)



Arch2 accumulator position



Arch2bis accumulator position



Adopted approach

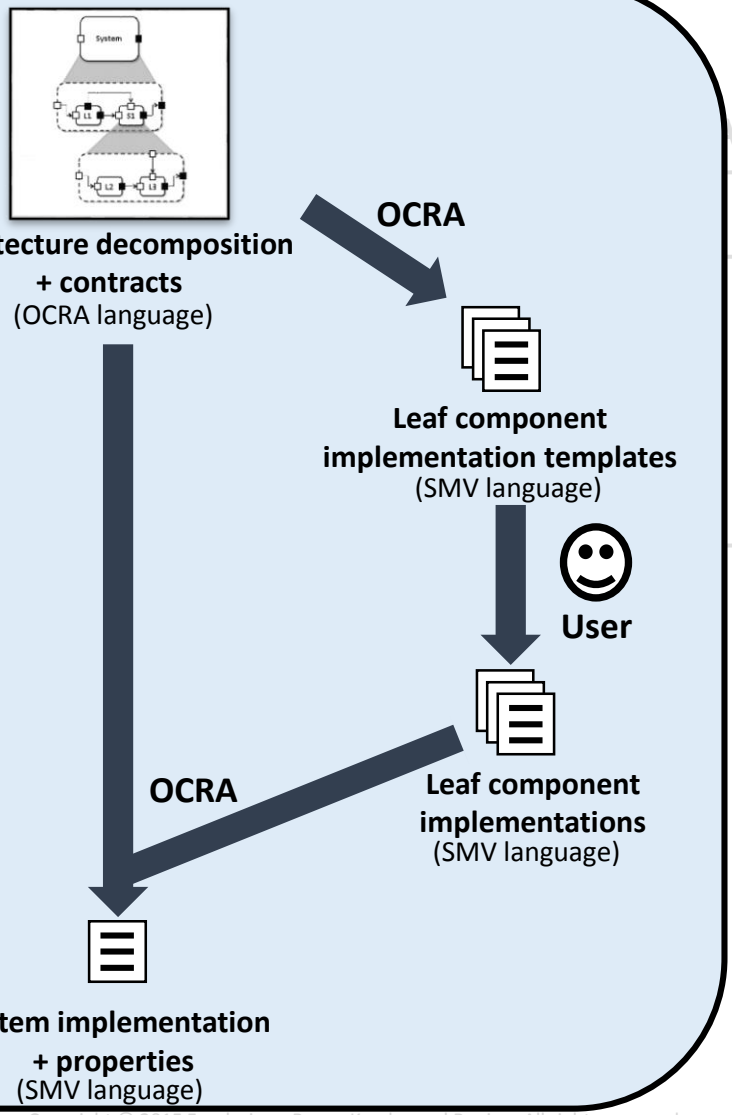
ANALYSIS

MODELING

Architecture decomposition & Contracts

Semi-automatic Generation

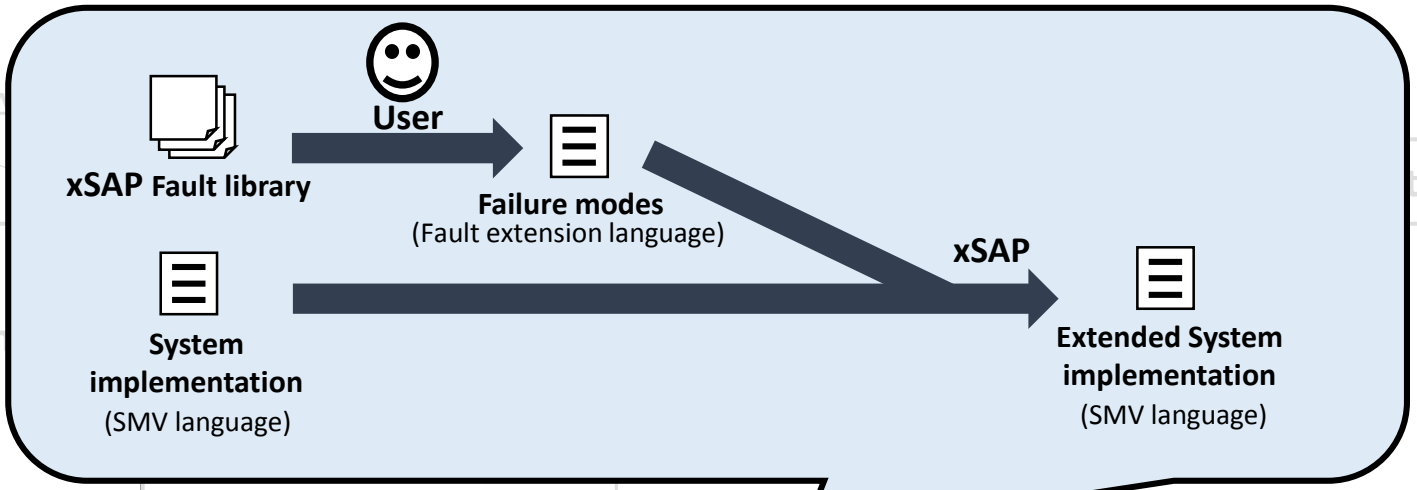
Behavioral Implementation (Leaf components & System)



assessment

Fault trees computation

Adopted approach



ANA
MODELING
tation
Architecture decomposition & Contracts
Semi-automatic Generation

Behavioral Implementation (Leaf components & System)

M

- Automatic compositional verification — OCRA
- Automatic monolithic verification — nuXmv

$M \models \varphi$

- Failure modes defined by the user
- Generation of the extended system implementation

xSAP

$M \rightsquigarrow M_{[F]}$

Formal modeling

- Hydraulic circuits are unidirectional
- Hydraulic pressures, braking force and ground speed are representing as bounded integer (0..10)
- Commands and power are Boolean
- Wheel speed becomes a wheel status: rolling or stopped
- Accumulator has an infinite reserve
- Discrete time
- All behaviors are instantaneous (except the wheel behavior)