Model based safety assessment of space operations

Toward integration of failure analysis of system and operation

22/10/2015

JP Blanquart Airbus Defence & Space

C. Seguin, P. Bieber ONERA

retour sur innovation

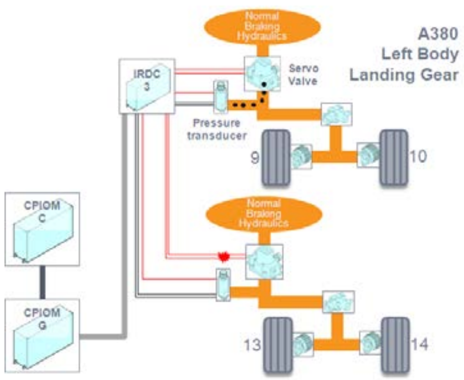
Presentation overview

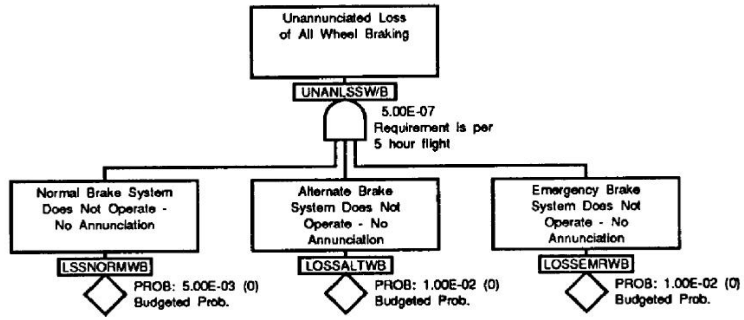
- Our understanding of MBSA principles
- Joint lessons learnt by ONERA/Airbus Defence & Space for space operations
- Conclusion

MBSA Principle – 1/3

- Principle 1: RAMS model closer to design models
  - Achieve *failure propagation model* to support RAMS analysis
  - *Structure* the failure propagation model *as the nominal reference model*

Braking system example:
high level view of the physical architecture

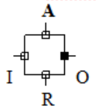


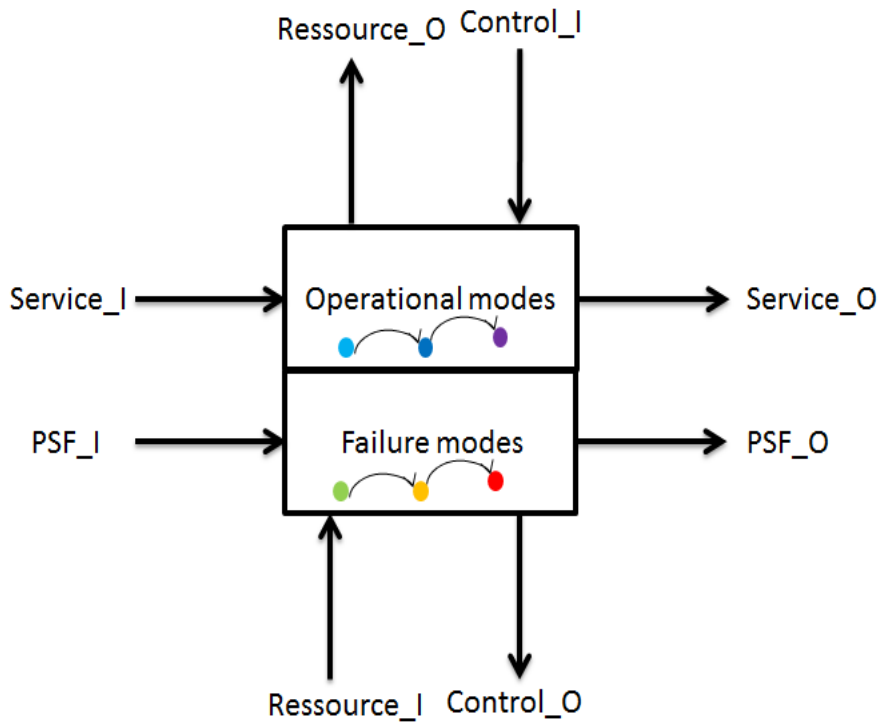


Fault tree with top level event "Loss of all wheel braking"

MBSA Principle – 2/3

- Principle 2: Component based model to master the complexity
  - Encapsulate in components the knowledge about *static/dynamic* failure propagation rules
  - Make explicit the *interfaces/internal states* impacting propagation

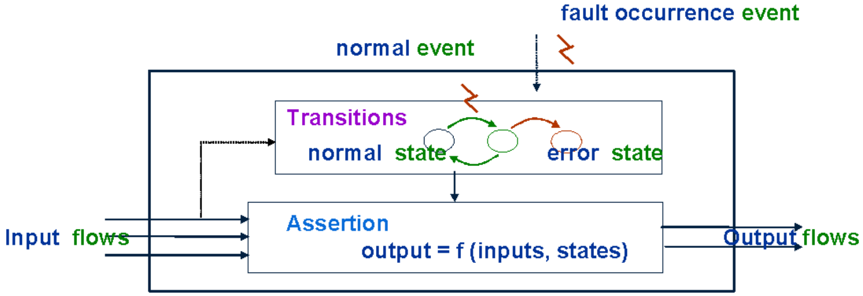
Component "Basic_service"			
			
Services provided by the component			
Service Name	Service presentation (role, conditions of use, …)		
Basic_service	Generic service that provides a correct output if and only if it receives an input, is activated, has the needed resource and is ok.		
Component interfaces			
Interface Name	Role	Orientation	Value type
	(S, C, R, PSF, other…)	(In, Out, In/Out)	
I	Service	In	Bool
A	Control	In	Bool
R	Resource	In	Bool
O	Service	Out	Bool
Component control states			
Control State Name	Role (F, R, M, A, other)	Value type (range of modes or attribute values)	
Ok	Reliability	Bool (ok or not ok)	
Service measures			
Measure Name	Measure parameters	Measure estimation	
Failure rate	lambda	10-3 per hour	
Specification of the variations of "basic_service"			
Variation Name	Guards Over state/interface	Triggers (condition/ event)	Effects over states/interfaces
Service_ok	True	I and A and R and Ok/-	O=true
Service_ko	True	Not (I and A and R and Ok)/-	O=false
Component_faulty	True	True/fail (lambda)	Ok=false



MBSA Principles - 3/3

- Principle 3: Tool based assessment of formal models
  - Associate component models with *formal semantics* to specify rigorously how the failures are propagated in the overall system
  - Use tools to automatically perform on the formal semantics usual RAMS computation

Example of formal model: AltaRica mode automata



Computation supported by AltaRica

- Simulation / failure injection
- Fault tree / sequence of events generation
- Stochastic simulation
- Model-checking

Example of related tools

- Industrial tools: Cecilia OCAS (Dassault Aviation) / SIMFIA (APSYS)
- Academic tools : LaBri, FBK, ONERA, IRT Systemix …

Lessons learnt for Space System Safety

- Application to safety/FDIR of technical systems
  - ATV control system (European project ASSERT)
  - Formation flying (CNES project)
  - FDIR validation: for AOCS with TAS / for Thermic & Power system with Airbus Defence & Space

- Feedback:
  - MBSA mature for safety assessment and early validation of FDIR principles
  - Need for complementary models & tools for analysis of detailed design
    - Formal models closer to physics exists: timed / hybrid automata
    - Robust & scalable assessment tools are still needed

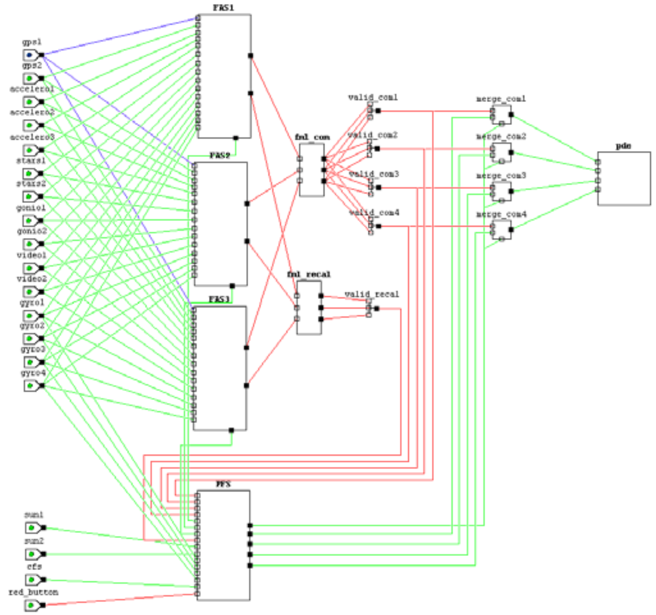
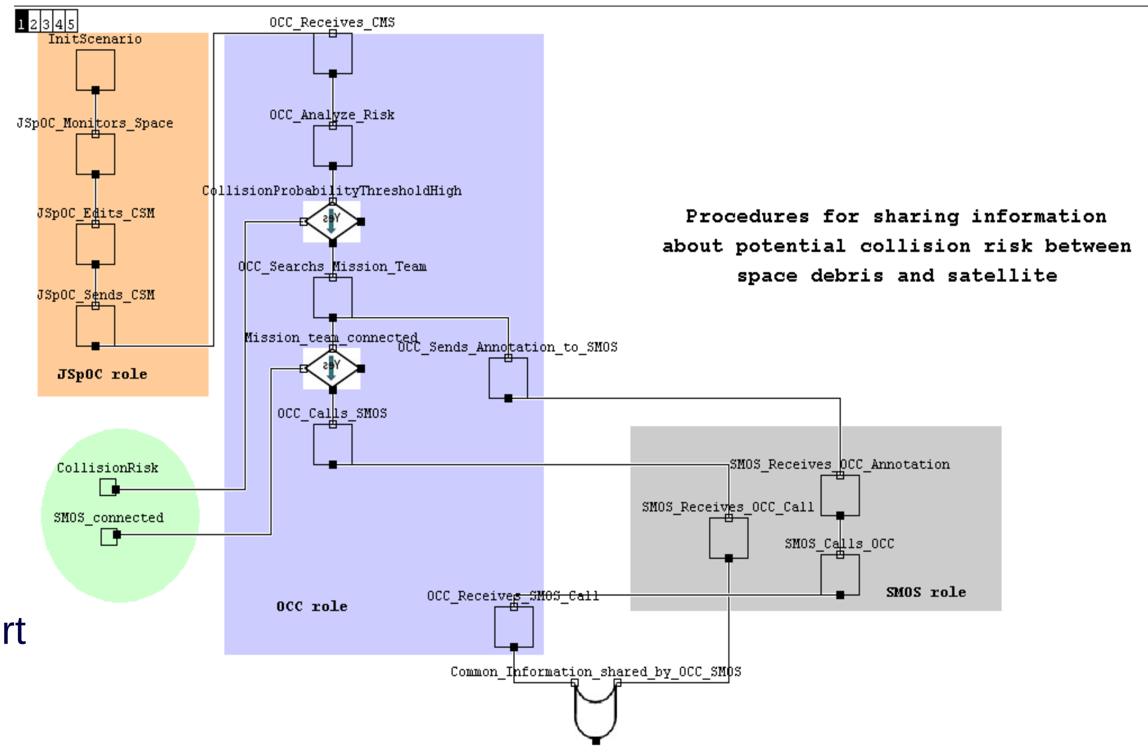


Figure 26: AltaRica model Top-level view of ATV architecture 37

Lessons learnt for Space Operation Safety

- Application to safety analysis of socio-technical systems (project ESA IFA, DGA EXDRO)
  - Satellite operation, organization of space debris management
  - UAV operation (collision avoidance)

- Feedback:
  - MBSA principles valid also for socio-technical systems
    - Encouraging results about models of human tasks and organization
  - Integrated analysis of technical and social views
    - Composition principle very useful
    - But very big models: support needed to browse, extract subpart, build view from models.



Conclusion

- Positive feedback on MBSA in several cases
  - a key success point is to find the relevant formal semantics for the modelling and analysis purpose
  - Opportunity to exchange with COMPASS team to take the best from each one of the underlying formal models?
- A lot of tools available with different status
  - Tested on our side: mature tool for safety assessment (e.g. OCAS)
  - Less test on tools for other RAMS needs or more detailed analysis
  - Opportunity to exchange with COMPASS to test
    - Testability/diagnosability tools
    - Duration analysis for FDIR validation
- More general new trends
  - Adapt principles developed for technical system safety assessment to address now also the socio-technical aspects
  - Need not only for computation tools but also tools to browse, consult, extract and recompose models more efficiently