COMPASS without AADL towards COMPASS-STAR

Alessandro Cimatti

Fondazione Bruno Kessler

COMPASS is great, but…

- What if AADL modeling does not work for us
  - Because our process relies on a different tool chain
  - Because we have synchronous composition
  - Because of copyright, we can’t use COMPASS
- Overview of efforts using COMPASS process w/o AADL
- Take away message

AADL-independent COMPASS workflow

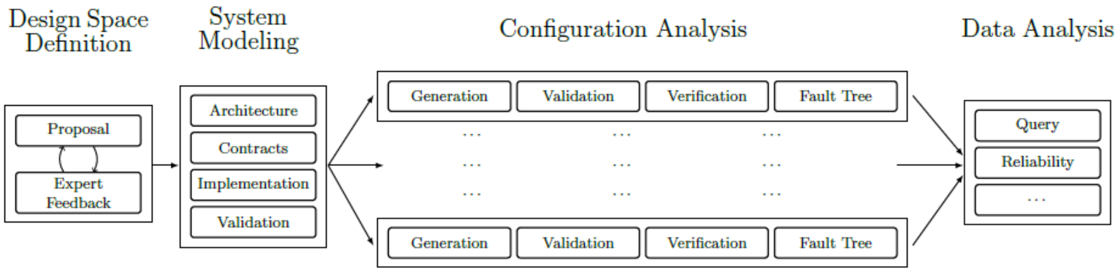
NextGEN air traffic control Exploring functional allocation

- Joint FBK-NASA effort
- Key issue: ensuring Loss-of-separation
- Formal support for analysis of ~2000 configurations
- Parameterized modular modeling with OCRA/SMV
- Contracts for modular reasoning and sanity checks
- Model extension and FTA over reference requirements with xSAP
- Data Analysis of configuration space based on comparison of
    - minimal cut sets
    - reliability measures

References:

- https://es-static.fbk.eu/projects/nasa-aac/
- C. Mattarei, A. Cimatti, M. Gario, S. Tonetta, K.Y. Rozier: *Comparing Different Functional Allocations in Automated Air Traffic Control Design*. FMCAD 2015
- M. Gario, A. Cimatti, C. Mattarei, S. Tonetta, K.Y. Rozier: *Model Checking at Scale: Automated Air Traffic Control Design Space Exploration*. CAV (2) 2016: 3-22

- Process:



Design Space Definition

Proposal

Expert Feedback

System Modeling

Architecture

Contracts

Implementation

Validation

Configuration Analysis

Generation

Validation

Verification

Fault Tree

...

Generation

Validation

Verification

Fault Tree

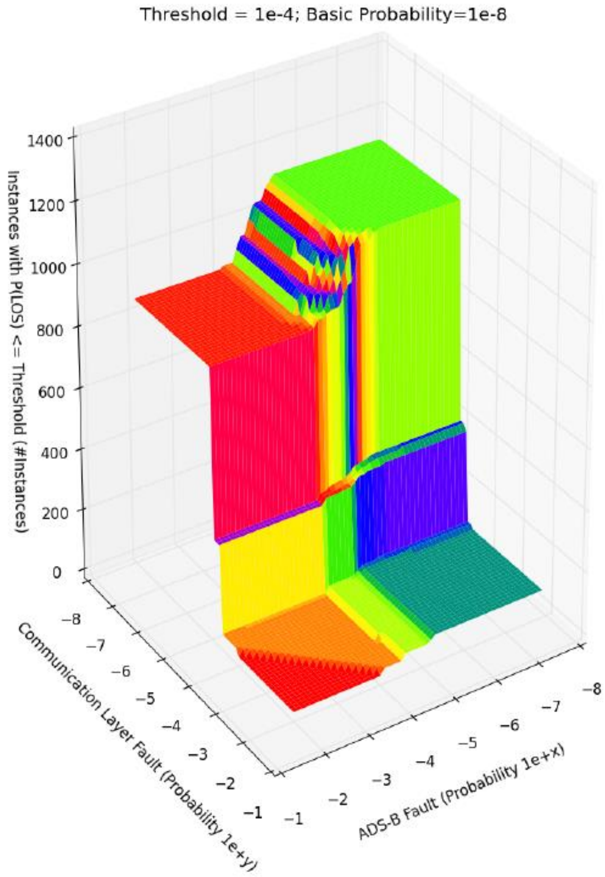
Data Analysis

Query

Reliability

...

- Example: impact of communication faults on Loss-of-separation probability

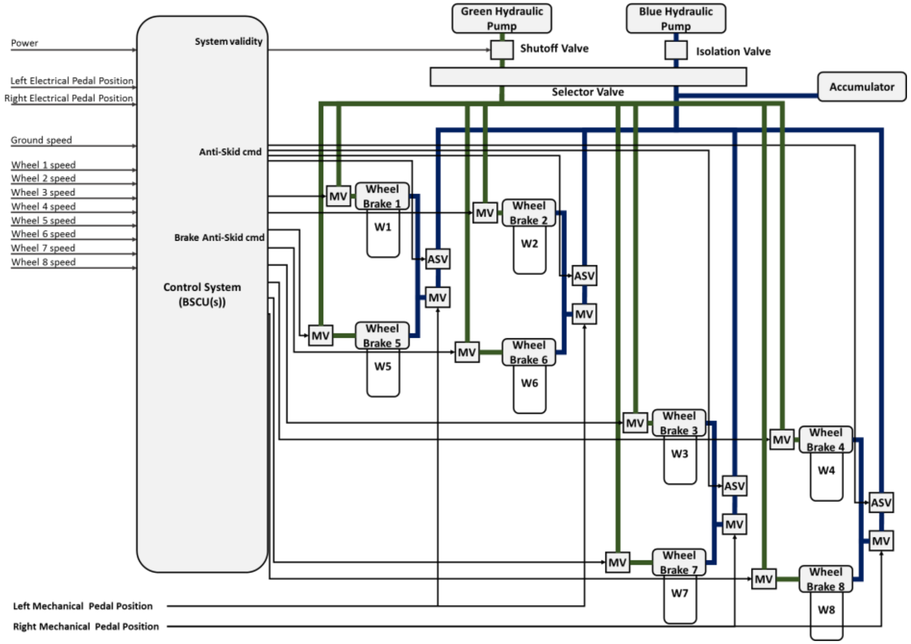


An experience in railways

- Abderrahmane El-Hallabi-Kettani (Alstom)
- Feasibility study on ERTMS Unisig (ERA railway agency) Subset-026, chapter 4
- Train driving mode transition machine
- Simple yet representative modeling exercise
- Approach
  - Hierarchical modeling and contracts with OCRA
  - Behaviours in nuXmv
  - MBSA via xSAP
- Generate FEI, FMS, FTA, FMEA and analyse the associated results

Boeing-FBK
AIR 6110 Wheel Brake System

- Revisit informal AIR 6110 case study with formal methods
- Multiple architectures
  - Different forms of redundancy
- Tool chain
  - OCRA for hierarchical decomposition
  - nuXmv for modeling and verification
  - xSAP for fault extension and fault tree analysis



References:

- https://es-static.fbk.eu/projects/air6110/
- M. Bozzano, A.Cimatti, A. Fernandes Pires, D. Jones, G. Kimberly, T. Petri, R. Robinson, Stefano Tonetta: Formal Design and Safety Analysis of AIR6110 Wheel Brake System. CAV (1) 2015: 518-535

Honeywell’s study

- Identify Safety Issues in Integration of Complex Digital Systems
    - FAA Broad Agency Announcement TCBAA-15-00001
- Chris Wilkinson and Brendan Hall
    - Honeywell Aerospace Advanced Technology
    - MIT, U. North Dakota, Certification Services Inc.
- Phases of the study
    - Tool selection: AADL-based COMPASS, OCRA/nuXmv/xSAP
    - Case study: AIR 6110 Wheel Brake System revisited
    - Integration within SysML based front-end
- Interesting research directions
    - Non linear dynamics
    - Contract debugging
    - Closed loop circuits (hydraulic, electrical) with a return path

Wilkinson, C., Hall, B., Driscoll, K., et al, “Integration of Complex Digitally Intensive Systems”, FAA Streamlining Assurance Processes Conference, Richardson TX, 13-15 September 2016.

COMPASS without AADL

Take away message:

AADL-independent COMPASS workflow

- Support for integrated contract-based hierarchical decomposition, functional verification, MBSA
- From COMPASS[AADL] …
- … to COMPASS[*]
- … aka COMPASS-STAR