COMPASS @ FBK: history, present, future

Alessandro Cimatti

Fondazione Bruno Kessler

cimatti@fbk.eu

FBK: Fondazione Bruno Kessler

- FBK: Private research foundation in Trento, Italy
- The Embedded Systems research unit
  - Marco Bozzano, Stefano Tonetta
  - Alberto Griggio, Marco Roveri
  - 25-30 people

- Research, tools and technology transfer
- Tech transfer:
  - Railways, space, avionics, process control, hardware design

- Research topics:
  - Satisfiability Modulo Theories
  - Model checking, abstraction, temporal logics, contract-based design
  - Planning, Execution monitoring, FDIR

FBK: ESA-funded projects

- COMPASS, AUTOGEF, FAME, HASDEL, CATSY
  - Requirements validation, Functional verification, safety analysis
  - Contract-based design
  - Fault detection, identification and recovery
- FOREVER
  - Contract-based design within the ESA development process
- OMC-ARE, IRONCAP (ESOC)
  - On-board model checking
  - Automated planning

Model-based design, MBSA

- Model based methods are prominent for development of control systems
  - Models to represent high level views of the system
  - Requirements precisely captured
  - Verification of high level model
  - Automated coded generation, deployment
- Model based methods are increasingly applied for the safety assessment of systems under faulty conditions

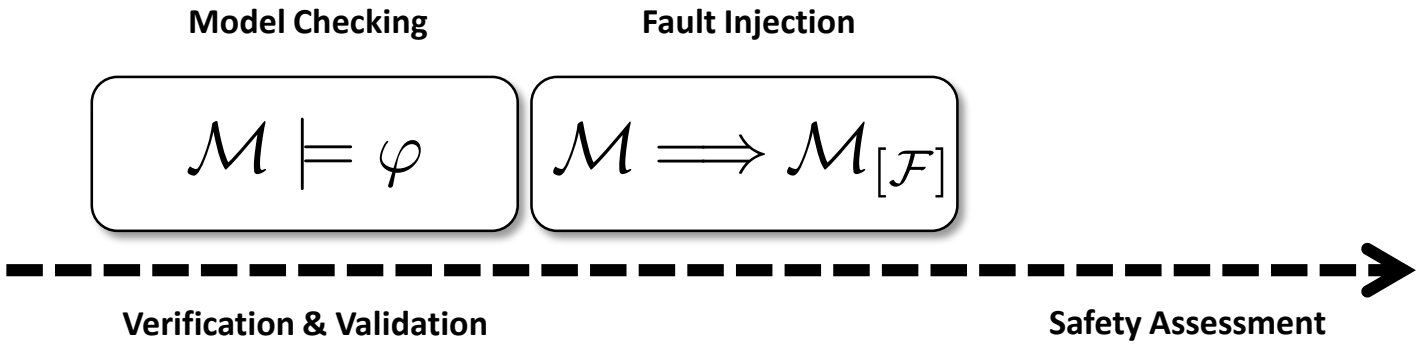
What can MBSA do?

- From nominal models to extended models
  - Fault extension
- Automated generation of
  - Fault trees
  - FMEA tables
  - Reliability measures

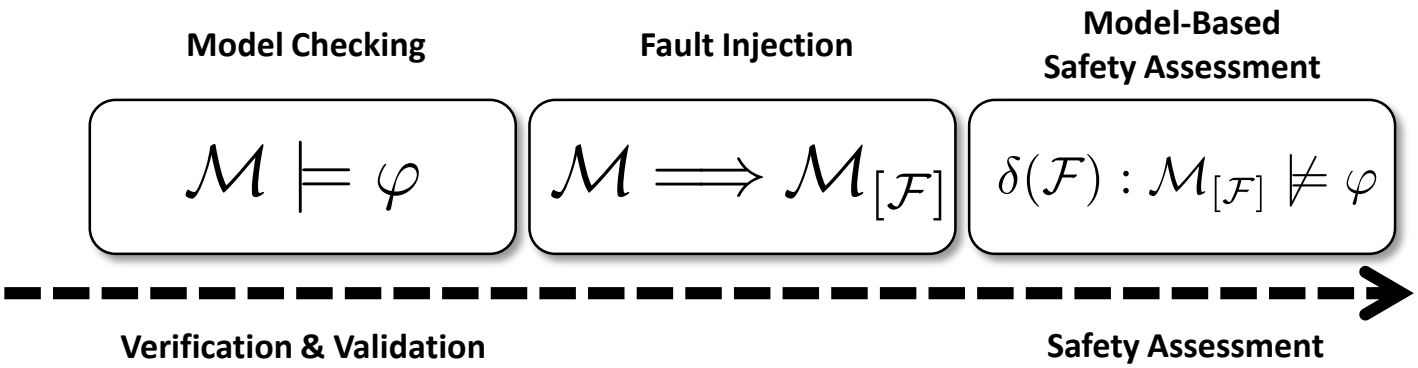
- SAFECOMP’17 and IMBSA’17 conferences @ Trento

Formal Verification, Validation, and Safety Assessment

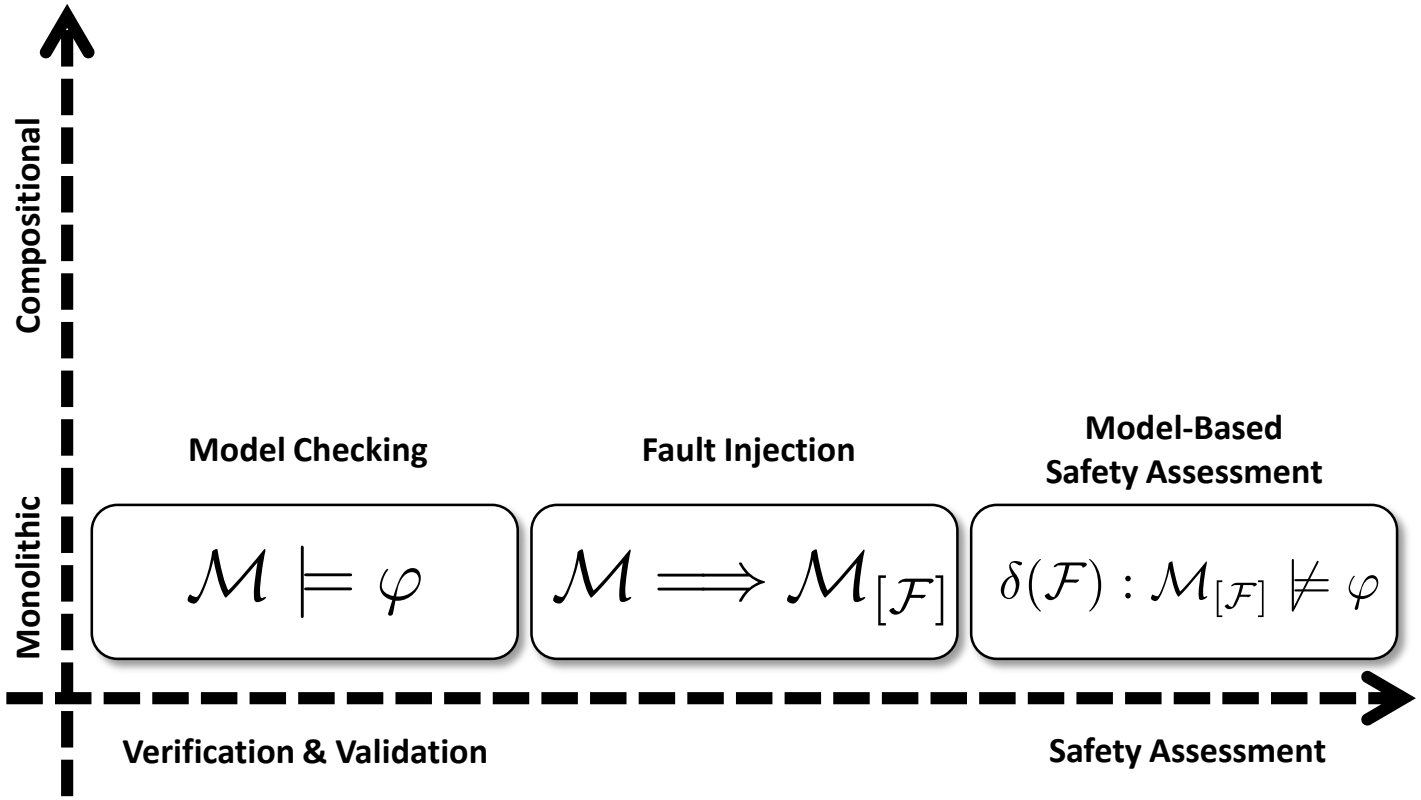
Formal Verification, Validation, and Safety Assessment



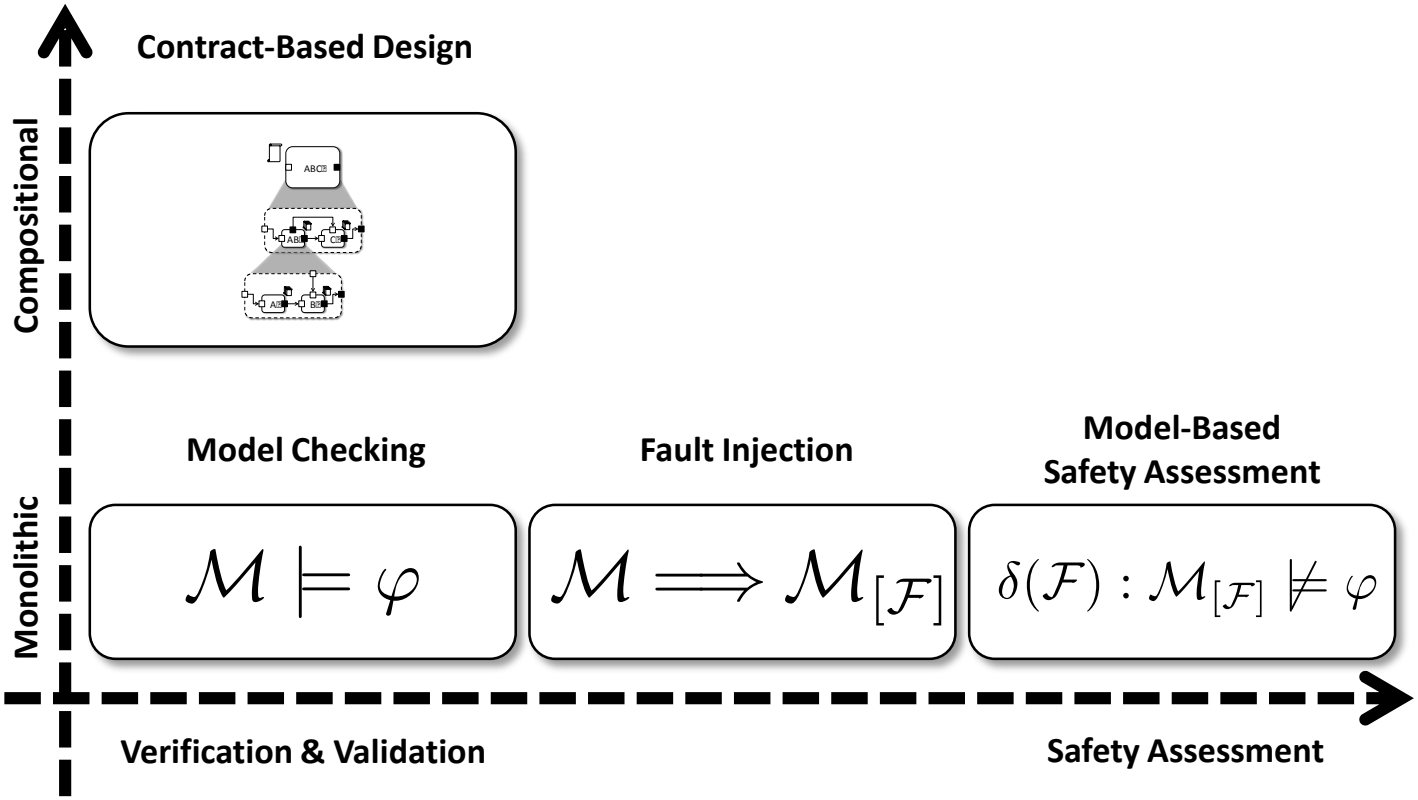
Formal Verification, Validation, and Safety Assessment



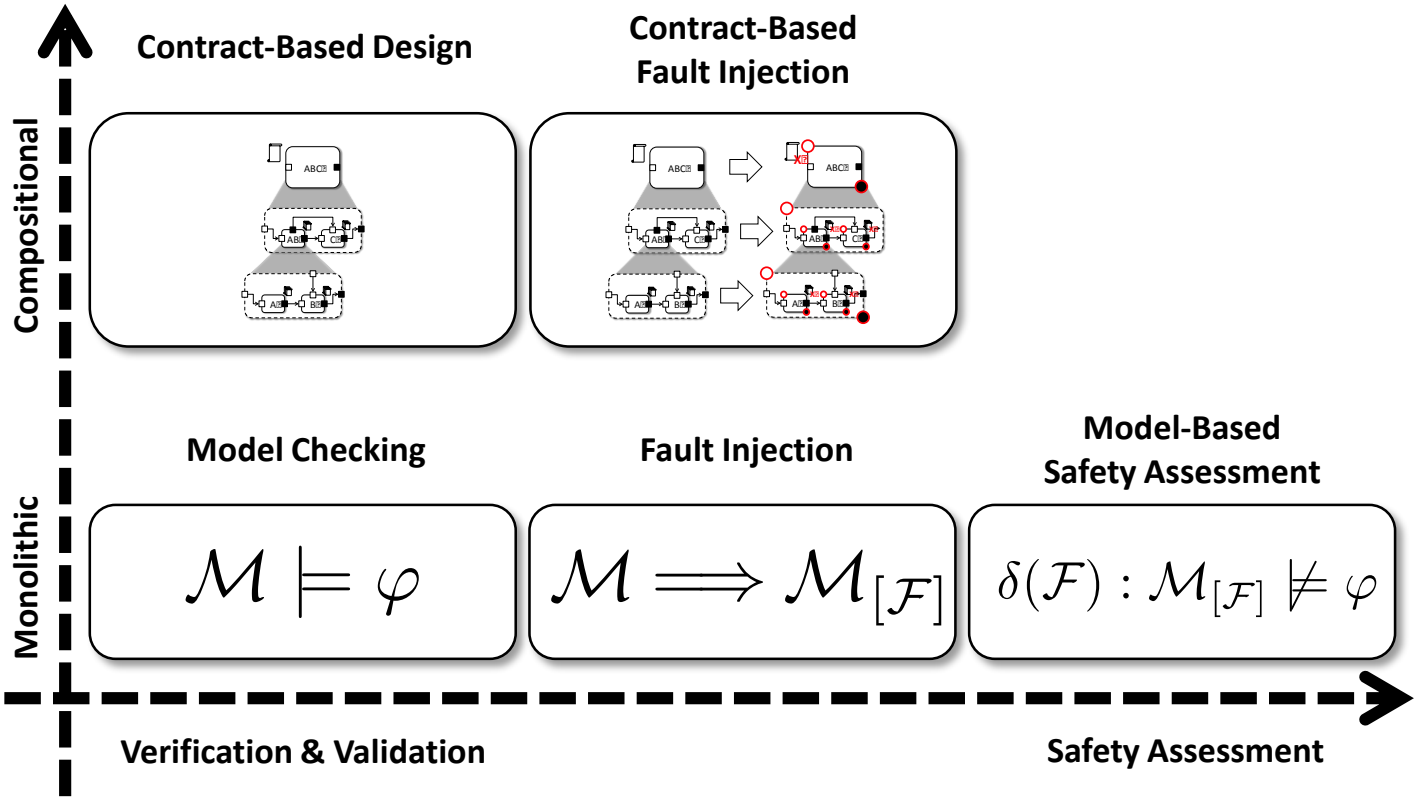
Formal Verification, Validation, and Safety Assessment



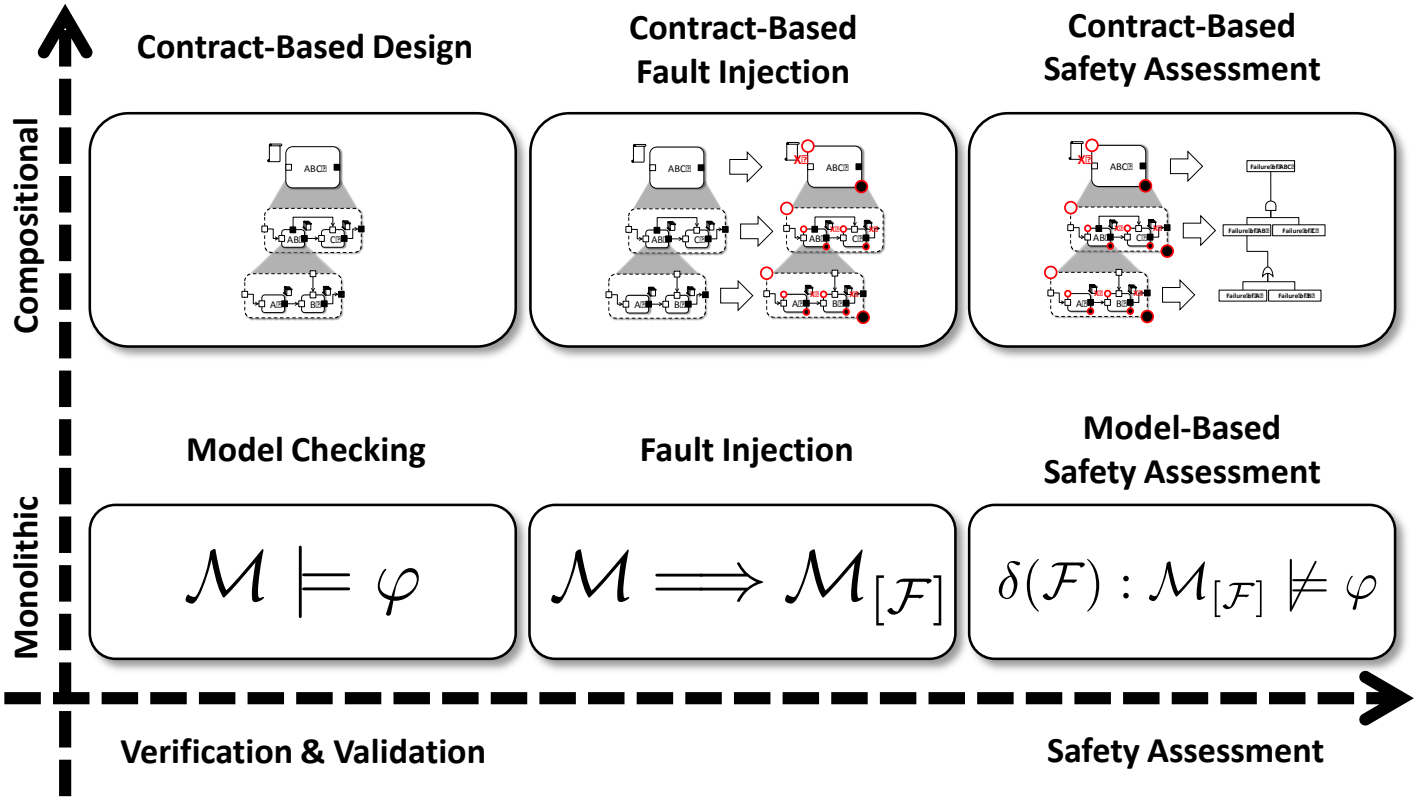
Formal Verification, Validation, and Safety Assessment



Formal Verification, Validation, and Safety Assessment



Formal Verification, Validation, and Safety Assessment



The “third” dimension

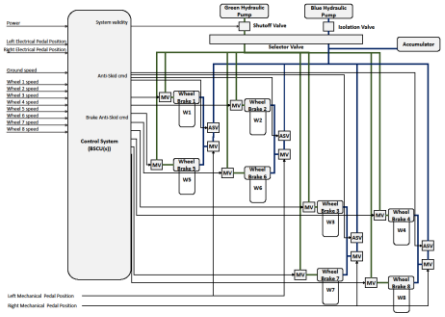
- ✓Which functions?
  - No fault vs fault
- ✓Structure?
  - Monolithic vs contract-based hierarchical decomposition
- Language expressiveness
  - Finite state, synchronous
  - Infinite state, synchronous
  - Infinite state, asynchronous
  - *Timed/hybrid, asynchronous*

Tool chain

- Infinite-state transition systems
  - The **OCRA** tool for contract-based design
    - http://ocra.fbk.eu/
  - The **nuXmv** model checker
    - http://nuxmv.fbk.eu/
  - The **xSAP** platform for safety analysis
    - http://xsap.fbk.eu/
- Hybrid systems
  - **HyCOMP** as a model checker
    - http://hycomp.fbk.eu/

A Wheel Brake System

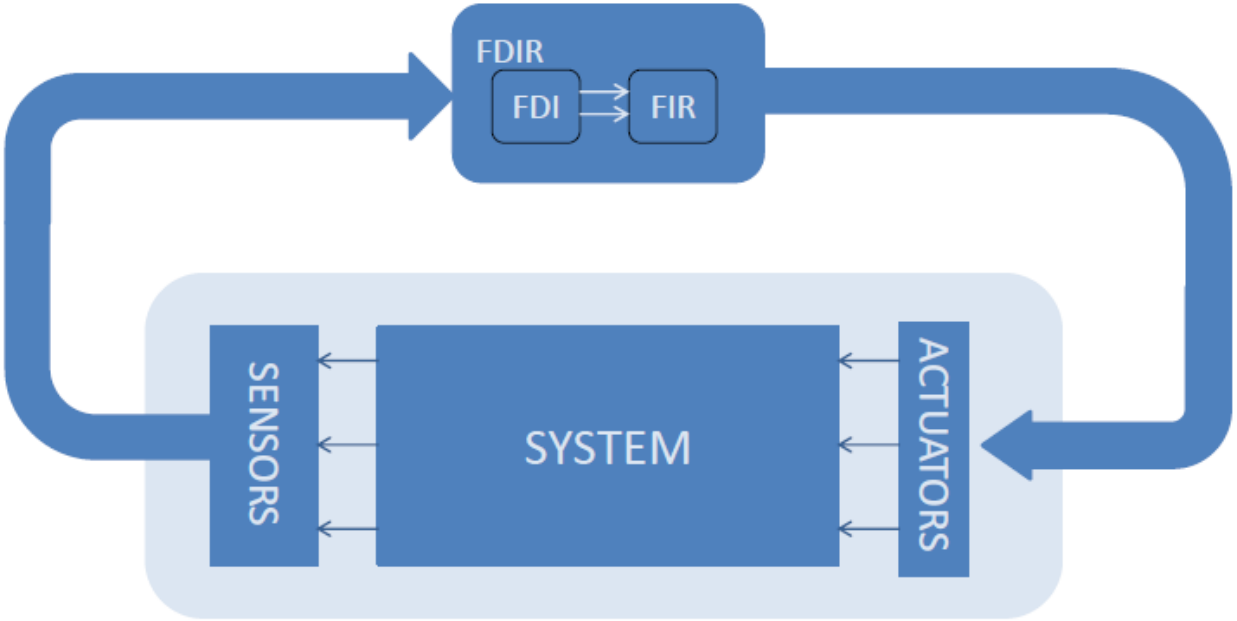
- Control brake for aircraft wheels
- Redundancy
  - Multiple BCSU
  - Hydraulic plants
- Functions
  - Asymmetrical braking
  - Antiskid
    - Single wheel/coupled
    - depending on control mode



Applications

- Joint project with Boeing on MBSA
  - Formal Design and Safety Analysis of AIR6110 Wheel Brake System [CAV'15]
- Adopted in NASA project on analysis of NextGen
  - Comparing Different Functional Allocations in Automated Air Traffic Control Design [FMCAD'15]
- Within the COMPASS tool chain
  - SLIM: AADL-based modeling language
  - Specific design techniques for FDIR

Fault Detection, Identification and Recovery (FDIR)



Towards Model Based FDIR

- Key problem: partial observability
- A theory of FDIR
  - Framework: temporal epistemic logic
    - What does observer know?
  - Many subtle issues
    - Sync vs async
    - Connection between plant and FDI
    - Distribution vs centralization
- Related topics
  - Diagnosability, Recoverability
  - Specification, Validation, Verification and Synthesis of FDI components

COMPASS
issues for the future

From COMPASS to COMPASS-STAR?

- Fundamental insight:
  - Underlying functions independent from modeling language
  - Examples:
    - SLIM modeling, and AADL for security (D-MILS)
    - The AltaRica language
    - Fortiss' AutoFocus3
    - Direct modeling in OCRA/SMV
- COMPASS-STAR[*L*] defines the functions regardless of the modeling language
- *language* could be your favourite modeling language
  - SLIM-AAD, Altarica, Simulink, UML, SysML
  - OCRA/nuXmv/XSAP tool chain as the backend

Artifacts for modeling support

- Libraries
  - Trusted components w/ contracts
  - Error models, automated model extension
- Information from models
  - Interconnection diagrams
  - Abstract machines (e.g. via predicate abstraction)
  - Fault Trees
  - FMEA tables
  - TFPG

Engines

- Optimize engines
  - Exploit contract-based design to increase scalability
  - Push FDIR-specific verification
    - Epistemic temporal logic
- Tighter integration with probabilistic models
  - COMPASS probabilities as two-stage RWTH Aachen model checkers from qualitative models

Support for design space exploration

- Modeling in the large
  - Parameters to represent design choices
  - Automate parameter space exploration
  - Quality measures for different solutions
- Synthesis of parameter valuations
  - Which values to timers/thesholds give more stability with respect to model perturbation?
- Synthesis of observability requirements
  - Which configurations of sensors that are sufficient for diagnosability/recoverability?

Conclusions

- Formal account of safety analysis and FDIR
- Supported by formal tools
- The need for a structured process

- FDIR Challenges:
  - FDI-system connection models
    - Synchronous vs asynchronous composition
    - Cycle-based vs event based
  - Centralized vs distributed approach
  - Temporal epistemic logic as back-end
  - Fault-tolerance evaluation of redundancy architectures

FUTURE of COMPASS

- How to achieve stronger COMPASS penetration?
- ADCSS FDIR session: valuable industrial feedback!
- Increase maturity of tools
  - Need for available case studies!
- Barriers to use in large companies
  - Sticky market… large tool vendors
    - But see AIR 6110 WBS experience
  - Automate connections to/from COMPASS
  - Training: courses, case studies
- Support adoption from SME's

Some (mildly) provocative statements

- Need for case studies
  - Fundamental step for FDIR community building
- Modeling language should not be a blocking issue
  - The techniques are largely independent
  - Towards COMPASS-STAR?
- Lack of GUI should not be a blocking issue
  - Textual language + artifacts viewers profitably applied in industrial settings
- Is there a need for a change?
  - “Existing process is good enough”
- “excel is not enough for designing spacecrafts” [BB, 2015, personal communication]