COMPASS3

“Consolidation of COMPASS Tools”

Marco Bozzano - Fondazione Bruno Kessler

Harold Bruintjes - RWTH Aachen University

TEC-ED & TEC-SW Final Presentation Days

ESA-ESTEC, December 7th, 2016

 © FBK; all rights reserved

Outline

- COMPASS
- History of COMPASS
- The COMPASS3 Project
- The COMPASS 3.0 Toolset
- Future Perspectives

- DEMO

© FBK; all rights reserved

Outline

- **COMPASS**
- History of COMPASS
- The COMPASS3 Project
- The COMPASS 3.0 Toolset
- Future Perspectives

- DEMO

© FBK; all rights reserved

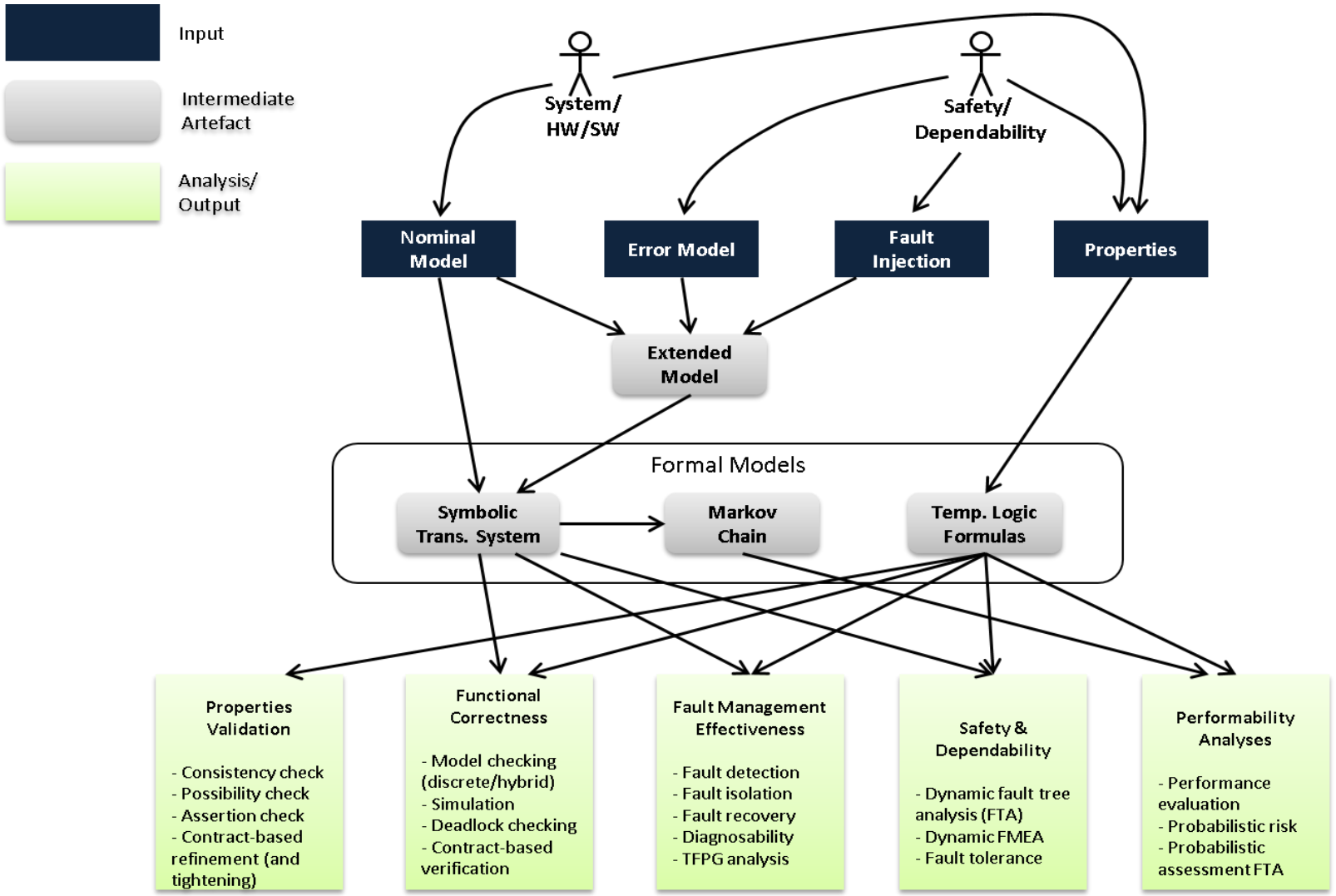
COMPASS

- Methodology and toolset for **System-Software co-engineering**
- Toolset development began in 2008
- Highlights
  - **Model-based** (modeling language is **SLIM**, a variant of AADL)
  - Based on **formal verification** engines (**model checking**)
  - Automated model extension
    - **Nominal model + Error Model + Fault Injections→ Extended model**

© FBK; all rights reserved

COMPASS

- Functionalities



© FBK; all rights reserved

Outline

- COMPASS
- **History of COMPASS**
- The COMPASS3 Project
- The COMPASS 3.0 Toolset
- Future Perspectives

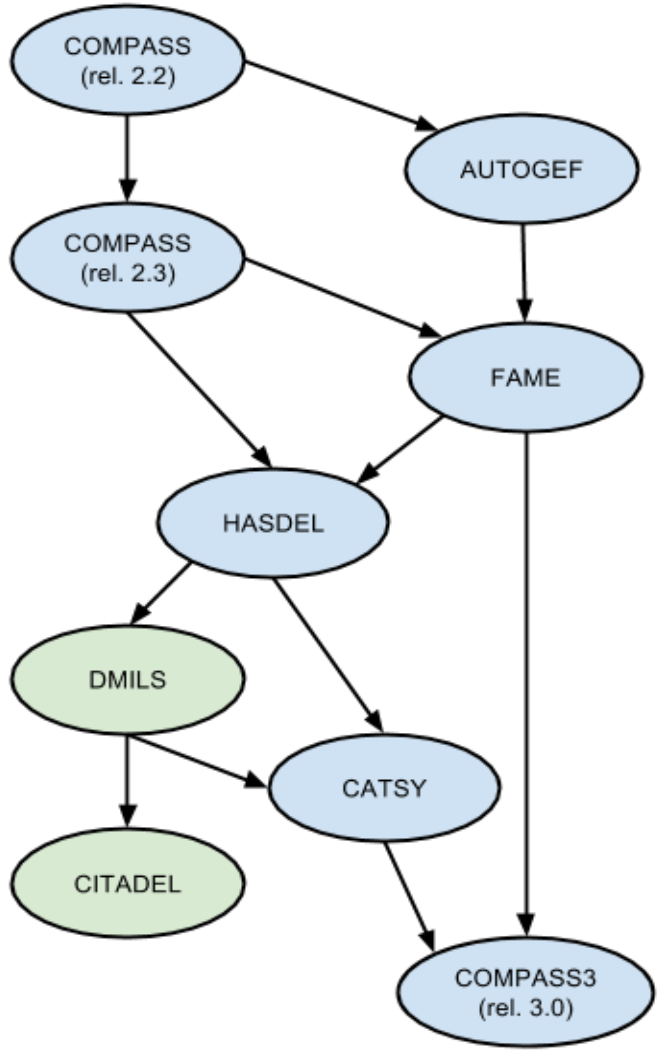
- DEMO

© FBK; all rights reserved

History of COMPASS

- Developed within several projects
  - COMPASS (2008 - 2011)
  - AUTOGEF (2011 - 2013)
  - FAME (2012 - 2014)
  - HASDEL (2013 - 2014)
  - DMILS (2013 - 2015)
  - CATSY (2014 - 2016)
  - CITADEL (2016 - 2018)

  - COMPASS3 (2015 - 2016)



ESA - funded

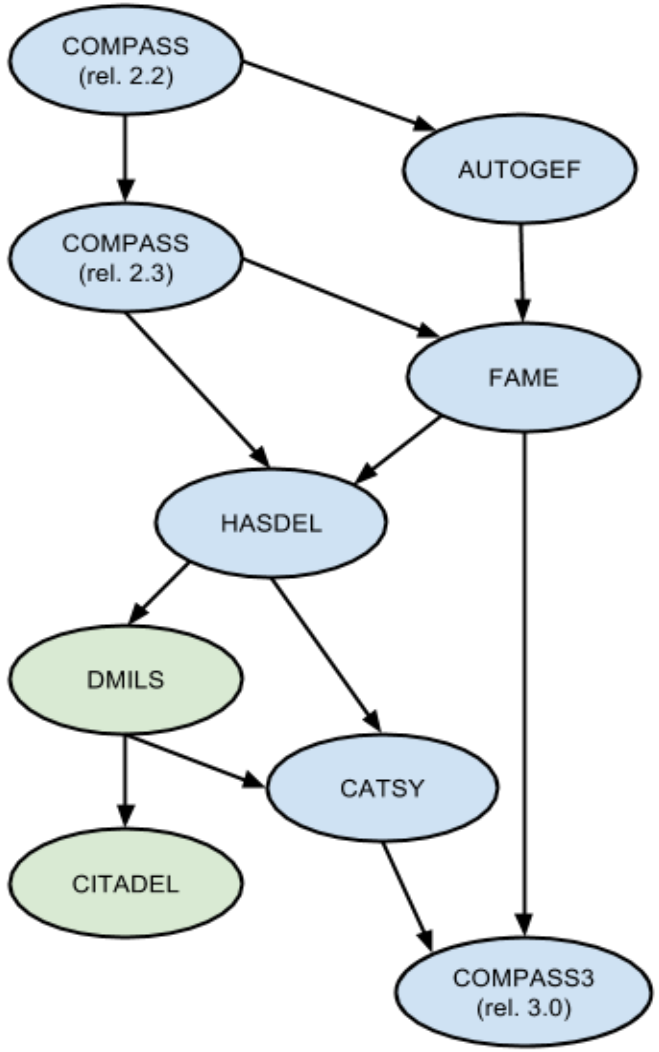
EU-funded

© FBK; all rights reserved

History of COMPASS

- Developed within several projects
  - COMPASS (2008 - 2011)

Correctness, Modelling and Performance of Aerospace Systems



ESA - funded

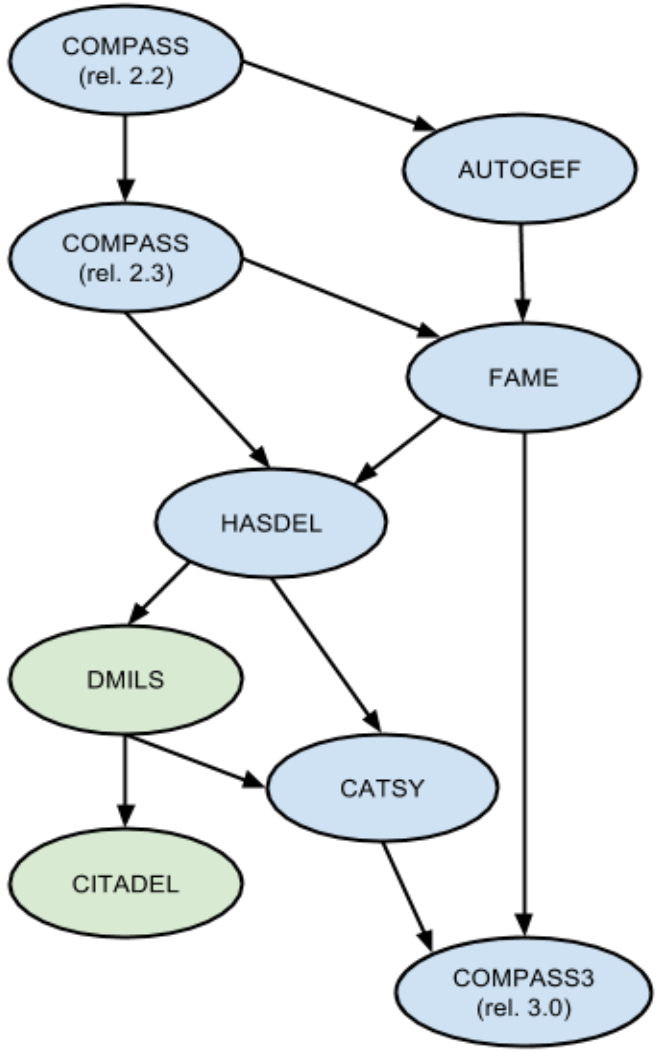
EU-funded

© FBK; all rights reserved

History of COMPASS

- Developed within several projects
  - AUTOGEF (2011 - 2013)

Automated generation of FDIR for the compass integrated toolset



ESA - funded

EU-funded

© FBK; all rights reserved

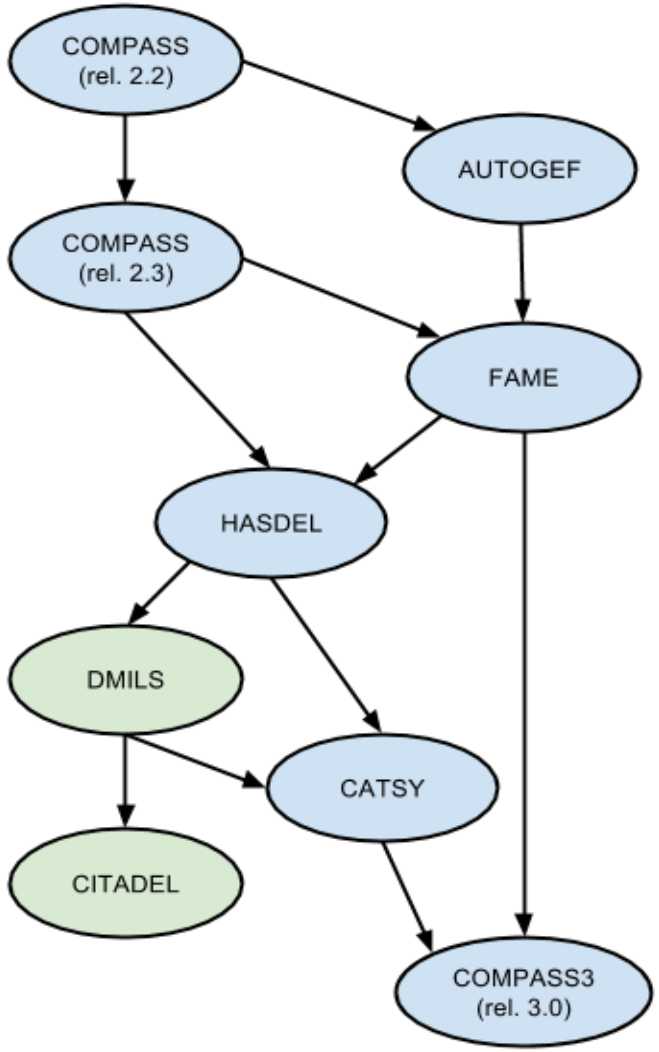
History of COMPASS

- Developed within several projects
  - FAME (2012 - 2014)

FDIR Development and Verification & Validation Process

ESA - funded

EU-funded



© FBK; all rights reserved

History of COMPASS

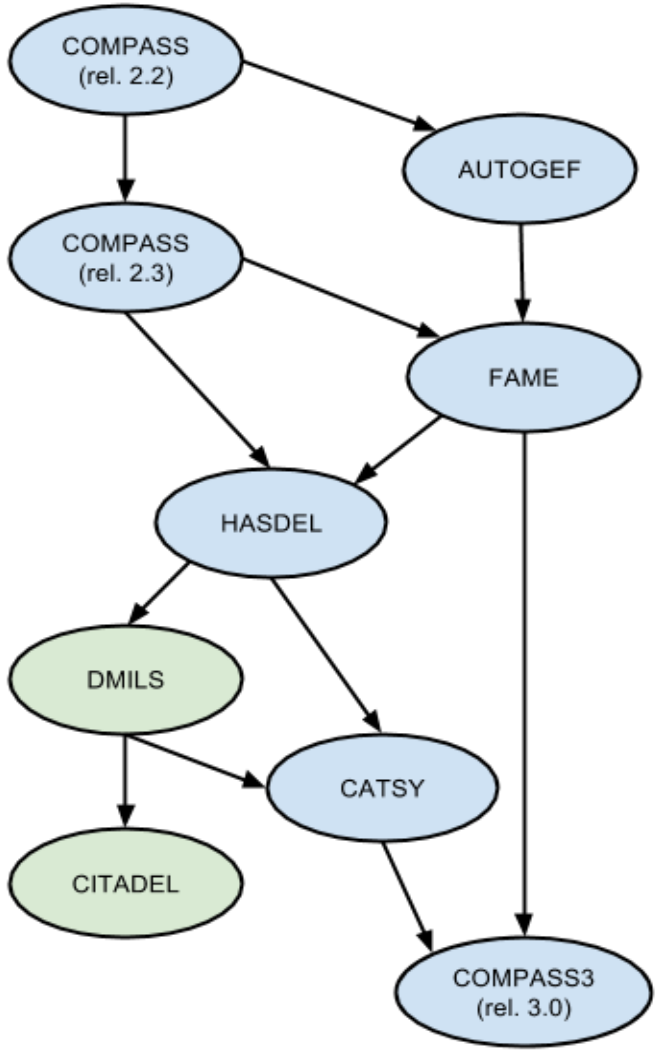
- Developed within several projects

  - HASDEL (2013 - 2014)

Hardware-Software Dependability for Launchers

ESA - funded

EU-funded



© FBK; all rights reserved

History of COMPASS

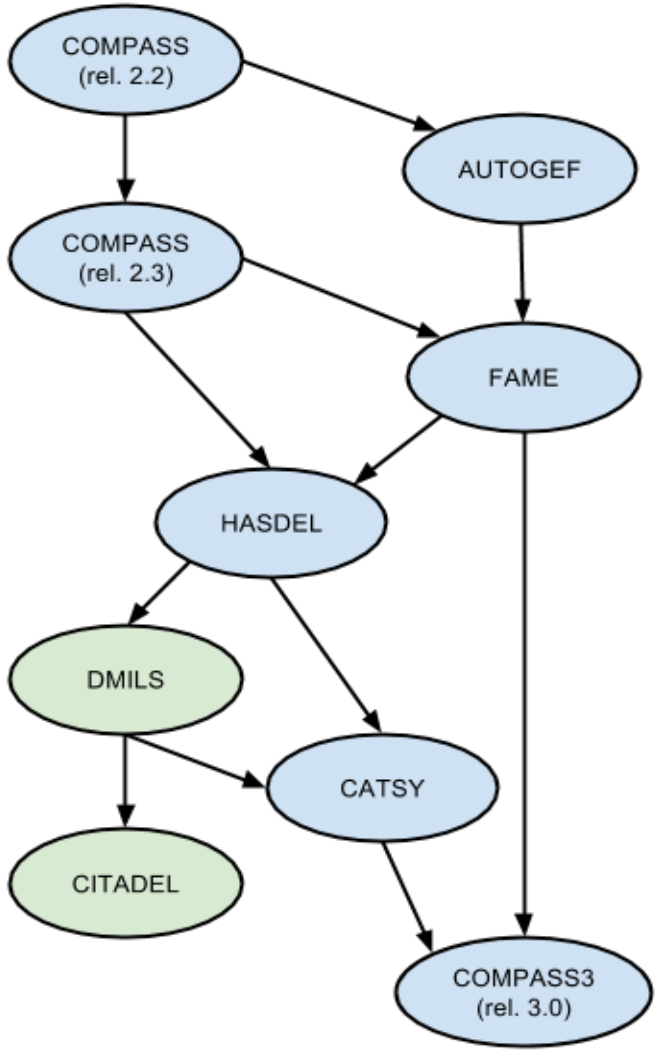
- Developed within several projects

  - DMILS (2013 - 2015)

Distributed MILS for Dependable Information and Communication Infrastructure

ESA - funded

EU-funded



© FBK; all rights reserved

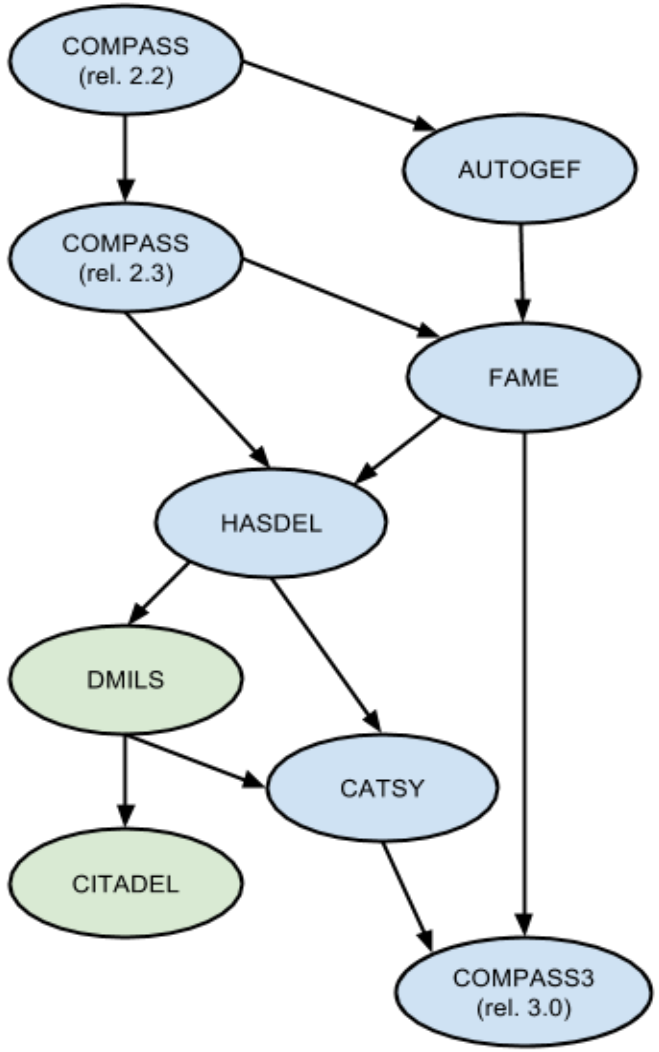
History of COMPASS

- Developed within several projects

Catalog of System and Software Properties

- CATSY (2014 - 2016)

Compare today's Catsy presentation



ESA - funded

EU-funded

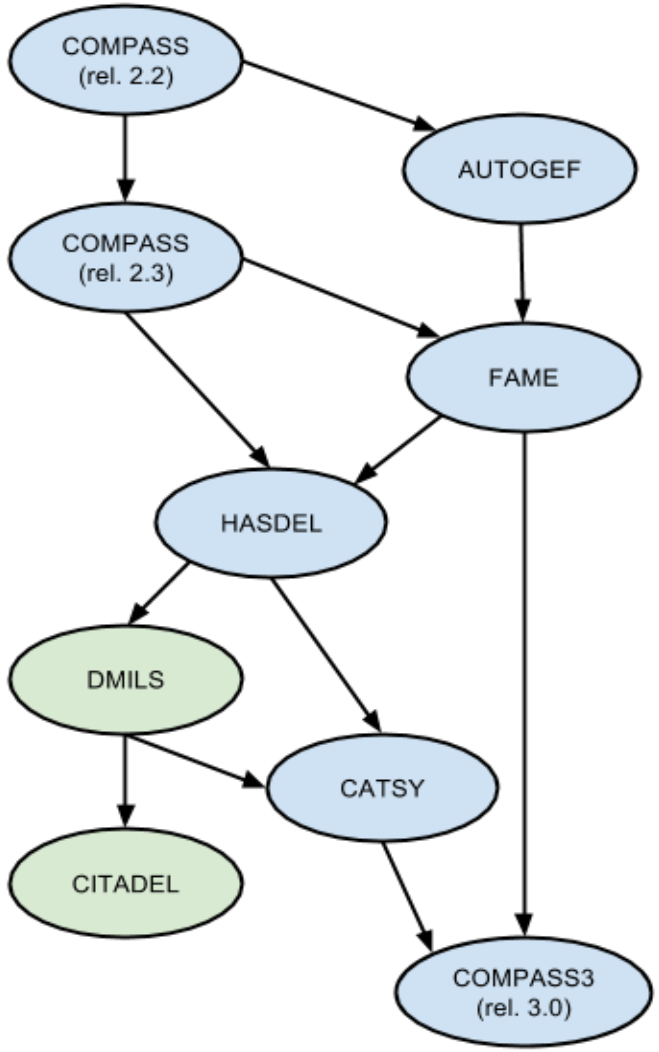
© FBK; all rights reserved

History of COMPASS

- Developed within several projects

Critical Infrastructure Protection Using Adaptive MILS

- CITADEL (2016 - 2018)



ESA - funded

EU- funded

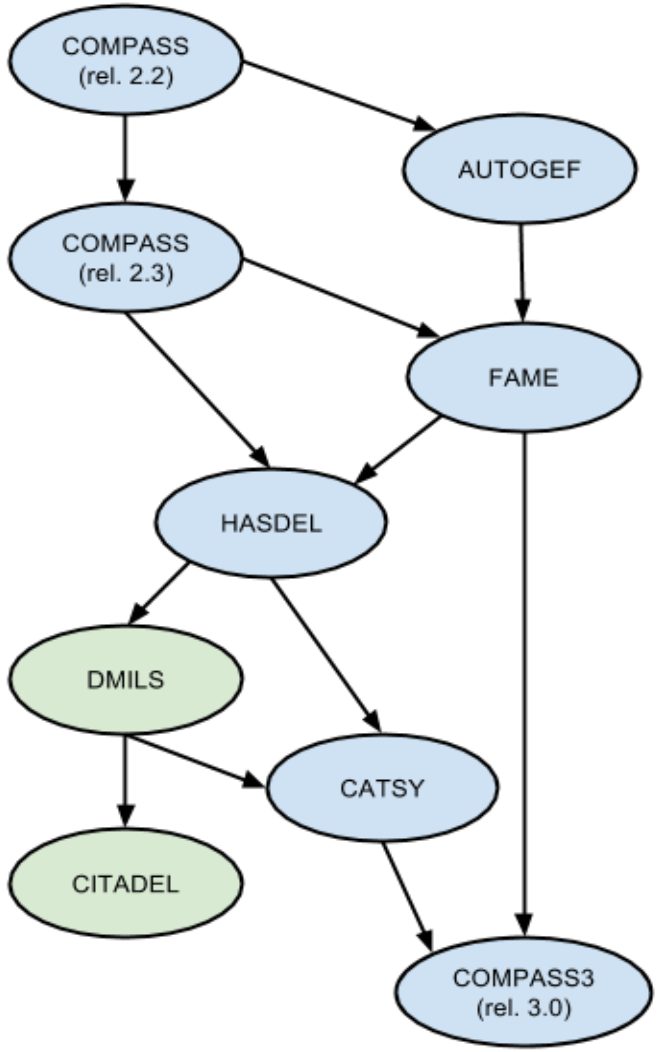
© FBK; all rights reserved

History of COMPASS

- Developed within several projects

Consolidation of COMPASS Tools

- COMPASS3 (2015 - 2016)



ESA - funded

EU-funded

© FBK; all rights reserved

Outline

- COMPASS
- History of COMPASS
- **The COMPASS3 Project**
- The COMPASS 3.0 Toolset
- Future Perspectives

- DEMO

© FBK; all rights reserved

The COMPASS3 Project

- **ESA Contract No. 4000115870/15/NL/FE/as**
- **ESA Technical Officer: Marcel Verhoef**
- Time span:
  - December 2015 - December 2016
- Consortium
  - Fondazione Bruno Kessler, Trento (Italy) (contractor)
  - RWTH Aachen University (Germany) (sub-contractor)
- Project Goals
  - Consolidation of existing COMPASS toolchain
  - Pick, integrate, and harmonize selected features from previous projects

© FBK; all rights reserved

COMPASS3 Contributions

- SLIM 3.0
  - Consolidated input language
  - Syntax and semantics - updated and fully documented
  - Improved alignment with AADL
  - Summary of new features
    - Observability attribute
    - New forms of communication and port connections
    - New types
    - Timing-related constructs and time units
    - Security-related concepts
    - Abstract component types and properties
- New example suite
  - Examples picked /extended from previous projects + new examples

© FBK; all rights reserved

COMPASS3 Contributions

- Overview of toolset enhancements
  - Improved GUI layout and usability
  - New engines (nuXmv, xSAP) and options
  - New state-of-the-art routines for verification and FTA
  - Property validation
  - Monte Carlo simulation
  - CSSP (Catalog of System and Software Properties) (from Catsy)
  - Contract-based design and verification
  - Compositional reasoning
  - Hierarchical FTA

© FBK; all rights reserved

COMPASS3 Contributions

- Maintainability
  - Porting to python 2.7
  - Linking with latest versions of libraries
  - Improved code quality and portability
  - Continuous integration
    - Development based on git repository
    - Automatic testing machinery integrated with git repository

© FBK; all rights reserved

COMPASS3 Contributions

- Documentation and dissemination
  - User manual (UPDATED)
    - Covers new functionality
    - Categorization of examples in terms of size, features, complexity
  - Tutorial (NEW)
    - Hands-on tutorial on the use of COMPASS
    - Suitable for self-study of courses
    - Covers the main functionality of the toolset
    - Hints and tips
  - Web portal compass-toolset.org (NEW)
    - Single access point to all COMPASS-related information
    - Links to previous projects
    - Publications, download page, FAQ, contact points, etc.
  - Roadmap document
    - Identifies strength and limitations, evaluates future actions

© FBK; all rights reserved

Outline

- COMPASS
- History of COMPASS
- The COMPASS3 Project
- **The COMPASS 3.0 Toolset**
- Future Perspectives

- DEMO

© FBK; all rights reserved

The COMPASS 3.0 Toolset

- Implementation
  - GUI + Command Line Interface
  - Python & PyGTK
  - Packaging as a python module
  - Verification engines: NuSMV, nuXmv, xSAP, MRMC, IMCA, Sigref
- Distribution
  - Release COMPASS 3.0
  - Expected delivery date: December 16th, 2016
  - Released as source code and as a pre-installed virtual machine
  - Available for ESA member states
  - Download page: http://www.compass-toolset.org/tools-download
  - Support: compass-support@lists.rwth-aachen.de
  - Announcements: compass-announce@lists.rwth-aachen.de
- Documentation: example suite, user manual, tutorial

© FBK; all rights reserved

Outline

- COMPASS
- History of COMPASS
- The COMPASS3 Project
- The COMPASS 3.0 Toolset
- **Future Perspectives**

- DEMO

© FBK; all rights reserved

The Future of COMPASS

- COMPASS Roadmap
  - Public document (draft) open for feedback
  - See https://indico.esa.int/indico/event/161
  - Analyzes the current status and the future of COMPASS
  - Final version due on December 16th
  - To be discussed tomorrow at the MBSSE Workshop

- MBSSE Workshop (Model Based System and Software Engineering)
  - Here - tomorrow (09:00 - 17:10)
  - Invited talks + short elevator pitches + group discussions and brainstorming
    - Share ESA's vision on MBSSE, with focus on COMPASS, TASTE and OSRA
    - Showcase some experiences gained from MBSSE applications in on-going projects
    - Discuss the potential alignment with other model-based technologies such as SysML and Arcadia
    - Identify opportunities for further collaboration, harmonization and consolidation
    - Identify next steps for technology exploitation and R&D

© FBK; all rights reserved

COMPASS Roadmap: Overview

- Goal: improve usability, visibility, market penetration, industrial usage
- Summary of future directions
  - Toolset
    - Enhance usability, TRL, compatibility with AADL
    - Develop front-end for other input languages, integration with design environments
  - Process
    - Generation of ECSS documentation, support for certification
  - Research
    - Various open research directions
    - Publications, dissemination (tutorials, courses, PhD schools)
  - Community
    - Involve the community in the identification of the needs and solutions
    - Push industrial usage/adoption of the toolset
  - Integration with ESA initiatives
    - TASTE, OSRA, …

© FBK; all rights reserved

Future Events

- Conferences in September 2017
  - **SEFM** (Software Engineering and Formal Methods) (06-08 Sept. 2017)
  - **IMBSA** (Model-Based Safety and Assessment) (11-13 Sept. 2017)
  - **Safecomp** (Computer Safety, Reliability and Security) (13-15 Sept. 2017)
- Organized by FBK, co-located in Trento, Italy
- IMBSA/Safecomp joint session on aerospace
- Web sites:
  - http://sefm17.fbk.eu
  - http://imbsa2017.fbk.eu
  - http://safecomp17.fbk.eu

© FBK; all rights reserved

Outline

- COMPASS
- History of COMPASS
- The COMPASS3 Project
- The COMPASS 3.0 Toolset
- Future Perspectives

- **DEMO**

© FBK; all rights reserved

DEMO

DEMO follows …

© FBK; all rights reserved