

The Future of COMPASS

Workshop Summary Report

Alessandro Cimatti Joost-Pieter Katoen
cimatti@fbk.eu katoen@cs.rwth-aachen.de
Fondazione Bruno Kessler RWTH Aachen University

Marcel Verhoef
Marcel.Verhoef@esa.int
European Space Agency

ESTEC, 22 October 2015

Abstract

COMPASS is a toolset for model based verification, safety and performance analysis of complex aerospace systems. It has been developed in the last years, under funding of the European Space Agency (ESA), in response to the need of a more formal and comprehensive approach to the problem of fault detection, isolation and recovery (FDIR) in autonomous systems.

On 23 October 2015, the *Future of COMPASS* workshop was held at ESTEC. During the workshop, representatives of the European academia, industry and the ESA presented the results achieved so far based on COMPASS, and discussed the strengths and weaknesses of the approach. This document describes the content of the workshop, and outlines the outcomes and the directions of future research and development.

Contents

1	Introduction	3
2	Workshop Program	4
2.1	Visions	4
2.1.1	The ESA vision	4
2.1.2	The FBK vision	5
2.1.3	The RWTH Aachen University vision	5
2.2	Technical developments	6
2.3	Applications	7
3	Discussion	8
3.1	Language	8
3.2	Analysis	9
3.3	Tools	10
3.4	Usage and Process	10
4	Planned activities	11
5	Conclusions	11
A	List of participants	12
B	Call for participation	13
C	Workshop Program	14

1 Introduction

The COMPASS toolset COMPASS is a toolset for the evaluation of system-level correctness, safety, dependability and performability of on-board computer-based aerospace systems. It supports a comprehensive process for system-software co-engineering, by covering Requirements Validation, Functional Correctness, Safety and Dependability Analysis, Performability Analysis, and has specific capabilities for the analysis and synthesis of Fault Detection, Identification and Recovery. The AADL-based input language allows for a natural modeling of the nominal and erroneous behaviours of discrete, timed and probabilistic systems. At its core, COMPASS integrates advanced model checking and probabilistic engines for the analysis of dynamic systems.

The COMPASS toolset has been developed since 2008, with funding of the European Space Agency, by Fondazione Bruno Kessler (FBK), Trento, and the RWTH Aachen University, through the projects COMPASS, AUTOGEF, FAME, HASDEL, CATSY, and COMPASS3.

Workshop Objectives COMPASS provides a wide range of techniques for the design and analysis of system safety and reliability. Its applicability has already been demonstrated in several case studies in the space domain [32, 15, 21], and also in other areas [27].

In order to understand how to bring these promising results to higher technology readiness levels, on October 23, 2015 a workshop was organized at ESTEC. The organizers invited participants from the European Space Agency, national space agencies, industry and academia, and tried to reach out to new potential users or new contributors to this initiative. The objective was to identify hurdles of introducing COMPASS in industrial practice, and discuss and explore ways these hurdles can be taken or circumvented, with potential solutions both in technology as well as process.

The workshop featured more than forty attendees, who interacted to discuss ideas and insights that will help to define the roadmap and policies for the future developments and deployment of the COMPASS toolset. Issues discussed at the workshop included the adequacy of the modeling language; forms of analysis that are missing that should be improved; whether the process associated with the toolset covers all the phases; applicability in the large; and extensions to other input languages.

The workshop program was organized in a set of presentations, and in an open discussion. The call for participation and the program are available in appendix. The slides of the presentations are available from the COMPASS workshop web site (<https://indico.esa.int/indico/event/110/>).

The COMPASS workshop was preceded by a special section on FDIR, held at the ESA Workshop on Avionics, Data, Control and Software Systems - <https://indico.esa.int/indico/event/85/>. Industrial and academic partners presented the state of the art in FDIR, and exchanged ideas on how to improve it. The discussion clearly highlighted the potential for a model-based approach for complex missions, and in some sense set the stage for the workshop.

Workshop Outcomes The open discussion helped to identify a number of directions to be pursued in order to increase the penetration of the COMPASS toolset in the current industrial practice. These include the release of COMPASS 3.0, a unified toolset integrating the functions developed in the previous projects, a second edition of the workshop, the empowerments of the user community of the COMPASS toolset, as well as the preparation of comprehensive training material and courses to be delivered in the second half of 2016.

Content This document is structured as follows. In Section 2 we review the content of the presentations. In Section 3 we report the most important points the discussion, and in Section 4 we describe the outcomes of the discussion. In Section 5 we draw some conclusions. In the appendices, we report the call for participation, the program, and the list of participants.

2 Workshop Program

In the first session, the perspectives of the ESA, FBK and RWTH were presented.

2.1 Visions

2.1.1 The ESA vision

Marcel Verhoef (ESA) presented the vision towards a structured software factory, dedicated to the design and development of space systems. The presentation covered the rationale underlying the proposed ITT's issued in the last years, (including projects oriented to the architecture definition, such as OMC-ARE, and to process, such as FOREVER and FAME). Model-based software and systems engineering was proposed as a way to manage complexity and retain consistency by way of automation and tool support.

The COMPASS toolset is intended to cover the high level (upstream) requirements and architecture phases of the development process, and to complement the TASTE toolset, which is dedicated to downstream design and implementation phases. The artifacts resulting from the upstream phases shall be aligned with the Space-Avionics Open Interface Architecture (SAVOIR). FDIR design and analysis are identified as a critical step to be moved upstream in the design cycle, as they are major risk and cost drivers in current and future space missions. FDIR is a true cross-cutting concern at system level, which affects almost all subsystems and therefore many design artifacts. The challenge is to assess the coherency of all this information, sooner rather than later, such that the implementation of FDIR, usually in the on-board software, can be properly verified and validated.

The Compass family of projects have provided a rich arsenal of tools to improve this situation and demonstrated their positive impact on several case studies. Apart from consolidation of those results, we need to better understand

how to bridge the gap between the state of the art and the state of practice, in order to improve the development of future space systems. The workshop aims to identify and discuss some of these obstacles and possible antidotes.

2.1.2 The FBK vision

Alessandro Cimatti presented the activities carried out at Fondazione Bruno Kessler within various ESA-funded projects. The underlying idea is an integrated view model based design and verification, model based safety assessment, and model-based FDIR. The unifying framework is temporal logic model checking for infinite state transition systems. It features extensions to safety analysis based on [14] and to FDIR discussed in [13]. This view is supported by the integration of the back-end tools nuXmv [23], OCRA [28] and xSAP [5]. The underlying techniques rely on advanced SMT-based model checking for infinite state transition systems, including predicate abstraction [29] and parameter synthesis [7]. The back-end is also used in integration with different languages (e.g. Altarica [16]), and in design space exploration [19, 35].

2.1.3 The RWTH Aachen University vision

Joost-Pieter Katoen presented several directions for new possible features for the COMPASS toolset: parameter synthesis, model repair, efficient analysis of dynamic fault trees, AADL2Simulink, and model-based testing of AADL models. Currently, the COMPASS toolset supports performability evaluation: given an AADL model equipped with an error model, one can analyse the probability of an error occurring within a given deadline. The underlying technique that is used is probabilistic model checking. This however requires that all probabilities occurring in the error models are known and put into the AADL model. In many cases, these probabilities are not known in advance, or at best lower and upper bounds are only known. It would therefore be interesting—and technically challenging—to consider parametric error models, in which the probabilities of faults are left (partially) unknown. Parameter synthesis focuses on determining all parameter instances such that the probability of a catastrophic failure in the entire model occurs (within a given time bound) with a given low probability. Although this is a harder problem than model checking, first approaches [31, 33] indicate that for a limited number of parameters, this problem is rather feasible and scalable. This technique thus would allow to determine e.g., the maximal tolerable fault probability such that the overall AADL model still satisfies its requirement. Another important application of this technique is model repair [36, 3]. Here, the basic idea is to tune the probabilities of a given model in such a way that a model that refutes a given performability requirement is changed such that the resulting model satisfies the requirement. Current approaches consider changes of the transition probabilities only; changes of the underlying topological structure are not considered. Different approaches exist, such as global repair [3], and the more recent technique to repair a model locally in an iterative fashion [36]. For AADL error models this technique opens the way

to tune error models such that a given performability property holds.

Dynamic fault trees (DFTs) are a well-known extension to standard fault trees that cater for common dependability patterns, such as spare management, functional dependency, and sequencing. Analysis of DFTs relies on extracting an underlying stochastic model, such as Bayesian networks, continuous-time Markov chains (CTMCs), stochastic Petri nets, and interactive Markov chains. The expressive power of DFTs is larger than that of static fault trees, and often lead to fault models that are more succinct, and thus more comprehensible. This however, comes at a price: the analysis of DFTs is more involved. It is therefore important to simplify DFTs prior to their analysis so as to make their analysis simpler and cheaper (in terms of computational resources). Key techniques are to generate the underlying state space in a compositional manner; recently this has been complemented by a novel technique to reduce the state space of DFTs prior to their analysis. The key idea is to consider DFTs as (typed) directed graphs and manipulate them by graph transformation, a powerful technique to rewrite graphs via pattern matching. We [34] present a catalogue of 28 (families of) rules that rewrite a given DFT into a smaller, equivalent DFT, having the same system reliability and availability. Experiments with 170 DFTs, originating from standard examples from the literature as well as industrial case studies from aerospace and railway engineering showed encouraging results. Rewriting enabled to cope with 49 DFTs that could not be handled before. For the other fault trees rewriting pays off, being much faster and more memory efficient, up to two orders of magnitude. This comes at no run-time penalty: graph rewriting is very fast and the stochastic model generation is significantly accelerated due to the DFT reduction. This opens the possibility of having supporting more expressive fault trees, and considering techniques on how to solve them efficiently in the COMPASS toolset.

All analysis possibilities supported by the COMPASS toolset, are model based. There are currently no (or very limited) means to check the conformance of a hardware/software implementation with respect to the AADL model. Model-based testing [20] is a technique that allows for doing this. The underlying idea is to steer the automated test generation process by the AADL model. The tests are then turned into executable test cases for a given implementation; such test cases thus are depending on the implementation at hand. As the model is used to steer the test generation; testing is sound—if an executable test fails, the implementation is not conform the AADL model; if it passes, the implementation is compliant. Finally, the possibility of AADL2Simulink was presented in which fragments of AADL are automatically translated into Simulink models. This enables amongst others the possibility to exploit automated code generation facilities for Simulink to AADL models.

2.2 Technical developments

The session on technical developments covered several aspects.

Harold Brintjes (RWTH Aachen) presented the features of SLIM, the language of the COMPASS toolset, with specific reference to the error model. The

talk described the possibility to associate error descriptions with information on the dynamics of faults, and with probability distribution.

Marco Bozzano (FBK) gave an overview of the model-based safety analysis techniques implemented in the COMPASS toolset and presented the MBSA process defined in the context of the FAME project [8, 13].

Stefano Tonetta (FBK) presented a contract-based approach to the verification of MILS-AADL models developed in the CATSY project. The approach is based on the following ingredients [30]: an architecture language, where components are decomposed into components, and implemented by state machines; a contract language, where assumptions and guarantees are represented as temporal logic formulae; a logical proof system, supporting the notion of correct contract refinement. The approach is supported by the OCRA toolset [28].

Benjamin Bittner (FBK, currently visiting ESTEC within an NPI project) reported on the application of Timed Failure Propagation Graphs (TFPG) methods [12, 9]. Precisely describing how failures propagate through a system is fundamental for successfully designing contingency mechanisms. The presentation showed the limits of current analyses such as FMECA in modeling failure propagations, based on a use case of the Solar Orbiter mission of ESA. TFPGs enable formal modeling of propagations, and formal reasoning about the relationship between failure modes, failure effects, and monitors, including propagation delays and contexts.

2.3 Applications

The session on applications included several pitch talks with overviews of various COMPASS-related activities.

Rance DeLong (The Open Group) presented an overview of the DMILS project [27], an EU-funded project where the COMPASS toolset has been extended to specify information policies, and adopted as a front-end for the configuration of the separation kernel.

Harald Ruess (Fortiss) discussed the practical experience of usage of the COMPASS toolset within the DMILS project.

Panagiotis Katsaros (Tessaloniki) gave an overview of model repair techniques [11, 37, 1, 4, 36, 25, 24].

Jean-Paul Blanquart (Airbus DS) presented an industrial perspective on model based safety assessment of space operations developed in the HASDEL project, and discussed the need for integration of failure analysis of system and operation.

Harold Brintjes (RWTH Aachen) presented an application of the stochastic MonteCarlo simulation techniques developed within the HASDEL project and applied to the analysis of a satellite system [21].

Silvia Mazzini (INTECS) presented the results of the FOREVER project [2], where the contract-based framework of [30, 28] was integrated within the CHESS [26] toolset for model-based software engineering, and customized for the ESA software reference architecture.

3 Discussion

The presentations were followed by an open discussion. Some of the questions that were posed to the audience were: Is the modeling language adequate? Which forms of analysis are missing, or should be improved? Is the process covering all the phases? Can the toolset be applied in the large? Should it be extended to other input languages?

The discussion was carried along two parallel directions: (i) where does COMPASS go? How is it going to be extended and/or improved? which are new algorithms and feature to be investigated/ developed? (ii) how can we go to real engineering? This requires input from the prime contractors! Where do they see the COMPASS capabilities in the currently adopted process? The COMPASS development team needs to understand what is the target of application, in order to prioritize the development and define the next steps.

There was a general agreement on several general facts:

- the cost of modeling is a real barrier for adoption. Thus, tooling may be helpful to reduce the modeling cost. Also improving the artifacts on which these models are based (i.e. by prescribing how information shall be organised, supported by automated extraction of this data), and starting earlier with writing (and maintaining) simple and abstract models are considered approaches to overcome these issues.
- it is fundamental to have access to case studies of realistic size.
- a policy based on small steps is more likely to success than proposing a disruptive change; integration into current practices must be supported in order to enable uptake of Compass
- look for low-hanging fruits to foster interest in the tool. In the railway domain, the low hanging fruits was improving traceability. A possible low-hanging fruit is the production of design documentation as required by the ECSS standard, as input for preliminary and critical design reviews (PDR, CDR). Increasing the quality of the input documents for those reviews, implicitly consistent by generation from the system model, will undoubtedly improve the effectiveness of these reviews.

The outcomes of the discussion was organized along the following categories: Language, Analysis, Tool, Process.

3.1 Language

- investigate the streamlining of SLIM (the AADL-based input language of the COMPASS toolset) with the official AADL. This could open up the possibility to reuse many existing tools. It was specifically suggested to investigate the alignment of SLIM with new version of error model. More in general, the AADL extensibility mechanism was mentioned as interesting.

- the extensions towards other languages (Altarica, Simulink, SysML) was discussed. It was pointed out that translations back and forth from SLIM and other models may be possible, and that the underlying SMV model could be used to maintain an alignment. The mix-and-match integration of models written in different languages was perceived to be of lower priority.
- A point was raised regarding the ability of the language to support extensions for adaptivity and dynamic reconfiguration. Satellite constellations and elastic architectures were identified as notable examples of applications.

The bottom line was that many input languages are possible, and that none will ever be a perfect solution. Suitable compromises will have to be sought.

3.2 Analysis

- A requirement is the analysis of the effect of reconfiguration actions on a TFFPG, i.e. to distinguish between reconfiguration effects on failure propagations.
- How sensitive is the model with respect to a given property? What parts of the model are easy to change without breaking it, and which ones are not? The key issue is to understand the robustness of the design.
- Scalability of the analysis, considering the trade-off between precision and quality of results (e.g. by supporting an explanation of the depth covered in bounded model checking). Consider also the conservative estimates provided by recent fault tree computation techniques [14].

Another form of trade-off can be seen at the architectural level, where components (possibly in presence of redundancy) are treated as black boxes, and modeled by means of Uninterpreted Functions [18, 17].

- Sensitivity analysis, also referred to as bottleneck analysis: what are the reasons for not reaching the output.
- Requirements relaxation: instead of forcing the improving of components to meet overly stringent requirements, relax the requirements to a degree that does not hinder the properties of the design.
- Support parametric analysis: in many situations, it is unreasonable to instantiate the parameters of the model to specific values, simply because reasonable values are not known yet. Thus, analysis techniques that support the delayed choice of the parameter values are required.
- A fundamental question is how to assess the quality of the model. An option is to simulate with respect to an expected scenario. Model validation with respect to scenario validation. Different from model based testing.

- Another interesting function is model-to-model comparison, where the model under analysis is compared against a reference model. If the reference both models are formal, this is similar to sequential equivalence checking. If the reference models is informal (e.g. represented by a set of executions), a possibility is to check if the traces can be re-execute on the model under analysis. TFGP's can also be used as reference models.

3.3 Tools

- The integration into Eclipse or other design environments was discussed. The agreement was that the development of the COMPASS toolset will focus on developing and providing services for integration, but will not directly take on any integration.
- Of course, many interesting design environments and repositories of interest for integration exist. An example is the Electronic Data Sheet (EDS); another is the coupling of Capella (architecture only, no behaviour) with the modeling capabilities of behavioural aspects in SLIM.
- It is very important to investigate the relation with other design and development tools adopted with ESA, such as the TASTE toolset. Preliminary experiments are available in [22].
- It is important to define a clear business model for the maintenance of the tool.

3.4 Usage and Process

- An industrial use case is documentation generation. The quality of diagrams should be improved. Consider also other forms of output that can be generated from models, e.g. abstract machines, Message Sequence Charts.
- The primes are using very similar FDIR concepts, based on Packet Utilization Standard (PUS). This aspect should be taken into account in COMPASS, so that a link to the PUS is maintained, with possibility to customize the models to the standard practice. This can be done by means of modeling primitives at a higher level, especially if an FDIR reference architecture is defined by ESA.

This approach was followed in the FOREVER project, with the introduction of a library of high level constructs to support a direct link to the Software Reference Architecture.

- The importance of a set of representative and available case studies in avionics and space was stressed, both to as well as an example of best practices.

4 Planned activities

Several relevant activities are planned.

The CATSY project is ongoing, and will result in the extension of the toolset with techniques for property-based and contract-based design.

The COMPASS3 project (1.12.2015 – 31.12.2016) aims at the consolidation of the COMPASS toolset, with the integration within a unique platform, of the relevant results of the previous projects. The development of the toolset will be supported more aggressive software engineering techniques (e.g. continuous integration). The COMPASS3 project will also provide additional training material and a collection of case studies, and will deliver a development roadmap for the COMPASS toolset.

The roadmap preparation will be organized in two phases, first by identifying a list of requirements by means of a structured questionnaire, and then prioritizing them based on the feedback from the potential users.

Other steps currently under discussion include a hands-on training session and an official presentation of the COMPASS roadmap in mid 2016, and a second edition of the COMPASS workshop.

5 Conclusions

This document summarizes the content of the COMPASS workshop, held in ESTEC on 22 October 2015. We overview the content of the presentations, and the outcomes of the discussion.


Two key needs have been identified. First, there is a strong need to connect the COMPASS toolset to the engineering tools currently used in the industrial practice. Second, it is fundamental that realistic case studies be made available to support the evaluation and tuning of the COMPASS toolset.

We welcome feedback and suggestions that can help the definition of a development roadmap for the COMPASS toolset and the related research. If you have feedback or questions please contact the organizers.

A List of participants


Name	Institution	City	Country
Mr. BITTNER, Benjamin	Fondazione Bruno Kessler	Trento	Italy
Mr. BLANQUART, Jean-Paul	Airbus Defence and Space	Toulouse	France
Mr. BOS, Victor	Space Systems Finland	Espoo	Finland
Dr. BOZZANO, Marco	Fondazione Bruno Kessler	Trento	Italy
Mr. BRUNTIJES, Harold	RWTH Aachen	Aachen	Germany
Prof. CHAUDRON, Michel	Chalmers University and Gothenborg University	Sätrö	Sweden
CIMATTI, Alessandro	Fondazione Bruno Kessler, Trento, Italy	Trento	Italy
Mr. DE FERLUC, Răgis	THALES ALENIA SPACE	Reading	France
Mr. DELONG, Rance	The Open Group	Reading	United Kingdom
Mr. DISSAUX, Pierre	Ellidiss Technologies	Brest	France
Mr. FISCHER, Philipp M.	Simulation and Software Technology	Braunschweig	Germany
Mr. GONSCHOREK, Tim	Otto-von-Guericke-University	Magdeburg	Germany
JUNG, Andreas	ESTEC/ESA	Noordwijk	Netherlands
Dr. KAPELLOS, Konstantinos	TRASY5	Brussels	Belgium
Prof. KATSDEN, Joost-Pieter	RWTH Aachen University	Aachen	Germany
Prof. KATSAROS, Panagiotis	Aristotle University of Thessaloniki	Thessaloniki	Greece
Mr. KOVALOV, Andrii	DLR	Braunschweig	Germany
Mr. LEORATO, Cristiano	RHEA c/o ESA/ESTEC TEC-SW	CRETEIL	France
Mrs. MAZZINI, Silvia	Intecs	Pisa	Italy
Dr. MOROZOV, Andrey	TU Dresden	Dresden	Germany
Prof. NOLL, Thomas	RWTH Aachen University	52056 Aachen	Germany
Mr. OGANESSIAN, Andrei	ESA	Noordwijk	Netherlands
Prof. ORTMEIER, Frank	Otto-von-Guericke-University	Magdeburg	Germany
Mr. PERROTTIN, Maxime	ESA	Noordwijk	Netherlands
Prof. PORTINALE, Luigi	University of Piemonte Orientale	Alessandria	Italy
Dr. RUESS, Harald	fortiss GmbH	Munich	Germany
Dr. RUGINA, Ana	ESA	Noordwijk	Netherlands
Mr. SANMARTÃO, Joaquim	CTD	Barcelona	Spain
Mr. SCHAUS, Volker	DLR Simulation and Software Technology	Braunschweig	Germany
Mr. SILVEIRA, Daniel	GMV	Lisboa	Portugal
Mr. TIPALDI, Massimo	OHB System AG	Bremen	Germany
TONETTA, Stefano	FBK-irst	Trento	Italy
Dr. VERHOEF, Marcel	ESA/ESTEC	Noordwijk	Netherlands
Mr. YUSHTEIN, Yuri	ESA/ESTEC	Noordwijk	Netherlands

B Call for participation



The Future of COMPASS

Call for Participation



Workshop organized by the European Space Agency,
Fondazione Bruno Kessler, and RWTH Aachen

ESTEC, 22 October 2015

Context: COMPASS is a toolset for the evaluation of system-level correctness, safety, dependability and performability of on-board computer-based aerospace systems. It supports a comprehensive process for system-software co-engineering, by covering Requirements Validation, Functional Correctness, Safety and Dependability Analysis, Performability Analysis, and has specific capabilities for the analysis and synthesis of Fault Detection, Identification and Recovery. The AADL-based input language allows for a natural modeling of the nominal and erroneous behaviours of discrete, timed and probabilistic systems. At its core, COMPASS integrates advanced model checking and probabilistic engines for the analysis of dynamic systems.

COMPASS has been developed since 2008, with funding of the European Space Agency, by Fondazione Bruno Kessler (FBK), Trento, and the RWTH Aachen, through the projects COMPASS, AUTOGEF, FAME, HASDEL, and CATSY.

Objective: COMPASS provides a wide range of techniques for the design and analysis of system safety and reliability, whose applicability has already been demonstrated in several case studies. The objective of the workshop is to understand how to bring these promising results to higher technology readiness levels. We would like to interact with the audience to identify hurdles of introducing COMPASS in industrial practice, and discuss and explore ways these hurdles can be taken or circumvented, with potential solutions both in technology as well as process.

The workshop organizers welcome attendance from ESA, national space agencies, industry and academia, in particular new potential users or new contributors to this initiative. Questions that we would like to discuss at the workshop include:

Is the modeling language adequate? Which forms of analysis are missing, or should be improved? Is the process covering all the phases? Can the toolset be applied in the large? Should it be extended to other input languages?

Ideally, the workshop will result in a list of ideas and insights that will help to define the roadmap and policies for the future developments and deployment of the COMPASS toolset.

Tentative Structure:

8.30-9.30 Vision:

- ESA / FBK / RWTH vision for COMPASS future

9.30-10.30 Current State:

- Technical Achievements (e.g., projects and technical results)
- Practical Achievements (e.g., successful applications of COMPASS)
- Relation with other ESA projects (e.g., TASTE)


10.30-11.00 Coffee Break

11.00-12.00 Limitations and Future Directions:


- Experience and needs from ESA and industrial side
- Technical developments that might be interesting

12.00-12.45 Open Discussion

12.45-13.00 Round-up and closing remarks





Info/registration at <https://indico.esa.int/indico/event/110/>



C Workshop Program

The Future of COMPASS

Workshop organized by the European Space Agency,
Fondazione Bruno Kessler, and RWTH Aachen
ESTEC, 22 October 2015



8.30-9.30 Vision

- Marcel Verhoef: ESA vision for COMPASS future
- Alessandro Cimatti: FBK vision for COMPASS future
- Joost-Pieter Katoen: RWTH vision for COMPASS future

9.30-10.30 Current State

- Thomas Noll: Error modeling in COMPASS
- Marco Bozzano: Safety Assessment in COMPASS
- Stefano Tonetta: Contract-based verification of AADL models
- Benjamin Bittner: Fault propagation modeling and analysis via TFFG

10.30-11.00 Coffee Break

11.00-12.00 Open Challenges and Future Directions

- Rance De Long: The Marriage of COMPASS and MILS
- Harald Ruess: COMPASS in the D-MILS project - an experience report
- Jean-Paul Blanquart: Model based safety assessment of space operations – toward integration of failure analysis of system and operation
- Harold Bruintjes: A Statistical Approach for Timed Reachability in AADL Models
- Silvia Mazzini: The FoReVer MBSE solution for system composition correctness analysis

12.00-12.45 Open Discussion

12.45-13.00 Round-up and closing remarks

Context: COMPASS is a toolset for the evaluation of system-level correctness, safety, dependability and performability of on-board computer-based aerospace systems. It supports a comprehensive process for system-software co-engineering, by covering Requirements Validation, Functional Correctness, Safety and Dependability Analysis, Performability Analysis, and has specific capabilities for the analysis and synthesis of Fault Detection, Identification and Recovery. The AADL-based input language allows for a natural modeling of the nominal and erroneous behaviours of discrete, timed and probabilistic systems. At its core, COMPASS integrates advanced model checking and probabilistic engines for the analysis of dynamic systems.



COMPASS has been developed since 2008, with funding of the European Space Agency, by Fondazione Bruno Kessler (FBK), Trento, and the RWTH Aachen, through the projects COMPASS, AUTOGEP, FAME, HASDEL, and CATSY.

Objective: COMPASS provides a wide range of techniques for the design and analysis of system safety and reliability, whose applicability has already been demonstrated in several case studies. The objective of the workshop is to understand how to bring these promising results to higher technology readiness levels. We would like to interact with the audience to identify hurdles of introducing COMPASS in industrial practice, and discuss and explore ways these hurdles can be taken or circumvented, with potential solutions both in technology as well as process. The workshop organizers welcome attendance from ESA, national space agencies, industry and academia, in particular new potential users or new contributors to this initiative.

Questions that we would like to discuss at the workshop include:

Is the modeling language adequate? Which forms of analysis are missing, or should be improved? Is the process covering all the phases? Can the toolset be applied in the large? Should it be extended to other input languages?

Ideally, the workshop will result in a list of ideas and insights that will help to define the roadmap and policies for the future developments and deployment of the COMPASS toolset.



Info/registration at <https://indico.esa.int/indico/event/110/>

References

- [1] Paul C. Attie, Ali Cherri, Kinan Dak Al Bab, Mohamad Sakr, and Jad Saklawi. Model and program repair via SAT solving. In *13. ACM/IEEE International Conference on Formal Methods and Models for Codesign, MEMOCODE 2015, Austin, TX, USA, September 21-23, 2015*, pages 148–157. IEEE, 2015.
- [2] Laura Baracchi, Alessandro Cimatti, Gerald Garcia, Silvia Mazzini, Stefano Puri, and Stefano Tonetta. Requirements refinement and component reuse: The forever contract-based approach. In Alessandra Bagnato, Leandro Soares Indrusiak, Imran Rafiq Quadri, and Matteo Rossi, editors, *Handbook of Research on Embedded Systems Design, Advances in Systems Analysis, Software Engineering, and High-Performance Computing*, pages 209–241. IGI Global, 2014.
- [3] Ezio Bartocci, Radu Grosu, Panagiotis Katsaros, C. R. Ramakrishnan, and Scott A. Smolka. Model repair for probabilistic systems. In Parosh Aziz Abdulla and K. Rustan M. Leino, editors, *Tools and Algorithms for the Construction and Analysis of Systems - 17th International Conference, TACAS 2011, Held as Part of the Joint European Conferences on Theory and Practice of Software, ETAPS 2011, Saarbrücken, Germany, March 26-April 3, 2011. Proceedings*, volume 6605 of *Lecture Notes in Computer Science*, pages 326–340. Springer, 2011.
- [4] Ezio Bartocci, Radu Grosu, Panagiotis Katsaros, C.R. Ramakrishnan, and Scott A. Smolka. Model repair for probabilistic systems. In Parosh Aziz Abdulla and K. Rustan M. Leino, editors, *Tools and Algorithms for the Construction and Analysis of Systems*, volume 6605 of *Lecture Notes in Computer Science*, pages 326–340. Springer Berlin Heidelberg, 2011.
- [5] Benjamin Bittner, Marco Bozzano, Roberto Cavada, Alessandro Cimatti, Marco Gario, Alberto Griggio, Cristian Mattarei, Andrea Micheli, and Gianni Zampedri. The xsap safety analysis platform. In Marsha Chechik and Jean-François Raskin, editors, *Tools and Algorithms for the Construction and Analysis of Systems - 22nd International Conference, TACAS 2016, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2016, Eindhoven, The Netherlands, April 2-8, 2016, Proceedings*, volume 9636 of *Lecture Notes in Computer Science*, pages 533–539. Springer, 2016.
- [6] Benjamin Bittner, Marco Bozzano, and Alessandro Cimatti. Automated synthesis of timed failure propagation graphs. In Subbarao Kambhampati, editor, *Proceedings of the Twenty-Fifth International Joint Conference on Artificial Intelligence, IJCAI 2016, New York, NY, USA, 9-15 July 2016*, pages 972–978. IJCAI/AAAI Press, 2016.

- [7] Benjamin Bittner, Marco Bozzano, Alessandro Cimatti, Marco Gario, and Alberto Griggio. Towards pareto-optimal parameter synthesis for monotonic cost functions. In *Formal Methods in Computer-Aided Design, FMCAD 2014, Lausanne, Switzerland, October 21-24, 2014*, pages 23–30. IEEE, 2014.
- [8] Benjamin Bittner, Marco Bozzano, Alessandro Cimatti, and Xavier Olive. Symbolic synthesis of observability requirements for diagnosability. In Jörg Hoffmann and Bart Selman, editors, *Proceedings of the Twenty-Sixth AAAI Conference on Artificial Intelligence, July 22-26, 2012, Toronto, Ontario, Canada*. AAAI Press, 2012.
- [9] Benjamin Bittner, Marco Bozzano, Alessandro Cimatti, and Gianni Zampedri. Automated verification and tightening of failure propagation models. In *Proceedings of the 30th AAAI Conference on Artificial Intelligence (AAAI 2016)*, 2016. (to appear).
- [10] Benjamin Bittner, Marco Bozzano, Alessandro Cimatti, and Gianni Zampedri. Automated verification and tightening of failure propagation models. In Dale Schuurmans and Michael P. Wellman, editors, *Proceedings of the Thirtieth AAAI Conference on Artificial Intelligence, February 12-17, 2016, Phoenix, Arizona, USA*, pages 907–913. AAAI Press, 2016.
- [11] Borzoo Bonakdarpour, SandeepS. Kulkarni, and Fuad Abujarad. Symbolic synthesis of masking fault-tolerant distributed programs. *Distributed Computing*, 25(1):83–108, 2012.
- [12] Marco Bozzano, Alessandro Cimatti, Marco Gario, and Andrea Micheli. Smt-based validation of timed failure propagation graphs. In Blai Bonet and Sven Koenig, editors, *Proceedings of the Twenty-Ninth AAAI Conference on Artificial Intelligence, January 25-30, 2015, Austin, Texas, USA*, pages 3724–3730. AAAI Press, 2015.
- [13] Marco Bozzano, Alessandro Cimatti, Marco Gario, and Stefano Tonetta. Formal design of fault detection and identification components using temporal epistemic logic. In Erika Ábrahám and Klaus Havelund, editors, *Tools and Algorithms for the Construction and Analysis of Systems - 20th International Conference, TACAS 2014, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2014, Grenoble, France, April 5-13, 2014. Proceedings*, volume 8413 of *Lecture Notes in Computer Science*, pages 326–340. Springer, 2014.
- [14] Marco Bozzano, Alessandro Cimatti, Alberto Griggio, and Cristian Mattarei. Efficient anytime techniques for model-based safety analysis. In Daniel Kroening and Corina S. Pasareanu, editors, *Computer Aided Verification - 27th International Conference, CAV 2015, San Francisco, CA, USA, July 18-24, 2015, Proceedings, Part I*, volume 9206 of *Lecture Notes in Computer Science*, pages 603–621. Springer, 2015.

- [15] Marco Bozzano, Alessandro Cimatti, Joost-Pieter Katoen, Panagiotis Katsaros, Konstantinos Mokoš, Viet Yen Nguyen, Thomas Noll, Bart Postma, and Marco Roveri. Spacecraft early design validation using formal methods. *Rel. Eng. & Sys. Safety*, 132:20–35, 2014.
- [16] Marco Bozzano, Alessandro Cimatti, Oleg Lisagor, Cristian Mattarei, Sergio Mover, Marco Roveri, and Stefano Tonetta. Safety assessment of altair models via symbolic model checking. *Sci. Comput. Program.*, 98:464–483, 2015.
- [17] Marco Bozzano, Alessandro Cimatti, and Cristian Mattarei. Automated analysis of reliability architectures. In *2013 18th International Conference on Engineering of Complex Computer Systems, Singapore, July 17-19, 2013*, pages 198–207. IEEE Computer Society, 2013.
- [18] Marco Bozzano, Alessandro Cimatti, and Cristian Mattarei. Efficient analysis of reliability architectures via predicate abstraction. In Valeria Bertacco and Axel Legay, editors, *Hardware and Software: Verification and Testing - 9th International Haifa Verification Conference, HVC 2013, Haifa, Israel, November 5-7, 2013, Proceedings*, volume 8244 of *Lecture Notes in Computer Science*, pages 279–294. Springer, 2013.
- [19] Marco Bozzano, Alessandro Cimatti, A. Fernandes Pires, D. Jones, G. Kimberly, T. Petri, R. Robinson, and Stefano Tonetta. Formal design and safety analysis of AIR6110 wheel brake system. In Daniel Kroening and Corina S. Pasareanu, editors, *Computer Aided Verification - 27th International Conference, CAV 2015, San Francisco, CA, USA, July 18-24, 2015, Proceedings, Part I*, volume 9206 of *Lecture Notes in Computer Science*, pages 518–535. Springer, 2015.
- [20] Manfred Broy, Bengt Jonsson, Joost-Pieter Katoen, Martin Leucker, and Alexander Pretschner, editors. *Model-Based Testing of Reactive Systems, Advanced Lectures [The volume is the outcome of a research seminar that was held in Schloss Dagstuhl in January 2004]*, volume 3472 of *Lecture Notes in Computer Science*. Springer, 2005.
- [21] Harold Brintjes, Joost-Pieter Katoen, and David Lesens. A statistical approach for timed reachability in AADL models. In *45th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, DSN 2015, Rio de Janeiro, Brazil, June 22-25, 2015*, pages 81–88. IEEE, 2015.
- [22] Roberto Cavada, Alessandro Cimatti, Luigi Crema, Mattia Roccabruna, and Stefano Tonetta. Model-based design of an energy-system embedded controller using taste. In John S. Fitzgerald, Constance L. Heitmeyer, Stefania Gnesi, and Anna Philippou, editors, *FM 2016: Formal Methods - 21st International Symposium, Limassol, Cyprus, November 9-11, 2016, Proceedings*, volume 9995 of *Lecture Notes in Computer Science*, pages 741–747, 2016.

- [23] Roberto Cavada, Alessandro Cimatti, Michele Dorigatti, Alberto Griggio, Alessandro Mariotti, Andrea Micheli, Sergio Mover, Marco Roveri, and Stefano Tonetta. The nuxmv symbolic model checker. In Armin Biere and Roderick Bloem, editors, *Computer Aided Verification - 26th International Conference, CAV 2014, Held as Part of the Vienna Summer of Logic, VSL 2014, Vienna, Austria, July 18-22, 2014. Proceedings*, volume 8559 of *Lecture Notes in Computer Science*, pages 334–342. Springer, 2014.
- [24] George Chatzieftheriou, Borzoo Bonakdarpour, Panagiotis Katsaros, and Scott A. Smolka. Abstract model repair. *Logical Methods in Computer Science*, 11(3), 2015.
- [25] Taolue Chen, E.M. Hahn, Tingting Han, M. Kwiatkowska, Hongyang Qu, and Lijun Zhang. Model repair for markov decision processes. In *Theoretical Aspects of Software Engineering (TASE), 2013 International Symposium on*, pages 85–92, July 2013.
- [26] Antonio Cicchetti, Federico Ciccozzi, Silvia Mazzini, Stefano Puri, Marco Panunzio, Alessandro Zovi, and Tullio Vardanega. CHESS: a model-driven engineering tool environment for aiding the development of complex industrial systems. In Michael Goedicke, Tim Menzies, and Motoshi Saeki, editors, *IEEE/ACM International Conference on Automated Software Engineering, ASE’12, Essen, Germany, September 3-7, 2012*, pages 362–365. ACM, 2012.
- [27] Alessandro Cimatti, Rance DeLong, Davide Marcantonio, and Stefano Tonetta. Combining MILS with contract-based design for safety and security requirements. In Floor Koornneef and Coen van Gulijk, editors, *Computer Safety, Reliability, and Security - SAFECOMP 2015 Workshops, ASSURE, DECSoS, ISSE, ReSA4CI, and SASSUR, Delft, The Netherlands, September 22, 2015, Proceedings*, volume 9338 of *Lecture Notes in Computer Science*, pages 264–276. Springer, 2015.
- [28] Alessandro Cimatti, Michele Dorigatti, and Stefano Tonetta. OCRA: A tool for checking the refinement of temporal contracts. In Ewen Denney, Tefik Bultan, and Andreas Zeller, editors, *2013 28th IEEE/ACM International Conference on Automated Software Engineering, ASE 2013, Silicon Valley, CA, USA, November 11-15, 2013*, pages 702–705. IEEE, 2013.
- [29] Alessandro Cimatti, Alberto Griggio, Sergio Mover, and Stefano Tonetta. IC3 modulo theories via implicit predicate abstraction. In Erika Ábrahám and Klaus Havelund, editors, *Tools and Algorithms for the Construction and Analysis of Systems - 20th International Conference, TACAS 2014, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2014, Grenoble, France, April 5-13, 2014. Proceedings*, volume 8413 of *Lecture Notes in Computer Science*, pages 46–61. Springer, 2014.

- [30] Alessandro Cimatti and Stefano Tonetta. Contracts-refinement proof system for component-based embedded systems. *Sci. Comput. Program.*, 97:333–348, 2015.
- [31] Christian Dehnert, Sebastian Junges, Nils Jansen, Florian Corzilius, Matthias Volk, Harold Bruintjes, Joost-Pieter Katoen, and Erika Ábrahám. Prophesy: A probabilistic parameter synthesis tool. In Daniel Kroening and Corina S. Pasareanu, editors, *Computer Aided Verification - 27th International Conference, CAV 2015, San Francisco, CA, USA, July 18-24, 2015, Proceedings, Part I*, volume 9206 of *Lecture Notes in Computer Science*, pages 214–231. Springer, 2015.
- [32] Marie-Aude Esteve, Joost-Pieter Katoen, Viet Yen Nguyen, Bart Postma, and Yuri Yushtein. Formal correctness, safety, dependability, and performance analysis of a satellite. In Martin Glinz, Gail C. Murphy, and Mauro Pezzè, editors, *34th International Conference on Software Engineering, ICSE 2012, June 2-9, 2012, Zurich, Switzerland*, pages 1022–1031. IEEE, 2012.
- [33] Nils Jansen, Florian Corzilius, Matthias Volk, Ralf Wimmer, Erika Ábrahám, Joost-Pieter Katoen, and Bernd Becker. Accelerating parametric probabilistic verification. In Gethin Norman and William H. Sanders, editors, *Quantitative Evaluation of Systems - 11th International Conference, QEST 2014, Florence, Italy, September 8-10, 2014. Proceedings*, volume 8657 of *Lecture Notes in Computer Science*, pages 404–420. Springer, 2014.
- [34] Sebastian Junges, Dennis Guck, Joost-Pieter Katoen, Arend Rensink, and Mariëlle Stoelinga. Fault trees on a diet - - automated reduction by graph rewriting -. In Xuandong Li, Zhiming Liu, and Wang Yi, editors, *Dependable Software Engineering: Theories, Tools, and Applications - First International Symposium, SETTA 2015, Nanjing, China, November 4-6, 2015, Proceedings*, volume 9409 of *Lecture Notes in Computer Science*, pages 3–18. Springer, 2015.
- [35] Cristian Mattarei, Alessandro Cimatti, Marco Gario, Stefano Tonetta, and Kristin Y. Rozier. Comparing different functional allocations in automated air traffic control design. In *Formal Methods in Computer-Aided Design, FMCAD 2015, Austin, Texas, USA, September 27-30, 2015*, pages 112–119. IEEE, 2015.
- [36] Shashank Pathak, Erika Ábrahám, Nils Jansen, Armando Tacchella, and Joost-Pieter Katoen. A greedy approach for the efficient repair of stochastic models. In Klaus Havelund, Gerard J. Holzmann, and Rajeev Joshi, editors, *NASA Formal Methods - 7th International Symposium, NFM 2015, Pasadena, CA, USA, April 27-29, 2015, Proceedings*, volume 9058 of *Lecture Notes in Computer Science*, pages 295–309. Springer, 2015.
- [37] Andréa W. Richa and Christian Scheideler, editors. *Stabilization, Safety, and Security of Distributed Systems - 14th International Symposium, SSS*

2012, Toronto, Canada, October 1-4, 2012. Proceedings, volume 7596 of *Lecture Notes in Computer Science*. Springer, 2012.