Summary of the Thesis "Scalable Safety and Reliability Analysis via Symbolic Model Checking: Theory and Applications"

Cristian Mattarei
Stanford University, Stanford, California (USA)
mattarei@stanford.edu

***Abstract*—Assuring safety and reliability is fundamental when developing a safety critical system. In fact, a possible failure in ground, naval and avionic transportation; water and gas distribution; or nuclear, eolic, and photovoltaic energy production can cause significant damages to both humans and the environment. The continuous increase in the design complexity of safety critical system calls for a never ending search for new and more advanced analytical techniques, able to assure that undesired consequences are highly improbable.**

This thesis [1] presents a novel methodology oriented to automatize the safety and reliability analyses of critical systems. The proposed approach integrates a series of techniques, based on symbolic model checking, into the current development process of safety critical systems. Their application to a series of real-world case studies, developed in collaboration with NASA and the Boeing Company, is then described in order to demonstrate performance and expressivity of the proposed methodology.

INTRODUCTION

Over the past few decades, the complexity of safety critical systems has been dramatically increased. To give an example, the Airbus A380 aircraft is composed of about 4 million components, produced by over 1500 companies from 30 different countries. Thus, assuring safety and reliability of a critical system is a very demanding process, which requires considering all possible operational conditions, especially when part of the components are not behaving correctly, e.g., due to a failure. Given such level of complexity, pure manual inspection techniques are not sufficient to guarantee that the system meets the prescribed safety and reliability requirements.

Over the years, different automated and semi-automated approaches have been proposed, and model-based safety assessment (MBSA) represents one of the most prominent. MBSA is oriented to unify the different safety analyses by providing a single well-defined model of the system. Furthermore, applications of this technique allow for the automatic generation of standard safety artifacts such as Fault Trees and FMEA tables. The following integration of symbolic model checking techniques into MBSA has enabled support of the development process with formal formal validation, verification, and safety assessment. Most importantly, these techniques allow for a coherent and formally defined relation between nominal (i.e., when failures are not considered) and safety system models, while providing the possibility to automatically generate the required artifacts. However, the advantages of the symbolic model checking based MBSA techniques are limited by poor scalability and performance, which do not allow them to be applied to real-world systems, without sacrificing the expressivity of the analyses. In fact, the generation of more complex artifacts such as multi-layered fault trees and reliability measures are not practically achievable via these techniques.

The objective of this thesis is to define a set of novel MBSA techniques, based on symbolic model checking, that are able to overcome the limitations of previous approaches. The resulting methodology is able to achieve a significant level of scalability, without compromising the expressiveness, thus permitting automated safety and reliability analyses of real-world systems.

More specifically, the proposed methodology improves the process by covering three main aspects. First, it provides a significant improvement in the performance of the back-end engines, by reducing the problem to parametric model checking. Second, it defines the first fully automated technique that relies on the aforementioned engines, for the generation of structured hierarchical fault trees. Third, it introduces

a novel and very efficient technique for the analysis of safety critical redundant architectures. Moreover, these techniques have been integrated into a comprehensive and coherent formal analysis framework that supports the system development during the design process. To demonstrate its effectiveness, the proposed methodology was applied to several real-world case studies in collaboration with NASA and the Boeing Company.

The remainder of this summary provides an overview of the techniques described in the main parts of the thesis.

Symbolic Techniques for Minimal Cutsets Computation (Part II)

The safety and reliability analysis of a critical system requires considering all necessary faulty conditions that allow the system to exhibit an undesired behavior. Every automated MBSA technique should start by identifying this set of conditions, called the Minimal Cutsets (MCS).

A significant portion of this thesis is focused on this aspect, since the pre-existing techniques suffered from significant scalability and performance issues. This work reduces the cutsets computation to a parametric model checking problem, and solves it with a new technique that builds upon the IC3 model checking algorithm, while relying on SAT and SMT (i.e., Satisfiability Modulo Theories) solvers as back-end engines. Intuitively, this approach analyzes the solution space by organizing it in MCS cardinality layers, which differs from the previous ones that were increasing the depth of system executions. A comparison with previous works demonstrates the remarkable gain in terms of scalability and performance, showing that the new technique is able to solve 30% more industrial problems, considering the set under analysis.

Another important advantage of the proposed approach consists of its anytime capability. More specifically, this new technique computes only the cutsets that are minimal, and unlike previous approaches, it allows for an on-line and incremental production of the results. In fact, it enables the possibility to continuously refine the lower and upper bounds of the probability of reaching the undesired condition, which converge when the algorithm terminates. In addition to that, the thesis provides an extension to support the MCS generation given an (undesired) system condition that is expressed in Linear Temporal Logic, instead of the pure propositional one. This enables expressing more complex behaviors, such as the expected reaction to a command, or the receipt of a message.

The research activities described in this part have contributed to the following publications:

- "Model Checking and Safety Assessment of Altarica models", 11th International Workshop on Automated Verification of Critical Systems (AVoCS), 2011;
- "Safety Assessment of AltaRica Models via Symbolic Model Checking", Science of Computer Programming Journal (SCP), 2015;
- "Efficient Anytime Techniques for Model-Based Safety Analysis", 27th International Conference in Computer Aided Verification (CAV), 2015.

Compositional Safety Analysis (Part III)

The advances provided by the new and efficient techniques for the MCS computation described in the previous section enable the automated formal analysis of real-world complex systems. However, the number of MCS that characterizes such systems can be quite huge (i.e., more than 100 thousand in one of the case-studies), thus they require a significant effort to understand the result of the analysis. Moreover, the standard symbolic model checking based MCS computation can be applied only in the case of complete system behavioral definition, resulting in a requirement that is not always compliant with the development process of a safety critical system. In fact, such a process is characterized by an iterative refinement of the system design: from the high-level system requirements, through the architecture definition, to the characterization of the low-level components behavior. These aspects motivate the research described in this part, which introduces a technique that integrates contract-based design (CBD) and model-based safety assessment into a coherent formal framework. More specifically, CBD is a paradigm that supports the definition of hierarchical component-based systems, where each component is enriched with a contract defining assumptions and behavioral guarantees, respectively, on its input and output ports. This technique has the advantage of natively supporting step-wise refinement and compositional analysis.

In the proposed technique, the contract-based design, used to represent the nominal system, is then extended in order to consider the system under failure conditions and perform the safety analysis. More specifically, each component is extended with two special ports representing internal and external failures, and the contract is modified in order to describe how these ports are related with nominal assumptions and guarantees. The synthesis of the relations between each component failure ports, which relies on the LTL

MCS computation described in Part II, allows for the generation of a structured and hierarchical fault tree. This technique, called contract-based safety assessment is thereafter applied to a case study described in the Aerospace Recommended Practice (ARP) 4754: Guidelines for Development of Civil Aircraft and Systems. This application shows the capability of producing, in a completely automated way, the very same result prescribed by the ARP, which is conducted by relying on previous (semi-automated) approaches.

The research activities described in this part have contributed to the following publication:

- "Formal Safety Assessment via Contract-Based Design", 12th International Symposium of Automated Technology for Verification and Analysis (ATVA), 2014.

Redundant Architecture Analysis (Part IV)

Safety critical systems should guarantee a high level of reliability, and fault tolerance. A general approach to guarantee such properties consists in adding redundant components that are able to provide a specific and critical functionality even in case of system failures. Thus, the main objective consists of varying the system architecture in order to improve the reliability, while preserving the intended behavior. This can be achieved by applying architectural redundancy patterns such as the Triple Modular Redundancy (TMR), which consists of triplicating a critical component and evaluating the correct behavior under majority. However, deciding which architecture is able to guarantee the highest level of reliability is not an easy task, especially considering that TMR is just one of the many possible patterns that can be applied in different parts of the system.

The techniques described in this part are oriented to solve this problem, by providing the first fully automated technique able to formally analyze the redundant architectural systems definition. The proposed approach extends a symbolic state machine language (i.e., SMV) to support the definition of uninterpreted functions. The purpose of this extension is to provide the ability to define the system without any assumption on the concrete behavior. This aspect is particularly important when analyzing redundant architectural descriptions, since they should guarantee an increase of system reliability that is independent from the components behavior. In addition to the standard formal validation and verification of the architecture, this part introduces a novel technique that generates the closed form of the reliability function. More specifically, this function relates the components failure probabilities with the probability of the entire system failure, and it gives the ability to analyze its reliability characteristics without instantiating on specific failure probabilities. The underlying engine of the reliability analysis is based on the MCS computation described in Part II, and the system modeling integrates with the architectural description introduced with the contract-based safety assessment technique. Those aspects are particularly important to provide a comprehensive formal framework.

The automated analysis of such formal models requires relying on a verification technique that supports uninterpreted functions i.e., SMT. However, the SMT-based MCS generation (i.e., AllSMT) experiences significant scalability issues. In fact, the analysis of system architectures with more than 20 redundant components quickly becomes intractable. In order to overcome this limitation, a technique based on predicate abstraction is defined. Intuitively, the theoretical result that has been introduced shows that, under specific conditions, it is possible to independently apply the predicate abstraction to each system module, and perform the analysis on the resulting Boolean formula. The experimental results described in this part show that the resulting technique, called modular abstraction, is able to outperform the SMT-based approach by 3 orders of magnitude. This improvement in terms of performance and scalability enables the analysis of very large redundant architectural descriptions, composed of more than 140 redundant components in less than 110 seconds.

The research activities described in this part have contributed to the following publications:

- "Automated Analysis of Reliability Architectures", 18th International Conference on Engineering of Complex Computer Systems (ICECCS), 2013;
- "Efficient Analysis of Reliability Architectures via Predicate Abstraction", 9th International Haifa Verification Conference (HVC), 2013;
- "Formal Reliability Analysis of Redundant Architectures", - under review - Reliability Engineering and System Safety Journal (RESS), 2017.

Tools and Integrated Process (Part V)

All the techniques introduced in this thesis have been then implemented and integrated into a set of tools to provide a coherent and comprehensive verification framework. In particular, 1) the nuXmv model checker integrates the extension of the parametric

model checking solver; 2) xSAP, which builds upon nuXmv, provides the interface to the MCS computation and encodes the problem into a parametric model checking one; 3) OCRA, which provides the support for CBD, relies on xSAP to perform the safety analysis, and to provide the redundant architecture analysis.

The software infrastructure has been designed and developed to yield a comprehensive formal analysis platform, able to integrate different techniques and methodologies into the current safety critical system development process. An important feature is the use of uniform modeling languages, and verification engines.

The research activities described in this part have contributed to the following publication:

- "The xSAP Safety Analysis Platform", 22nd International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS), 2016.

Case Studies (Part VI)

A significant effort has been devoted to the formal analysis of different real-world case studies, in order to evaluate the effectiveness and efficiency of the techniques proposed in this thesis.

The *Triple Modular Generator* case study describes a redundant aircraft based electrical system, and while being reasonably small, it is highly representative of the application of symbolic model checking based safety analyses. This case study illustrates the challenges that characterize the development of a controller able to react to the system failures in order to maintain the intended functionality.

The whole formal analysis toolset has also been applied to the *Automated Air Traffic Control Design Exploration*. More specifically, the Federal Aviation Administration (FAA) expects an increase of 4 times the number of civil airplanes in the next 20 years, thus the definition of new air traffic control systems is mandatory to guarantee a satisfactory level of safety. This case study comes from a project with NASA, and the objective was to analyze the safety characteristics of more than 1600 different possible designs for the next generation of the automated air traffic control system. In this project, the application of CBD, and the integration of safety and reliability analyses have been fundamental in order to handle the remarkable system complexity and extract representative results.

The chapter *Reliability of Fly-by-Wire architectures* describes the application of the redundant architecture analysis techniques to two industry-standard redundant architectures i.e., the Fly-By-Wire systems of Boeing 777 and Airbus A340. FBW systems are highly critical in modern aircraft, since they completely rely on electrical-based actuation to drive the flight surfaces. Those two systems are also highly redundant, in fact the Boeing 777 extends the concept of TMR by defining a system that is triple-triple redundant. In the case of the Airbus A340, the system applies a double redundancy pattern for each of the 5 computational units. The approach introduced in this thesis has been very effective, considering that the modeling required only 20 man-hours for each system, while providing a comprehensive set of powerful analysis such as formal validation, verification, safety, and reliability.

A collaboration with the Boeing Company also required performing a *Formal Design and Safety Analysis of the AIR6110 Wheel Brake System*. In this project, the techniques described in the compositional safety analysis part have been applied to the analysis of an aircraft based wheel braking system, described in the Aerospace Information Report (AIR) 6110. This case-study was oriented to compare the standard monolithical MCS computation (Part II), with contract-based safety assessment (CBSA). In fact, when analyzing large real-world systems, CBSA compositional verification becomes fundamental. The results of the evaluation show that the whole monolithical fault tree analysis of the AIR6110 required more than 1000 minutes, while CBSA was able to analyze the system in about 1.5 minutes. Moreover, the fault tree produced by the method based on contract-based design was able to significantly increase the interpretability of the results, generating a tree (in one specific case) with 400 leaves, while for the monolithical one (i.e., just the MCS) there were more than 7800.

The research activities described in this part have contributed to the following publications:

- "Comparing Different Functional Allocations in Automated Air Traffic Control Design", 15th International Conference in Formal Methods in Computer-Aided Design (FMCAD), 2015;
- "Model Checking at Scale: Automated Air Traffic Control Design Space Exploration", 28th International Conference in Computer Aided Verification (CAV), 2016.

References

[1] Cristian Mattarei. *Scalable Safety and Reliability Analysis via Symbolic Model Checking: Theory and Applications*. PhD thesis, University of Trento, Trento, Italy, 2 2016.