Newcastle University

COMPUTING SCIENCE

Proceedings of the Workshop on Engineering Dependable Systems of Systems (EDSoS) 2014

Richard Payne, Zoe Andrews and Uwe Schulze (Eds.)

TECHNICAL REPORT SERIES

No. CS-TR-1416 July 2014

TECHNICAL REPORT SERIES

No. CS-TR-1416 July, 2014

Proceedings of the Workshop on Engineering Dependable Systems of Systems (EDSoS) 2014

R. Payne, Z. Andrews and U. Schulze (Eds.)

Abstract

The first workshop on Engineering Dependable Systems of Systems (EDSoS 2014) was a forum for researchers and engineers in academia and industry to foster an exchange of research ideas, results and experiences and to advance the state of the art in dependable engineering of SoSs. The discipline of SoS engineering is still in its infancy and the application of established dependability concepts and fault-tolerance techniques in this context has not been fully explored. Four full papers and an extended abstract were selected for the workshop, and were complemented by additional contributions from our invited speakers Hermann Kopetz and Claire Ingram.

Printed and published by Newcastle University,
Computing Science, Claremont Tower, Claremont Road,
Newcastle upon Tyne, NE1 7RU, England.

Bibliographical details

PAYNE, B., ANDREWS, Z., SCHULZE., U. (EDS.)

Proceedings of the Workshop on Engineering Dependable Systems of Systems (EDSoS) 2014
[By] R. Payne, Z. Andrews and U. Schulze (Eds.)
Newcastle upon Tyne: Newcastle University: Computing Science, 2014.

(Newcastle University, Computing Science, Technical Report Series, No. CS-TR-1416)

Added entries

NEWCASTLE UNIVERSITY
Computing Science. Technical Report Series. CS-TR-1416

Abstract

The first workshop on Engineering Dependable Systems of Systems (EDSoS 2014) was a forum for researchers and engineers in academia and industry to foster an exchange of research ideas, results and experiences and to advance the state of the art in dependable engineering of SoSs. The discipline of SoS engineering is still in its infancy and the application of established dependability concepts and fault-tolerance techniques in this context has not been fully explored. Four full papers and an extended abstract were selected for the workshop, and were complemented by additional contributions from our invited speakers Hermann Kopetz and Claire Ingram.

About the Editors

Richard Payne obtained his PhD in 2012 at Newcastle University under the supervision of Prof. John Fitzgerald, titled Verifiable Resilience in Architectural Reconfiguration. As part of his PhD, Richard provided a basis for the formal verification of policies defined using a reconfiguration policy language (RPL) for the governance of resilient component-based systems. Richard worked as an RA on the Ministry of Defence funded SSEI project and was involved in the 'Interface Contracts for Architectural Specification and Assessment' sub task, investigating the use of contract-based interface specification in system of systems architectural models. Richard is now working on the COMPASS project, on the use of model-based techniques for developing and maintaining systems of systems, involved with work in architectural modelling, fault modelling and tool development.

Zoe Andrews is a Research Associate on the COMPASS project. In particular, she is exploring ways of modelling and analysing faults in systems of systems. Zoe was awarded her PhD (supervised by Prof. John Fitzgerald) on "Continuous Probability Distributions in Model-Based Specification Languages" in 2012. This investigated ways in which stochastic reasoning could be combined with logical reasoning for the specification and analysis of fault-tolerant systems. Zoe also worked as an RA on the ReSIST network of excellence and was responsible for work on developing metadata-based descriptions of resilience mechanisms and providing support for decision making over such mechanisms.

Dr.-Ing Uwe Schulze was awarded a Dipl.-Ing. degree and Ph.D. degree (Dr.-Ing.) in computer sciences at the Research Group Operating Systems, Distributed systems of the University of Bremen in 2004. Uwe has worked for more than 6 years at Verified Systems International GmbH on projects for automated testing of safety critical systems and embedded systems in the avionics domain. Uwe's research is focused on model-based test procedure generation from SysML models.

Suggested keywords

DEPENDABILITY
SYSTEMS OF SYSTEMS
SECURITY
FAULT MODELLING
VERIFICATION
CLOUD COMPUTING
CONTRACTUAL MODELLING

Proceedings of the Workshop on Engineering Dependable Systems of Systems (EDSoS) 2014

Richard Payne, Zoe Andrews and Uwe Schulze (Editors)

The first workshop on Engineering Dependable Systems of Systems (EDSoS 2014) was a forum for researchers and engineers in academia and industry to foster an exchange of research ideas, results and experiences and to advance the state of the art in dependable engineering of SoSs. The discipline of SoS engineering is still in its infancy and the application of established dependability concepts and fault-tolerance techniques in this context has not been fully explored.

SoS engineering encompasses a wide range of application domains; including emergency response, military, aerospace, transport, audio/visual and power grids. The constituent systems of an SoS are often independent, distributed and heterogeneous. Emergent properties related to dependability, such as security, safety and reliability are hard to predict and maintain due to the interaction of constituents within SoSs. The challenges posed by the characteristics of SoSs are further exacerbated by the increasing complexity of the requirements (and their tracing) of the SoS, the complexity of its underlying constituent systems and the increasing reliance being placed on the SoS. The engineering of dependable SoSs is essential to provide trust in large-scale critical systems.

Four full papers and an extended abstract were selected for the workshop, with a selection process carried out by the Program Committee, taking into account the relevance to the workshop topics, quality, technical soundness and originality of each submission. This was complemented by additional contributions from our invited speakers Hermann Kopetz and Claire Ingram.

We wish to thank all authors who submitted papers to EDSoS 2014, the Program Committee and additional reviewers for their thorough and thoughtful reviews, the EDCC organising committee and the support staff in CSR, Newcastle University. The organisation of the workshop was made possible through the use of EasyChair.

The regular workshop papers were published in the ACM CoRR repository, in this document just the abstracts are presented along with the URLs for the full papers. In addition we include the abstracts (and where possible, URLs for extended abstract versions of these) for the invited talks.

Keywords

Dependability; Systems of Systems; Security; Fault modelling; Verification; Cloud computing; Contractual modelling

Organising Committee

Richard Payne (Newcastle University, UK)
Zoe Andrews (Newcastle University, UK)
Uwe Schulze (Bremen University, DE)

Program Committee

Dave Banham (Rolls Royce, UK)
Andrea Bondavalli (University of Florence, IT)
Bettina Buth (HAW Hamburg, DE)
John Fitzgerald (Newcastle University, UK)
Michael Gainford (Altran, UK)
Alan Harding (BAE Systems, UK)
Bernhard Josko (OFFIS, DE)
Mohamed Kaâniche (LAAS-CNRS, FR)
Tim Kelly (University of York, UK)
Klaus Kristensen (Bang & Olufsen, DK)
Kim Larsen (Aalborg University, DK)
Alexandre Mota (Universidade Federal de Pernambuco, BR)
Frank Ortmeier (Otto-von-Guericke-Universität Magdeburg, DE)
Yiannis Papadopoulos (University of Hull, UK)
Holger Pfeifer (TU München, DE)

Contents

Why a Global Time is Needed in a Dependable SoS? (invited talk)

Author: Hermann Kopetz

Abstract: A system-of-systems (SoS) is a large information processing system formed by the integration of autonomous computer systems (called constituent systems, CS), physical machines and humans for the purpose of providing new synergistic services and/or more efficient economic processes. In a number of applications, e.g robotics, the autonomous CSs must coordinate their actions in the temporal domain to realize the desired objectives. In this paper we argue that the introduction of a proper global physical time establishes a shared view about the progress of physical time and helps to realize the temporal coordination of the autonomous CSs. The available global time can also be used to simplify the solution of many challenging problems within the SoS, such as distributed resource allocation, and helps to improve the dependability and fault-tolerance of the SoS.

Keywords: System-of-Systems; Global time; Clock synchronization; Sparse time base; Error detection; Dependability

URL: `http://arxiv.org/abs/1404.6772`

SoS Fault Modelling at the Architectural Level in an Emergency Response Case Study

Authors: Claire Ingram, Steve Riddle, John Fitzgerald, Sakina Al-Lawati and Afra Alrbaiyan.

Abstract: Systems of systems (SoSs) are particularly vulnerable to faults and other threats to their dependability, but frequently inhabit domains that demand high levels of dependability. For this reason fault tolerance analysis is important in SoS engineering. The COMPASS project has previously proposed a Fault Tolerance Architecture Framework (FMAF), consisting of a collection of viewpoints that support systematic reasoning about faults in an SoS at the architectural level. The FMAF has been demonstrated previously with an analysis of an example fault in an emergency response SoS. In this paper we present further examples of the FMAF's practical use, by analysing different types of faults drawn from the same emergency response case study. These example faults exercise different aspects of the FMAF, demonstrate its use in more complex fault modelling scenarios, and raise new questions for further development.

Keywords: Systems of Systems; Fault tolerance; Architecture

URL: `http://arxiv.org/abs/1404.7778`

Deployment Calculation and Analysis for a Fail-Operational Automotive Platform

Authors: Klaus Becker, Michael Armbruster, Bernhard Schaetz and Christian Buckl

Abstract: In domains like automotive, safety-critical features are increasingly realized by software. Some features might even require fail-operational behavior, so that they must be provided even in the presence of random hardware failures. A new fault-tolerant SW/HW architecture for electric vehicles provides inherent safety capabilities that enable fail-operational features.

In this paper, we introduce a formal model of this architecture and an approach to calculate valid deployments of mixed-critical software-components to the execution nodes, while ensuring fail-operational behavior of certain components. Calculated redeployments cover the cases in which faulty execution nodes have to be isolated. This allows to formally analyze which set of features can be provided under decreasing available execution resources.

Keywords: Fault-Tolerance; Fail-Operational; Deployment

URL: `http://arxiv.org/abs/1404.7763`

Fault Modelling in System-of-Systems Contracts

Authors: Zoe Andrews, Jeremy Bryans, Richard Payne and Klaus Kristensen

Abstract: The nature of Systems of Systems (SoSs), large complex systems composed of independent, geographically distributed and continuously evolving constituent systems, means that faults are unavoidable. Previous work on defining contractual specifications of the constituent systems within SoSs does not provide any explicit consideration for faults. In this paper we address that gap by extending an existing pattern for modelling contracts with fault modelling concepts. The proposed extensions are introduced with respect to an Audio Visual SoS case study from Bang & Olufsen, before discussing how they relate to previous work on modelling faults in SoSs.

Keywords: Systems of Systems; Modelling; Architectural Frameworks; Contracts; Faults

URL: `http://arxiv.org/abs/1404.7775`

A Flow Sensitive Security Model for Cloud Computing Systems

Authors: Wen Zeng, Chunyan Mu, Maciej Koutny and Paul Watson

Abstract: Federated cloud systems increase the reliability and reduce the cost of computational support to an organization. The resulting combination of secure private clouds and less secure public clouds impacts on the security requirements of the system. To meet these security requirements, applications need to be located within different clouds, which strongly affects the information flow security of the entire system. In this paper, a flow sensitive security model for a federated cloud system is proposed, secure information flow in such a system is analyzed using coloured Petri nets, and opacity of cloud computing systems is introduced. In this study, the entities of a federated cloud system are assigned security levels of a given flow lattice. A transition system is used to describe the behavior of the system, and coloured Petri nets are used to analyze the correctness of the entire system. As a result, one can track the information flow. Moreover, one can analyze the impact of different resource allocation strategies, and the opacity of the system.

Keywords: Opacity; Coloured Petri nets; Information flow security; Federated cloud system; Information lattice

URL: `http://arxiv.org/abs/1404.7760`

Towards Verification of Constituent Systems through Automated Proof

Authors: Luís Diogo Couto, Simon Foster and Richard Payne

Abstract: This paper explores verification of constituent systems within the context of the Symphony tool platform for Systems of Systems (SoS). Our SoS modelling language, CML, supports various contractual specification elements, such as state invariants and operation preconditions, which can be used to specify contractual obligations on the constituent systems of a SoS. To support verification of these obligations we have developed a proof obligation generator and theorem prover plugin for Symphony. The latter uses the Isabelle/HOL theorem prover to automatically discharge the proof obligations arising from a CML model. Our hope is that the resulting proofs can then be used to formally verify the conformance of each constituent system, which is turn would result in a dependable SoS.

Keywords: Systems of Systems; Theorem Proving; Proof Obligations; Constituent Systems; UTP; VDM; CML

URL: `http://arxiv.org/abs/1404.7792`

Towards a roadmap of modelling and simulation in SoSs (invited talk)

Author: Claire Ingram

Abstract: Systems of systems (SoS) is a challenging field for modelling and simulation, but, as large systems typically operating in domains that have significant social impact, our ability to analyse SoSs and justify the reliance we place upon them is increasingly important. The COMPASS project will deliver a roadmap outlining a vision for the future of model-based techniques for SoSs, and pointing to future work which builds on COMPASS's tools and methods. This invited talk outlined the approach COMPASS will adopt for technology roadmapping and the work conducted so far.