Institution: University of Hull

Unit of Assessment: 11 Computer Science and Informatics

Title of case study: HiP-HOPS: A novel method and tool for dependability analysis and optimisation of systems

1. Summary of the impact (indicative maximum 100 words)

The University of Hull has pioneered a novel method and tool for dependability analysis and optimisation of critical engineering systems known as Hierarchically Performed Hazard Origin and Propagation Studies (HiP-HOPS).

a) HiP-HOPS (http:\\hip-hops.eu) has been successfully commercialised in conjunction with software houses ITI GmbH (Germany) and ALL4TEC (France). Over 30 licences for the tool have been sold since 2011 with total income for all partners estimated at £300,000.
b) The method and tool have been taken up by large organisations including Volvo, Toyota, Honda, Fiat, Continental, Germanischer Lloyd, Embraer and Honeywell.
c) HiP-HOPS has contributed to the specification of EAST-ADL, an emerging design language developed as an automotive industry standard, confirming industrial reach and acceptability.
d) The Dependable Systems research group is pursuing impact on the new automotive safety standard ISO-262626 and have contributed to setting up the new IFAC DCDS workshop – a key forum for disseminating research on dependability to industry.

2. Underpinning research (indicative maximum 500 words)

The evaluation and optimisation of dependability of computer-based safety critical systems is a very challenging problem. Over the last fifteen years, work on model-based dependability analysis has resulted in new approaches that partly automate and simplify the synthesis of dependability evaluation models. HiP-HOPS is one of the first and presently the most advanced among modern compositional dependability analysis techniques. It was originally conceived by Professor Papadopoulos during his PhD research at York and has been developed in Hull since 2001. The technique has produced significant innovations and key findings within the period all of which progress the state-of-the-art and have been extensively published. These are listed below and mostly covered in references mentioned in [1-3] and further detailed in the 8 submitted REF outputs (Papadopoulos, Parker and Walker) which stem from new developments in HiP-HOPS:

a) Fast linear-time algorithms for model-based synthesis of (temporal) fault trees and (sequential, multiple failure mode) Failure Modes and Effects Analyses (FMEAs).
b) A language for the description of inheritable and reusable component failure patterns.
c) A new temporal logic (PANDORA) that facilitates analysis of temporal fault trees.
d) Model-based algorithms for real-time diagnosis and correction of failures.
e) Algorithms for design space exploration and multi-objective optimisation of system designs via automatic model transformations using meta-heuristics.
f) Contributions to the EAST-ADL error model annex and algorithms for automatic allocation of safety requirements in the form of Safety Integrity Levels.

A number of other contemporary dependability analysis techniques including FSAP-NuSMV, Software Deviation Analysis, and DCCA have used variants of state-modelling, model-checking and fault simulation as a means of inferring the effects of component failures in a system. In theory, these techniques offer a higher degree of automation than HiP-HOPS. However, extra automation comes at a price – that of much higher computational complexity. The analysis of individual failure modes via simulation or model-checking is computationally expensive and the often forward, inductive nature of the analysis creates difficulties, especially when combinations of failures need to be considered [2].

In HiP-HOPS, the analysis of propagation of failures is done by a deductive algorithm which links effects on system outputs to causes in the architecture. Synthesis of fault trees is achieved in

linear time, and although the subsequent fault tree analysis can still be time-consuming, overall simplicity has enabled not only application of the technique to large systems but also its unique combination with computationally greedy heuristics such as Genetic Algorithms [1]. An additional difficulty with most formal dependability analyses techniques is that they typically define their own language for nominal and failure modelling which is not always fully compatible with widely used design languages and tools. HiP-HOPS, on the other hand, focuses only on failure modelling and can easily complement design languages focusing on descriptions of nominal behaviour. It has so far been demonstrated to work as an add-on to EAST-ADL, Matlab Simulink, and Simulation X [3].

In summary, HiP-HOPS offers certain advantages to other contemporary techniques, and these have driven the industrial impact of the method. These advantages are: compatibility with a range of modelling notations; scalability of the analysis; and unique capabilities for fault modelling, temporal analysis and architectural optimisation via automatic model transformations.

HiP-HOPS was developed in a string of European Projects [4-6] with input from large industrial organisations across the transport industries who have since become commercialisation partners and users of this research. Papadopoulos (Senior Lecturer, 2001-2007; Reader, 2007-2011; Professor, 2011–present) has led the development of this work. Bottaci (Senior Lecturer, 1986-present) has contributed to the formalisation of aspects of HiP-HOPS Walker and Parker (both Research Assistants, 2008-2011; Lecturers, 2011-present) are authors of the PANDORA temporal logic and optimisation algorithms respectively. All the above mentioned staff have been in the University of Hull for the duration of the REF period, and further back in the period since 2001 when much of the underpinning research that led to this impact case was carried out.

3. References to the research (indicative maximum of six references)

Publications (all peer reviewed in high quality journals)

1. I Wolforth, M Walker, L Grunske, Y Papadopoulos (2010), Generalisable Safety Annotations for Specification of Failure Patterns, Software Practice and Experience, 40(5):453-483, DOI: 10.1002/spe.966
2. M Adachi, Y Papadopoulos, S Sharvia, D Parker, T Tohdo (2011), An approach to optimization of fault tolerant architectures using HiP-HOPS, Software Practice and Experience, 41:1303-1327, DOI: 10.1002/spe.1044
3. M Walker, M-O Reiser, S Tucci, Y Papadopoulos, H Lonn, D Parker, D-J Chen (2013) Automatic Optimisation of System Architectures using EAST-ADL, Journal of Systems & Software, 86(10): 2467–2487, DOI: 10.1016/j.jss.2013.04.001.

Grants (all peer reviewed, FP6-FP7 European grants)

1. (Duration: 2010 – 2013), MAENAD (FP7 Grant 260057) – Modelling Analysis Evaluation of Novel Architectures for Dependable Electric Vehicles (with Fiat, Volvo, 4S, MetaH Continental, Delphi, French Atomic Authority, TU Berlin, RIT Stockholm)
   European Commission, Principal Investigator : Papadopoulos, £239,437
2. (Duration: 2008 – 2010), ATESST2 (FP7 Grant 224442) - Advancing Traffic Efficiency and Safety through Software Technology (with Volvo Technology, Volkswagen, Continental, French Atomic Authority, TU Berlin)
   European Commission, Principal Investigator : Papadopoulos, £178,873
3. (Duration 2005 – 2009, partly in period), SAFEDOR (FP6 IP Grant 516278) - Safe Design Operation and Regulation, FP6 Integrated Project (53 partners including all major ship classification authorities in Europe, shipyards, equipment manufacturers and operators)
   European Commission, Principal Investigator : Papadopoulos, £213,078 (€20 million in total)

4. Details of the impact (indicative maximum 750 words)

HiP-HOPS has achieved industrial, economic and societal impact and it is widely recognised as one of the techniques that define the state-of-the-art in dependability analysis and optimisation of systems. This section first presents the three strategic activities through which impact was pursued in the period and then details the industrial, economic and societal impact achieved.

Impact Strategy and Activities (2008-present):

a) Commercialisation of the HiP-HOPS tool and global engagement with large industrial users, including Volvo, Fiat and Continental in Europe, Denso and Toyota in Japan, Embraer in Brazil and Honeywell in the USA. Over 30 licences of the tool have been sold to these organisations since 2011 (see details of impact including value of sales under heading "Details of Impact Achieved" below and sources to corroborate impact: 3,4,5).
b) Technology transfer to industry through European Projects including three projects in the automotive and shipping domains (see refs [4-6] in section 3) and consultancies. Research has been transferred to R&D departments and system design teams. A consultancy for the Flemish Mechatronic Institute (2012) has led to seven HiP-HOPS licences deployed in various companies that are members of this organisation (see details of impact including benefits for companies involved under heading "Details of Impact Achieved" and sources to corroborate impact: 1,2,6,7,8,9).
c) Organisation of events focused on HiP-HOPS and related model-based dependability analysis technologies. Papadopoulos has co-organised and co-chaired multi-session tracks and tool sessions in successive IFAC symposia on Information Problems in Manufacturing and IFAC World Congress in 2008. This activity led to the establishment of the IFAC Workshop on Dependable Control of Discrete Event Systems which provides the main forum for technology transfer to industry on the field of dependability. IFAC DCDS'13 was co-organised by the University of Hull and co-chaired by Papadopoulos (http://dcds13.net.dcs.hull.ac.uk/). DCDS'13 was financially supported by Bosch and was attended by senior representatives of British industries. There were three sessions on state-of-the-art in Model-based Safety Assessment with strong representation of HiP-HOPS. There was strong interest from the Head of the Software Centre of Excellence in Rolls Royce, a seminar was given (04/11/2013) and technology transfer to the company is being explored.

Details of Impact Achieved:

1. Economic impact (2008–present)

A consortium agreement with ITI GmbH (a German Computer-Aided Engineering specialist software house), and Germanischer Lloyd was signed in May 2010, and HiP-HOPS was commercially launched in January 2011. Germanischer Lloyd (GL) is a major international register of shipping with enormous influence in the industry and actively promotes this technology in the shipping industry. This development has sprung out of SAFEDOR, the largest ever project on safety funded by the EU with 53 partners and a total budget of €20 million, where the University of Hull had a key role as provider of technologies for automated safety analysis and design optimisation. ALL4TEC in France, a company specialising in provision of tools and services for system safety analysis, is also commercialising HiP-HOPS to its clients in the context of a sub-licensing agreement with the University of Hull.

Commercialisation activities have started to contribute directly to the economy of the UK since 2011 via HiP-HOPS sales currently at £60,000 by the University of Hull which controls the HiP-HOPS licence. Additional benefits to commercialisation partners are estimated at £240,000. The latter are arising from stake in the sale of HiP-HOPS, additional sales of modelling tools linking to HiP-HOPS, and services such as training and application modelling. There are also economic benefits – via improvements in the processes of safety analyses achieved by HiP-HOPS – which contribute to reduced costs arising both from automation and efficiencies but also safer product/system development for the industrial users of the tool. It is difficult to quantify the latter, and no studies have been done on this, but the growing uptake of the technology is very promising in this respect, and included is a list of users that can provide estimates on such benefits in this section.

2. Impact on industrial practice (2008 –present)

In a string of European and industrial funded projects, HiP-HOPS has directly contributed to the specification of the error modelling capabilities of EAST-ADL, an emerging architecture description language developed as an automotive industry standard for the design of vehicle control systems by a consortium of automotive companies. As a result of this work, in 2011, the

EAST-ADL association was founded to manage the standardisation and evolution of the language, and promote its adoption in the automotive industry. The University of Hull is a founding member of this association and Papadopoulos is among two academics sitting on the 5-member board. This development is important because it confirms wide reach and acceptability of the method and is preparing the ground for further industrial and societal impact in the future.

HiP-HOPS has recently been extended with a novel approach to automatic allocation of safety requirements to components of a system architecture. The proposed process can support and simplify the implementation of the upcoming automotive safety standard ISO26262. A member of the corresponding ISO committee has been involved in evaluating this proposal with a view to influencing the refinement and implementation of the standard (see corroborating evidence 2).

Through commercialisations, EAST-ADL and consultancies funded by Toyota, the Flemish Mechatronic Institute and others, HiP-HOPS has been taken up by automotive companies which include Volvo, Toyota, Volkswagen, Daimler, Fiat, Siemens, Continental, Ricardo and Mecel. HiP-HOPS is being experimentally used in the design of new active safety systems by these companies. Daimler have developed their own implementation of HiP-HOPS. In the aerospace sector, HiP-HOPS is being used by Honeywell and Embraer for improved system design. New work (2012-present) of potentially high impact in the sector is focused on harmonising HiP-HOPS with AADL, the emerging Architecture Analysis and Design Language which is becoming an industry standard in the aerospace industry. Embraer (see corroborating evidence 8) have developed their own implementation in HiP-HOPS. The continual and growing involvement of these companies with HiP-HOPS shows the benefits they have acquired in streamlining, rationalising and improving dependable design. Their involvement in over 50 HiP-HOPS publications within the period, reported case studies (including in refs [1-3] in section 3 and the eight submitted REF outputs on HiP-HOPS), as well as personal communication with the industrial contacts cited in section 4, will confirm these benefits.

3. Societal impact (2008 –present)

Industrial applications in large scale show that HiP-HOPS speeds up the safety analysis process by automating part of it and thus enabling multiple iterations of safety analysis that help to improve the design of safe systems. The impact on safety improvements is difficult to quantify at this stage, but users largely agree (see industrial contributions to publications and sources to corroborate impact 6-9) that the process significantly improves classical safety analysis and influences positively the safety of systems which can in turn significantly reduce risks of life losses as well as property and environment damages caused by system failures

5. Sources to corroborate the impact (indicative maximum of 10 references)

All references to organisations below are supported by factual statements.

1. Contribution to the specification of the EAST-ADL language (Hull is central in EU projects where language was defined – see http://www.atesst.org and http://www.maenad.eu, founding members of the EAST-ADL association, Papadopoulos is among two academics sitting on the 5-member association board, and HiP-HOPS is one of EAST-ADL supporting tools – see association website http://www.east-adl.info/)
2. Influence of HiP-HOPS is the new AUTOMOTIVE safety standard, Member of ISO Committee
3. Commercialisation of HiP-HOPS with ITI GmbH (Commercialisation Agreement available on request from University of Hull).
4. Commercialisation of HiP-HOPS with ALL4TEC (Sublicensing and distribution agreement available on request from University of Hull).
5. Data to corroborate the value of sales of HiP-HOPS (Can be provided by University of Hull).
6. Impact on Japanese industry - experience with large clients of HiP-HOPS, testimony by Managing Director of commercialisation partner (ITI GmbH), Germany.
7. Impact on automotive sector (BOSCH), Functional Safety Manager, Bosch Automotive (Tier 1 supplier), Germany.
8. Impact on aerospace sector (EMBRAER), Manager responsible for Modelling and Simulation in Embraer and project Leader of in-house developed HiP-HOPS tool.
9. Impact on shipping sector (GERMANISCHER LLOYD), Head of Department Strategic Research, Germanischer Lloyd.