HAL
open science

Automatic Decomposition of Safety Integrity Levels: Optimization by Tabu Search

Luis Silva Azevedo, David Parker, Martin Walker, Yiannis Papadopoulos, Rui Esteves Araùjo

To cite this version:

Luis Silva Azevedo, David Parker, Martin Walker, Yiannis Papadopoulos, Rui Esteves Araùjo. Automatic Decomposition of Safety Integrity Levels: Optimization by Tabu Search. SAFECOMP 2013 - Workshop CARS (2nd Workshop on Critical Automotive applications : Robustness & Safety) of the 32nd International Conference on Computer Safety, Reliability and Security, Sep 2013, Toulouse, France. pp.NA. hal-00848213

HAL Id: hal-00848213

https://hal.science/hal-00848213v1

Submitted on 25 Jul 2013

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Automatic Decomposition of Safety Integrity Levels: Optimization by Tabu Search

Luís Silva Azevedo[1], David Parker[1], Martin Walker[1], Yiannis Papadopoulos[1], Rui Esteves Araújo[2]

[1]Department of Computer Science, University of Hull, United Kingdom
l.p.azevedo@2012.hull.ac.uk,{d.j.parker, martin.walker, y.i.papadopoulos}@hull.ac.uk
[2]INESC TEC, Faculdade de Engenharia, Universidade do Porto, Portugal
raraujo@fe.up.pt

Abstract. Automotive Safety Integrity Levels (ASILs) are used by ISO 26262, the new automotive functional safety standard, to categorize the stringency of safety requirements. In the course of a hierarchical system design, ASILs are iteratively allocated to subsystems and components. This ASIL decomposition allows for redundant elements to share the responsibility of meeting a given ASIL and finding efficient decomposition solutions has a significant, positive, impact on development costs. This paper describes a novel technique that uses Tabu Search to explore the solution space efficiently. We have applied the technique to a case study of a hybrid braking system.

Keywords: ISO 26262, ASIL decomposition optimization, Fault Tree Analysis, HiP-HOPS, Tabu Search

1 Introduction

ISO 26262 is the functional safety standard for the passenger vehicle industry. It defines a complete safety lifecycle for the development of electrical and/or electronic systems. ISO 26262 demands a great effort from both automotive manufacturers and part suppliers, who find themselves in need of improved ways to manage safety and be compliant with the new standardized methodologies. One of the key concepts of the standard is traceability: the ability to track safety requirements from system level safety features down to detailed software and hardware design.

ISO 26262 uses the concept of an Automotive Safety Integrity Level (ASIL) to represent the stringency of safety requirements. It defines 4 ASILs: from A (least stringent requirements) to D (most stringent requirements). Specifying QM (Quality Management only) implies no special safety requirements. Throughout the development of a system, a combination of ASILs will impose appropriate requirements that, if fulfilled, reduce risk to a residual level. Safety requirements (in the form of ASILs) can then be refined and allocated iteratively, from the system and subsystem level to the detailed hardware and software component design.

ISO26262 provides guidance for ASIL reduction when in the presence of redundancy. The process is termed *ASIL decomposition* and is an algebraic approach based on assigning integer numbers to the different ASILs: QM-0; A-1; B-2; C-3; D-4. Where multiple system elements must fail together to violate a top-level safety requirement (Safety Goal (SG)), ASIL decomposition can be applied as shown in (1).

$$\sum ASIL_i = ASIL_{SG} \tag{1}$$

Finding effective ASIL decompositions is crucial as it allows fulfillment of the high level safety requirements without incurring unnecessary expense. However, to manually perform such task in complex systems is difficult and error-prone. The technique presented in [1] allows automated ASILs decomposition by building a linear programming problem to minimize the total number of ASILs. An interesting feature of the approach is the facility for the designer to specify 'fixed' ASILs for particular components based on previous experience with an architectural element. A small case study is presented but scalability is not addressed.

Ideally, finding an optimal decomposition should be performed using the exact cost information of every component and each of its ASIL implementations; however, some of those elements may be completely new developments, and therefore, no individual cost information is available. Conceptually, [1] uses a linear cost heuristic where each ASIL presents a cost equal to its integer number assigned by the ASIL decomposition rules. This represents a fairly simplistic cost model and instead, multiple heuristics can be formulated to evaluate ASIL cost. For example, one may decide that the cost "jump" from ASIL B to C should be bigger than any other. The use of different cost heuristics therefore often results in different 'optimal' decomposition solutions to the same problem.

In [2], we previously introduced a technique for automatic decomposition of ASILs using HiP-HOPS, a state of the art safety and reliability analysis tool. The tool can determine, through automated fault tree analysis, how the failures of low-level elements can cause system level function failures. This analysis identifies which components, failing simultaneously, result in the violation of a safety goal, thus allowing the safety goal's ASIL to be decomposed amongst those components. One important feature of this technique is that it allows ASIL decomposition to be applied hierarchically, helping to manage complexity and facilitating distributed development. Subsystem level elements can be assigned with an ASIL before the details of the system are known, thus allowing the ASIL requirements to be sent in advance to the suppliers. The suppliers can apply the same procedure to decompose ASILs amongst the elements of their (sub)architectures while still ensuring that the final product meets the ASIL targets defined at the system level.

However, the previous approach used exhaustive search techniques that do not perform well for large systems. The focus of this paper therefore builds on HiP-HOPS to achieve a scalable automation of ASIL decomposition by using Tabu Search (TS), an efficient optimization method.

It is important to note that our technique does not allocate ASILs to components, but rather directly to their failures. This allows better refinement of requirements when a component presents more than one failure mode. Nevertheless, if the designer

requires, different heuristics can be applied, such as choosing the highest ASIL of the component's failure modes, to provide a component allocation.

We formalize ASIL decomposition optimization as the search for the vector of ASILs x, corresponding to the n failure modes of a system that minimizes the total ASIL-dependent cost, C, while respecting the feasibility restrictions of ASIL algebra.

2 ASIL Decomposition Optimization By Tabu Search

We have previously developed algorithms that seek to exhaustively, but intelligently, search the ASIL decomposition solution space. However, due to the combinatorial nature of the problem, scalability remains an issue. Moreover, as there is no standardized ASIL cost function and multiple options can be applied, it is difficult to formulate a problem domain-dependent search algorithm. Thus, we directed our research to meta-heuristic techniques, which are acknowledged to be flexible when tackling problems with different characteristics. Furthermore, metaheuristics are known to perform faster for large-scale problems than exhaustive techniques with some applications being shown to outperform deterministic algorithms, such as Branch and Bound [3].

One drawback to using meta-heuristics is that there is no guarantee of finding the global optimal solution. Nonetheless, it is very likely that during a system design, ASIL decomposition would be iterated due to design changes and supply chain restrictions. Therefore we aim to provide a technique that achieves near-optimal solutions efficiently whilst still offering advantages over manual approaches, thus contributing to a more competent development of dependable systems. The Steepest Ascent Mildest Descent (SAMD) method is a member of the Tabu Search family [4]; the work we present here is based on its application to the optimization of system reliability by Hansen and Lih [5]. SAMD is meant for maximization, but this work aims at optimization of ASIL-dependent costs which is a minimization task. The method was therefore adapted to a Steepest Descent Mildest Ascent (SDMA) version. SDMA follows the steepest descent direction until a local minimum is reached, and then it uses the mildest ascent route to escape from it. Returning to the local minimum is avoided by means of an adaptive memory structure that forbids reverse movements during a pre-defined number of iterations, p.

The algorithm starts from a feasible solution. The steepest descent direction is then pursued, which for the ASIL decomposition problem means iteratively decrementing the ASIL of the failure that results in the highest system cost reduction. Once the decrease of any failure ASIL implies violating the decomposition rules, a minima has been identified; in such scenario the mildest ascent route is followed by incrementing the ASIL of the failure which results in the lowest system cost growth. A variable, f_i, stores the number of iterations to forbid decrementing the ASIL of failure i after an ascent move has been taken. Initially f_i is assigned with the value of p and is subsequently decremented with each iteration that the algorithm completes. We continue following the Hansen and Lih approach by also not allowing, for a number of iterations p', the increase of a failure's ASIL after a descent move has taken place. f'_i, in contrast to f_i, is not decreased in every iteration but only when further ASIL reduc-

tions are accomplished. In this way, ascent moves are forbidden for longer and diversification of the search direction is encouraged [5]. *p'* was defined independently of *p*; their values are dynamically altered as this reduces the sensitivity of the algorithm to the selection of such parameters. *p* is changed between 0 and *n*, and *p'* between 0 and 0.4*n*; single increments are performed to *p* and *p'* every 3 and 4 iterations, respectively, and both reset their count after their upper bounds have been reached. As Tabu structures may forbid visiting attractive solutions we have extended Hansen and Lih's algorithm by allowing a tabu move restriction to be overruled if this means obtaining a better solution than those found so far. Finally, the search stops after a pre-defined number of repetitions have passed without improving the best known solution.

3 Case Study

The case-study uses the model of a brake-by-wire system for electrical vehicles whose propulsion system features one electrical motor per wheel. Braking is assured by means of a hybrid strategy that combines the action of the electrical motors and electromechanical brakes. For further details on this system, the reader is referred to [6]. We have modeled it considering just one braking unit, but as braking can be controlled independently for each wheel, this does not affect the validity of the analysis.

We have considered two hazards for the hybrid braking system: no braking after command (H1) and wrong value braking (H2). ASILs D and A were assigned to H1 and H2, respectively. For this illustrative case study we did not perform the risk assessment process proposed by ISO 26262; instead ASILs were assigned to hazards solely based on their severity. Subsequently, we linked system output deviations with the 2 identified hazards: H1 is caused by the omission of output of both breaking devices and H2 by an incorrect value output deviation of at least one of them.

While performing individual failure annotations to the components, 24 failure modes were identified. This gives a total search space size of 5^{24} ($\approx 5.96 \times 10^{16}$). By applying qualitative FTA with HiP-HOPS, information about failure propagation in the system was obtained in the form of Minimal Cut Sets (MCSs). MCSs represent the minimal combination of events that result in a system level failure; they can either contain a single failure that directly causes the hazard, or multiple failures that together cause it. For the hybrid braking system the following MCSs were obtained:

- 19 MCSs for H1:1 single point of failure and 18 dual point failures;
- 11 MCSs for H2:10 single points of failure and 1 dual point failure.

To test our algorithm we have defined the ASIL cost heuristics shown in Table 1.

Table 1. ASIL cost heuristics

	QM	A	B	C	D
Linear	0	10	20	30	40
Logarithmic	0	10	100	1000	10000
Experiential	0	10	20	40	50

We repeated the algorithm 10 times for each cost function, and the maximum number of iterations without improvement was fixed to 5000. An initial feasible solution was created by setting the ASILs of all failures to ASIL D (4); diversity in the search direction was provided by randomly choosing the failure ASIL to modify when multiple moves presented the same best cost variation. All tests were carried in a machine equipped with an Intel i5 processor clocked at 3.40GHz and with 8GB of RAM.

The results of the application of our TS-based decomposition optimization method to the hybrid braking system are presented in Table 2. For each cost heuristic the best solution was identified a priori with the use of an exhaustive technique. *Best* represents the cost of the previously identified optima; *NBest* counts how many runs found the global optimal; *Iter* gives the algorithm average iteration when the best solution was found and *CPU* lists the average processing time (in seconds).

Table 2. Tests results

	Best	NBest	Iter	CPU
Linear	380	10	65	0.007
Logarithmic	11300	10	58	0.006
Experiential	390	10	170	0.008

The algorithm was able to return the optimal solution for all the cost heuristics in every run. For the logarithmic function the best ASIL allocations were found by following the steepest descent direction from the initial solution, hence the smallest *CPU* and *Iter* values. That was not the case for the remaining cost functions; we show in Fig. 1 how our method performed in one run for the experiential cost evaluation: it firstly pursued the steepest descent direction from the initial solution and then escaped successive local optimal until it reached the global minimum on iteration 414.

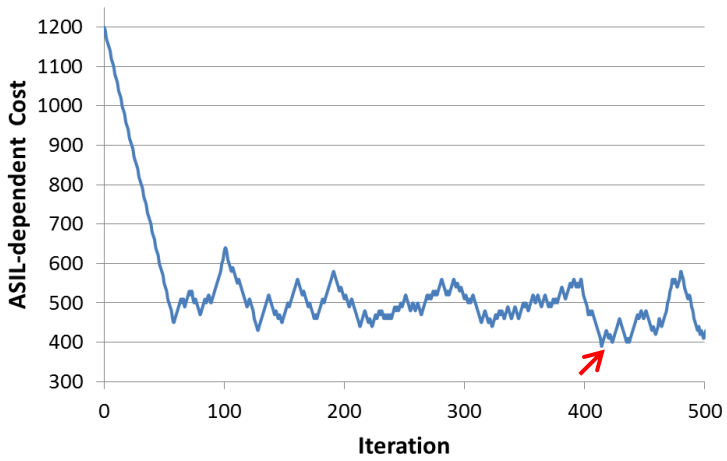

Fig. 1. Results of test with experiential ASIL cost heuristic.

4 Conclusions

Being able to find efficient ASIL decompositions significantly reduces the development efforts and consequently has substantial implications for the development costs. We propose a technique to automate ASIL decomposition as part of HiP-HOPS, a model-based safety and reliability analysis tool. We have shown in this paper the outcome of applying the minimization of ASIL-dependent cost by TS to a hybrid braking system. Although focused on ISO 26262 guidelines, our approach can be applied in principle to current and future similar SIL reduction techniques.

The results for the optimization technique we propose are deemed very satisfactory, both in processing time and quality of the solutions obtained; TS has shown the flexibility to successfully tackle ASIL decomposition optimization with different cost functions. The size of the illustrative case study we present here does not allow drawing definitive conclusions about the TS technique scalability; however we have applied it to another model, with hundreds of failure modes and thousands of cut sets, and it was able to find useful solutions within a matter of seconds whereas the exhaustive technique has not completed such model with over a month of processing time. To further develop the technique proposed here we look to extend it to allow the designer to use a mix of different cost heuristics for specific categories of components and/or to include relative cost information between those categories. Finally, we find it valuable that [1] incorporates the designer experience in the optimization process. In the future, our technique will also allow designers to mark their preferences, but instead of rigidly confining the search, it will favor solutions that include such choices while still allowing for other good solutions to be identified.

References

1. Mader, R., Armengaud, E., Leitner, A., Steger, C.: Automatic and Optimal Allocation of Safety Integrity Levels. In: Proceedings of the Reliability and Maintainability Symposium (RAMS 2012), pp. 1-6 (2012)
2. Papadopoulos Y., Walker M., Reiser M.-O., Weber M., Chen D., Törngren, Servat D., Abele A., Stappert F., Lönn H., Berntsson L., Johansson R., Tagliabo F., Torchiaro S., Sandberg A.: Automatic Allocation of Safety Integrity Levels. In: Proceedings of the 1st Workshop on Critical Automotive applications: Robustness and Safety (CARS'10), 27th April 2010, Valencia, Spain. Pages 7-10. ACM, New York, NY, USA. ISBN: 978-1-60558-915-2, doi> 10.1145/1772643.1772646 (2010)
3. Lin, M-H, Tsai, J-F., and Yu, C-S.: A Review of Deterministic Optimization Methods in Engineering and Management, Mathematical Problems in Engineering, vol. (2012), Article ID 756023, 15 pages (2012)
4. Hansen, P. and Jaumard, B.: Algorithms for the maximum satisfiability problem. Computing, volume (44), issue 4, pp. 279- 303 (1990)
5. Hansen, P. and Lih, K.-W.: Heuristic reliability optimization by tabu search. Annals of Operations Research, volume (63), pp. 321-336 (1996)
6. de Castro, R., Araújo, R.E, and Freitas, D.: Hybrid ABS with Electric motor and friction Brakes. In: IAVSD 2011 - 22nd International Symposium on Dynamics of Vehicles on Roads and Tracks, Manchester, UK, 2011 (2011)