Available online at www.sciencedirect.com

ScienceDirect

IFAC Papers Online CONFERENCE PAPER ARCHIVE

IFAC-PapersOnLine 49-3 (2016) 184–190

Comparing Automatic Allocation of Safety Integrity Levels in the Aerospace and Automotive Domains

Ioannis Sorokos, Luis P. Azevedo, Yiannis Papadopoulos, Martin Walker, David J. Parker

University of Hull, Hull, HU6 7RX, UK
(+44 (0)1482 465981, e-mail: {I.Sorokos@2012., Y.I.Papadopoulos@, L.P.Azevedo@2012., D.J.Parker@, Martin.Walker@} hull.ac.uk).

Abstract: Safety standards guide the development of systems whose operation raises concerns about safety. We focus our attention on the automotive and aerospace standards, ISO 26262 and ARP4754-A respectively. Both standards advocate a process for controlled allocation of safety integrity requirements that starts early in the design and continues as the system architecture is being refined. This procedure may generate a plethora of feasible design variants, all satisfying system safety requirement, but each having different allocations of integrity to components and different costs. In this paper, we describe a model-based safety analysis method for automating this allocation process in a way that cost-optimal design variants are selected. We show that the proposed method is generic and can satisfy both the automotive and aerospace safety standards with application to both industries. We apply the method using both standards on a common case study and discuss the differences in the results obtained, reflecting on the commonalities and differences between the two standards.

Keywords: safety-critical systems; safety requirements; ASIL allocation; DAL allocation; optimisation.

1. INTRODUCTION

Safety-critical systems are systems whose malfunction or loss of function can potentially impact safety in significant ways, i.e., by threatening serious harm or even loss of life. To address such concerns, safety standards have been produced to guide development in domains where safety-critical systems are common, such as the automotive, aerospace, nuclear and healthcare industries. Mitigation of hazardous risk — the combination of the likelihood of an event endangering safety with the event's impact — is typically established as the focal point of the imposed regulations. Towards this end, developers are required to demonstrably implement safety measures within their systems to reduce such risk to "a level as low as reasonably possible" (HSE, 2001, p. 8). These measures are encapsulated in the form of Safety Integrity Levels (SILs), which are embodied in similar concepts across standards. For the ISO 26262 (ISO, 2011) and the ARP4754-A (SAE, 2010), these levels are referred to as Automotive Safety Integrity Levels (ASILs) and Development Assurance Levels (DALs). Both standards encourage addressing safety from the earliest stages of development rather than let it emerge as an after-thought. The standards propose a top-down process of evaluating safety risks, assigning SILs to mitigate them and verifying them upon implementation.

With each level of architectural refinement, standards permit allocating lower levels of safety integrity when the system is designed with adequate redundancy or alternative risk-mitigating designs. Higher levels of integrity effectively incur additional costs in terms of development time and effort. Thus, there is incentive to evaluate the space of potential allocations and select those that minimise such costs while still abiding by the rules of the relevant standards. We define this as the "safety integrity requirements allocation problem" and, in this paper, demonstrate means of solving it optimally for both standards. In section 2, a more detailed view of the allocation process advocated within each of the two standards will be presented, to highlight their similarities and differences. In the next section, an overview on the optimisation techniques we applied to solve the problem for each domain will follow. Finally, a case study on a wheel braking system model, optimally allocating ASILs and DALs on it will be presented.

2. BACKGROUND

Contemporary safety standards promote a departure from prescriptive measures of past standards, instead favouring an argument-based approach (Leveson, 2011). Effectively, the developers are not bound to implementing measures solely for the sake of filling out a compliance checklist. Instead, they are encouraged to assess their system's risk, analyse the main causes of risk and implement measures which convincingly mitigate it. The concept of the Safety Integrity Level (SIL), introduced in the domain-neutral IEC 61508 standard, is indicative of this paradigm. Each SIL encapsulates the level of rigour with which safety activities must be conducted without enforcing specific

10.1016/j.ifacol.2016.07.031

means of doing so. In the automotive domain, these qualitative indicators are referred to as Automotive SILs (ASILs) in ISO 26262 and in the aerospace domain as Development Assurance Levels (DALs) in ARP4754-A. In both domains, there are 5 such levels, from the lowest level of safety to the highest: ASIL QM, to A, to D and from DAL E to DAL A respectively.

As development progresses, the system's architecture evolves hierarchically until it reaches low level software and hardware. Traceability of ASILs and DALs is intended to be maintained throughout this process and be updated as significant architectural changes occur. When the system's architecture includes fault-tolerant design, such as with redundant elements, it is possible to reduce the levels of the elements contained within that design while the overall architecture still meets the higher integrity level. This reduction is supported on the basis of combining risk mitigation under the assumption of independence of failures between those elements, a concept further detailed in section 2.3. As an instance of this reduction, if we consider (Fig. 1), we can observe a system with three internal components.

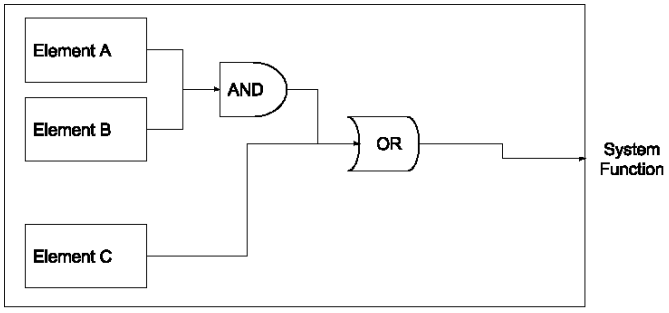

Fig. 1. Decomposition Example

At first glance, given that each of the elements contribute to the system's function, so each should inherit the system's ASIL or DAL. However, two of those components only cause the system function to fail when they fail in combination (A and B), whereas the third can originate the function failure by itself (C). Component C inherits the full system SIL, but the standards allow the components A and B to be developed to a reduced level (there are several standard-dependent options for this, see 2.1 and 2.2). This process is referred to as "decomposition". The example is arguably simplistic; in a real system, the internal elements could also participate in other systems and an allocation decision would have to contemplate the impact of the components' failures on those systems. With modern architectures containing dozens of subsystems and hundreds of components, the number of potential combinations can grow to a size which cannot be efficiently explored with manual or exhaustive techniques. Optimisation techniques, such as those presented in Section 3 can be used to accomplish this task. However, we will first contrast the differences in each standard's approach to allocating integrity levels.

2.1. Safety Requirements in ISO 26262

In ISO 26262, ASILs are identified once a hazard and risk analysis has been performed. This analysis identifies what the safety consequences of each system function's malfunction can be. Furthermore, the severity, likelihood of occurrence and controllability (by the driver) of each hazard is evaluated. Depending on the combination of these attributes, each hazard is assigned an ASIL. The higher the severity and likelihood and the lower the controllability, the higher the ASIL. Once the architecture has developed a set of systems which implement these functions, system-level safety requirements known as Safety Goals (SGs) are produced. The standard then specifies a hierarchy of increasingly detailed safety requirements to address these SGs. Each of these requirements inherit the ASIL from their parent in the hierarchy, with the ASIL eventually reaching software or hardware safety requirements. At each step of this process, these requirements are also assigned to corresponding elements in the system architecture, which needs to both meet them and satisfy the ASIL they are linked to. As further elements of the architecture are designed, the ASILs can be decomposed, following the logic presented in (Fig. 1). Alongside this decomposition, the standard applies safety requirements appropriate to the level of architecture considered, which actually inherit the decomposed ASIL. The particular rules for decomposing in ISO 26262 are known as the "ASIL algebra" (Azevedo et al., 2014a, p. 3). According to this algebra, each ASIL is represented with an integer from 0 to 4 corresponding to the levels QM and A to D. Elements directly causing a SG failure are assigned the corresponding ASIL, as per the example. Independent elements which need to fail in unison for that to happen are allowed to split the burden of the ASIL. The rule for the ASIL algebra is that the sum of the numerical ASILs must meet the SG ASIL. So, for example, decomposing an ASIL C (or ASIL 3) to two components can be achieved – among other options – by assigning one ASIL B and the other ASIL A (ASIL 2 + ASIL 1 = ASIL 3).

2.2. Safety Requirements in ARP4754-A

In ARP4754-A, DALs are similarly allocated for the first time during the Functional Hazard Analysis (FHA). The FHA is very similar to the hazard analysis in ISO 26262, with the main difference being the absence of the concept of controllability. This can be attributed to the stricter approach to safety when aircraft are considered. As before, once hazards have been identified, each of the system's functions is assigned a Function DAL (FDAL) to address its potential hazard. The FDAL is also inherited by the system implementing said function as a System DAL (SDAL). As each system's architectural elements emerge, allocation of DALs to those elements follows the pattern established in (Fig. 1). In the case of DALs, the allocation algebra once more assigns 0 to 4 to levels E to A. The rule