Hazard Relation Diagrams: a diagrammatic representation to increase validation objectivity of requirements-based hazard mitigations

Bastian Tenbergen[1,2], Thorsten Weyer[2], Klaus Pohl[2]

Abstract: This talk is based on a paper published in the Requirements Engineering Journal in May 2017 [TWP17]. During the development of safety-critical systems, the development process must ensure that requirements, which are defined to mitigate a hazard, are adequate. Adequacy of such hazard-mitigating requirements (HMRs) means that the requirements may not oppose the system's operational purpose and must sufficiently avoid, reduce, or control, the occurrence of the conditions that trigger the hazard. However, information about the occurrence of the hazard's trigger conditions are a work product of hazard analyses during early stages of safety assessment, while HMRs are a work product of requirements engineering. Dependencies between HMRs and hazard analysis results are implicit and tacit. In consequence, there's a risk that during validation, inadequacy of HMRs regarding their ability to mitigate a hazard remains covert. The result may be that the system is assumed to be safe, but in fact may still cause injury or death. We introduced Hazard Relation Diagrams (HRDs) as a means to integrate and graphically visualize hazard analysis results with HMRs. Herein, we also provide insights into their empirical evaluation and show that HRDs increase objectivity in rationales containing adequacy judgments.

Principles and Visual Notation of Hazard Relation Diagrams

Hazard Relation Diagrams integrate HMRs with the hazard they are intended to mitigate in a single diagram [TWP15]. During validation, HRDs is reviewed individually and sequentially, thereby allowing for alternative mitigations to be validated with regard to each respective hazard. HMRs are depicted using modeling elements of UML activity diagrams. HRDs contain exactly one hazard and several mitigation partitions to support different multiplicities between hazards and HMRs. The dashed mitigation partitions surround the HMRs and can be distributed across "geometrically" distant areas within the same or several activity diagrams. HRDs contain the hazard's tree of trigger conditions, the conceived safety goal, and one Hazard Relation, which is an n-ary association relating the hazard, trigger conditions, safety goal, and mitigation partitions. An example is shown in Fig. 1 (activity labels are removed for legibility).

Empirical Evaluation Shows Increases in Review Objectivity

In two empirical experiments involving a total of 168 graduate and undergraduate students [TWP17], the hypothesis was investigated whether there is an impact on

[1] State University of New York at Oswego, NY, USA, bastian.tenbergen@oswego.edu
[2] University of Duisburg-Essen, paluno, Germany {thorsten.weyer, klaus.pohl}@paluno.uni-due.de

objectivity when using HRDs to validate the adequacy of HMRs (treatment condition) versus using activity diagrams (control condition). Participants were asked to review 10 hazard mitigations and judge if the hazard can still occur during operation and to justify their judgement in a written rationale. Rationales were categorized into those that mention "semantics" or "syntax" (i.e., diagram properties also found in activity diagrams, see also combined variable H1.a), or mention "mitigation," "trigger condition," or "safety goals" (i.e., properties specific to HRDs, see also combined variable H1.b). Fig. 2 shows the differences between treatment (black bars) and control (grey bars) conditions. Significant differences bear p-value, effect size, and achieved statistical power and show that using HRDs, judgments were more often based on objective information about the hazard, rather than on the diagram's meaning or style.

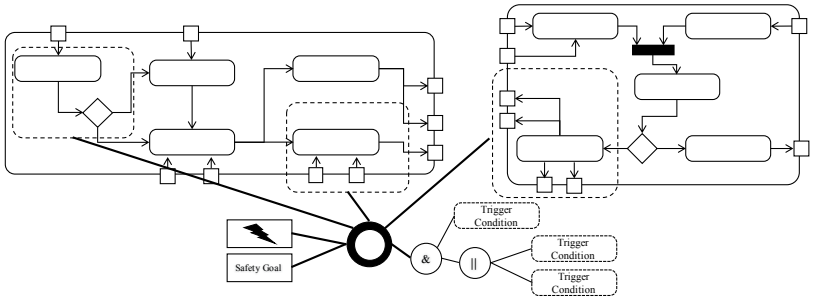

Fig. 1. Example of a HRD with three mitigation partitions surrounding HMRs in two activity diagrams.

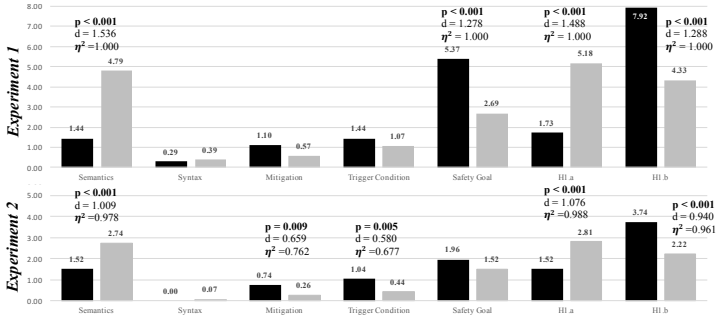

Fig. 2. Experimental Results show signitificantly more Judgments based on Hazard Analyses using HRDs.

References

[TWP15] B. Tenbergen, T. Weyer, and K. Pohl, "Supporting the validation of adequacy in requirements-based hazard mitigations," in Springer LNCS 9013, 2015, pp. 17-32.

[TWP17] B. Tenbergen, T. Weyer, and K. Pohl, "Hazard Relation Diagrams: A Diagrammatic Representation to Increase Validation Objectivity of Requirements-based Hazard Mitigations," in Requirements Eng J. DOI: 10.1007/s00766-017-0267-9.