Generating Review Models to Validate Safety Requirements

Bastian Tenbergen[1] Thorsten Weyer[2]

Abstract: This talk discusses our approach for automatically generating review models for safety-critical systems presented in the paper [TW21] published in the Feb. '21 issue of the Journal of Software and Systems Modeling. We present a semi-automated formal approach and tool support to generate Hazard Relation Diagrams. Enabled by mitigation tables, the approach consists of two transformation steps using OMG's QVTo language [OMG16].

Keywords: Safety requirements; Hazards; Validation; Adequacy; Modeling relation diagrams

1 Introduction

Developing safety-critical systems includes identifying hazards and defining corresponding mitigations at the earliest possible stage of development. The thusly identified hazard-mitigating requirements (HMRs) must be valid with regard to the intended functionality and render the system sufficiently safe during operation. Yet, validating HMRs is burdened by the fact that hazards and their HMRs are a work product of safety assessment and requirements engineering, respectively. These work products are poorly integrated such that during validation, the information needed to determine the adequacy of HMRs is not available to stakeholders, potentially leading to lingering covert safety hazards. To aid in the validation of HRMs, we have proposed, improved, and evaluated [TWP18] a novel diagram type called "Hazard Relation Diagrams" (HRDs) which represent requirements, hazards, and their mitigation together in a single review model.

2 Generating Hazard Relation Diagrams

HRDs are generated from UML activity diagrams containing hazard-inducing requirements (HIRs) and tables containing the results of functional hazard analysis (FHA). HRDs contain one hazard per mitigation, however may contain multiple mitigation partitions for HMRs in geometrically distant areas in the activity diagram. HRDs are generated by first specifying HMRs using a mitigation template containing deletions, additions, and substitutions of activity diagram model elements documenting the HIRs. One mitigation

[1] State University of New York at Oswego, Dept. of Computer Science, NY, USA bastian.tenbergen@oswego.edu

[2] Technische Hochschule Mittelhessen, Gießen, Germany thorsten.weyer@mni.thm.de

template corresponds to one mitigation partition in the diagram that highlights the changes from HIRs to HMRs. Afterwards, the hazard, trigger conditions, and the safety goal from the FHA are appended into the activity diagram with HMRs, thus completing the HRD.

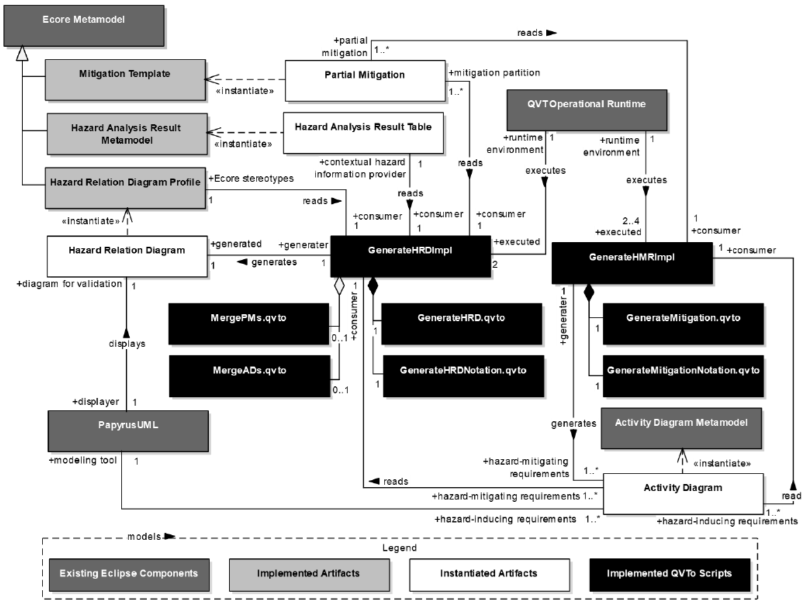

Fig. 1: Structure and Technical Interplay of the Tool Prototype Components.

Based on a canonical artifact formalization, transformation scripts have been implemented using OMG's Query/View/Transformation Operational Mappings language [OMG16] to implement the generation process. The metamodel of the tool prototype is shown in Fig. 1.

3 Data Availability

QVTo scripts, proof-of-concept implementation, and empirical data on the effectiveness of HRDs are available at `https://github.com/tenbergen/hazardrelationdiagrams`.

References

[OMG16] Object Management Group: Query/View/Transformation (QVT) Specification. OMG Document Number formal/2016-06-03., 2016. Version 1.3.

[TW21] Tenbergen, Bastian; Weyer, Thorsten: Generation of hazard relation diagrams: formalization and tool support. Software and Systems Modeling, 20(1):175–210, Feb 2021.

[TWP18] Tenbergen, Bastian; Weyer, Thorsten; Pohl, Klaus: Hazard Relation Diagrams: a diagrammatic representation to increase validation objectivity of requirements-based hazard mitigations. Requirements Engineering, 23(2):291–329, Jun 2018.