Experimental Material for the Empirical Evaluation of Hazard Relation Diagrams

Bastian Tenbergen

paluno – The Ruhr Institute for Software Technology,
University of Duisburg-Essen, Germany
bastian.tenbergen@paluno.uni-due.de

1 Purpose

This purpose of this document is to explain the experimental material used in the empirical evaluation of Hazard Relation Diagrams. The experimental material was used in the pilot study reported in [1]. After the pilot study was concluded, the experimental material was improved based on the findings of the pilot study and subsequently used in an empirical investigation on the impact of Hazard Relation Diagrams into review objectivity, effectiveness, and effectivity. We are making the experimental material available to researchers free of charge in hopes that our empirical study will be replicated and results confirmed.

2 Use of the Experimental Material in the Study

We used an excerpt of a requirements specification for the adaptive cruise control system as the basis for the experimental material. This entailed one activity diagram comprising five hazard-inducing requirements, for which a FHA was conducted. A total of ten hazards were identified during FHA, five of which were randomly selected and *adequately* mitigated. To do so, for each hazard, a variation of the activity diagram was derived containing hazard-mitigating requirements that will avoid the hazard during operation. This yielded five activity diagrams containing adequate hazard-mitigating requirements. The other five hazards were *inadequately* mitigated. To do so, for each hazard, a variation of the activity diagram was derived containing hazard-mitigating requirements with semantic mistakes allowing the hazard to still occur during operation. This yielded five activity diagrams containing inadequate hazard-mitigating requirements. All ten activity diagrams were used for the control condition of the experiment. For the treatment condition, each adequate and inadequate activity diagram was extended into a corresponding Hazard Relation Diagram. The experimental material consisted hence of ten activity diagrams for the control condition and ten Hazard Relation Diagrams for the treatment condition. The control condition furthermore included FHA results.

3 Files included in the Archive

The following explains the files included in this archive.

- **ACC Function Model.jpg** The excerpt of the functional requirements of the Adaptive Cruise Control System based on [2] and [3] that was the basis of the experimental material.
- **FHA-table-complete v5.png** The results of the Functional Hazard Analysis that was conducted based on "ACC Function Model.jpg".
- **Mitigation H0 Example Adequate/Inadequate AD.jpg** An example hazard that was adequately or inadequately mitigated, respectively, and where the hazard-mitigating requirements were documented in a conventional activity diagram. This file was used in the pre-experimental briefing as well as in the "dry runs".
- **Mitigation H0 Example Adequate/Inadequate HRD.jpg** An example hazard that was adequately mitigated and where the hazard-mitigating requirements were documented in a Hazard Relation Diagram. This file was used in the pre-experimental briefing as well as in the "dry runs".
- **Mitigation H* AD.jpg** These files constitute the experimental material that was used during data collection in the control condition. The asterisk * represents the unique ID of the diagram, i.e. a number from 1-10. This ID refers to the ID of the hazards from "FHA-table-complete v5.png".
- **FHA_H*.jpg** These files constitute the row of the "FHA-table-complete v5.png" that was also used during the control condition. The asterisk * represents the unique ID of the diagram, i.e. a number from 1-10. This ID refers to the ID of the hazards from "FHA-table-complete v5.png".
- **Mitigation H* HRD.jpg** These files constitute the experimental material that was used during data collection in the treatment condition. The asterisk * represents the unique ID of the diagram, i.e. a number from 1-10. This ID refers to the ID of the hazards from "FHA-table-complete v5.png". Since the Hazard Relation Diagrams contain the information from "FHA-table-complete v5.png", the treatment condition received no further experimental material.
- **survey.hazardreview.2014-11-19.xml** This is a backup configuration file of the implemented experiment from SoSci Survey [5]. The experiment can be replicated by importing this file to the experiment configuration tool. Note, that some proprietary files not included in this archive are referenced in the configuration file.

4 List of Adequately and Inadequately Mitigated Hazards

Some hazards from "FHA-table-complete v5.png" were randomly selected and adequately mitigated, while others are inadequately mitigated. The following Table 1 lists, which hazards have been adequately and inadequately mitigated and states example rationales by the experimenters which were used as a baseline to gauge the validity of participant responses. The column "Rationale (Alternative)" contains alternative rationales that participants identified which may considered valid as well.

Table 1. List of Adequately and Inadequately Mitigated Hazards and Rationales.

Hazard ID	Adequate?	Rationale (Experimenter)	Rational (Alternative)
H1	Yes	The distance to the vehicle driving ahead is considered during computation of the velocity.	
H2	Yes	The driver is informed, if a vehicle is detected.	Not a reasonable implementation of the safety goal. Driver should only be informed in dangerous situations.
H3	Yes	The function "Compute Road Friction Coefficient" checks the desired speed by means of TLC weather information obtained from the radio.	1. The weather conditions cannot be obtained from the radio, since there is no information given that this information stems from a TLC service. 2. The system does not wait for the driver's response.
H4	No	The decision "Current Speed == Target Speed" is semantically wrong.	The Distance, respectively, the driver's acceleration command is not being considered.
H5	No	The control flow "Initiate Emergency Brake" should not be sent to "Integrate Sensor Data", as the emergency braking command would be replaced by a regular braking maneuver during the next continuous iteration of the control loop.	1. Five seconds is too long until collision 2. Safety goal not fulfilled
H6	No	"Radio Program" is semantically wrong.	The distance is neither considered in "Computer Acceleration" nor in "Compute Brake Force". Safety goal is hence not fulfilled.
H7	No	The data "Distance to Vehicle Ahead" cannot be obtained from "Compute Optimal Velocity".	"Compute Engine Torque" does not receive distance information. Safety goal is hence not fulfilled.
H8	Yes	The function "Compute Engine Torque" checks, if the driver pressed the gas pedal.	Safety goal is fulfilled.
H9	No	Wrong mitigation: The brake pedal should be checked and the function "Compute Brake Force" must be modified correspondingly.	Safety goal is not fulfilled.
H10	Yes	The distance to the vehicle driving ahead is considered when computing brake force or engine torque.	1. Safety goal is fulfilled 2. Mitigation does not necessarily prevent too strong brake force.

5 License and Permissions

Acknowledgments. This research was partly funded by the German Federal Ministry of Education and Research under grant number 01IS12005C. We thank Arnaud Boyer of Airbus Defence and Space for his consultation regarding FHA. We thank Dr. Frank Houdek from Daimler for the consultation on the Adaptive Cruise Control system. We thank Dr. Kai Petersen, Marian Daun, and André Heuer for their feedback on the study design.

References

[1] Tenbergen, B., Weyer, T., Pohl, K.: Supporting the Validation of Adequacy in Requirements-based Hazard Mitigations," in Proceedings of the 21st International Working Conference on Requirements Engineering: Foundations for Software Quality, 2015, pp. 17-32.

[2] Mao, J., Chen, L.: Runtime Monitoring for Cyber-physical Systems: A Case Study of Cooperative Adaptive Cruise Control. In Proceedings of the 2nd International Conference Intelligent System Design and Engineering Applications, 2012, pp. 509–515.

[3] Caramihai, S., Dumitrache, I.: Urban Traffic Monitoring and Control as a Cyber-Physical System Approach. In: Advanced Intelligent Control Systems and Computer Science, Springer, Heidelberg, 2013, pp. 355–366.

[4] http://creativecommons.org/licenses/by-nc-sa/4.0/

[5] https://www.soscisurvey.de/