The Importance of Active Choices in Hazard Analysis and Risk Assessment

Rolf Johansson

The Importance of Active Choices in Hazard Analysis and Risk Assessment

Rolf Johansson
SP Technical Research Institute

***Abstract* — According to the functional safety standard for road vehicles, ISO 26262, the list of safety goals shall be shown to be complete. Especially when considering highly automated driving, this may lead to the formulation of very general hazardous event. On the one hand this may make it easier to show completeness, but on the other hand it may cause that too strong ASIL attributes are allocated on too much of the implementation, implying unnecessary high cost. This position paper claims that carefully chosen explicit failure models in the hazard definitions, will generally enable more cost-efficient and still safe E/E systems for road vehicles. This is especially important for highly automated driving and autonomous vehicles, where many safety goals may have an impact on a large part of the entire E/E architecture.**

Keywords — ISO 26262, hazard analysis and risk assessment, safety goals, failure models, highly automated driving.

I. INTRODUCTION

When performing a hazard analysis and risk assessment (HA&RA) in the domain of road vehicles according to ISO 26262 [1], it is a challenge to make the list of Safety Goals (SG) complete and correct, still not forcing the implemented functionality to become too expensive. This is a variant of the classical problem in design verification, saying that if you are not so detailed in the analysis you need instead to be conservative. The more details you put in your analysis, the smaller margins are needed. In an analogous way the HA&RA can be based on few and general hazards and situations, or a larger number of more detailed ones. In the former case the benefit is a shorter HA&RA, easier to perform and easier to show complete. The cost for this is a design that might be much more expensive because of the higher values and or/the broader implications of the safety goals. In the latter case the cost might be lower, but this requires a more elaborated HA&RA. This position paper argues that safety goal formulation, is an active choice and that it in many cases is worth the effort to be more explicit and elaborated in the HA&RA. The paper is organized as follows. In section II is argued for how to verify completeness of a HA&RA. Section III presents why it can be said that a HA&RA that is an activity that can be performed in many valid ways and thus important make a choice about. In section IV it is argued how to elaborate the HA&RA and especially identifying several hazards constituted by different tolerance margins. Section V then tells why this is extra important for autonomous vehicles, where the cost implications may be significantly higher. Finally section VI concludes the paper and summarizes the claims of this position paper.

II. HAZARD ANALYIS AND RISK ASSESSMENT COMPLETENESS

The hazard analysis and risk assessment (HA&RA) is the activity prescribed in ISO26262 [1] which results in a list of safety goals (SG) that together are sufficient to fulfil, in order to keep an item functionally safe. The input to this activity is the item definition which contains the functional description on which the scope of functional safety is based.

The method to reach a complete list of sufficient SGs is to first generate a complete list of hazardous events (HE), and then make sure that each of the HEs are covered by at least one SG.

A hazardous event is specific with respect both to situation and to hazard. The list of HEs can be seen as complete if it covers all combinations of situations and hazards relevant for the item of concern. Situation includes both the environmental conditions and the vehicle state. This means that it is possible to formulate dedicated HEs investigating the effect of rain, snow, darkness, road friction, road steepness, other vehicles, vulnerable road users etc, but also elaborating the effect of e.g. the ego vehicle speed.

Of course there are potentially an infinite number of possible situations that can be defined. There are several categorizations made to structure what situations to consider, both internal to companies and more publicly published, e.g. [2], [3] and [4]. A claim in this position paper is that such lists are of limited use when determining what situations to consider in a specific HA&RA.

The hazards specify how the item can fail in a potentially dangerous way. This means that the list of HEs should contain the safety-critical failing possibilities of the functionality described in the item definition.

The list of HEs can be claimed to be complete if there is no candidate HE that would require another SG not already in the list. Another way to formulate this is to say that the list of HEs needs to cover all the dimensioning cases. We do not need to list a number of combinations of hazards and situations, which would be covered by the already identified safety goals.

The above implies that a method for proving completeness of a HA&RA is to challenge it by trying to formulate more HEs. If we cannot formulate any new HE, not already covered by the list of SGs, we can conclude that

we are ready with the HA&RA activity. In ISO26262 [1], it is required in paragraph 7.4.5.1 of part 3 to verify the completeness of the HA&RA. However, there are no criteria for what is considered as a valid argument for completeness.

This paper claims that a good method for verification of HA&RA completeness, is to let a review team challenge the list of HEs looking for a candidate HE that is not covered by the list of SGs. If the review team cannot identify such an HE, they may conclude completeness of the HA&RA.

III. The HA&RA trade-off problem

The previous section elaborated the semantics of completeness of a HA&RA. However, this doesn't say anything how detailed the situations and the hazards should be defined. This position paper claims that this is always a choice, and never completely given by the item definition. For the same item definition, the length of the list of considered HEs may differ very much, all of them still fulfilling the completeness criteria.

As an example let us consider an automatic emergency brake (AEB). In a very short version there are two HEs in the list. Both consider the situation 'driving'; the one the hazard 'omission' and the other the hazard 'commission'. The situation 'driving' here will cover all possible conditions when the vehicle is driving. If we can argue that when we are not driving, neither a commission failure nor an omission failure will be considered as severe at all, we can conclude that this list of situations is complete.

When determining the ASIL attribute for these two HEs, we can argue that they both are: E4, S3 and C3. The justification for the situation 'driving' becoming E4 is obvious. This situation includes all driving situations and hence also the cases when either there is a vehicle close behind driving at high speed, or rather close in front standing still. In both these cases the controllability is very low and the severity is very high. This implies that an ASIL D attribute will be inherited to all parts of the E/E systems implementing the AEB. This in turn will put a high cost to the implementation.

An alternative HA&RA may list a number of different situations, and also more elaborated hazards. In the list of situations, it may be relevant to identify the most critical situations for the omission and the commission failures, respectively. If such critical situations (implying S3 and C3), can be identified as having a lower exposure, such a strategy is worthwhile. If we for example can argue that the situations where the AEB really saves our life (omission is S3) are quite rare (the drivers are skilled, having a safe strategy), the omission hazard will not imply an ASIL D safety goal. This means that if we can argue that the emergency situations when the actuation of an AEB really makes a difference between life and death are less frequent than E4, we will lower the ASIL D implication otherwise being the case.

We can go even further in detailing the HA&RA activity by detailing the hazards. In the above example we only consider the omission and commission failures of the AEB. This means that either the AEB works properly, exactly as intended, or it doesn't brake at all when needed, or it fully activates the braking in an improper situation. What if the omission is not complete, but only, for example, a little bit too late in the brake activation? In the simple list of hazards only containing omission and commission, we consider only the cases that either everything is OK or it doesn't work at all. It might be fruitful also to introduce some margins in which we still consider it as jeopardizing safety, but requiring lower risk reduction.

For an AEB, a hazard of a too late activation by 0,1 s may include potential consequences of collisions, but the impact speed may be limited causing the maximal severity to be lower as well. If we foresee the design solutions to become very expensive to claim full timeliness with high ASIL, it might be a good idea to specifically address a limited timing failure by a SG having a lower ASIL attribute than a complete omission failure.

Which Hazards to detail, and how, is a design choice. This paper claims that it should be an active choice to what detail the hazards are formulated in the HA&RA.

IV. Towards more detailed hazardous events

The Hazop guide words [5] are in most cases an efficient way to find candidates for detailing the hazards. By starting with the functionality claimed in the item definition, applying the Hazop guide words may in most cases become candidates for more detailed hazards. For the guide words implying quantifications like 'too much', 'too little', 'too late', and 'too early', it is also a good idea to consider several intervals.

In our timing failure in the AEB example above, we could have three failure boundaries: less than 0,04 seconds too late resulting in QM, less than 0,10 seconds causing ASIL A, less than 0,25 seconds ASIL B, and arbitrary timing failures implying ASIL C. All of these will become dimensioning in the sense that no one of them can be seen as covered by the other ones. The hazard implying the highest ASIL attribute (ASIL C in this example), is the one restricted by no tolerance at all. When going down in integrity level, the required margin restricting the hazard becomes harder to fulfil. Either the timing margin is tough or the integrity attribute is tough, not both at the same time. In a similar way can any hazard be detailed considering different degrees of failing according to the Hazop guide words; too little, too much, too early, too late.

V. Implications from highly automated driving

When introducing vehicles capable of highly automatic driving (HAD) or even autonomous vehicles, the activity of HA&RA becomes more complex. Furthermore, the implications of many safety goals are spread on a larger part of the E/E systems of the vehicle. This implies that ending the HA&RA activity with a few safety goals that could be regarded as too unelaborated, and thus potentially too conservative, may generate a significant increase in cost of the vehicle.

The more complex the functionality implemented by the E/E systems, and the more each SG will cause effects on a large portion of the E/E systems, the more important is it to be careful when performing the HA&RA. This paper claims that for autonomous vehicles and for HAD it is very important to perform active choices of how detailed the situations and the hazards are considered in the evaluation of hazardous events. The potential cost saving are significant when comparing more elaborated HA&RA with more general ones.

VI. Conclusions and Future Work

This position paper argues for the importance of a detailed and elaborated hazard analysis and risk assessment (HA&RA).

Firstly it argues for a methodology valid for the problem of HA&RA verification with respect to completeness. The conclusion is that if a review team can find any candidate hazardous event (HE) not covered by any listed safety goal (SG), the completeness is shown not to hold. If no such candidate HE can be found by the review team, the verification can be seen as showing completeness of the HA&RA.

Secondly is argued for the importance of being detailed enough in terms of situations and of hazards when defining what hazardous events to consider. The claim is that a lower number of hazardous events may imply a more expensive solution than a more elaborated list of HEs. Note that both ways, the HA&RA may be shown to be complete. This means that both ways are fulfilling all aspects in ISO26262, but the one implies a more expensive solution than the other.

Furthermore, it is argued for the importance of finding explicit failure models for all hazards. It is claimed that the Hazop guide words are relevant in most cases. Even if originally the set of failures is considered as limited by commission and omission, it may make sense to introduce failures reflecting most of the Hazop guide words.

Then it is claimed that it in many cases may make sense to generate several failures from the quantitative guide words like: too little, too much, too early and too late. This may introduce a set of hazards where some are more restricting in the tolerated failure margin and other are more restricting in the required safety integrity. Having an idea of the cost drivers in the design, might to an extent generate a differentiation of the safety goals based on this kind of SG detailing.

Finally, this paper takes the position of arguing for the importance of being detailed enough in the HA&RA for HAD and autonomous vehicles. It is claimed that the cost of a too conservative SG is significantly higher for such vehicles because of broader implications of each SG. This implies that the potential to save cost by elaborating the HA&RA is significant for autonomous vehicles.

Acknowledgment

This work has been financed by The Swedish government agency for innovation systems (VINNOVA) in the FUSE project (ref 2013-02650).

References

[1] ISO, "International Standard 26262 Road vehicles -- Functional safety", 2011.

[2] Martin, H., Winkler, B., Leitner, A., Thaler, A., Cifrain, M., Watzenig, D., “Investigation of the influence of non-E/E safety measures for the ASIL determination”, 39th Euromicro Conference Series on software Engineering and advanced Applications, 2013.

[3] Jang, H.A., Hong, S-H, Lee, M.K., “A Study on situation analysis for ASIL Determination”, Journal of Industrial and Intelligent Information Vol. 3, No. 2, 2015.

[4] Verband der Automobilindustrie e.V. (VDA), "Situationskatalog E-Parameter nach ISO 26262-3" 2015.

[5] IEC, "International Standard 61882 Hazard and operability studies (HAZOP studies) - Application guide", 2001.