Efficient Identification of Safety Goals in the Automotive E/E Domain

Rolf Johansson

Efficient Identification of Safety Goals in the Automotive E/E Domain

Rolf Johansson

Abstract— **This paper addresses the problem of how to identify all safety goals for an item in the automotive E/E domain. The paper gives a background on the problem of hazard analysis and risk assessment in general, and for the automotive domain in particular. A key factor for success is to identify all the relevant hazardous events, which task constitutes a paradox. Either the specification of the possible driving situations and the system hazards are done too general and abstract implying a too conservative analysis, or done too detailed and specific ending up with an almost infinite list of hazardous events to consider. This paper addresses this paradox by the formulation of a number of rules enabling to reduce the potentially infinite set of candidates of hazardous events to a limited number, still sufficient to cover all safety goals. Besides that it enables solving the paradox of becoming both detailed and limited, it also can be used as a tool for reviewing the completeness of a set of safety goals.**

Index Terms— **Hazard analysis, Automotive, ISO 26262.**

I. Introduction

In all domains of functional safety, it is essential to perform a complete and correct Hazard analysis and risk assessment (HA&RA). The purpose of this activity is to identify and categorize all Hazards, i.e. all potential sources of accidents caused by erroneous behaviour of the function under consideration. In the automotive domain, the rules for HA&RA are given by part three of the ISO 26262 standard [1]. The goal of this HA&RA is to produce the so called Safety Goals. The rest of the standard prescribes how to guarantee that all these Safety Goals in the end are fulfilled, thus implying functionally safe road vehicles. However, in order for the complete vehicle to act functionally safe, first the set of items analysed must be complete, and secondly, for every item the set of Safety Goals must be complete. This paper addresses the latter problem.

In the process to identify the Safety Goals, the standard ISO 26262 prescribes to analyse all Hazardous Events that might have an impact on this set. This means that all possible failures of the Item of concern should be considered, and for all driving scenarios and all environmental conditions. The combined effect of the driving scenarios and the environmental conditions are called 'situation' in the ISO 26262 terminology. As there is no predefined standard set of situations, this would potentially generate an infinite number of Hazardous Events to analyse. The question is whether we can come up with a way to identify if there is a limited set of Hazardous Events that completely identifies the full set of Safety Goals. The reason why this would work is that a large number of Hazardous Events do not contribute to the identification of a unique Safety Goal. What we need is a way to identify a limited set of Hazardous Events, which still cover all Safety Goals for the item.

In ISO 26262 it is prescribed that the HA&RA shall be done, and that there shall be performed a verification activity showing the "completeness with regard to situations and Hazards". However, there is no information how to solve the problem of showing completeness. This paper addresses this problem. The remainder of the paper is structured as follows. The next section presents the HA&RA activity of ISO 26262, and why it is considered as a hard problem to identify a limited, but still efficient set of Safety Goals. In section III is introduced the concept of formulating rules to identify which Hazardous Event that are of interest when formulating the Safety Goals. Section IV is giving a structure how to categorize all possible pairs of Hazardous Events. The following section formulates the set of rules necessary, and section VI then shows the completeness and consistency of this set. The paper ends with a summary and conclusions.

II. Background

It is well known in the area of functional safety, that the quality of the HA&RA is critical for the relevance of all other risk reducing activities prescribed by a standard. In Birch et al. [2] is discussed how the complete safety case is dependent on a proper identification of the Safety Goals in the automotive domain, which in turn is dependent on the Hazardous Events. There are a number of techniques in this area which have in common that they address how to avoid missing any candidate Hazard. Often mentioned are Preliminary Hazard Analysis, HAZOP and FMEA. Other recommendations exist like a generic method by Jesty et al. [3] based on a state machine model of the transitions between a failure occurring in a system and a Hazardous Event.

In the following we are addressing specifically the HA&RA as specified for the automotive domain. Even though there are many similarities, there are also a number of fundamental differences between the industrial domains, as is pointed out in a comparative study by Blanquart et al. [4]. Section 7 of [1] prescribes in detail how an HA&RA shall be done according

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

Rolf Johansson is with SP Technical Research Institute of Sweden (e-mail: rolf.johansson@sp.se).

to ISO 26262. In principle it consists of the following activities:

- Identify all relevant Situations
- Identify all relevant Hazards
- Combine Situations and Hazards to Hazardous Events
- Perform classification of Hazardous Events
- Identify Safety Goals covering all Hazardous Events
- Verify completeness and consistency

The end result of the HA&RA is a set of Safety Goals, each having an ASIL attribute that is limiting the occurrence of a certain Hazard. One Safety Goal may cover several different Hazardous Events, which implies that it gets the highest ASIL value among those. For each Hazardous Event, the ASIL attribute is calculated by determining a factor for each of: severity (S), exposure (E) and controllability (C). For each given Hazardous Event these factors may be determined by application experts, and may include driver controllability experiments, field data collection, etc. The problem of how to determine ASIL attribute of a given Hazardous Event is not addressed in this paper. Here is rather the focus how to find a list of Hazardous Events for which it is worth getting high confidence in the E, S and C factors.

As said above, in the automotive E/E domain, the HA&RA problem is explicitly decomposed into finding the Situations and the Hazards, and analysing all resulting effects. When performing this work, different organizations have different templates for identification of the Hazardous Events of concern. A frequent pattern is to separate the driving conditions from the environmental conditions. The former is focused on the state and the intended manoeuvres of the vehicle (driving at 70km/h, full braking, etc), and the latter describes the state outside the vehicle (dark, wet road, playing child on the road etc). There are initiatives to formalize the potentially infinite number of Situations. In Jang et al. [5] the authors present a template where they decompose the Situation into properties for vehicle, road and environment. For each of these they propose a number of properties to determine, each with some standard alternatives. Even in this rather simplistic template, the number of possible alternatives for each situation is about 50 millions. Then are still not the different possible Hazards considered. Multiplying the number of possible Hazards for a given Item, with 50 million would generate a prohibitively long list of possible Hazardous Events. This is not what the authors propose, but this shows that even if there is a standardized set of Situations and/or of Hazards, there will be a need for techniques to identify which Hazardous Events that are important for identification of the Safety Goals.

The German automotive organization VDA has created a standardized list of situations [6]. The aim of this list is to harmonize the determination of the exposure factor between vehicle OEMs when performing the HA&RA.

Martin et al [7] presents a study where the original list of Hazardous Events consists of 640 candidates. This list was reduced by checking the 'plausibility of the combinations' into 121 Hazardous Events. After this reduction, they started the classification and ASIL determination. This presented example is far from unique in the number of Hazardous Events to consider, and still it might be the case that this HA&RA is not detailed enough to allow a precise (not too conservative) formulation of Safety Goals. This is why this paper addresses the task of enabling of automatic reduction of a potentially infinite list of Hazardous Events.

As pointed out in [8] it becomes even more important to find a carefully chosen set of Safety Goals when introducing vehicles capable of highly automatic driving (HAD) or even autonomous vehicles. The implications of many such 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. This also motivates why it is important to identify rules assisting in formulating an efficient set of Safety Goals.

III. Rules for Identification of Dominance and Non-Dominance

There are a number of cases when adding a new Hazardous Event would not extend the list of already identified Safety Goals. Such Hazardous Events are of no interest, as the objective of the list of Hazardous Events, is to identify the list of Safety Goals. It would be beneficiary to have a set of rules that automatically can check whether a given candidate Hazardous Event would generate a new Safety Goal, or if it can be considered as redundant. We call such rules Dominance rules, as they identify if one Hazardous Event can be identified as dominated by other already identified Hazardous Events. Obviously we want to reduce a given list of Hazardous Events so that all the dominated ones are omitted from the final list.

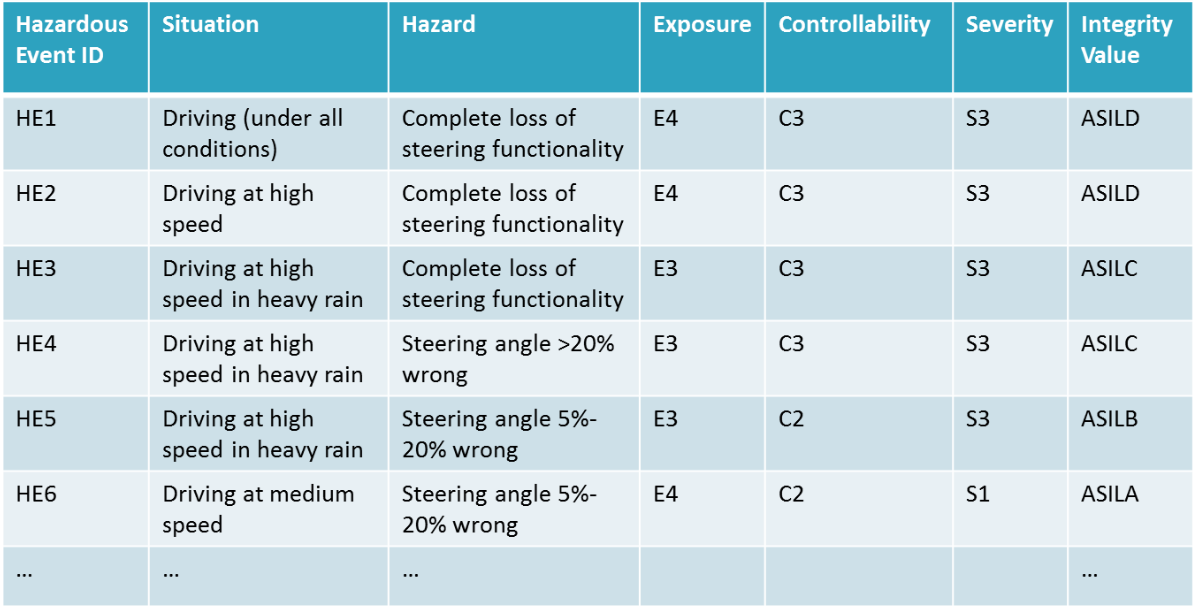
In a similar way it would be efficient to have a set of rules that could clearly identify if a Hazardous Event will generate a unique Safety Goal that is not covered by any other Safety Goal. We call such rules Non-Dominance rules, as they identify Hazardous Events that cannot be identified as dominated by any other already formulated Hazardous Event.

In this paper we identify eight explicit rules that together cover all cases for determining dominance and non-dominance, respectively. These rules can be used in at least two ways. The first use case is to review a list of candidate Hazardous Events, and remove all of these that can be shown as dominated by any of the others. For the remaining Hazardous Events, it is then possible to show that they pairwise show non-dominance. The second use case is to review a list of Hazardous Events with respect to its completeness. This means that rules for non-dominance are used to identify candidates missing in the list.

IV. Categorizing Hazards and Situations

Today, different organizations have a little bit of difference in their methodology how to list the Hazardous Events and how to perform the resulting analysis. For the following

Table 1. Example extract of a Hazardous Event table



Hazardous Event ID	Situation	Hazard	Exposure	Controllability	Severity	Integrity Value
HE1	Driving (under all conditions)	Complete loss of steering functionality	E4	C3	S3	ASILD
HE2	Driving at high speed	Complete loss of steering functionality	E4	C3	S3	ASILD
HE3	Driving at high speed in heavy rain	Complete loss of steering functionality	E3	C3	S3	ASILC
HE4	Driving at high speed in heavy rain	Steering angle >20% wrong	E3	C3	S3	ASILC
HE5	Driving at high speed in heavy rain	Steering angle 5%-20% wrong	E3	C2	S3	ASILB
HE6	Driving at medium speed	Steering angle 5%-20% wrong	E4	C2	S1	ASILA
…	…	…				…

discussion, it is not necessary to include so many columns in the table that often are used.

In the following, we will use an example Item that we call Lane Keeping Assistance in Steering (LKA Steering). Once activated, this functionality takes the responsibility for the vehicle to stay in lane. Unless overridden by the driver, the LKA controls the steering of the vehicle. In the Table 1 is depicted a set of example Hazardous Events for the chosen example.

Even in this simplified example, it is not obvious if the part of the list of Hazardous Events (HE) in Table 1 is long enough to generate the identification of all Safety Goals, or if some of the HE are not contributing at all to the analysis. Let us first have a look on the effect of the different classification factors: Exposure (E), Controllability (C), and Severity (S). When setting up a detailed list of HE, it is of interest to identify the situations which constitute a border between two different values for at least one of the factors E, C or S. In our example this means that we shall identify the sizes of the steering angle failure, and the Situations, where (at least) one of the factors changes from one level to another. In the next section we look a little deeper in the question how these columns relate to each other.

A. Analysis of Exposure, Controllability and Severity

The Exposure factor is a direct function of the Situation, and independent of the Hazard. The definition of the E factor is that it categorizes how often a vehicle is in a given situation. If the situation is very general, the E factor will be higher than if we confine the situation. For example, comparing the HE2 and HE3 in Table 1, they only differ in how specific the situation is defined. For the more general situation of HE2 we argue that the factor should become E4, while the confinement made in HE3 implies a lowering of the E factor to E3. This lowering in turn implies a lowering of the resulting ASIL attribute. The HE2 is the more conservative case to consider. This means that it is a valid classification, but it might become too restrictive if there is no situation other than those in HE3 that will have the same effect on Controllability and Severity for the given Hazard.

The Controllability factor is a function of not only the situation, but also of the Hazard and the Severity. The interpretation of the C factor would be expressed as: "How easy is to avoid the specified Severity in this Situation given this Hazard". In our example (comparing HE4 and HE5) we say that there is a limit when the steering angle suddenly becomes 20% wrong, for the driver being able to avoid an S3 accident, when driving at high speed in heavy rain. For an error of more than 20% we consider it a C3, while staying in the interval between 5% and 20%, it will be lowered to a C2. As before, it is not the point of this example to be fully correct, but to illustrate the principles.

The Severity factor is also a function of all: the Situation, the Hazard and the Controllability. This means that the S and C factors respectively are mutually dependent on their interpretation for a given Hazardous Event. The interpretation of the S factor would be interpreted as "What might be the Severity given the specified C-factor in this situation given this Hazard". In our example list of Hazardous Events, there is a limit when we compare HE5 and HE6. The difference between these two cases is that the Severity is reduced when lowering the speed to medium.

When looking at all three of these factors, we conclude that Severity and Controllability are dependent and should be interpreted in any actual pair. It makes sense to interpret the Controllability factor as how easy it is to avoid a given Severity.

We conclude that when looking for the dimensioning Hazardous Events, it would be of interest to find those Situations and Hazards where any of the three factors E, C or S will change its value. The reason for this is that any such case also will imply a change in the ASIL attribute value. We conclude that there is no meaning of having two Hazardous Event candidates that only differs a little bit in the definition of the situation, if this will not imply any change of any of the E, C, or S factors.

The question is whether all changes of Situations implying a change in any of the E, C, or S factors are relevant to consider, and what set of Hazards to take into account. This question is further elaborated in the following sections.

B. *Categorizing Situations*

When comparing two Situations, this means that both the driving scenarios and the environmental conditions are considered. When saying that two Situations are identical, this implies identity for everything specifying a Situation. One Situation can be seen as a special case of another. In our example, the Situation of HE1 (driving, under all conditions) can be seen as a general Situation of which the Situation of HE2 (driving at high speed) is a special case. Two Situations can also be seen as mutual exclusive. The Situations 'driving at high speed' (HE2) and 'driving at medium speed' (HE7), can never include any common scenario. Finally two Situations can be over-lapping. This implies that some special Situations only may occur according to one of the Situations, some only to the other, and some to both. These four possible relations are depicted in figure 1.

.

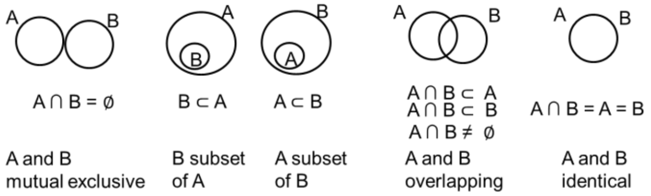


Fig. 1. Categorizing relations between two Situations A and B

To clarify the subset relation we can formulate two implications:

$A \subset B$ ⇨Any possible situation in A will also be a possible situation in B.

$A \subset B$ ⇨Guaranteeing the absence of any situation in B, will also guarantee the absence of that situation in A.

For our example we can list the following Situations:

A: Driving (under all conditions)
B: Driving at high speed
C: Driving in heavy rain
D: Driving at high speed in heavy rain
E: Driving at low speed on dry road

Then we can derive the following pairwise relations:

$B \subset A$; $C \subset A$; $B \cap C \neq \emptyset$ (overlapping); $D \subset B$; $D \subset C$; $D \cap E = \emptyset$ (mutual exclusive)

Testing the conclusions as above, on some of these relations, we get:

$D \subset C$ ⇨ Any Situation that may be characterized as 'Driving at high speed in heavy rain' may also be characterized as 'Driving in heavy rain'.

$D \subset C$ ⇨ Guaranteeing the absence of any Situation that may be characterized as 'Driving in heavy rain' will imply the absence of any Situation possible to characterize as 'Driving at high speed in heavy rain'.

$B \subset A$ ⇨ Any Situation that may be characterized as 'Driving at high speed' may also be characterized as 'Driving'.

$B \subset A$ ⇨ Guaranteeing the absence of any Situation that may be characterized as 'Driving' will imply the absence of any Situation possible to characterize as 'Driving at high speed'.

This is in line with our intuitive understanding of these relations. The relations of these five example Situations can be depicted as either a Venn diagram or as partially ordered relations shown in the figure 2 below.

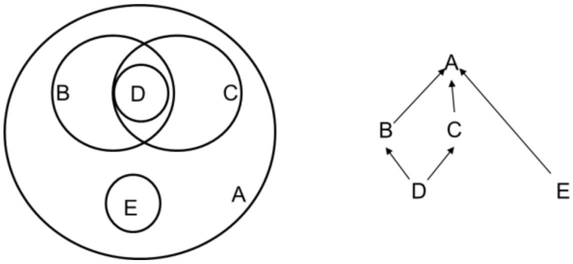


Fig. 2. Relations between example Situations

C. *Categorizing Hazards*

In a similar way as for the possible Situations, we can also categorize the possible relations between any two Hazards. Naming the two Hazards X and Y, respectively, the possible relations are as depicted in figure 3.

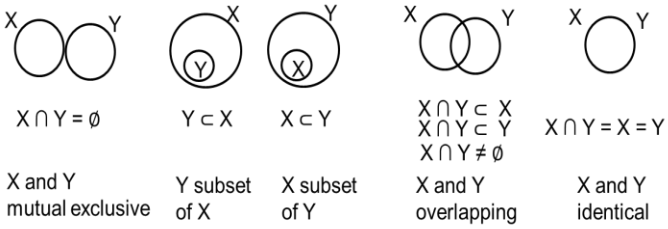


Fig. 3. Categorizing relations between two Hazards X and Y

To clarify the subset relation we can formulate two conclusions:

$X \subset Y$ ⇨ Any possible Hazard in X will also be a possible Hazard in Y.

$X \subset Y$ ⇨ Guaranteeing the absence of any Hazard in Y, will also guarantee the absence of that Hazard in X.

For our example we can list the following Hazards:

X: complete loss of steering functionality
Y: steering angle delayed too late >0.5 s

Z: steering angle more than 20% wrong
V: steering angle more than 5% wrong
U: steering angle between 5% and 20% wrong
W: any loss of steering functionality

Then we can derive the following pairwise relations:

$X \subset Y$; $X \subset Z$; $X \subset V$; $X \subset W$; $U \cap Z = \emptyset$ (mutual exclusive); $Y \cap Z \neq \emptyset$ (overlapping); $U \subset V$; $Z \subset V$; $V \subset W$; $Y \subset W$; $U \subset W$; $Z \subset W$

Testing the conclusions as above, on some of these relations, we get:

$X \subset V$ ⇨ Any Hazard that is characterized as ‘Complete loss of steering functionality’ could also be characterized as ‘Steering angle more than 5% wrong’.

$X \subset V$ ⇨ Guaranteeing the absence of any Hazard that is characterized as ‘Steering angle more than 5 % wrong’ will also imply the absence of any Hazard possible to characterized as ‘Complete loss of steering functionality’.

$Z \subset W$ ⇨ Any Hazard that is characterized as ‘Steering angle more than 20% wrong’ could also be characterized as ‘any loss of steering functionality.

$Z \subset W$ ⇨ Guaranteeing the absence of any Hazard that is characterized as ‘Any loss of steering functionality’ will also imply the absence of any Hazard possible to be characterized as ‘Steering angle more than 20% wrong’.

If the difference between the two Hazards X and W, was not completely clear before, these clarifications have hopefully made the semantics of any of the Hazards in the list above clearer. The relations of these six example Hazards can be depicted as either a Venn diagram or as partially ordered relations shown in the figure 4 below.

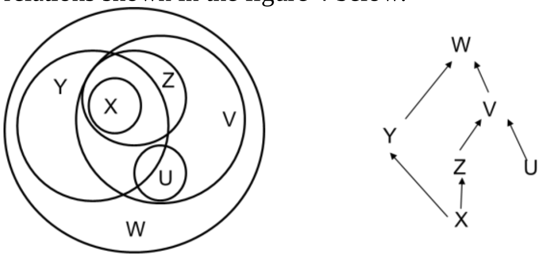


Fig. 4. Relations between example Hazards

D. *Categorizing the Effects on the E, C and S Factors*

In the previous sections we have categorized the relation between two Hazardous Events by first looking at the Situation column and then at the Hazard column. The remaining columns necessary to categorize are the ones for Exposure, Severity, Controllability, and the concluded ASIL value. As pointed out earlier, the important thing when comparing two HE, is the resulting ASIL value. Any difference in the E, C or S factors will imply a difference in the resulting ASIL value. The E, C, S factors are still important to list in the HE tables because they give guidance to the classification of the Situations and the Hazards. When choosing how confined/general a certain Situation or a certain Hazard should be expressed, the ideal cases would be those that result in differences in any of the E,C or S factors.

Once a Hazardous Event is formulated, for the purpose of determining dominance, it is sufficient to only consider the resulting ASIL value. The relation between ASIL values is easier to categorize than the relation between Situations or between Hazards. In fact there are three possible relations. Either the two HE have identical ASIL values, or the one is higher or the other is higher. The symbols =, > and < are used for this in the following sections of this paper.

V. Rules for Reducing Candidates of Hazardous Events

In the following we use the notation as of the table 2 below when discussing the relation between Hazardous Events in a table. For the rules defined in the coming sections we compare the two general Hazardous Events HE1 and HE2. HE1 has the general Situation A, the Hazard X, and gets the concluded ASIL attribute value ASIL1, when analysing the resulting effects on Exposure, Controllability and Severity. For HE2 the Situation is denoted B, the Hazard Y, and the resulting ASIL value ASIL2.

Table 2. General notation in Hazardous Event table used in formulation of rules

Hazardous Event ID	Situation	Hazard	Integrity Value
HE1	‘A’	‘X’	‘ASIL1’
HE2	‘B’	‘Y’	‘ASIL2’
HE3	‘C’	‘Z’	‘ASIL3’
…	…	…	…

A. *Rules for Identification of Dominance*

There are a number of cases when adding a new Hazardous Event would not contribute to the list of already identified Safety Goals. Such Hazardous Events are of no interest, when the objective of the list of Hazardous Events is to identify the list of Safety Goals. A first obvious example is when the candidate HE has exactly the same Situation and the same Hazard as an already listed HE, but a lower ASIL value. The same applies if it is only a difference in Situation or a difference in Hazard, and the other two columns are identical. In all these cases we can directly conclude that the candidate HE will not add any Safety Goal compared to the ones already identified. Thus, we can formulate our first rule of dominance:

Rule DI: Dominance exists if two columns show relation ’identical’ and the third one has the relation ’⊂’ or ‘<‘.

Our next observation is that for a given Hazard, there will only become one resulting Safety Goal (this is how Safety Goals are identified). Thus if two Hazardous Events have the same Hazard, but different ASIL values, the one with the lowest ASIL value does not add anything to the analysis. This leads us to the second rule of dominance:

Rule DII: Dominance exists if Hazard show relation ’identical’ and the Integrity values are different (regardless of relation for Situation).

In a next step, we can conclude three more observations possible to aggregate into one rule. 1) A more general Situation with a higher ASIL value will dominate as long as the Hazard relation is identity. 2) A more general Hazard with a higher ASIL will dominate as long as the Situation relation not implies a subset relation in the opposite direction. 3) When both Situation and Hazard are more general, this will cause dominance if the ASIL value is not lower. We aggregate these observations into our third rule of dominance:

Rule DIII: If two or more columns have the relation ’⊂’ or ‘<‘, there is dominance if they are all in the same direction, given that the column Hazard does not have the relation ‘mutual exclusive’ or ‘overlapping’.

Finally, we have the case when the one Hazard is a special case of the other (a subset), and the more confined Hazard also has a lower ASIL value. In this case, the more general Hazard with the higher ASIL value will generate the dimensioning Safety Goal, and the other Hazardous Event will not add anything to the analysis. This will always hold, independent of how general the Situations are defined. This leads to the fourth and last rule of dominance:

Rule DIV: Dominance exists if Hazard has ’⊂’ relation in the same direction as the Integrity value has the ‘<‘ relation, regardless of the Situation relation.

For now we say that these are the only four rules of dominance needed to categorize all possible cases where one Hazardous Event can be seen as dominated by another. In a section VI, there is a proof that no other rules are needed, i.e. these four rules of dominance are complete. Before this, the rules for non-dominance are identified.

B. Rules for Identification of Non-Dominance

In the previous section we identified the rules identifying when one Hazardous Event makes another one unnecessary, i.e. when the other does not imply a unique Safety Goal. In order to determine the relation between any two Hazardous Events, it is as important to conclude when they both contribute to unique Safety Goals.

Our first observation regarding such so called non-dominance, is when we are comparing two mutual exclusive Hazards or two overlapping Hazards. As long as both Hazardous Events are based on a Hazard which is (partly) unique, this will also imply that it will contribute to a unique Safety Goal. We can hence formulate our first rule of non-dominance:

Rule NI: There is never dominance between two mutual exclusive Hazards or between two overlapping Hazards.

Next observation is that a more specific Hazard having a higher ASIL attribute than the general Hazard will add a new Safety Goal, but the first Safety Goal will still stay unique. For example, we can have one Safety Goal stating that we shall avoid steering angle failures above 20% by ASILD, and another one stating that we shall avoid steering angle failures above 5% by ASILC. The first one is more restrictive regarding the ASIL value, while the second is more restrictive regarding the threshold above which a deviation is considered as a failure. This means that no one of these two Safety Goals includes the other one, and they are hence both to be considered as unique. This leads us to the formulation of our second rule of non-dominance:

Rule NII: If the Hazard and Integrity relations are in different directions, there is never dominance.

Furthermore, we can observe that even if the Integrity value is identical for a pair of Hazardous Events, they will still both contribute to unique Safety Goals if either of Situation or Hazard cannot be seen as a subset of the other one. If either of the Situation or the Hazard relations, are mutual exclusive or overlapping, this implies that we cannot say that the Safety Goal derived from the one HE will include the Safety Goal derived by the other. This leads us to the formulation of the third rule of non-dominance:

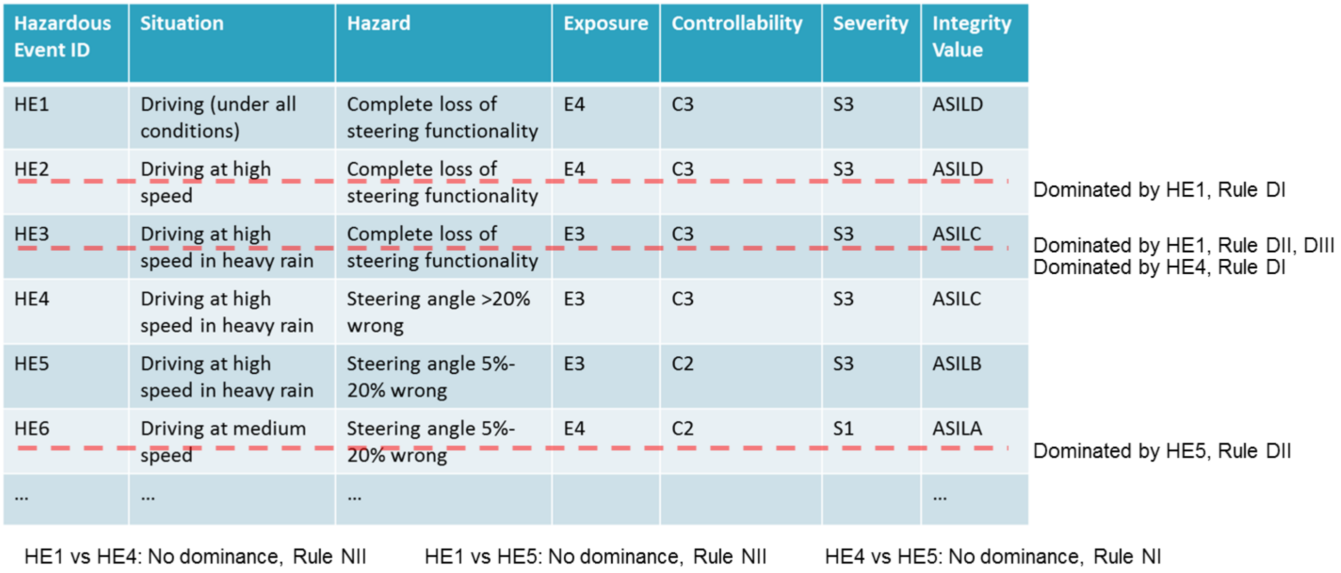
Rule NIII: There is never dominance if Integrity value relation is 'identical', and any of the other two relations are either 'mutual exclusive' or 'overlapping’.

Finally, we conclude that even if the Integrity relation between two Hazardous Events is ‘identical’, this will still imply two unique Safety Goals if the relations for Situation and Hazard both have a subset relation, but in different directions. This leads us to the conclusion of the fourth rule of non-dominance:

Rule NIV: There is no dominance if Integrity value relation is 'identical', and the other two relations are in different directions.

We have now formulated 4+4 rules to determine whether any pair of Hazardous Events will generate one or two Safety Goals. In the former case we call that dominance, and in the latter case non-dominance. In the next section we investigate to what extent these eight rules are complete and consistent. We want that all possible pairs of Hazardous Events are handled by at least one rule, and that there will never be any conflicting rules for any pair of Hazardous Events.

Table 3. Example extract of a Hazardous Event table, revisited



Hazardous Event ID	Situation	Hazard	Exposure	Controllability	Severity	Integrity Value	
HE1	Driving (under all conditions)	Complete loss of steering functionality	E4	C3	S3	ASILD	
~~HE2~~	~~Driving at high~~ speed	~~Complete loss of~~ steering functionality	~~E4~~	~~C3~~	~~S3~~	~~ASILD~~	Dominated by HE1, Rule DI
~~HE3~~	~~Driving at high~~ speed in heavy rain	~~Complete loss of~~ steering functionality	~~E3~~	~~C3~~	~~S3~~	~~ASILC~~	Dominated by HE1, Rule DII, DIII Dominated by HE4, Rule DI
HE4	Driving at high speed in heavy rain	Steering angle >20% wrong	E3	C3	S3	ASILC	
HE5	Driving at high speed in heavy rain	Steering angle 5%-20% wrong	E3	C2	S3	ASILB	
~~HE6~~	~~Driving at medium speed~~	~~Steering angle 5%-20% wrong~~	~~E4~~	~~C2~~	~~S1~~	~~ASILA~~	Dominated by HE5, Rule DII
…	…	…				…	

HE1 vs HE4: No dominance, Rule NII HE1 vs HE5: No dominance, Rule NII HE4 vs HE5: No dominance, Rule NI

VI. Completeness and Consistency of the Rules

In the previous chapter we categorize any pair of Hazardous Events as the combined effect of the relations for Situation, Hazard and ASIL value, respectively. For the Situation and the Hazard relations, there are five different possibilities each: Identical, Mutual exclusive, overlapping, and a subset relation in any of the two directions. For the ASIL value relation, there are three possibilities: Identical, and the one is higher or the other is higher. In total this implies 5*5*3=75 different possibilities to categorize the relation between any pair of Hazardous Events. Below in table 4, there is an extensive list of all these 75 possibilities, and for each is also noted what rules for dominance and for non-dominance that apply.

The first row in this table is about when the two Hazardous Events are identical, and thus no comparison is motivated. For the remaining 74 rows there is some difference between the two compared Hazardous Events. We observe that for every row in this list, there is at least one rule that is found applicable. Furthermore we observe that there is no row where there is one rule for dominance and another for non-dominance at the same time. The fact that all rows are covered by at least one rule, and that there is no row showing any contradicting rules, implies that our set of 4+4 rules is complete and consistent.

VII. Discussion

Our eight rules for determining dominance or non-dominance can be used in at least two ways. The first use case is to review a list of candidate Hazardous Events, and remove all of these that can be shown as dominated by any of the others. For the remaining Hazardous Events, it is then possible to show that they pairwise show non-dominance. The second use case is to review a list of Hazardous Events with respect to its completeness. This means that rules for non-dominance are used to identify candidates missing in the list. Let us go back to our example with LKA steering list of Hazardous Events from Table 1. As shown in the Table 3 we can now conclude that neither of the candidates HE2, HE3, and HE6 will conclude to the identification of a unique Safety Goal. Furthermore, we can also make sure that the remaining Hazardous Events, all contribute to a unique Safety Goal.

We can then continue our review by challenging this list by trying to add more Hazardous Events. However, we only add those candidates that are shown not to become dominated by one of the existing ones. We might come up with a new candidate that dominates one of the HE already in list, which implies that the new one will replace the dominated one.

In our example we can now consider all combinations of Situations and Hazards to find out whether any of these would generate a dimensioning Hazardous Event. Given that we have chosen these Situations and Hazards, respectively, and that they catch the cases when any of the E, C or S factors can change its value, we can argue for the completeness of the concluded list of Hazardous Events. Our rules give a hint which potential Hazardous Events to consider, which means that we can find arguments for a number of Hazardous Events at the time, why not to consider any of them (as they would be dominated by an existing Hazardous Event).

For example, given that we have HE1 in our list above, we can directly conclude that we do not need to look for any other Situation to combine with this Hazard, as they would all be dominated. The argument for this conclusion is that HE1 will not have a lower ASIL than any other HE, and also that no other Situation could be seen as a superset to the Situation of HE1. We can formulate it by saying that comparing HE1: <A,X,ASIL1> with any other HEk: <B,X,ASIL2> (the same Hazard), HEk will always be dominated by HE1. The argument for this is that ASIL2 is not greater than ASIL1 (ASIL1=ASILD), and B is always a subset of A (A is the most general situation). This means that either ASIL2=ASILD and then rule DI is applicable, or ASIL2 has a lower value and then rule DII is applicable. In a similar way as in the example above, a number of candidate Hazardous Events can in many situations be evaluated simultaneously.

Table 4. Investigation of all possible pairs of HE

Situation	Hazard	Integrity	Dominance	Rule(s)
Identical	Identical	Identical	–	Identity
Identical	Identical	ASIL1	HE2	Rule DI. DII
Identical	Identical	ASIL2	HE1	Rule DI. DII
Identical	Mutual	Identical	No Dominance	Rule N1. NII
Identical	Mutual	ASIL1	No dominance	Rule NI
Identical	Mutual	ASIL2	No dominance	Rule NI
Identical	X subset of Y	Identical	HE2 dominates	Rule DI
Identical	X subset of Y	ASIL1	HE2 dominates	Rule DIII.
Identical	X subset of Y	ASIL2	No dominance	Rule NII
Identical	Y subset of X	Identical	HE1 dominates	Rule DI
Identical	Y subset of X	ASIL1	No dominance	Rule NII
Identical	Y subset of X	ASIL2	HE1 dominates	Rule DIII.
Identical	Overlapping	Identical	No dominance	Rule NI. NIII
Identical	Overlapping	ASIL1	No dominance	Rule NI
Identical	Overlapping	ASIL2	No dominance	Rule NI
Mutual	Identical	Identical	No dominance	Rule NIII
Mutual	Identical	ASIL1	HE2 dominates	Rule DII
Mutual	Identical	ASIL2	HE1 dominates	Rule DII
Mutual	Mutual	Identical	No dominance	Rule NI. NIII
Mutual	Mutual	ASIL1	No dominance	Rule NI
Mutual	Mutual	ASIL2	No dominance	Rule NI
Mutual	X subset of Y	Identical	No dominance	Rule NIII
Mutual	X subset of Y	ASIL1	HE2 dominates	Rule DIII.
Mutual	X subset of Y	ASIL2	No dominance	Rule NII
Mutual	Y subset of X	Identical	No dominance	Rule NIII
Mutual	Y subset of X	ASIL1	No dominance	Rule NII
Mutual	Y subset of X	ASIL2	HE1 dominates	Rule DIII.
Mutual	Overlapping	Identical	No dominance	Rule NI. NIII
Mutual	Overlapping	ASIL1	No dominance	Rule NI
Mutual	Overlapping	ASIL2	No dominance	Rule NI
A subset of B	Identical	Identical	HE2 dominates	Rule DI
A subset of B	Identical	ASIL1	HE2 dominates	Rule DII
A subset of B	Identical	ASIL2	HE1 dominates	Rule DII
A subset of B	Mutual	Identical	No dominance	Rule NI. NIII
A subset of B	Mutual	ASIL1	No dominance	Rule NI
A subset of B	Mutual	ASIL2	No dominance	Rule NI
A subset of B	X subset of Y	Identical	HE2 dominates	Rule DIII
A subset of B	X subset of Y	ASIL1	HE2 dominates	Rule DIII.
A subset of B	X subset of Y	ASIL2	No dominance	Rule NII
A subset of B	Y subset of X	Identical	No dominance	Rule NIV
A subset of B	Y subset of X	ASIL1	No dominance	Rule NII
A subset of B	Y subset of X	ASIL2	HE1 dominates	Rule DIV
A subset of B	Overlapping	Identical	No dominance	Rule NI. NIII
A subset of B	Overlapping	ASIL1	No dominance	Rule NI
A subset of B	Overlapping	ASIL2	No dominance	Rule NI
B subset of A	Identical	Identical	HE1 dominates	Rule DI
B subset of A	Identical	ASIL1	HE2 dominates	Rule DII
B subset of A	Identical	ASIL2	HE1 dominates	Rule DII
B subset of A	Mutual	Identical	No dominance	Rule NI. NIII
B subset of A	Mutual	ASIL1	No dominance	Rule NI
B subset of A	Mutual	ASIL2	No dominance	Rule NI
B subset of A	X subset of Y	Identical	No dominance	Rule NIV
B subset of A	X subset of Y	ASIL1	HE2 dominates	Rule DIV
B subset of A	X subset of Y	ASIL2	No dominance	Rule NII
B subset of A	Y subset of X	Identical	HE1 dominates	Rule DIII
B subset of A	Y subset of X	ASIL1	No dominance	Rule NII
B subset of A	Y subset of X	ASIL2	HE1 dominates	Rule DIII.
B subset of A	Overlapping	Identical	No dominance	Rule NI. NIII
B subset of A	Overlapping	ASIL1	No dominance	Rule NI
B subset of A	Overlapping	ASIL2	No dominance	Rule NI
Overlapping	Identical	Identical	No dominance	Rule NIII
Overlapping	Identical	ASIL1	HE2 dominates	Rule DII
Overlapping	Identical	ASIL2	HE1 dominates	Rule DII
Overlapping	Mutual	Identical	No dominance	Rule NI. NIII
Overlapping	Mutual	ASIL1	No dominance	Rule NI
Overlapping	Mutual	ASIL2	No dominance	Rule NI
Overlapping	X subset of Y	Identical	No dominance	Rule NIII
Overlapping	X subset of Y	ASIL1	HE2 dominates	Rule DIII.
Overlapping	X subset of Y	ASIL2	No dominance	Rule NII
Overlapping	Y subset of X	Identical	No dominance	Rule NIII
Overlapping	Y subset of X	ASIL1	No dominance	Rule NII
Overlapping	Y subset of X	ASIL2	HE1 dominates	Rule DIII.
Overlapping	Overlapping	Identical	No dominance	Rule NI. NIII
Overlapping	Overlapping	ASIL1	No dominance	Rule NI
Overlapping	Overlapping	ASIL2	No dominance	Rule NI

VIII. Conclusion

We have defined eight rules to be used for the identification of a minimal set of Hazardous Events necessary to identify all Safety Goals of an Item. The rules are used to compare any two candidates of Hazardous Events to conclude whether they are both generating a unique Safety Goal, or whether the one Hazardous Event can be seen as uninteresting (dominated by the other).

The rules are based on a categorization of the Situations, the Hazards and the ASIL attribute values, respectively. Regarding the ASIL attribute values, the integrity levels are either equal, or one of them is higher than the other. For both Situations and for Hazards, we use set theory to describe any pairwise relation. We show that our eight rules are complete and consistent. The completeness is shown as any possible combination of relations between Situations, Hazards, and ASIL attribute value, is covered by at least one rule. Consistency is shown as none of these possible combinations implies both dominance and non-dominance. This means that any combination is uniquely identified as either dominance or non-dominance.

This set of rules makes it possible to solve the paradox of being specific in the list of Situations and Hazards, and still end up with a limited number of dimensioning Hazardous Events. Today, many companies fear to be too detailed in the Hazard Analysis, as it might generate a potentially infinite number of Hazardous Events. Instead they run the risk of becoming unnecessarily conservative in the analysis, leading to a too expensive product. By applying a methodology where these eight rules are applied in the generation and the review of Hazardous Events, it is feasible to generate a list that is at the same time complete and precise.

References

[1] ISO, 26262-3:2011, Road vehicles — Functional safety — Part 3, Concept phase, 2011.

[2] Birch, J., Rivett, R., Habli, I., Bradshaw, B., Botham, J., Higham, D., Jesty, P., Monkhouse, H., Palin, R., "Safety Cases and their role in ISO 26262 Functional safety Assessment", SAFECOMP, Toulouse, 2013.

[3] Jesty, P.H., Ward, D.D., Rivett, R.S., ""Hazard Analysis for programmable automotive Systems", Proceddings of 2nd International Conference on system Safety, IET, 2007.

[4] Blanquart, J-P, Astruc, J-M, Baufreton, P., Boulanger, J-L., Delseny, H., Gassino, j., Ladier, G., Ledinot, E., Leeman, M., Machrouh, J., Quere, P., Ricque, B., "Criticality categories across safety standards in different domains", ERTS2 congress on embedded real time system and software, Toulouse, 2012.

[5] 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.

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

[7] 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.

[8] Johansson, R, "The Importance of Active Choices in Hazard Analysis and Risk Assessment", CARS 2015 - Critical Automotive applications: Robustness & Safety, 2015.