Safety Argument Strategies for Autonomous Vehicles

Andrzej Wardziński

Gdansk University of Technology, Department of Software Engineering
Narutowicza 11/12, 80-952 Gdansk, Poland
andrzej.wardzinski@eti.pg.gda.pl

Abstract. Assuring safety of autonomous vehicles requires that the vehicle control system can perceive the situation in the environment and react to actions of other entities. One approach to vehicle safety assurance is based on the assumption that hazardous sequences of events should be identified during hazard analysis and then some means of hazard avoidance and mitigation, like barriers, should be designed and implemented. Another approach is to design a system which is able to dynamically examine the risk associated with possible actions and then select the safest action to carry it out. Dynamic risk assessment requires maintaining the situation awareness and prediction of possible future situations. We analyse how these two approaches can be applied for autonomous vehicles and what strategies can be used for safety argumentation.

1. Introduction

Nowadays we can notice a tendency towards designing systems which are more and more autonomous. In some countries we can get on autonomous buses [1]. In DARPA Urban Grand Challenge the autonomous vehicle mission was to drive 100 km in urban environment and obey traffic rules (however vehicles were not required to interpret street signs nor traffic lights) [2, 3].

Intuitively we feel that autonomous systems are not only more complex, but autonomy introduces new problems that may require quite novel approach for design and development of such systems. This raises a question how much autonomous systems differ from non-autonomous ones and whether we can apply the same approach to safety assurance. It is not certain if the existing methods and techniques would be adequate and sufficient.

Our objective is to investigate the issues of autonomy for safety-critical systems and the ways of safety assurance. In Section 2 we introduce the problem of autonomous vehicle safety and two approaches for safety assurance. The traditional approach is presented in Section 3. We discuss the structure of safety argument, advantages and disadvantages of the approach. The second approach is more complex as it uses the situation awareness model to identify safe and risky actions. The approach is discussed in Section 4. We analyse the difficulties for constructing convincing safety argument and possible types of evidence. The results are summarised in Section 5.

2. Autonomous Vehicle Safety

Autonomy is a broad concept and there are many definitions of this term and a few levels of autonomy can be identified [4, 5]. Generally autonomy relates to freedom to determine own actions and behaviour. For the needs of the paper we will assume that autonomy of a mobile system is the ability to accomplish a given mission without human intervention. That means that the system should be able to make decisions how the mission goals could be achieved and how to cope with changes in the environment and threats.

Autonomous vehicle control system should:

- plan the mission taking into account the context of the environment (for example other vehicles),
- act according to the plan to accomplish the mission,
- adapt the plan to changes in the environment,
- ensure safety (avoid collisions),
- efficiently use energy and prevent energy loss.

In the paper we will focus on safety of a single vehicle. We make no assumptions about the communication with other vehicles. Vehicles can communicate or carry out their missions without any communication. We will not refer to vehicle communication in the paper.

When we say that the vehicle should ensure safety we primarily think of avoiding collisions with other vehicles or objects. The vehicle should keep "safe" distance from other vehicles and objects. There are probably many ways of designing a system which satisfies these requirements but generally we can say that there are two approaches. The approaches differ in the way system safety is perceived and assured.

1. The first approach is based on the analysis of possible accident scenarios and designing protection mechanisms (barriers) that prevent transitions to unsafe states. The way the hazardous situations are detected and accidents are avoided is determined during hazard analysis.
2. The second approach is based on dynamic risk assessment. The vehicle control system evaluates the risk of possible actions and then selects the one that is the least risky in the context of current situation and environment conditions.

We will discuss and compare these two approaches. The description of the approaches will be somewhat simplified to show the contrast how safety can be perceived and assured. In our discussion we will focus on the rationale of the approaches and ways of demonstrating safety – what strategy can be used to argue that the system is safe.

3. The Approach Based on Predetermined Vehicle Risk Assessment

The first method to achieve autonomous vehicle safety is based on the traditional approach to hazard analysis and safety assurance. The objective is to identify event sequences leading to accidents and then design mechanisms to control the risk. System safety is usually achieved by implementation of safety barriers. The concept of a barrier explains the idea of the approach.

3.1. The Concept of a Barrier

Hollnagel [6] defines a barrier as an obstacle, an obstruction or a hindrance that may either (a) prevent an action from being carried out or an event from taking place, or (b) thwart or lessen the impact of the consequences. There are many forms of barriers. Hollnagel classified barriers as [6]:

- *material barriers*, e.g. a fence,
- *functional barriers*, when a specific precondition is defined which has to be fulfilled before an action can be carried out,
- *symbolic barriers*, e.g. signs and signals that have to be perceived and interpreted,
- *immaterial barriers*, that is using the knowledge to follow the rules of allowed behaviour (e.g. Highway Code).

This classification shows that many different means can be used as barriers for autonomous vehicles. Usually we will combine different types of barriers to achieve more confidence in vehicle safety.

The mechanism of a barrier is intentionally simple to assure its high reliability. When a barrier is detected (we will use symbol e_1 to denote the event of barrier detection) then a specific action a_1 is to be carried out. At the moment it is not relevant whatever technology we use – barrier detection and reaction can be implemented as a mechanical, hydraulic, electric or software system. We can use safety analysis techniques like Event Trees to describe barriers (see Fig. 2).

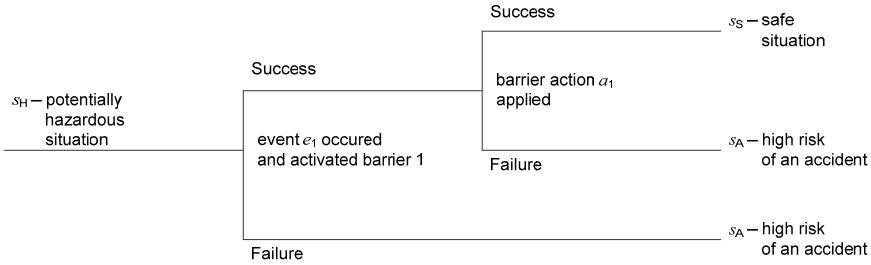

Fig. 1. Event Tree for a barrier activated when an event e_1 occurs and action a_1 defined for the barrier.

In the example presented in Fig. 1 we assume that barrier action a_1 guarantees prevention of the accident (or gives some probability of a success). Usually we assign probabilities to events and the tree branches (events outcomes) to calculate probabilities of possible scenarios.

When the system barriers are implemented as software functions we can generalize the code structure to look like this:

```
if       e1 detected  then  a1
else if  e2 detected  then  a2
…
else     other actions
```

Different events e_1, e_2, …, e_n can be defined for each barrier. The efficiency of barriers is analysed on the system level during hazard analysis and then barriers usually can be implemented and verified separately.

We call the approach the predetermined risk assessment as the risk is assessed during the hazard analysis stage of the system development. The barrier conditions and actions definitions remain unchangeable during system operation however there are possibilities for some degree of flexibility as presented in the next Section.

3.2 Examples of Barriers Use for Autonomous Vehicles

Barriers used for autonomous vehicle safety assurance can be as simple as bumper sensors or distance sensors to detect an obstacle and then stop. However barriers can be far more complex and sophisticated.

Spriggs in [7] describes an autonomous system which operates near to an airport's runaways and uses GPS coordinates to ensure operation in the allowed area only. The vehicle control system has a definition (map) of a safe designated area. GPS coordinates serve as a barrier to ensure that the vehicle will not leave the safe area.

Robertson in [3] presents kinematic motion study for a vehicle operating in an urban environment and competing in DARPA Urban Challenge [2]. The result of the study was used to define safety regions for the vehicle motion. The safety region is an area that is required to be free from other vehicles in order to continue driving. If the safety region is occupied by any vehicle the system should stop and wait until the safe region is clear. The system uses a set of sensors to calculate its position in the terrain (on the road) and positions of other vehicles and objects. This knowledge is presented as a situation awareness model and is used to plan the vehicle movement.

These two examples show that a barrier can be a complex mechanism. The characteristic of the approach is that the condition that activates a barrier is set up during the hazard analysis. The occurrence of the condition is binary – the barrier should be activated or not. We can say that this represents a binary view on safety.

The assumption of the binary view on safety is that all the risk can be avoided (or reduced according to ALARP principle) when we define a set of conditions that activate barriers (safety functions). This often leads to vast "safety margins". For example an autonomous vehicle has to stop and wait while most of human drivers would assess that it is safe to go ahead.

3.3 Safety Argument Strategy

The approach is intended to be simple and easy for verification. We expect that the safety argument structure would be relatively simple. We will discuss a simplified generic model of safety argumentation using GSN notation [8, 9]. There are many possible ways of structuring safety arguments for barriers and we have chosen a structure which emphasizes the fact that usually each barrier can be designed, implemented and verified almost independently from other barriers. The main part of such safety argument is presented in Fig. 2.

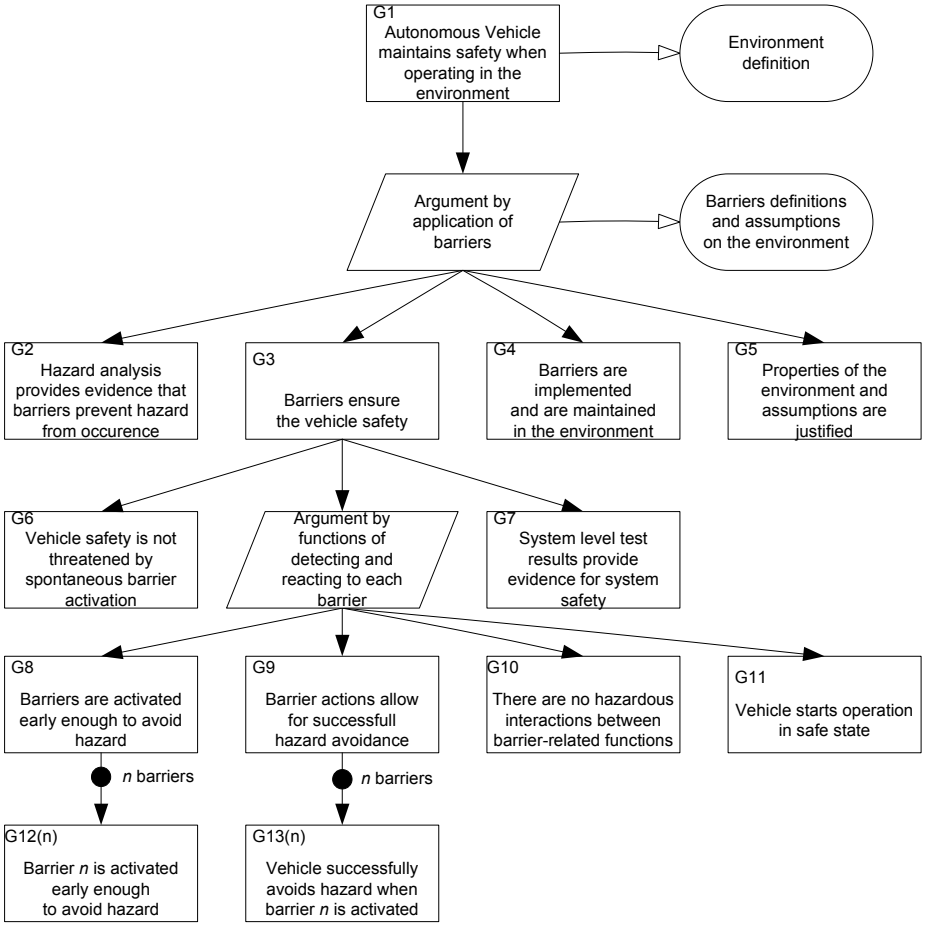

Fig. 2. General safety argument schema for barriers

There are four main claims that have to be justified in order to demonstrate system safety. The first claim (G2) relates to the system hazard analysis which should provide evidence that barriers prevent hazard occurrence. That means that the vehicle will not enter unsafe area (e.g. will avoid collision). This requires a thorough analysis of the vehicle and environment properties to create a conceptual model of the system states and possible transitions. The analysis should:

- identify safe states of the systems and hazardous states,
- identify possible accident scenarios,
- define means to prevent hazardous transitions leading to accidents (e.g. barriers),
- check barriers completeness and assess probability of hazard occurrence for conditions that do not activate barriers,
- assess probability of barrier failures and evaluate likelihood of the hazard,
- provide evidence that the analysis is complete and no relevant factors had been overlooked.

We should note that barriers form a consistent and comprehensive system in hazard analysis phase only. Claims G12 and G13 relate to each barrier separately. All the logic of system safety is built on the hazard analysis level. In the system we implement and then demonstrate each barrier function independently. The safety argument for each barrier relates to its design, implementation, tests and verification.

Only during system level tests the barrier system mechanism is validated as a whole (G7). There are also some conditions in the environment which are to be fulfilled or barriers may fail otherwise. Usually barriers need some kind of devices or equipment (e.g. GPS satellites) to be maintained in the system environment (G4). Sometimes we also need some justification for environment properties or assumptions on such properties (G5). An example of such assumption is maximum possible acceleration of other vehicles in the environment.

3.4 Summary of the Predetermined Risk Assessment Approach

The main objective of the predetermined risk assessment is to provide highly reliable, simple, manageable, efficient, economical and verifiable solution that assures the system safety goals. This works very well for non-autonomous systems. The approach can also be applied for autonomous vehicles however we should be aware of some limitations.

It is important to notice that binary safety model (division of possible states into safe ones and unsafe ones) is an abstraction of the reality aimed in making safety assurance techniques simpler, more reliable, easier to demonstrate and verify. That does not mean that in reality safety is a binary attribute. It is just a simplification that makes safety assurance process more effective.

The great advantage is that during hazard analysis we decompose the system safety problem and then analyse each barrier separately. Each barrier can be independently designed, implemented and tested. Additional work is required when barriers depend on each other. When barriers interrelationship becomes more complex the amount of work and difficulty of safety argumentation rises. If we had ten interrelated barriers we would have to analyse hundreds of combinations.

Another disadvantage of the approach is that it is not flexible and the system performance deteriorates when it is operating in an open environment as the vehicle cannot adapt its behaviour to the changes in the environment. For example a vehicle mentioned in Section 3.2 can wait for a long time until the safety region is clear. Most of human drivers would asses the safe region as too vast and would assess the vehicle behaviour as very protective. This approach is well suited for a situation of low traffic and low speed. The approach works well when there is only a limited number of vehicles and for most of the situations the safety region is clear.

There are some areas of applications for which such limitation could be a big disadvantage or even not acceptable. The approach is difficult to apply when the application domain requirements relate to:

- need for efficient space utilization, like congested road traffic;
- reactions for unexpected failures and events especially when stopping is not a proper way to ensure safety;
- driving in a terrain for which barriers are not implemented and maintained;

– competition between vehicles and situations like racing;
– military missions, escorting and guarding when the mission goals require taking some risk.

It seams that application of this approach alone to autonomous systems would make it difficult to achieve performance goals.

4. Dynamic Risk Assessment

In real world humans do not perceive safety in a binary way. We are not used to distinguish only two states: "this is not safe – I have to react to this" and "this is safe – no reaction is needed" (however we often react to some events). We are used to talk about the risk of an activity or a situation. We often say that something is more or less risky in some situations. That leads to a conclusion that situation safety should not be perceived as a binary condition but we should rather say that a situation can be characterised with a specific risk level depending on the attributes relevant to safety.

4.1 Dynamic Risk Assessment Approach

The concept of risk as an attribute of a situation is quite widely used in hazard analysis. When we analyse accident scenarios we identify situation attributes (events) as risk factors which contribute to hazard.

The idea of the risk assessment approach is to design a system which is able to perceive and interpret risk factors and then assess how far it is on the scale starting from an absolutely safe state and ending with an accident. The system should be able to assess the risk of the situation *before* carrying out a specific action. In that way the system would be able to select safe actions and avoid actions leading to hazards.

The concept of situation risk assessment for autonomous vehicles was described in [10, 11]. The general requirement for the system is to maintain *situation awareness* which allows for action planning taking into account risk level of particular actions. The concept of situation awareness is used in psychology and in robotics but it is quite new for safety-critical systems.

The general architecture of an autonomous vehicle control system using situation awareness model is presented in Fig. 3. In our analysis we will focus on the situation awareness model and *Task planning* process. The general algorithm of the *Task planning* process consists of following steps:

1. Select possible scenarios of actions to be analysed and assessed.
2. Assess each scenario for:
   – mission progress,
   – compliance with formal safety rules (e.g. Highway Code),
   – situation risk level.
3. Choose the optimal scenario (according to the vehicle strategy).
4. Communicate tasks of the chosen scenario to the Control layer.

One should note that the "rules" mentioned in point 2 can be barriers. Barriers can be used for dynamic risk assessment approach however it is only one of three factors

of the situation assessment. An example of a rule is “vehicle to the right has the right of way” when two or more vehicles approach a crossing at the same time. Another rule can be “do not drive across the pavement”. Rules often can relate to barriers.

The goal of step 3 is to select the best action to carry it out. The selection criteria depend on the vehicle strategy. The strategy can give priority to safety or mission goals depending on the mission context and current situation. For the purposes of the paper we will assume that the strategy to assure vehicle safety and safety has higher priority then mission goals.

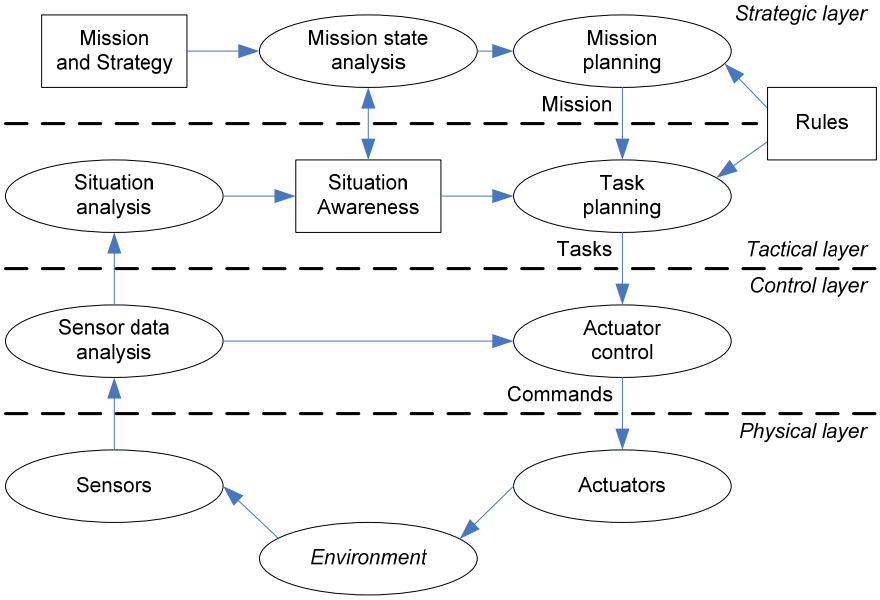

Fig. 3. Autonomous vehicle control system architecture

We assume that dynamic risk assessment would allow for:

- better system resilience and survivability in unexpected situations or in emergency;
- better performance in an open (non-controlled) environment when other entities (systems, vehicles or humans) can act independently,
- better ability to perform risky missions where some risk level has to be accepted and the system should balance between safety and mission goals,
- operation in areas where barriers are non existing or difficult to define and implement.

4.3 Safety Assurance Using Dynamic Risk Assessment

The system safety is assured by a complex mechanism of selecting the safest possible action for a given current situation. We will analyse this for the example similar to presented in Section 3.1. In Fig. 4. we have a set of hazardous situations SH and some

possible scenarios of actions presented as arrows leading to other situations. Barrier actions described in Section 3.1 are presented as transitions a_1 and a_2. The main difference in comparison to predetermined risk assessment is that the task of the vehicle control system is not to activate automatically the barrier function a, but assess the risk for each possible actions and then carry out the safest one. Depending on the specific situation it can be the action a or any other action, like action b_2 for situation s_{H2}.

The main prerequisite for the approach is situation awareness model which should provide means to distinguish situations attributes that are relevant for the system safety. The model should allow for situation perception, identification of possible actions and prediction of their results. The prediction should take into account changes in the environment and actions of other entities (vehicles).

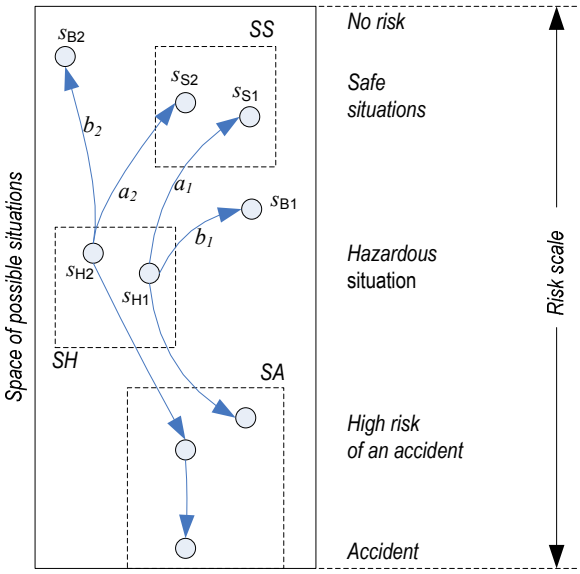

Fig. 4. Set of example situations and actions in context of the risk scale

A kinematic vehicle model forms the basis for the vehicle motion safety analysis. The model will tell us what the position of the vehicle will be when specific actions (like braking, acceleration and turning wheels) are carried out. When other vehicles operate in the same environment then the model should be extended with behaviour of other vehicles and possibly communication with them. When necessary the model should also take into account the possibility of presence of humans.

The critical function of the situation awareness model is to assess the risk of any current or predicted situation. Possible set of situations to be analysed and assessed will usually be bigger then a set of scenarios analysed for barriers (compare to Fig. 1).

For any current situation the control system will identify possible actions and assess the risk level associated with them and then select the safest one to be carried out (or other action according to the vehicle strategy). Selection of the safest action can be described as a following function using VDM-like notation:

vehicleAction(*s* : *Situation*) *as* : *ActionScenario*
post
as ∈ possibleScenarios(*s*)
∧
riskAssessment(s, *as*) =
min{ *ra* | *ra* = riskAssessment(*s*, *ax*) ∧ *ax* ∈ possibleScenarios(*s*) }

It is important to note that for a given situation s_{H1} the control system does not necessary need to activate the barrier function a_1. The objective of the approach is to create a model which can be used to identify the safest action for a given situation and the selected action can be different then action a_1 (like action b_1).

4.3 Safety Argument Strategy

Our analysis led us to the main question in this paper – how can we gain confidence that this approach will really ensure system safety and acceptably low risk of autonomous vehicle operation? Safety analysis of such systems is a subject of research and probably there are no established methods that solve the problem.

The situation awareness model plays the main role in safety assurance as the vehicle uses it to interpret the situation and to assess the risk of possible actions. The main difference in comparison with the barrier approach is the way we handle cause-consequences dependencies. In the traditional approach the model of system safety and hazardous cause-consequences dependencies is created by humans in hazard analysis phase. As a result separate safety functions for all barriers are designed and implemented. This is quite different when we intend the vehicle control system to maintain situation awareness and dynamically assess the risk. The model is to be analysed as a whole and its elements cannot be analysed in separation. Providing arguments for the system safety is more complex. A general schema of argumentation structure is presented in Fig. 5.

First we have to demonstrate that situation awareness model with dynamic risk assessment function is correct in terms of consistency with real vehicle and its operating environment and is sufficient and adequate for vehicle safety assurance (claim G2). In our analysis we have identified the main safety requirements for the situation awareness model:

1. The model should distinguish situations that are relevant for system safety (including safe, hazardous situations and accidents).
2. Attributes that are used to identify and classify situations should be possible to measure with the use of sensors or their values should be possible to be deduced from accessible information (risk factors are examples of situations attributes).
3. The model gives information what are the possible actions for current situation.
4. The model can predict and assess safety of a situation that will be the result of a given action (or action scenario). Prediction should take into account behaviour of other vehicles and events in the environment.

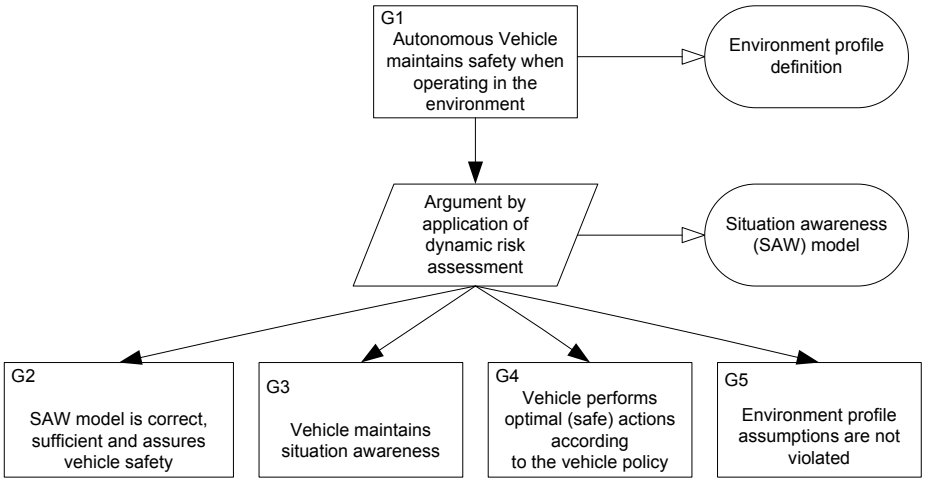

Fig. 5. Safety argument structure for dynamic risk assessment approach

5. The model should allow for representing incomplete or uncertain data, what leads to uncertain risk assessment [10]. The model should preserve safety when the risk assessment results are uncertain. The loss of situation awareness (when the control system is not able to assess the situation) is interpreted as unsafe situation.
6. Depth of prediction of future situations is sufficient to ensure avoidance of unsafe state what means that the vehicle after perceiving any dangerous situation has enough time to avoid accident.
7. The model implementation is effective within required time limits.

The satisfaction of the requirements should be verified and validated for a given vehicle and specific environment profile.

The next two claims relate to requirements that the systems should maintain the situation awareness (G3) and should use it to control the risk (G4). Claim G3 relates to processes that provide situation awareness information: *sensor reading*, *sensor data analysis* and *situation analysis* processes in system architecture presented in Fig. 3. The processes should provide reliable and up-to-date information to maintain the situation awareness. The next claim (G4) is related to the use of situation awareness knowledge and its functions (like risk assessment function) to steer the vehicle and to ensure vehicle safety. In system architecture presented in Fig. 3 the processes *task planning* and *actuator control* perform these tasks.

The system should be demonstrated to work safely when the operating environment is consistent with the assumed environment profile. Therefore we add the fourth claim (G5) to provide evidence why we think the operating environment will be consistent with the intended profile and how will we assure that the vehicle will not be used in other environment what could cause errors of the situation awareness model. Part of the claim justification should be related to assumptions about the behaviour of other vehicles.

Justification for claims G3 and G4 can be based on the system design analysis and demonstration of the traceable process of design, development, testing, verification and validation. Justification for the situation awareness model (G2) is more difficult.

At the moment we do not have effective methods for the situation awareness model analysis. One of the problems is that the model covers overall vehicle safety. That is quite different to traditional hazard analysis approach where we divide the analysis into as small pieces as it is possible and then analyse separately each hazard and each failure mode. Risk factors in the situation awareness model are interrelated and it is more difficult to analyse them separately. We will not be able to decompose the problem into separate and independent items. When we adjust the situation awareness model for better reaction for a single risk factor then we usually alter assessment of a broad set of situations.

The second difference to traditional safety assurance methods is the decision making process. The barrier approach assumes that the control system will react immediately when a specific condition is met. This is a direct cause-consequence relation. We can use analytical techniques like Event Tree Analysis or Fault Tree Analysis to examine effectiveness of barriers. When the system maintains situation awareness then the direct connection between the barrier activating event and the reaction is broken. If the vehicle strategy is to accept some risk level then the vehicle behaviour will differ from simple reaction to barrier activation condition.

Verification of the situation awareness model requirements presented in Section 4.2 is a very complex task even for simple simulated vehicle models. Probably it will not be possible to verify it manually and tool support will be needed.

The main problem that we had encountered during definition of a situation awareness model for a simple simulated autonomous vehicle was the correctness of the risk assessment function. The risk level for a safe situation or for an accident is easy to verify. However the risk level for intermediate states is more difficult for verification as we do not have real world values that can be measured and compared to. Humans can also differently assess the risk of the situation and our experience shows that the assessment can be subjective. The solution of the problem that we use is scenario risk profile analysis. The profile is used to present changes of the assessed risk level for a scenario. For example when a scenario starts with a safe state and ends with an accident we can observe how the risk level rises. We can also identify points in time when risk factors are detected by the vehicle or some specific conditions occurred. As a result of the analysis we can add additional risk factors or change ratings of existing risk factors to improve system ability to avoid hazard. It will be difficult for complex systems to design the correct situation awareness model and then prove its safety. The approach will be rather to analyse the system safety and then improve the model using methods like risk profile analysis.

Another problem is how to assess the system safety level as the environmental conditions has great influence on it. For example number of accidents will depend on behaviour of other vehicles, weather and road conditions and so on. The system safety requirements and safety performance can be defined and measured in the context of a specific environment profile only.

The last of the main problems is the certainty level for prediction of other vehicle actions. We have to accept some level of prediction uncertainty however there is some breaking point when the vehicle control system loses the ability to preserve safety. We discuss the problem of uncertainty in [10].

This all together gives us four types of evidence that can be used when constructing arguments for situation awareness model correctness (Fig. 6).

The first type of evidence (E1) is based on the analysis of the situation awareness model (kinematic model) and accident sequences. We analyse the model in the context of identified safety requirements.

Evidence E2 is based on the simulation results. We define some number of scenarios (safe, near-miss and accidents) and use them for analysis and simulation. The objective of a simulation scenario is to check if the vehicle can safely operate for a given scenario. To use large number of simulated scenarios an efficient simulation tool is needed and also tool support for scenarios definition and validation. This method is especially useful when it is used for testing of modified vehicle control system using a set of already validated and documented scenarios.

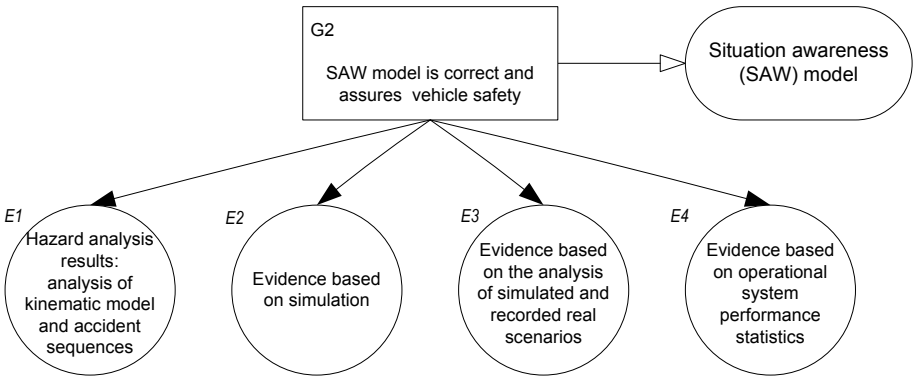

Fig. 6. Analysed types of evidence for claim of situation awareness model correctness

The third kind of evidence is the analysis of simulated and recorded real scenarios. We analyse the scenario risk profile to check how the risk level was rising before an accident, when the system became aware of the high risk level, how the risk level is assessed in absence of any threats and if we can explain observed variations in the scenario risk profile. Comparison of simulated scenarios and scenarios recorded during system operation will provide evidence for the situation awareness model consistency with real vehicle behaviour.

The last kind of evidence is based on data from the system operation. This data can be a subject to reliability growth modelling. Accidents experienced during system operation can be analysed to improve situation awareness model.

5. Summary

The use of situation awareness model and dynamic risk assessment is a novel approach for safety-critical systems. Nowadays most of safety-critical systems are not autonomous. For simple autonomous systems the traditional approach based on predetermined risk assessment and a concept of a barrier is sufficient for achieving safety and performance goals. Safety assurance methods and techniques for this approach are mature and efficient. Main safety argument strategy is to demonstrate

traceable process from safety requirements analysis, through design, development, tests, verification, validation to finally operation and maintenance.

In the future we can expect a tendency to use autonomous systems operating in more complex and less controlled environments. This will raise problems presented in the paper. The presented dynamic risk assessment approach would allow for development of resilient autonomous systems. The idea of a resilient system is to sail close to the area where accidents will happen, but always stay out of the dangerous area [13]. Dynamic risk assessment approach promises such abilities however it is very difficult to provide sound and convincing safety evidence. We have discussed our experience what strategy can be used for presenting safety argument for the use of dynamic risk assessment. The main problem is that the safety argument is not so straightforward as in the case of the predetermined risk assessment approach. Appropriate safety analysis methods for situation awareness model and dynamic risk assessment are not mature and are the subject of further research.

.

References

1. Buchanan. M., Anderson. J.E., Tegnér. G., Fabian. L., Schweizer. J.: Emerging Personal Rapid Transit Technologies - Introduction, State of the Art, Applications, In: Proceedings of the Advanced Automated Transit Systems Conference AATS 2005, Bologna, Italy (2005)
2. DARPA: Urban Challenge Rules, http://www.darpa.mil/grandchallenge (2006)
3. Robertson, S.W.H.: Motion Safety for an Autonomous Vehicle Race in an Urban Environment, In: 2006 Australasian Conference on Robotics & Automation, Auckland (2006)
4. Clough, B.T.: Metrics, Schmetrics! How The Heck Do You Determine A UAV's Autonomy Anyway? In: Proceedings of the 2002 PerMIS Workshop, NIST Special Publication 990 (2002)
5. Sholes, E.: Evolution of a UAV Autonomy Classification Taxonomy, In: 2007 IEEE Aerospace Conference, IEEE (2007)
6. Hollnagel, E.: Accidents and Barriers, In: J-M Hoc et al. (eds.) Proceedings of Lex Valenciennes, Volume 28, pp. 175--182, Presses Universitaires de Valenciennes (1999)
7. Springs, J.: Developing a Safety Case for Autonomous Vehicle Operation on an Airport, In: Redmill F, Anderson T. (eds.) Currect Issues in Safety-critical Systems – Proceeding of the Eleventh Safety-critical Systems Symposium, pp. 79--98, Springer-Verlag London (2003)
8. Bishop, P.G., Bloomfield, R., Guerra, S.: The future of goal-based assurance cases, In: Proceedings of Workshop on Assurance Cases, Supplemental Volume of the 2004 International Conference on Dependable Systems and Networks, pp. 390--395 (2004)
9. Kelly, T.P.: Arguing Safety – A Systematic Approach to Managing Safety Cases, PhD thesis, University of York (1998)
10. Wardziński, A.: The Role of Situation Awareness in Assuring Safety of Autonomous Vehicles, In: Górski J. (Ed.), SAFECOMP 2006, LNCS 4166, pp. 205--218, Springer-Verlag Berlin Heidelberg (2006)
11. Wardziński, A.: Dynamic Risk Assessment in Movement Planning for Autonomous Vehicles, In: International IEEE Conference on Information Technology, IT 2008, Gdansk (Poland), pp. 127-130, IEEE Press (2008)
13. Hollnagel, E., Woods, D.D., Leveson N.: Resilience Engineering, Ashgate (2006)