**Experiment-4: Provide information about a safety case, contextual information, evidence andGSN rules.**

**Prompt:**

You are a professional safety case developer assistant. I want you to create a safety case for the given system in Goal Structuring Notation (GSN) Format.

I will give you the following information in the form of Questions and Answers:

Question 1: What is a safety case?

Answer: A safety case is a structured argument, supported by evidence, intended to justify that a system is acceptably safe.

Question 2: What is the format of the safety case

Answer: I want you to generate a safety case in GSN Format

Question 3: What is the system for which you need to generate a safety case

Answer: The system is a Machine Learning (ML) algorithm that is used to implement the classification function of a Tire Noise Recognition (TNR) component of a vehicle. Tyre Noise Recognition (TNR) component is used to improve multiple vehicle-level functions. The TNR makes use of microphones positioned within the wheel housing to measure road surface noise to determine, in real time, whether the road is dry. Here, dryness is defined as a road surface without any materials between tyre and road surface. This classification is, in turn, used as an additional source of information by chassis control and powertrain systems to determine the current surface traction and thereupon adapt control parameters accordingly, i.e., a !dry surface requires adaptations for a consistent traction.

Question 4: What is the main objective of the safety case

Answer: The objective of the safety case is to develop a structured and convincing argument that the classifier fulfilled its technical requirements, with respect to functional insufficiencies that could lead to False Positives (FP) identifications of dry road surface conditions.Question 5: Additional Context about the system

In order to provide accurate information to the chassis control system, the TNR must process the audio signal with strict real-time requirements and be able to filter sampling anomalies caused by conditions such as the impact of loose gravel. Due to the runtime properties as well as the ability to process a wide range of signal patterns based on available data, a ML technique was chosen to implement the classification function of the TNR. Through limits imposed within the vehicle-level function, the remaining safety concerns regarding the ML-based classification were low enough to assign only Quality Management (QM) requirements to the TNR after completing the hazard and risk analysis according to ISO 26262. However, in order to increase the functional benefits of the vehicle-level function through usage of TNR information, it was decided to evaluate the impact of reducing the limits imposed within the vehiclelevel function. This in turn placed an increased safety load onto the TNR and hence led to the following functional safety requirement (FSR) allocated to the TNR:

– FSR x: The TNR shall not provide the result dry in case of a non-dry road surface (ASIL B).

In order to focus on factors affecting safety, the following relationship between classified and actual prevailing road surface condition was established:

– True-Positive (TP) Predicted dry while actually dry

– True-Negative (TN) Predicted !dry while actually !dry

– False-Negative (FN) Predicted !dry while actually dry

– False-Positive (FP) Predicted dry while actually !dry

Predicted dry while actually dry, Predicted !dry while actually !dry, Predicted !dry while actually dry, Predicted dry while actually !dry.

The misclassification FN only results in an overly conservative control strategy as higher traction is not actually needed but still activated, thereby not violating any safety goals. Hence, only the misclassification FP, which corresponds to FSR x, is safety-relevant.

Question 6: Are there any evidences?

The following methods were identified to provide explicit evidence corresponding to the V&V objectives. In some cases, existing evidence could be aligned with the V&V objectives, in other cases, additional tests and associated documentation were required. – Analysis: An understanding of the strengths and weaknesses of the chosen ML technique and model provided evidence for the inherent properties regarding robustness and generalisation. In addition, the prototypes generated by the algorithm (cf. Section 5) were amenable to examination by subject matter experts to confirm that they corresponded to known properties of the dry and! dry signals.

– Simulation: A simulation environment based on synthetic and recorded data was used for a focused verification of ML properties. Here, signal noise can also be simulated to verify the robustness of the classifier.

– Structured testing: The domain model was used to determine a set of test cases which cover all known properties which could influence the performance of the function. In addition, the test cases also included specific corner cases discovered during field tests and added to the regression test set.

– Field tests: Field tests, where the function was tested on real roads (both test track and public roads) were performed according to selected properties of the domain model. This allowed the coverage of conditions to be evaluated. Anomalies which could not be explained by the parameters of the domain model were used to iteratively refine the domain model.

I will explain what the components of the safety case in GSN so you can generate it efficiently.

1. Goal – Denoted by G. Documents the claims made in the argument. Goals should contain only claims. For the top-level claim, the creator should consider what is the most fundamental objective relevant in the context.

2. Strategy – Denote by S. Describe the reasoning that connects the parent goals and their supporting goals. They should only summarize the argument approach. To focus attention on the function of strategy elements, it is useful for the author to introduce a summary of the argument approach with a phrase such as “Argument by appeal to…”, “Argument by …”, “Argument across …”

3. Solution – Denoted by Sn. Make no claims but are simply references to evidence that provides support to a claim. Solution should refer only to evidence.

4. Context – Denoted by C. There can be two types of contexts, one is a reference to an artifact of some kind. Another is where it draws attention to explanatory contextual information.

5. Assumption – Denoted by A. Declares an assumption made in stating the claim. it is an unsubstantiated sentence. They are connected to the entirety of the argument.

6. Justification – Denoted by J. Does not alter the meaning of the claim made in the goal but provide rationale for its inclusion. They are local to the element to which they are linked.

In addition to the 6 elements described above, there are two types of relationships. InContextOf and SupportedBy.

Some additional contexts on the elements:

To simplify the logic of the argument, it is important to state claims atomically, that is to ensure that each goal element contains only one claim. Goal, context, and solution should be stated atomically. A single node should contain exactly one claim or reference. The use of more than one verb phrase in a goal statement often indicates that the goal contains multiple claims which is not correct. It is important that the text in GSN elements reflects the logical function for which the element was designed. Care should be taken to ensure that the strategies do not restate or redefine the argument process when it is clear from the goal structure. In such cases, the strategies can be omitted. When the relationship between goals and different levels are not clear, then a strategy can be inserted. Where the argument requires that a claim be made about the nature of the support a solution provides for a goal, this should not be stated as part of the solution. Rather, the claim should be stated as a goal to which the evidence item provides a direct solution.

In general, the textual element of arguments should be kept as brief as possible, though the statements made in strategies, justifications, assumptions, and textual definitions should be expressed using as much detail as is necessary for the reader to understand the nature and structure of the argument. Care should be taken to avoid ambiguity and not to overload the terminology. Goals should only contain claims, solutions should only refer to evidence, and strategies should only summarise the argument approach. The statements made in goal elements capture the claims made in the argument. They should be expressed in the form noun-phrase verb-phrase. The noun-phrase identifies the subject of the claim – i.e., the thing with which the statement is concerned. The verb-phrase defines a predicate – it serves to make some assertion about the subject. Care should also be taken to avoid the danger of overstatement when using expressions including ‘all’, ‘any’, ‘each’, ‘every’, ‘typical’ and similar words.

I will provide a table that shows the structural and semantic rules that should be followed while creating the elements:

|  |  |  |
| --- | --- | --- |
| **Element** | **Structural rules** | **Semantic Rules** |
| Structured prose | Directed acyclic graph |  |
| Goal | Allowed connections: Goal to goal, Goal to strategy, Goal to solution, Goal to context, Goal to assumption, Goal to justification | Noun phrase + verb phrase |
| Context | Allowed connections: Context to goal, Context to strategy | Type i: Noun phrase; Type ii: Noun-phrase + verb Phrase |
| Strategy | Allowed connections: Strategy to goal, Strategy to context, Strategy to assumption, Strategy to justification | Strategy statements contain a brief description of the argument approach. |
| Solution | Allowed connections: Goal to solution | Noun-phrase |
| Justification | Allowed connections: Justification to goal, Justification to strategy | Stated fully as necessary complete sentence. Should be a Noun phrase + verb phrase |
| Assumption | Allowed connections: Assumption to goal, Assumption to strategy | Stated fully as necessary complete sentence. Should be a Noun phrase + verb phrase |

Example safety case in GSN format:

G1: Map system is acceptably safe to operate

C1: Map systems is defined

C2: Map role and context

G2: All identified hazards have been eliminated or sufficiently mitigated

C3: Hazards identified from DAO

S1: Argumentation over identified hazard

A1: All hazards have been identified

G3: Hazard H1 has been eliminated

Sn1: Safety rules execution

Create a top-level safety case for the ML algorithm in GSN Format