You are an assistant who assist in developing an assurance case in a tree structure using Goal Structuring Notation (GSN) based on an existing assurance case pattern. Your role is to instantiate an assurance case pattern to create an assurance case. I will provide you with context information on assurance case and assurance case pattern. The context information for assurance case begins with the delimiter *“@Context\_AC”* and ends with the delimiter *“@End\_Context\_AC”* while the context information for assurance case pattern begins with the delimiter *"@Context\_ACP”* and ends with the delimiter *“@End\_Context\_ACP”*

*@Context\_AC*

An assurance case, such as a safety case or security case, can be represented using Goal Structuring Notation (GSN), a visual representation that presents the elements of an assurance case in a tree structure. The main elements of a GSN assurance case include Goals, Strategies, Solutions (evidence), Contexts, Assumptions, and Justifications.

Additionally, an assurance case in GSN may include an undeveloped element decorator, represented as a hollow diamond placed at the bottom center of a goal or strategy element. This indicates that a particular line of argument for the goal or strategy has not been fully developed and needs to be further developed.

I will explain each element of an assurance case in GSN so you can generate it efficiently.

1. Goal – A goal is represented by a rectangle and denoted as G. It represents the claims made in the argument. Goals should contain only claims. For the top-level claim, it should contain the most fundamental objective of the entire assurance case.
2. Strategy – A strategy is represented by a parallelogram and denoted as S. It describes the reasoning that connects the parent goals and their supporting goals. A Strategy should only summarize the argument approach. The text in a strategy element is usually preceded by phrases such as “Argument by appeal to…”, “Argument by …”, “Argument across …” etc.
3. Solution – A solution is represented by a circle and denoted as Sn. A solution element makes no claims but are simply references to evidence that provides support to a claim.
4. Context (Rounded rectangles) – In GSN, context is represented by a rounded rectangle and denoted as C. The context element provides additional background information for an argument and the scope for a goal or strategy within an assurance case.
5. Assumption – An assumption element is represented by an oval with the letter ‘A’ at the top- or bottom-right. It presents an intentionally unsubstantiated statement accepted as true within an assurance case. It is denoted by A
6. Justification (Ovals) – A justification element is represented by an oval with the letter ‘J’ at the top- or bottom-right. It presents a statement of reasoning or rationale within an assurance case. It is denoted by J.

*@End\_Context\_AC*

*@Context\_ACP*

Assurance case patterns in GSN (Goal Structuring Notation) are templates that can be re-used to create an assurance case. Assurance case patterns encapsulate common structures of argumentation that have been found effective for addressing recurrent safety, reliability, or security concerns. An assurance case pattern can be instantiated to develop an assurance case by replacing generic information in placeholder decorator with concrete or system specific information.

To represent assurance case patterns in GSN format, additional decorators have been provided to support assurance case patterns. These additional decorators are used together with the elements of an assurance case to represent assurance case pattern. I will explain each additional decorator below to support assurance case pattern in GSN.

1. Uninstantiated - This decorator denotes that a GSN element remains to be instantiated, i.e. at some later stage, the generic information in placeholders within a GSN element needs to be replaced (instantiated) with a more concrete or system specific information. This decorator can be applied to any GSN element.
2. Uninstantiated and Undeveloped – Both decorators of undeveloped and uninstantiated are overlaid to form this decorator. This decorator denotes that a GSN element requires both further development and instantiation.
3. Placeholders – This is represented as curly brackets “{}” within the description of an element to allow for customization. The placeholder "{}" should be directly inserted within the description of elements for which the predicate "HasPlaceholder (X)" returns true. The placeholder "{}" can sometimes be empty or contain generic information that will need to be replaced when an assurance case pattern is instantiated.
4. Choice - A solid diamond is the symbol for Choice. A GSN choice can be used to denote alternatives in satisfying a relationship or represent alternative lines of argument used to support a particular goal.
5. Multiplicity - A solid ball is the symbol for multiple instantiations. It represents generalized n-ary relationships between GSN elements. Multiplicity symbols can be used to describe how many instances of one element-type relate to another element.
6. Optionality - A hollow ball indicates ‘optional’ instantiation. Optionality represents optional and alternative relationships between GSN elements.

The following steps is used to create an assurance case from an Assurance cases pattern.

1. Create the assurance case using only elements and decorators defined for assurance cases.
2. Remove all additional assurance case pattern decorators such as (Uninstantiated, Placeholders, Choice, Multiplicity, Optionality, and the combined Uninstantiated and Undeveloped decorator)
3. Remove the placeholder symbol "{}" and replace all generic information in placeholders “{}” with system specific or concrete information.

*@End\_Context\_ACP*

We have defined the following predicate rules for the elements and decorator used in an assurance case to ease understanding of an assurance case. The predicate rules for the elements and decorator of an assurance case begins with the delimiter *“@Predicate\_AC”* and ends with the delimiter *"@End\_Predicate\_AC”*

*@Predicate\_AC*

1. Goal(G): True if G is a goal within the assurance case. This predicate is represented as Goal (ID, Description) where ID is the unique identifier for the goal, and description is the textual information of the goal.
2. Strategy(S): True if S is a strategy within the assurance case. This predicate is represented as Strategy (ID, Description) where ID is the unique identifier for the strategy and description is the textual information of the Strategy.
3. Solution (Sn): True if Sn is evidence within the assurance case. This predicate is represented as Solution (ID, Description) where ID is the unique identifier for the evidence or solution and description is the textual information of the evidence.
4. Context(C): True if C is a context within the assurance case. This predicate is represented as Context (ID, Description) where ID is the unique identifier for the context and description is the textual information of the context.
5. Assumption (A): True if A is an assumption within the assurance case. This predicate is represented as Assumption (ID, Description) where ID is the unique identifier for the assumption and description is the textual information of the assumption.
6. Justification (J): True if J is a justification within the assurance case. This predicate is represented as Justification (ID, Description) where ID is the unique identifier for the justification and description is the textual information of the justification.
7. Undeveloped(X): True if X is either a Goal(G) or Strategy(S) marked as undeveloped. This predicate is represented as Undeveloped(X), where X can be either a goal or strategy.

*@End\_Predicate\_AC*

We have defined the following predicate rules for the additional decorators used to support assurance case patterns to ease understanding. The predicate rules for the additional decorators to support assurance case pattern begins with the delimiter *“@Predicate\_ACP”* and ends with the delimiter *"@End\_Predicate\_ACP”*

*@Predicate\_ACP*

1. Uninstantiated (X): True if element X (can be any GSN element) is marked as uninstantiated.
2. UndevelopStantiated (X): True if element X is either a Goal(G) or Strategy(S) and is marked both as uninstantiated and undeveloped.
3. HasPlaceholder (X): True if element ‘X’ (can be any GSN element) contains a placeholder ‘{}’ within its description that needs instantiation.
4. HasChoice (X, [Y], Label): True if an element ‘X’ (either a Goal(G) or Strategy(S)) can be supported by selecting among any number of elements in [Y] (where Y can be any GSN element) according to the cardinality specified by an optional Label. The label specifies the cardinality of the relationship between ‘X’ and ‘Y’. A label is of the general form “m of n” (e.g. a label given as “1 of 3” implies an element ‘X’ can be supported by any one of three possible supporting elements in [Y])
5. HasMultiplicity (X, [Y], Label): True if multiple instances of an element X (either a Goal(G) or Strategy(S)) relate to multiple instances of another element [Y] (where Y can be any GSN element) according to the cardinality specified by an optional Label. The label specifies the cardinality of the relationship between X and Y. (i.e., how many instances of an element in X relates with how many instances of an element in [Y]. e.g. m of n implies m instances of an element in X must be supported by n instances of an element in Y)
6. IsOptional (X, [Y], Label): True if an element X (either a Goal(G) or Strategy(S)) can be optionally supported by another element [Y] (where Y can be any GSN element) according to the cardinality specified by an optional Label. The label specifies the cardinality of the relationship between X and Y. (i.e. an instance of an element in X may be supported by another instance of an element in [Y], but it is not required)

*@End\_Predicate\_ACP*

To represent an assurance case or assurance case pattern in GSN is equivalent to depicting in a hierarchical tree structure. To achieve this hierarchical tree structure, the below predicates have been defined to ease understanding of this structure. The predicate rules to support the structure of an assurance case or assurance case pattern begins with the delimiter *“@Predicate\_Structure”* and ends with the delimiter *“@End\_Predicate\_Structure”*

*@Predicate\_Structure*

1. IncontextOf (X, [N], D): True if element X at depth D has a neighbour [N] to the left or right at depth D, where ‘[N]’ can be an Assumption (A), Justification (J), or Context (C), ‘X’ can be a Goal (G), or Strategy (S) and ‘D’ represents the height or depth of the goal or strategy element and its neighbours in the GSN hierarchical structure.
2. SupportedBy (X, [C], D): True if element X at depth D has children [C] directly below it, where [C] can include Goal (G), Strategy (S), or Solution (Sn) and ‘X’ can be a Goal (G), or Strategy (S).

* If X is Strategy (S), [C] can only be Goal (G).
* If X is Goal (G), [C] can be either Goal (G), Strategy(S), or Solution (Sn).

*@End\_Predicate\_Structure*

Now, I will provide you with an example of an assurance case pattern in its predicate form and the corresponding assurance case derived from this pattern so that you can understand the process of instantiating an assurance case pattern to create an assurance case.

For example, an Assurance Case Pattern and the derived assurance case for BlueROV2 system (an underwater remotely operated vehicle) is given below. The assurance case pattern begins with the delimiter *"@Pattern"* and ends with the delimiter *"@End\_Pattern"* while the derived assurance case begins with the delimiter *"@Assurance\_case"* and ends with the delimiter *"@End\_Assurance\_case"*

*@Pattern*

Goal (G1, Hazards for {A :: System} addressed in accordance with ALARP principle.)

Goal (G2, No intolerable risks present in the system.)

Goal (G3, Risk from (B:: Hazard} has been reduced as low as reasonably practicable)

Goal (G4, Model {S:: BTD} accurately describes possible propagation of hazard {R:: Hazard})

Goal (G5, Quantitative risk estimates are accurate and below acceptable threshold)

Goal (G6, Possible hazard propagation paths correctly captured in BTD)

Goal (G7, Barriers in the BTD correctly describe their respective control action including any required system functions)

Goal (G8, All non-negligible threats have been identified)

Goal (G9, State probability distribution used for risk estimation is an accurate representation of expected system states)

Goal (G10, Estimated probability of {U:: Consequence} is below allowable threshold for severity class)

Strategy (S1, Argument by risk reduction/elimination of each hazard)

Strategy (S2, Argue that risk posed by any remaining hazards is negligible)

Strategy (S3, Argue that no other risks have been identified)

Strategy (S4, Apply ReSonAte to estimate level of risk from hazard condition {R:: Hazard})

Context (C1, Definition of "intolerable")

Context (C2, Assigned severity class is {C:: Hazard.Severity})

Assumption (A1, Function {T: Function} required by {S :: BTD} is available}

Solution (Sn1, Estimated risk level {V :: attr:RiskEst})

SupportedBy (G1, S1, 1)

SupportedBy (S1, [G2, G3], 2)

SupportedBy (G2, [S2, S3], 3)

SupportedBy (G3, S4, 3)

SupportedBy (S4, [G4, G5], 4)

SupportedBy (G4, [G6, G7, G8], 5)

SupportedBy (G5, [G9, G10], 5)

SupportedBy (G10, Sn1, 6)

IncontextOf (G2, C1, 3)

IncontextOf (G3, C2, 3)

IncontextOf (S4, A1, 4)

HasPlaceholder (G1)

HasPlaceholder (G3)

HasPlaceholder (C2)

HasPlaceholder (S4)

HasPlaceholder (A1)

HasPlaceholder (G4)

HasPlaceholder (G10)

HasPlaceholder (Sn1)

Uninstantiated (C2)

Uninstantiated (A1)

Uninstantiated (G4)

Uninstantiated (S4)

Uninstantiated (G10)

Uninstantiated (Sn1)

Undeveloped (S2)

Undeveloped (S3)

Undeveloped (G6)

Undeveloped (G7)

Undeveloped (G8)

Undeveloped (G9)

UndevelopStantiated (G1)

HasMultiplicity (S1, G3, 1 of \*)

HasMultiplicity (S4, A1, 0 of \*)

HasMultiplicity (G5, G10, 1 of \*)

HasChoice (G2, [S2, S3], 1 of 2)

*@End\_Pattern*

*@Assurance\_case*

G1: Hazards for BlueROV2 addressed in accordance with ALARP principle.

S1: Argument by risk reduction/elimination of each hazard

G2: No intolerable risks present in the system.

C1: Definition of "intolerable"

S2: Argue that risk posed by any remaining hazards is negligible (undeveloped)

S3: Argue that no other risks have been identified (undeveloped)

G3.0: Risk from Loss of Pipeline hazard has been reduced as low as reasonably practicable (undeveloped)

C2.0: Assigned severity class is Minor

G3.1: Risk from Deviation from Area hazard has been reduced as low as reasonably practicable (undeveloped)

C2.1: Assigned severity class is Minor

G3.2: Risk from Obstacle Encounter hazard has been reduced as low as reasonably practicable

C2.2: Assigned severity class is Major

S4: Apply ReSonAte to estimate level of risk from hazard condition Obstacle Encounter

A1.0: Function Obstacle Detection required by Obstacle Encounter BTD is available

A1.1: Function Command Authority required by Obstacle Encounter BTD is available

A1.2: Function Avoidance Logic required by Obstacle Encounter BTD is available

G4: Model Obstacle Encounter BTD accurately describes possible propagation of hazard Obstacle Encounter

G6: Possible hazard propagation paths correctly captured in BTD (undeveloped)

G7: Barriers in the BTD correctly describe their respective control action including any required system functions (undeveloped)

G8: All non-negligible threats have been identified (undeveloped)

G5: Quantitative risk estimates are accurate and below acceptable threshold

G9: State probability distribution used for risk estimation is an accurate representation of expected system states (undeveloped)

G10: Estimated probability of Collision is below allowable threshold for severity class

Sn1: Estimated risk level 10^-3 per hour

*@End\_Assurance\_case*

Now, I would provide you with domain information about a safety critical system for which you would create a safety case from a given safety case pattern. The domain information begins with the delimiter *“@Domain\_Information”* and ends with the delimiter *"@End\_Domain\_Information”*

*@Domain\_Information*

The provided domain information describes a safety-critical system called the Generic Patient-Controlled Analgesia (GPCA) system, also known as an infusion pump. This system faces two operational hazards: "Overinfusion" and "Underinfusion," which can have dire consequences for patient safety.

The following potential causes for these hazards are identified:

1. Flow rate does not match the programmed rate.
2. Programmed rate too low
3. Dose limit exceeded due to excessive bolus requests.
4. Bolus volume/concentration too high

To mitigate these hazards, eight safety requirements (SR1.1, SR1.2, SR1.4, SR1.5, SR1.10, SR3.4.6, SR6.1.3, SR6.1.4) have been established. Some of the properties of these safety requirements include:

1. "Flow rate sensor is equipped."
2. "Period (to trigger the underinfusion alarm) is 15 minutes."
3. "Flow rate is less than 90% of the programmed rate setting."

These safety requirement properties are based on references such as "FDA standard," "Expertise opinion," and "Previous knowledge."

Additionally, In the safety case pattern for the GPCA system, relationships between different placeholder items within the safety case pattern such as the mitigation relationship between safety requirements and potential causes of hazards are supported using the Object Constraint Language (OCL).

OCL is a formal language that allows the expression of constraints on UML models. For example, OCL expressions like scenario.spec and operations such as allInstances() can be used to model relationships. An OCL expression like scenario.spec.allInstances() can represent all instances of spec related to a particular scenario.

*@End\_Domain\_Information*