SOTIF

Category

1. Scope
2. Normative references
3. Terms and definitions
4. Overview and organization of SOTIF activities
5. Specification and design
6. Identification and evaluation of hazards
7. Identification and evaluation of potential functional insufficiencies and potential triggering conditions
8. Functional modifications addressing SOTIF-related risks
9. Definition of the verification and validation strategy
10. Evaluation of known scenarios
11. Evaluation of unknown scenarios
12. Evaluation of the achievement of the SOTIF
13. Operation phase activities

1. Scope of SOTIF

- the insufficiencies of specification of the intended functionality at the vehicle level; or
- the insufficiencies of specification or performance insufficiencies in the implementation of electric and/or electronic (E/E) elements in the system.

System

1. Functional insufficiencies
2. Incorrect and inadequate Human-Machine Interface (HMI) design(inappropriate user situational awareness, e.g. user confusion, user overload, user inattentiveness)
3. Functional insufficiencies of artificial intelligence-based algorithms.

External factor

1. Reasonably foreseeable misuse by the user or by other road participants.
2. Impact from active infrastructure and/or vehicle to vehicle communication, and external systems
3. Impact from vehicle surroundings (e.g. other users, passive infrastructure, weather, electromagnetic interference)

2. Normative references

Reference check

ISO 26262-1, Road vehicles — Functional safety — Part 1: Vocabulary

3. Terms and definitions

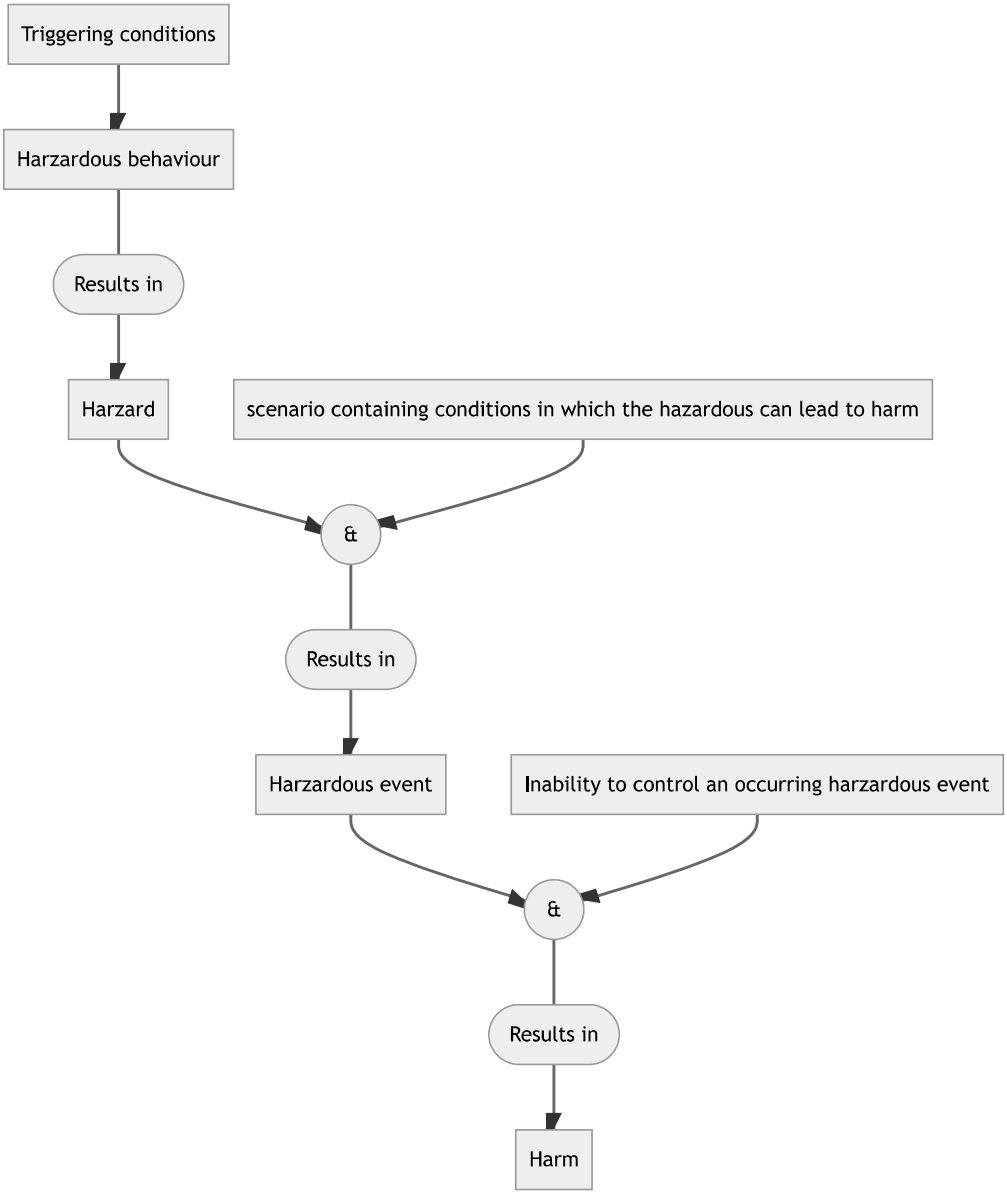
#	Acronym	Vocabulary	Definition
1		acceptance criterion	criterion representing the absence of an unreasonable level of risk

#	Acronym	Vocabulary	Definition
2		action	single act or behaviour that is executed by any actor in a scene
3		driving policy	strategy and rules defining acceptable actions at the vehicle level
4	DDT	Dynamic Driving Task	real-time operational and tactical functions required to operate a vehicle in traffic
5		DDT fallback	response by the driver or automation system to either perform the dynamic driving task (DDT) or transition to a minimal risk condition (MRC) after the occurrence of a failure(s) or detection of a functional insufficiency or upon detection of a potentially hazardous behaviour
6		ego vehicle	vehicle fitted with functionality that is being analysed for the SOTIF
7		event	occurrence at a point in time
8		functional insufficiency	insufficiency of specification or performance insufficiency
9		functional modification	alteration of a functional specification
10		fallback-ready user	user who is able to operate the vehicle and is capable of intervening to perform the DDT fallback as required and within a time span appropriate for the defined non-driving occupation
11		hazard	potential source of harm caused by the hazardous behaviour at the vehicle level
12		insufficiency of specification	specification, possibly incomplete, contributing to either a hazardous behaviour or an inability to prevent or detect and mitigate a reasonably foreseeable indirect misuse when activated by one or more triggering conditions
13		intended behaviour	behaviour of the intended functionality
14		intended functionality	specified functionality
15		levels of driving automation	mutually exclusive set of driving automation levels, ranging from Level 0 (no automation) to Level 5 (full automation), defining the roles of the driver or user and automation system in relation to each other
16	MRC	Minimal Risk Condition	vehicle state in order to reduce the risk, when a given trip cannot be completed
17		misuse	usage in a way not intended by the manufacturer or the service provider
18		misuse scenario	scenario in which misuse occurs
19		multiple-point functional insufficiency	functional insufficiency of an element leading to hazardous behaviour or inability to prevent or detect and mitigate a reasonably foreseeable indirect misuse only in conjunction with functional insufficiencies of other elements when activated by one or more triggering conditions
20	OEDR	Object and Event Detection and Response	tasks of the dynamic driving task (DDT) that include monitoring the driving environment and executing an appropriate response to objects and events to complete the DDT and/or the DDT fallback
21	ODD	operational design domain	specific conditions under which a given driving automation system is designed to function
22		performance insufficiency	limitation of the technical capability contributing to a hazardous behaviour or inability to prevent or detect and mitigate reasonably foreseeable indirect misuse when activated by one or more triggering conditions
23		risk	combination of the probability of occurrence of harm and the severity of that harm
24		reaction	response to an action by any actor in a scene
25	SOTIF	Safety Of The Intended Functionality	absence of unreasonable risk due to hazards resulting from functional insufficiencies of the intended functionality or its implementation
26		scenario	description of the temporal relationship between several scenes in a sequence of scenes, with goals and values within a specified situation, influenced by actions and events
27		scene	snapshot of the environment including the scenery, dynamic elements, and all actors' and observers' self-representations, and the relationships among those entities
28		single-point functional insufficiency	functional insufficiency of an element leading directly to hazardous behaviour or the inability to prevent or detect and mitigate a reasonably foreseeable misuse when activated by one or more triggering conditions
29		situational awareness	understanding of the situation

#	Acronym	Vocabulary	Definition
30		triggering condition	specific condition of a scenario that serves as an initiator for a subsequent system reaction contributing to either a hazardous behaviour or an inability to prevent or detect and mitigate a reasonably foreseeable indirect misuse
31		unreasonable risk	risk judged to be unacceptable in a certain context according to valid societal moral concepts
32		use case	description of a suite of related scenarios
33		validation target	value to argue that the acceptance criterion is met
34	VLSS	vehicle-level SOTIF strategy	set of vehicle-level requirements for the intended functionality used to support design, verification and validation activities to achieve the SOTIF

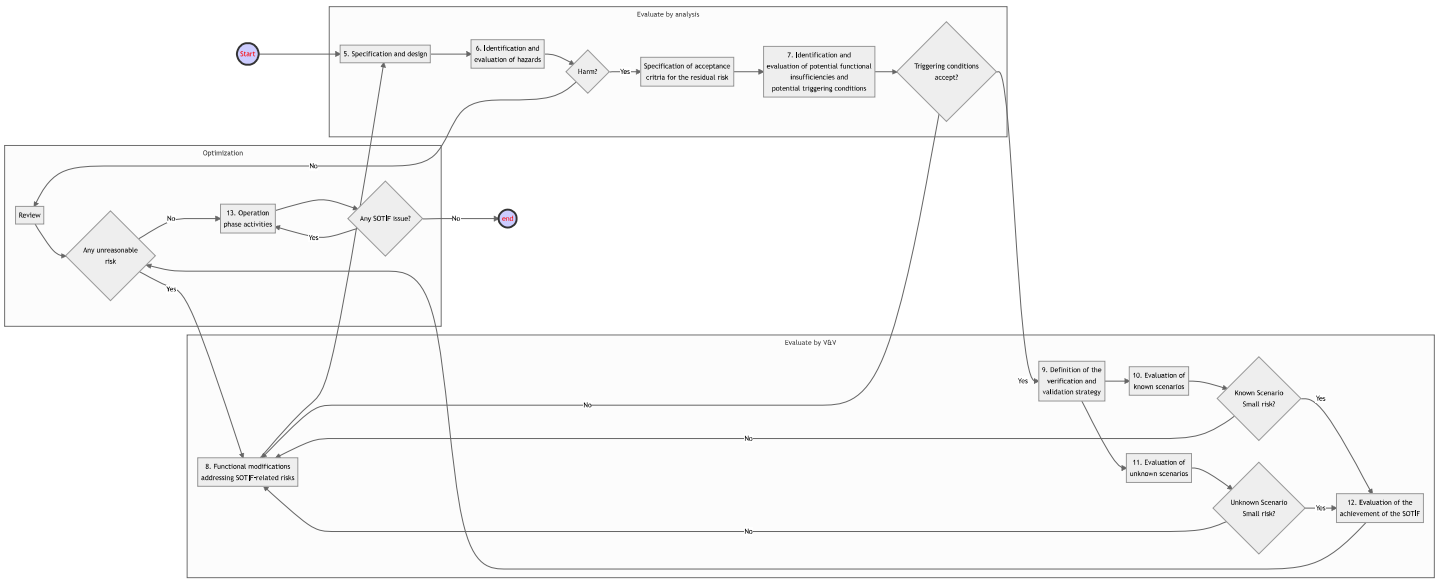
4. Overview and organization of SOTIF activities

4.2 SOTIF principles



4.3.1 Flow chart and structure of this document

> **tip on the diagram below**
>
> If you have no **HARM**, SOTIF process finish quickly.



5. Specification and design

5.2 Specification of the functionality and considerations for the design

ASK following Question to Supplier or Customer

Questions to supplier or internal customer	Points
Do you have the description of the intended functionality and the functionalities of the supporting subsystems and components including[ODD]?	4
Do you have the description of the intended functionality and the functionalities of the supporting subsystems and components including[the level and details of the automated driving function control authority over vehicle dynamics]?	4
Do you have the description of the intended functionality and the functionalities of the supporting subsystems and components including[the vehicle-level SOTIF strategy]?	4
Do you have the description of the intended functionality and the functionalities of the supporting subsystems and components including[the use cases in which the function can be active or inactive, and the transitions between them]?	4
Do you have the description of the intended functionality and the functionalities of the supporting subsystems and components including[the description of decision-making logic]?	4
Do you have[the design of the relevant system and its elements implementing the intended functionality]?	4
Do you have[the performance targets of the installed sensors, controllers, actuators or other inputs and components enabling the intended functionality]?	4
Do you have the dependencies of the intended functionality on, and interactions or interfaces with[the driver]?	4
Do you have the dependencies of the intended functionality on, and interactions or interfaces with[the driver interface (e.g. HMI), and how the interface is used to mitigate known reasonably foreseeable misuses]?	4
Do you have the dependencies of the intended functionality on, and interactions or interfaces with[the remote/back office operator]?	4
Do you have the dependencies of the intended functionality on, and interactions or interfaces with[the passengers, pedestrians, cyclists and other road users]?	4
Do you have the dependencies of the intended functionality on, and interactions or interfaces with[the relevant environmental conditions]?	4
Do you have the dependencies of the intended functionality on, and interactions or interfaces with[the road infrastructure and road furniture]?	4
Do you have the dependencies of the intended functionality on, and interactions or interfaces with[the data exchange to and from the cloud, inter-vehicle or other communication infrastructures and in-service telematics involving diagnostics and parameter updates]?	4
Do you have the dependencies of the intended functionality on, and interactions or interfaces with[the remote flashing of software updates]?	4
Do you have the dependencies of the intended functionality on, and interactions or interfaces with[the other functions of the vehicle that might interfere with the intended functionality, including the exchange of information, and the corresponding assumptions of use]?	4

Questions to supplier or internal customer	Points
Do you have[the reasonably foreseeable misuse]?	4
Do you have[the potential performance insufficiencies, identified triggering conditions and countermeasures of the system and its elements]?	4
Do you have[the system and vehicle architectures implementing the intended functionality]?	4
Do you have the warning and degradation concept such as [the warning strategies]?	4
Do you have the warning and degradation concept such as [the DDT fallback: takeover/fallback conditions and schemes for transitioning control from the automated driving system to the driver or another system within their respective use cases]?	4
Do you have the warning and degradation concept such as [the minimal risk condition schemes (e.g. autonomously exit lane and park, stop in path, fallbackready user)]?	4
Do you have the warning and degradation concept such as [the driver monitoring system and its operational effect on the fallback strategy]?	3
Do you have the procedures supporting data collection and monitoring during and after development of the intended functionality such as [the objectives and requirements for the data collection]?	3
Do you have the procedures supporting data collection and monitoring during and after development of the intended functionality such as [the architecture, implementation and mechanisms supporting the required data collection before SOTIF release]?	3
Do you have the procedures supporting data collection and monitoring during and after development of the intended functionality such as [the requirements, design and mechanisms that support data collection during the operation phase for SOTIF analysis, including possible cloud based, “Over The Air”, or RF communication technologies]?	2
Do you have [the mechanism, design and requirements that support risk mitigation abilities during operation]?	1
Total	100

Next Steps

If this is lower than 85% you have not achieved SOTIF, if you have **>86%**, go to **next step.**

5.3 System design and architecture considerations

Questions to supplier or internal customer	Points
Do you have [risk evaluation of hazardous behaviours (e.g. to achieve an S=0, C=0, or to obtain less constraining acceptance criteria);]?	10
Do you have [evaluation of the system's response to the identified triggering conditions (e.g. link to the analysis of a triggering condition showing unacceptable risk)]?	10
Do you have [verification and validation results for known hazardous scenarios (e.g. link to a verification test report showing unacceptable performance with respect to the requirements)]?	10
Do you have [validation results for unknown hazardous scenarios (e.g. link to a validation test report showing unacceptable performance with respect to a hazardous scenario or the validation targets)]?	10
Do you have [SOTIF release argument (e.g. link to report documenting reasons for rejecting release request)]?	10
Do you have [field monitoring process (e.g. link to report documenting new hazardous scenario discovered during field monitoring)]?	10
Do you have enough[measurements]?	6
Do you have enough[tracking]?	6
Do you have enough[target selection]?	6
Do you have enough[kinematic estimation]?	6
[false positive detections (e.g. ghosts, phantom objects) test cases]?	6
[false negative detections test cases]?	6
[driving policy level limitations such as considering occluded areas]?	4
Total	100

Next Steps

If this is lower than 85% you have not achieved SOTIF, if you have **>86%**, go to **Chapter 6.**

6. Identification and evaluation of hazards

Simple Term	Normal Terms	Math Terms	Computer terms	Range	type
Harm	Acceptance Harm rate	A_H	SFAccHarmRate	0.0…0~1.0	Float
Harzardous behaviour	Relevant Hazardous Behaviour	R_{HB}	SFRofHB	0.0…0~1.0	Float
Exposure	Probability of Exposure to Harzardous Behaviour	$P_{E:HB}$	SFProbEHB	0.0…0~1.0	Float
Controllability	Probability of Controllability to Exposure	$P_{C:E}$	SFProbCE	0.0…0~1.0	Float
Severity	Probability of Severity to Controllability	$P_{S:C}$	SFProbSC	0.0…0~1.0	Float

Mathmatical representation

$$A_H = R_{HB} \times P_{E:HB} \times P_{C:E} \times P_{S:C}$$

Example Method

Function	Type	Occurance type	Triggering Conditions	occurance = R_{HB}	Harzardous behaviour	harzard	Exposure =$P_{E:HB}$	Hazardous event	controllability =$P_{C:E}$	Seve = $P_$
AEB	Sensor	Front Radar	reflection from bridge	0.1	Collision from behind	presence of car following closely	0.02	Crash from back	0.3	0.5
BSD	Sensor	Rear Corner Radar	Noise reflection from metallic road	0.005	Collision from Side	presence of car speeding from cross road	0.02	Crash from Side	◯	◯
FCTA	Sensor	Front Corner Radar	does not detect bycycle	◯	collision with cyclist	◯	◯	◯	◯	◯
◯	Sensor	Rear USS	Low obstacle not detected	◯	collision to sharp object	◯	◯	◯	◯	◯
◯	Sensor	Side USS	reflection from Drainage	◯	cannot find parking spot	◯	◯	◯	◯	◯
◯	Sensor	Front USS	no reflection from fence	◯	◯	◯	◯	◯	◯	◯
◯	Sensor	Front Camera	obscured by Fog	◯	◯	◯	◯	◯	◯	◯
◯	Sensor	Rear Camera	sees sun directly from camera	◯	◯	◯	◯	◯	◯	◯
◯	Sensor	AVM Camera	Image blur by water dropplet	◯	◯	◯	◯	◯	◯	◯

Function	Type	Occurance type	Triggering Conditions	occurance = R_{HB}	Harzardous behaviour	harzard	Exposure =$P_{E:HB}$	Hazardous event	controllability =$P_{C:E}$	Seve = P_S
○	Sensor	GNSS	signal not received	○	○	○	○	○	○	○
○	Sensor	ADAS MAP	informs speed limit of 40Kph	○	○	○	○	○	○	○
○	Sensor	V2X	signal not received	○	○	○	○	○	○	○
○	Sensor	IMU	signal not received	○	○	○	○	○	○	○
○	ECU	Low Power	Lower than 9V	○	○	○	○	○	○	○
○	ECU	High Voltage	Higher than 16V	○	○	○	○	○	○	○
○	ECU	IDLE	idle mode	○	○	○	○	○	○	○
○	Com	Signal not received	TCAM does not respond	○	○	○	○	○	○	○
○	Com	Signal delay	more than 300ms have not sent signal	○	○	○	○	○	○	○
○	Human	Misuse1	Misuse1 signal not received	○	○	○	○	○	○	○
				○	○	○	○	○	○	○

7. Identification and evaluation of potential functional insufficiencies and potential triggering conditions

Question for investigation effort	points
Have you analyzed and be able to show us data of requirements	5
Have you analyzed and be able to show us data of the ODD(& its boundaries), use cases and scenarios	5
Have you analyzed and be able to show us data of accident statistics (STATS19 (UK), GIDAS (Germany), GES (US), CARE, IGLAD)	5
Have you analyzed and be able to show us data of boundary values	5
Have you analyzed and be able to show us data of equivalence classes	5
Have you analyzed and be able to show us data of functional dependencies	5
Have you analyzed and be able to show us data of common triggering conditions(Multiple sensors X Mutiple Environment)	5
Have you analyzed and be able to show us data of potential triggering conditions from field experience(Experts or Market) and lessons larnt(Customer Claims)	5
Have you analyzed and be able to show us data of system architecture (including redundancies)	5
Have you analyzed and be able to show us data of design of the sensors and potential technology limitations	5
Have you analyzed and be able to show us data of algorithms and their output or decisions	5
Have you analyzed and be able to show us data of system ageing(Lens become Yellow after 3 years)	5
Have you analyzed and be able to show us data of possible environmental changes over vehicle operational lifetime (eg. interference)	5
Have you analyzed and be able to show us data of external and internal interfaces(V2X)	5

Question for investigation effort	points
Have you analyzed and be able to show us data of design of the actuators and potential limitations	5
Have you analyzed and be able to show us data of accident scenarios(DSSAD/EDR)	5
Have you analyzed and be able to show us data of known misuse scenarios from field experience and other sources of lessons learnt a	3
Have you studied and be able to show us data of with test subjects	3
Have you analyzed and be able to show us data of use cases and scenarios	2
Have you analyzed and be able to show us data of users' interaction with the system	2
Have you analyzed and be able to show us data of HMI	3
Have you analyzed and be able to show us data of known human patterns of lack of use, misuse and automation complacency	3
Have you analyzed and be able to show us data of human capability to perform or switch between certain tasks	2
Have you analyzed and be able to show us data of relevant standards, regulations and guidelines	2
TOTAL	**100**

> **Next Steps**
>
> If this is lower than 85% you have not achieved SOTIF and go to **Chapter 8**, if you have **>86%**, go to **Chapter 9**.

8. Functional modifications addressing SOTIF-related risks

Expert explain about why SOTIF is important regarding

1. System modification
2. Functional restrictions
3. Handing over authority
4. Addressing reasonably foreseeable misuse
5. Considerations to support the implementation of SOTIF measures
6. Updating the input information for "Specification and design"
7. Work products

   And Do this review nextime!!

9. Definition of the verification and validation strategy

If you have passed the Chapter 7 , you should beable to show, how the **Evidence** was created and make sure this is correct.

> **Next Steps**
>
> If Evidence was Good enough go to **Chapter 10** and **Chapter 11**, respectively.

10. Evaluation of known scenarios

10.4 Planning algorithm verification

Expert shouldcheck following

1. Verification of the architectural properties including independence regarding triggering conditions, if applicable
2. In the loop testing (e.g. SIL, HIL, MIL) on selected SOTIF-related use cases and scenarios considering identified triggering conditions
3. Vehicle testing on selected SOTIF-related use cases and scenarios considering identified triggering conditions
4. Injection of inputs that trigger the potentially hazardous behaviour
5. Verification of proper compliance to the driving policy (e.g. achieving the MRC and operation upon exiting the ODD
6. Re-simulation of known hazardous scenarios to verify the effect of an implemented risk mitigation mechanism
7. Verification of robustness against input data being subject to interference from other sources, e.g. white noise, audio frequencies, signal-to-noise ratio degradation (e.g. by noise injection testing)
8. Requirement-based test (e.g. situation analysis, function, variability of sensor data)

Next Steps

If Expert says that this has **small or no risk** , then go to **Chapter 12**. If there is a **mid or high** risk then go to **Chapter 8.**

11. Evaluation of unknown scenarios

Uknown Check done bye expert	Example
Validation of robustness to signal-to-noise ratio degradation (e.g. by noise injection testing)	Validation of SNR (e.g. voltage change, ground wave, heat(cold) stroke, EMC stroke, etc.)
Validation of effects and properties provided by the architecture including independence regarding triggering conditions, if applicable	Independancy from triggering (e.g.
In the loop testing on randomized test cases (derived from a technical analysis and by error guessing)	Error guessing
Randomized input test	Input test
Vehicle-level testing on selected test cases (derived from a technical analysis and by error guessing) considering identified triggering conditions	trigger conditions
Long term vehicle test	Simulation of all combination
Fleet test	at least 5 vehicle is necessary to test
Test derived from field experience	This one, I have many experience but I cannot write all the experience
Test of corner cases and edge cases	Refer to Diagram I sent before
Comparison with existing systems	Benchmark!
Simulation based on random sequence of scenarios	Simulation of random combination
Test of potential misuses with random usage and naïve users	make human mistakes
Sensitivity analysis of the functionality concerning specific conditions of a scenario	RCS,Light,Sound intensity match
Analysis/simulation of relevant parameters	there is many paramemters especially in signals
Scenario exploration in real world	Check all the scenario with vehicle
Functional decomposition and probabilistic modelling (i.e. considering that the insufficiency condition of an element consists of multiple output insufficiencies of its sub-elements; see C.6.3.3)	First Sensor function composition and check the probability and Priority of fusion
Validation against ground truth	Tester must test sensor and test exact location and signal received should be benchmarked.

Next Steps

If Expert says that this has **small or no risk** , then go to **Chapter 12**. If there is a **mid or high** risk then go to **Chapter 8.**

12. Evaluation of the achievement of the SOTIF

Summarize your SOTIF as follows.

Report: Supplier name , Tested date: 2022-08-19

Evaluation of the achievement of the SOTIF

5. *Specification and design*

5.2	5.3	Result
86/100	86/100	**Pass**

6. *Identification and evaluation of hazards*

Defined	Result
86/100	**Pass**

7. *Identification and evaluation of potential functional insufficiencies and potential triggering conditions*

Identified	Result
86/100	**Pass**

9. *Definition of the verification and validation strategy*

Verified	Result
86/100	**Pass**

10. *Evaluation of known scenarios*

Evaluate	Result
86/100	**Pass**

11. *Evaluation of unknown scenarios*

Evaluate	Result
86/100	**Pass**

Expert Comments

Pros. Have done all the work related to SOTIF
Cons. May beable to worked little more evidence

> **Design** ⭐⭐⭐(3*20=60)
>
> > **Identification** ⭐⭐⭐⭐⭐(5*20=100)
> >
> > > **Verification** ⭐⭐⭐(3*20=60)

Record time	5	6	7	9	10	11	Design	Identification	Verification	Overall
2022-08-19	86/100	86/100	86/100	86/100	86/100	86/100	60/100	100/100	60/100	**92**/100

13. Operation phase activities

This documents is the part of single process we need to also define our processes of when to do this. My advise is that in Engineering Phase, SWQA also should be monitored before the SOTIF Analysis is done.