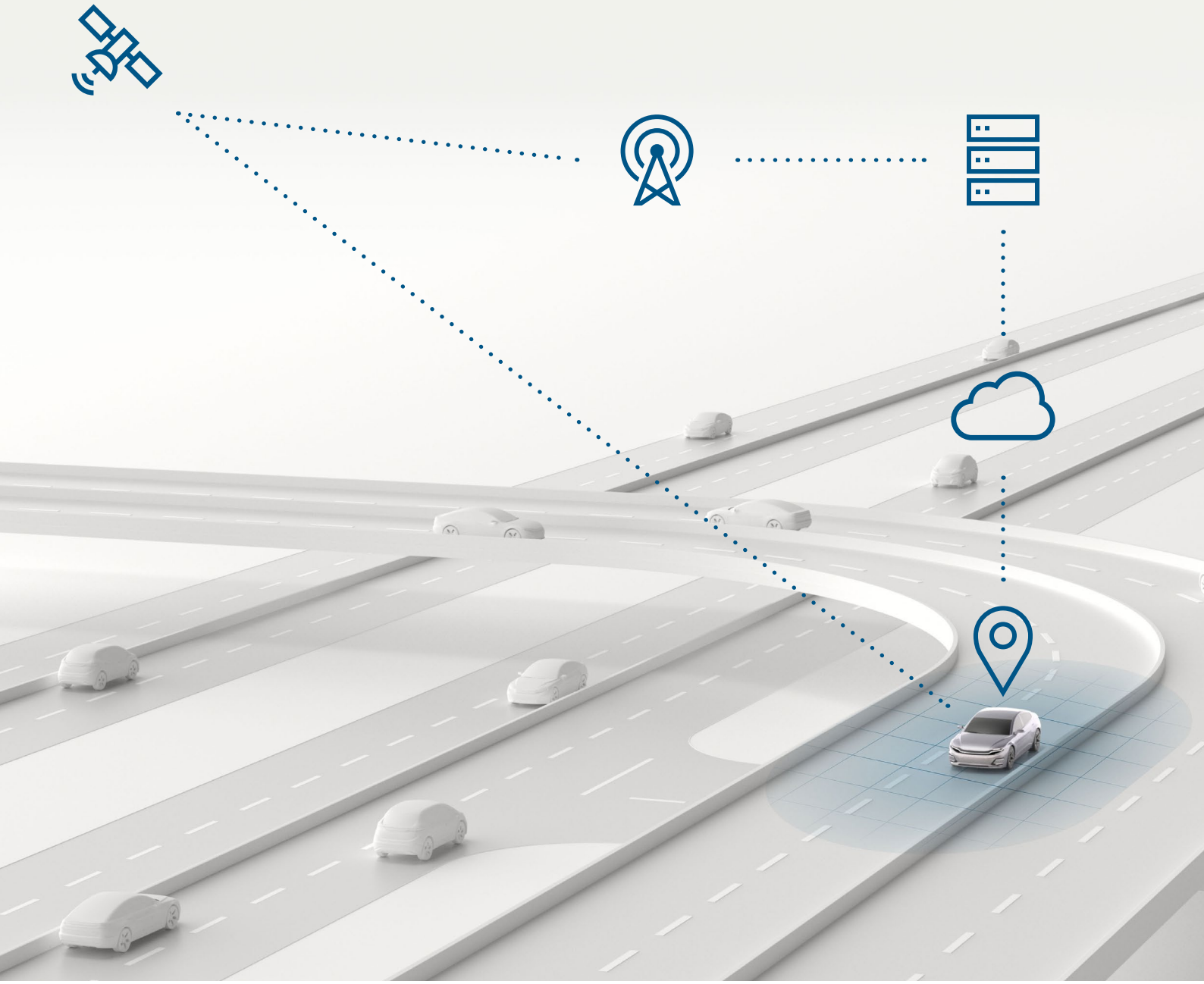


Whitepaper

SOTIF strategy for the validation of a GNSS based vehicle localization sensor

Invented for life

BOSCH

Table of contents

01
Abstract 03

02
VMPS system design and SOTIF parameters 04

03
Triggering conditions and SOTIF validation strategy 07

3.1 Test drive-based validation 11
3.2 Monte-Carlo based simulations 15
3.3 SOTIF-FTA verified by fault injections 18

04
SOTIF Release 22

05
Summary 23

Imprint 24

01
Abstract

The Vehicle Motion and Position Sensor (VMPS) is a precise and safe vehicle localization system that applies sensor fusion algorithms for absolute positioning at cm level with SOTIF requirements and ASIL-B safety classification. It has been developed to support functions used in Automated driving/Advanced driver assistance systems (AD/ADAS) like the activation or deactivation of AD functionalities, safe-stop maneuvers or lane keeping for SAE Level 3 and beyond. VMPS comprises a Global Navigation Satellite System (GNSS) receiver, high performance Inertial Measurement Unit (IMU) and Wheel Speed Sensors (WSS) to meet performance, availability, and safety requirements including both function safety and SOTIF. In addition, GNSS correction data and integrity status information processed from a global network of continuously operating GNSS reference stations (CORS) are applied. An international and interdisciplinary team of system, software, hardware, and correction service engineers together with leading industry partners developed VMPS for highly automated driving.

This paper focuses on the VMPS SOTIF (Safety of the intended functionality) validation strategy as a systematic and structured approach including the derivation of triggering conditions, the mapping to validation and verification activities, analysis of functional insufficiencies and output insufficiencies and finally the argumentation for the SOTIF release compliant to **ISO 21448**, the SOTIF standard [1]. The article introduces the VMPS system design, then covers the general strategy approach and focuses on the three VMPS SOTIF validation pillars:

01 Test drive validations for nominal driving conditions or specific corner case situations making a vehicle setup mandatory

02 Model in the Loop (MIL) Monte-Carlo simulations to cover degraded environmental conditions and sensor data quality variations

03 Fault Tree Analysis (FTA) supported by fault injection testing for verifying the impact of potential triggering conditions with low occurrence probability not covered by test drives

The article concludes with remarks on the VMPS SOTIF release and closes with a summary.

ISO 21448

Published in 06.2022 the norm provides a general argument framework and guidance on measures to ensure the safety of the intended functionality (SOTIF), which is the absence of unreasonable risk due to a hazard caused by functional insufficiencies.

[1] ISO 21448:2022, https://www.iso.org/standard/77490.html

02
VMPS system design and SOTIF parameters

VMPS is a GNSS based vehicle localization sensor aiming to provide a precise and safe position solution. The positioning concept is based upon the fusion of Global Navigation Satellite System (GNSS), Inertial Measurement Unit (IMU) and Wheel Speed Sensor (WSS) measurements enhanced by high-quality correction data and integrity status information provided by a GNSS correction service. The broadcast of correction data and integrity information is realized via OEM backend using cloud services. An overview of the most relevant system components of VMPS is depicted in Fig. 1.

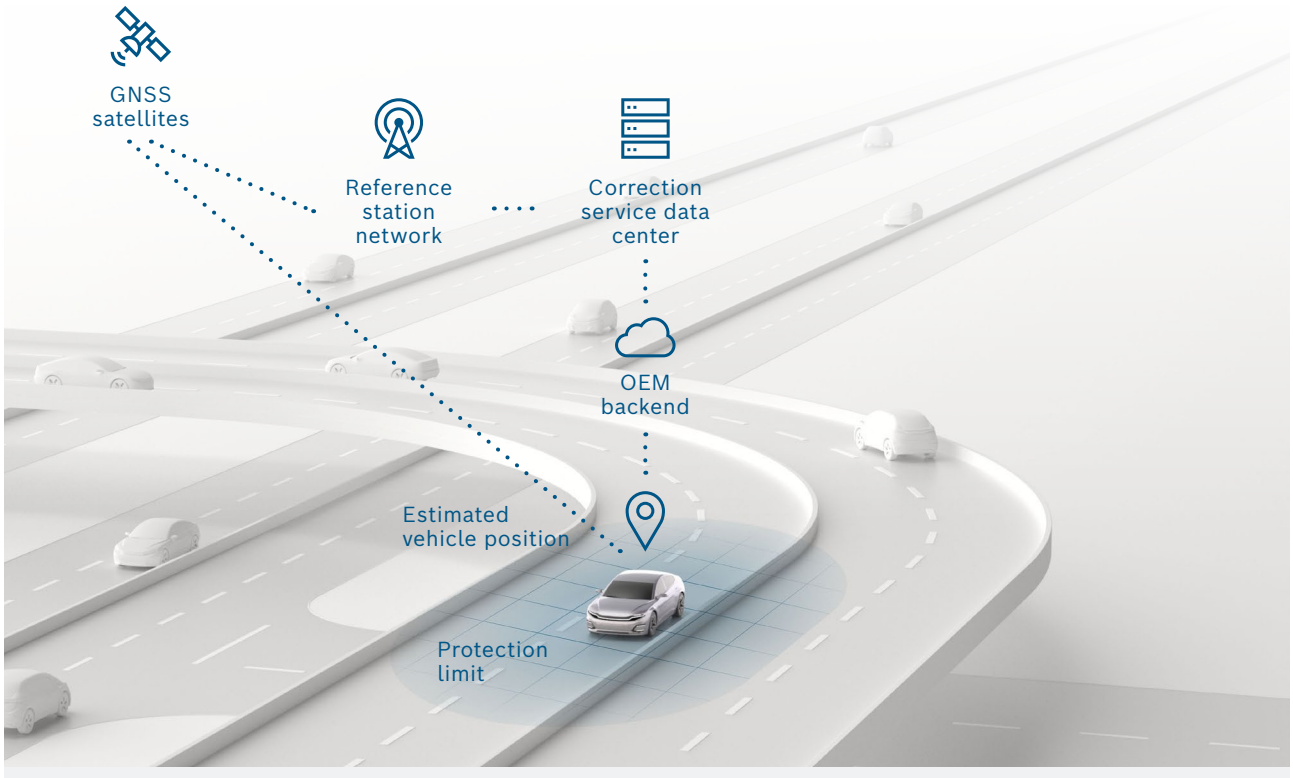


Figure 1: VMPS system design overview

Essential SOTIF relevant signals are the sensor fusion position and a corresponding protection level (PL) that is illustrated as a blue ellipse in Fig. 1. The PL is defined as a statistical upper bound error estimate for the positioning solution and thus reflects the localization uncertainty. Within the VMPS SOTIF concept, the protection level is in fact the most important input among others to rate the overall integrity status. Correction service integrity alerts or electronic/electrical (E/E) fault detections could likewise lead to an integrity loss but does not need to be linked to the PL in all cases. Instead, special integrity validity flags are introduced to convey the overall SOTIF status of the function in defined coordinate directions, e.g., along-track, across-track and up direction. These flags can further be used in combination with outputs of the functional safety monitoring and additional SOTIF monitoring to generate a holistic safety signal at the VMPS output. An outline of the cascade of SOTIF related VMPS output signals is depicted in Fig. 2. In total, there are three main quantities to reflect the positioning confidence: the estimated sensor fusion position accuracy, protection levels and integrity validity flags. A more detailed description of GNSS performance parameters including accuracy and integrity can for instance be found at the European Space Agency's (ESA) [2].

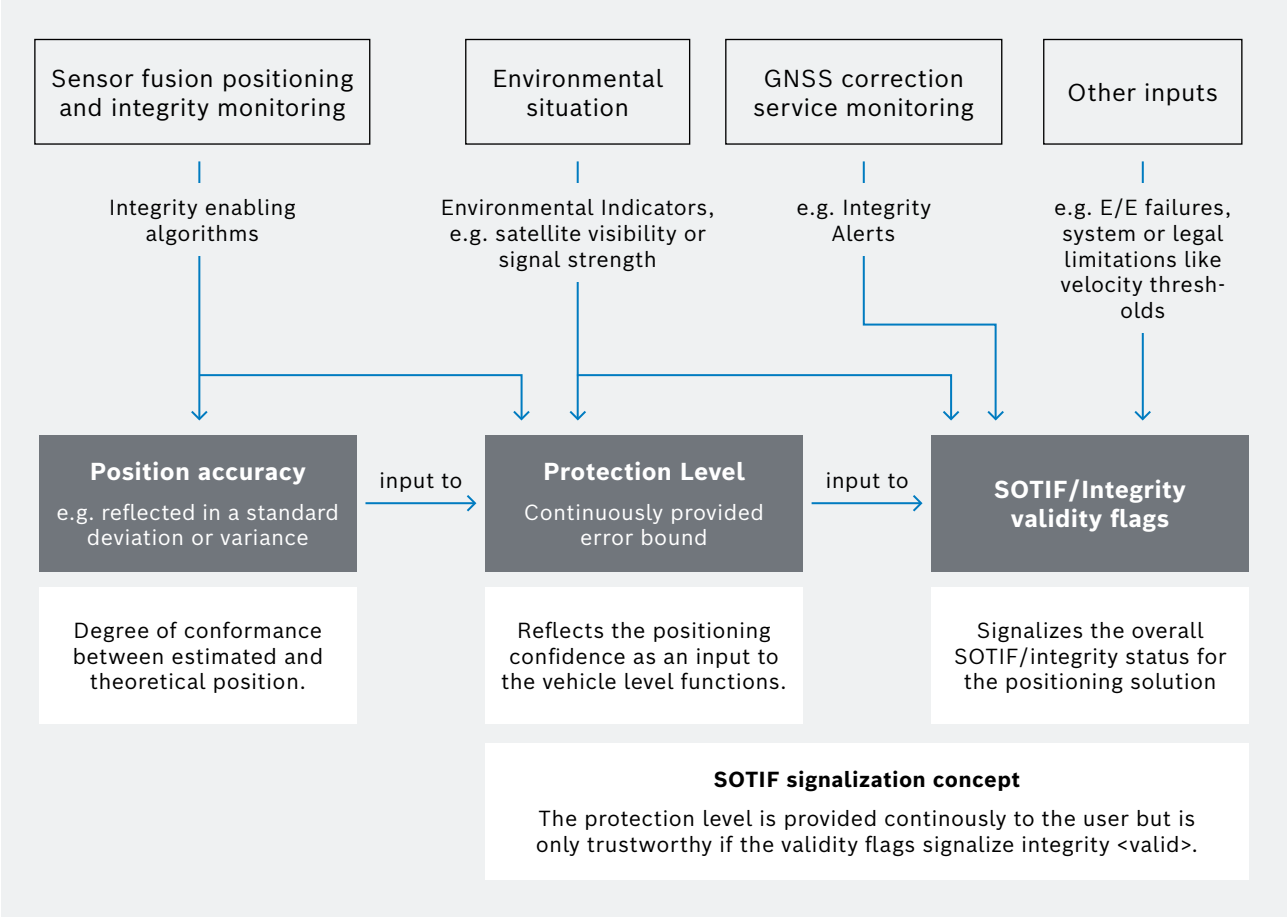


Figure 2: Cascade of essential SOTIF related VMPS output signals

[2] ESA, https://gssc.esa.int/navipedia/index.php/GNSS_Performances

SOTIF activities aim for evidence to argue freedom of unreasonable risk due to hazards resulting from functional insufficiencies of the intended functionality or its implementation[3] which, in case of VMPS, applies to the sensor fusion positioning. That means, the safety-related property is the positioning accuracy of the sensor fusion. The hazardous or unsafe behavior is an undetected positioning error (PE) that exceeds a specified safety critical threshold, the so-called Alert Limit (AL). The alert limit depends to a great extent on the use-case and customer needs. The minimum set of typical and essential SOTIF requirements for VMPS can be summarized as follows (the definitions are adapted from ESA[4]):

Alert Limit (AL):
The position error tolerance not to be exceeded without signalizing the loss of integrity or SOTIF, respectively, at the VMPS output.

Time-to-Alert (TTA):
The maximum allowable time elapsed from the occurrence of an integrity loss until signalizing it, e.g., via the integrity validity flags.

Target Integrity Risk (TIR):
The TIR is expressed as a probability (dimensionless) or as a probability per unit of time (commonly hour) and specifies the probability of the PE exceeding the AL without signalizing the loss of integrity within TTA. TIR describes the target rate and is typically specified by the customer whereas the term Hazardously Misleading Information (HMI) rate is used with respect to the corresponding VMPS validation result.

Integrity-Availability:
Integrity-availability is the percentage of time that the services of the system are usable by the user, i.e., in the VMPS context that a safe and reliable positioning output is available. It is a function of both the physical characteristics of the environment and the technical capabilities of the VMPS system.

The specification of these parameters depends on many SOTIF-related conditions, constraints, and limitations, for instance the defined Operational Design Domain (ODD), customer use-case for which the VMPS position shall be used and the vehicle level functional design. For a highway application that requires lane accurate localization an exemplary parameter set defined by the customer, typically the car manufacturer responsible for the functional design on vehicle level, could be a TIR at the order of $1e^{-4}$/h to $1e^{-6}$/h, AL of 2-4m and TTA of 5-10s. Such parameter set defines the basis for all further SOTIF activities like the analysis of triggering conditions and development of a SOTIF concept and strategy.

[3] ISO 21448:2022, https://www.iso.org/standard/77490.html

[4] ESA, https://gssc.esa.int/navipedia/index.php/Integrity

03
Triggering conditions and SOTIF validation strategy

To systematically document and analyze triggering conditions, positioning error sources are classified based on their origin, effect, or even propagation path. Triggering conditions that impact the VMPS positioning solution are manifold and only a subset with focus on GNSS error sources are shown in Fig. 3. In this example, the error classification is carried out by separating Signal-In-Space (SIS) and atmospheric propagation errors (blue band), i.e., mostly user position independent error sources on the one hand, and near-field environmental or user instrumental errors on the other hand.

SIS and atmospheric propagation errors include malfunctioning behavior of the satellite and its instruments or signal delays in the Earth's atmosphere. Both can mostly be compensated by the correction service either by the correction data itself or, in case of severe events, by issuing an integrity alert. Handling environmental impacts is an essential part of the VMPS sensor fusion and integrity concepts. SIS, atmospheric propagation errors, environmental and user instrumental errors, are then further decomposed into subclasses. A few examples like satellite orbit and clock, atmosphere, multipath, antenna,

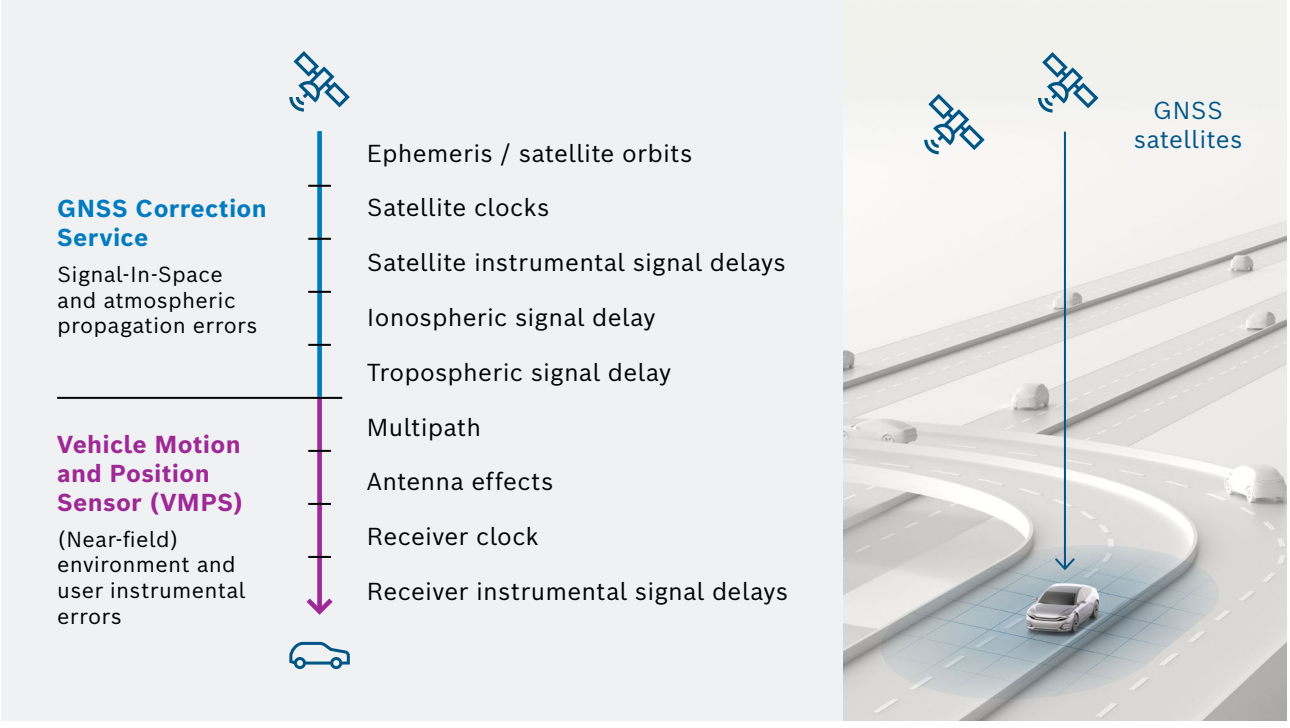


Figure 3: Overview of main GNSS error sources along signal transmission path

receiver, and instrumental signal delays at the satellite and receiver are depicted in Fig. 3. It shall be noted that a triggering condition is often connected to a combination of certain situational conditions, e.g., weather, geographical location, satellite constellation geometry, road surface, vegetation, etc. and due to the complexity, a further detailing is not shown here. Instead, a selection of VMPS examples in relation to the SOTIF cause-effect chain (adapted from ISO 21448[5]) is shown in Fig. 4 and Table 1, respectively. It shall be noted that ISO 21448 also depicts the inability to prevent an indirect misuse, i.e., usage in a way not intended by the manufacturer or the service provider, as part of the SOTIF cause effect chain. Misuse has been intentionally omitted here as the topic exceeds the scope of this article.

Term*	Triggering condition[6]	activates →	Functional insufficiency on element level[7]	results in →	Output insufficiency[7]	contributes to →	Hazardous behaviour on vehicle level
Definition*	Specific conditions of a scenario that serve as an initiator for a subsequent system reaction contributing to a hazardous behavior (...)		Insufficiency of specification or performance insufficiency, i.e., limitation of the technical capability contributing to a hazardous behavior (...) when activated by one or more triggering conditions.		An output insufficiency, either by itself or in combination with one or more output insufficiencies of other elements, contributes to either a hazardous behavior at the vehicle level (...)		
Selected VMPS examples	Environmental conditions causing GNSS signal quality degradations Atmospheric irregularities like ionosphere storms causing signal delays and interruptions Unannounced satellite orbit maneuvers causing inconsistencies with the assumed origin of the transmitting antenna		VMPS sensor fusion algorithm is not able to reflect insufficiencies via the accuracy estimation Inability to calculate the PL correctly (PL does not bound the resulting positioning error) and/or inability to not react in time under certain conditions Inappropriate fault detection, error handling and mitigation reaction by VMPS		HMI event: PE exceeds AL while VMPS does not signalize the integrity loss, e.g., via PL and/or integrity validity flags		

*according to ISO 2144

Figure 4: VMPS examples in relation to SOTIF cause-effect chain, based on ISO 21448 terms and definitions

[5] ISO 21448:2022, https://www.iso.org/standard/77490.html, Section 3.8, Figure 3b – Terms and definitions

[6] ISO 21448:2022, https://www.iso.org/standard/77490.html, Section 3.30

[7] ISO 21448:2022, https://www.iso.org/standard/77490.html, Section 3.8

Scenarios containing potential triggering conditions as well as potential triggering conditions are collected in the so-called validation catalogue (VC). The VC elements are derived for instance from the previously described classification of positioning error sources, customer requirements, ODD definition and use-case, system design, experience or even historical events, i.e., incidents that were observed in the past for instance by other navigation systems or comparable products. The VC lists all triggering conditions intended to be validated and analyzed and thus the starting point for the SOTIF V&V (Verification and Validation) activities. The VC is a living document that is frequently reviewed and iteratively updated throughout the development and SOTIF analysis cycle of the project. Every VC entry is then labeled as a nominal or exceptional event or scenario, depending on its occurrence probability:

Nominal Events/Scenarios:
All effects and behaviors that are expected to occur during a sufficiently large number of test drive hours are specified as nominal, i.e., systematic effects or periodic errors with an occurrence rate of $\geq 1e^{-2}$/h under the assumption that more than 1000 hours (at least an order of magnitude more data compared to the targeted error occurrence rate) of statistically representative test drives are evaluated. Representative means sufficiently diverse regarding scenarios and conditions regarding the specified ODD and use-case. Generally, all events which could be assessed by means of test drives are preferably also tested via test drives since the real-world behavior including interfaces and communication paths, vehicle design, chassis and mounting issues etc. is reflected in the data.

Exceptional Events/Scenarios:
All effects and behaviors expected with an occurrence probability $<1e^{-2}$/h for the specified ODD and use-case. Exceptional events are typically not covered by the given empirical test drive data basis, i.e., analytical methods or simulations become necessary.

In a next step, an adequate validation setup is allocated for each VC entry. A validation setup could be the vehicle, Hardware-in-the-Loop (HIL), Model-in-the-Loop (MIL) or even analytical methods like FTA.

Validation pillars

The VMPS SOTIF validation strategy is mainly based on the three so-called validation pillars:

The Test drive validation supports the validation of nominal events

(Monte-Carlo) simulation-based validation via MIL or HIL supports the validation of both nominal and exceptional events.

The FTA focuses on the analysis of exceptional events.

The method is summarized in Fig. 5. After collecting all triggering conditions in the VC, the validation activities on the selected platform are started. Every validation pillar aims to determine an HMI rate and an integrity-availability, both being mostly complementary due to the different focus on nominal and exceptional conditions. The FTA tool and method is not intended for availability analysis and thus only

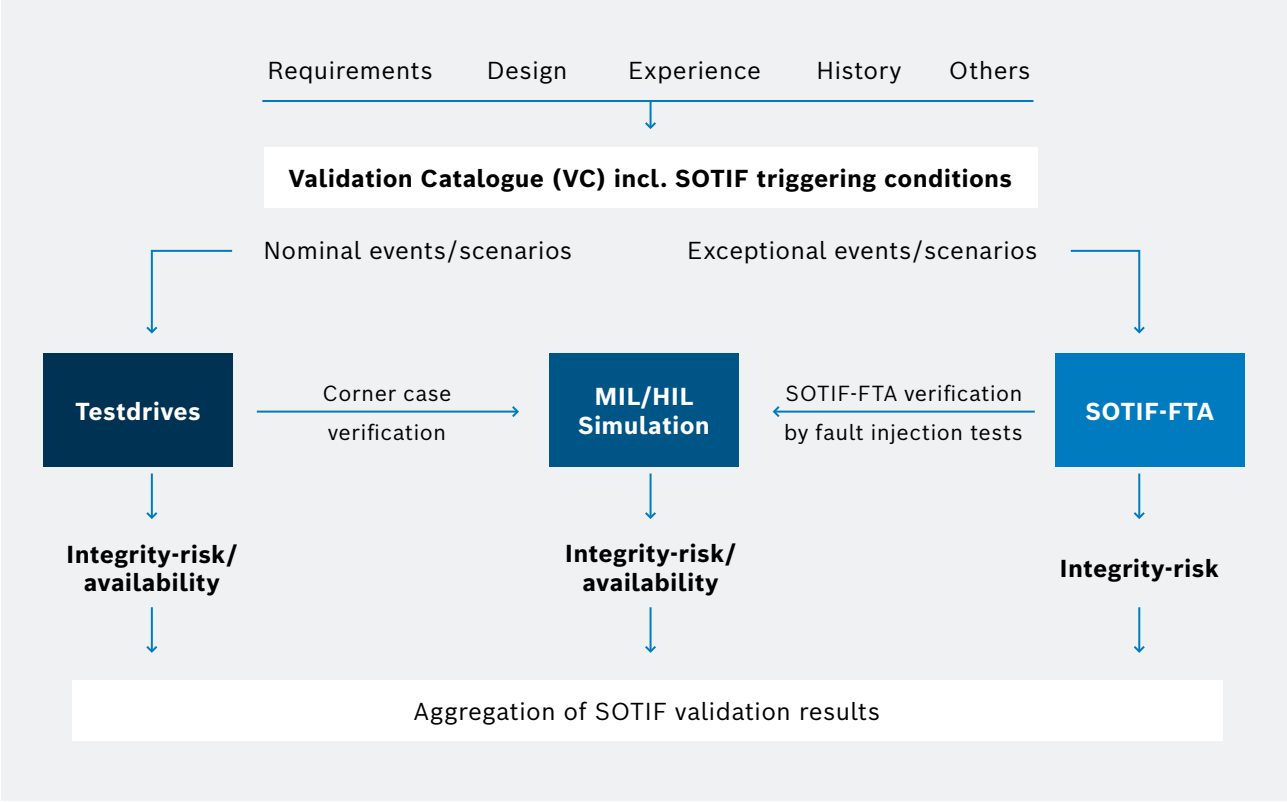


Figure 5: Flowchart outlining the essential steps of the SOTIF validation strategy and validation pillars

targets an HMI estimation. The evaluation of both HMI and integrity-availability as part of the SOTIF strategy is a very important aspect as SOTIF or safety mechanisms often tend to compromise integrity-availability ("The safest system is a non-available system") often driven by customer needs.

It shall further be noted that each validation pillar contains aspects of the SOTIF analysis related to both Area 2 (known, hazardous events and scenarios[8]) and Area 3 (unknown, hazardous events and scenarios[9]) and a clear separation is not pursued. Aspects that are covered in each validation pillar are for instance:

- → Statistical validation on large diverse datasets
- → Scenario-, event- and corner-case-oriented validation
- → Validation of sensor performance variations
- → System design verification
- → Sensitivity testing
- → etc.

In a last step, the results are aggregated into an overall HMI rate and integrity-availability that is considered in the VMPS SOTIF release argumentation. In the upcoming sections, the three SOTIF validation pillars and the SOTIF release are described in more detail.

[8] ISO 21448:2022, https://www.iso.org/standard/77490.html, Chapter 10

[9] ISO 21448:2022, https://www.iso.org/standard/77490.html, Chapter 11

3.1 Test drive-based validation

The test drive based SOTIF release aims at validating and releasing the integrity requirements based on real test drives. The specified TIR would theoretically require a much higher amount of data than the feasible amount of data that can be collected throughout a product development phase. For example, to validate a TIR of $1e^{-5}$/h empirically, significantly more than 100,000 hours of test drive data could be requested to apply common descriptive approaches. To overcome this issue, statistical forecasting methods can be applied to predict the sensor behavior based on a limited data set. Three crucial points need to be considered:

- The limited test drive data set is representative for the statistical behavior of the sensor
- The statistical forecasting methods are chosen appropriately being compatible with the system behavior
- Any remaining subcritical event, i.e., position error that appears as a statistical outlier even though not exceeding the AL, is thoroughly analyzed, and can be argued as safe with respect to the defined integrity requirements.

Fig. 6 illustrates the three major steps building up the test drive based SOTIF validation consisting of a) the selection of driving scenarios and maneuvers, b) data evaluation with focus on the sensor fusion position error and protection level behavior and finally c) the statistical HMI probability forecasting under consideration of specified integrity parameters like the AL and the TTA.

Figure 6: Major steps along the test drive based SOTIF validation

Test drive database and evaluation

A test vehicle equipped with the VMPS sensor as well as a significantly more precise (and more expensive) reference system is used to record the data. Driving scenarios and amount of data are defined beforehand to ensure a diverse and representative test coverage. The data is evaluated by comparing the VMPS positioning solution to the trajectory determined by the reference system, considered as the ground truth. To ensure the representativity of the data set, different aspects need to be considered. For instance, the integrity-relevant behavior of the test vehicle and in particular the positioning performance shall be close to the target system, e.g., the series vehicle for which the VMPS shall be released. This includes components not directly being part of the VMPS but impacting VMPS SOTIF. Examples are the GNSS antenna type and design, mounting positions of antenna and sensor, GNSS correction data quality or software. Furthermore, the ground truth information shall be, based on a rule of thumb, at least ten times more accurate as the accuracy level of the VMPS.

Vehicle motion and position sensor

Highly accurate absolute and relative vehicle positioning based on the global navigation satellite system (GNSS) and inertial sensors

10 cm	Absolute position (lat/long @1sigma)
ASIL B	Safety level
10^{-5}/h	Target integrity risk with 3m alert limit

https://www.bosch-mobility.com/en/solutions/sensors/vehicle-motion-and-position-sensor/

Test drive integrity validations focus on nominal conditions and corner cases that are initially known or have already been identified during the project development cycle. Another criterion for the selection of test drive maneuvers is the technical feasibility, e.g., on proving grounds. For an appropriate maneuver planning and test coverage, the driving scenarios are therefore collected in two databases:

Special scenario database:
Scenarios that include known corner cases (e.g., aqua planning, emergency breaking) as well as special vehicle setups (e.g., driving with a roof box or trailer) are defined and driven to account for conditions affecting different SOTIF relevant elements of the VMPS such as the GNSS signal reception behavior.

Statistical representativity database:
To be able to define a statistically representative data base, a representative variation of scenarios including but not limited to weather, traffic, and environmental conditions, as well as street types and trajectories, must be provided in the dataset. Additionally, depending on the specified TIR and the expected nominal performance of the system, a minimum amount of data is required to ensure sufficient confidence of the forecast estimate. Any remaining subcritical event, i.e., position error that appears as a statistical outlier even though not exceeding the AL, is thoroughly analyzed, and can be argued as safe with respect to the defined integrity requirements.

Statistical forecasting

After gathering the data and evaluating it with respect to the reference trajectory, a statistical forecasting approach based on the extreme value theory is used to fit a probability density function (PDF) to the data. In the next step, the fitted PDF is used to calculate the HMI probability by means of numerical integration.

Using this model, the so-called subcritical events are identified as statistical outliers, which can contribute significantly to an increase of the HMI probability. In a final validation step, these events are analyzed in detail to derive an argument for achieving SOTIF. A reasoning for the safe argumentation can be made by analyzing issues from different perspectives. Some examples are depicted in Fig. 7.

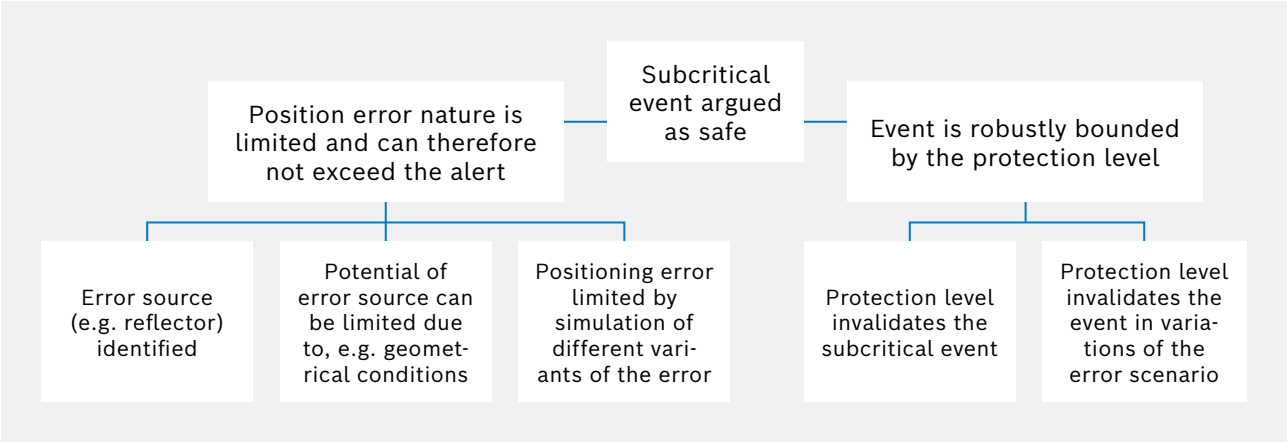


Figure 7: Safe argumentation of subcritical events

One example for an expectable and very dominant GNSS error source is multipath, i.e., GNSS signal reflections at environmental obstacles like buildings, vegetation or traffic inducing signal delays. Large position errors resulting from multipath can be analyzed with regards to the error envelopes of multipath. A GNSS observation error caused by multipath is limited by the scenario conditions influenced through the existing signal reflectors and the dynamics of the vehicle. To verify this assumption, the possible impact of a measurement error due to multipath on the sensor fusion solution can be analyzed using simulations. Supported by simulations of comparable scenarios it can thus be argued that the error cannot exceed the safety critical position error threshold in this scenario or a comparable one. Another option is to analyze the behavior of different integrity monitors or, e.g., the protection level calculation, to observe the reaction of these monitors with respect to the error sources in a certain scenario. The sensitivity of the monitoring can then be used to argue the VMPS multipath detection and mitigation capability.

Hence, by making sure that all known relevant and important scenarios are covered within this test and by analyzing the statistical behavior of the recorded data regarding the TIR, a forecast of the expected probability of HMI occurrence and integrity-availability is determined. Subcritical events that emerge from this statistical analysis as outliers are analyzed in detail to derive an argumentation for the absence of unreasonable safety risk.

3.2 Monte-Carlo based simulations

Monte-Carlo (MC) method-based Model-in-the-Loop (MiL) simulations are carried out to verify the system integrity covering for instance the following GNSS-related scenarios:

- GNSS and/or Correction data loss
- Challenging GNSS denied environment, i.e., degraded visibility conditions and multipath
- Correction data quality variations

Worst case driving scenarios are for instance derived from previous test drives or experience and are often characterized by high driving dynamics with challenging environmental conditions. Such scenarios are combined with Monte-Carlo method-based parameter variations. The approach will now be described in more detail.

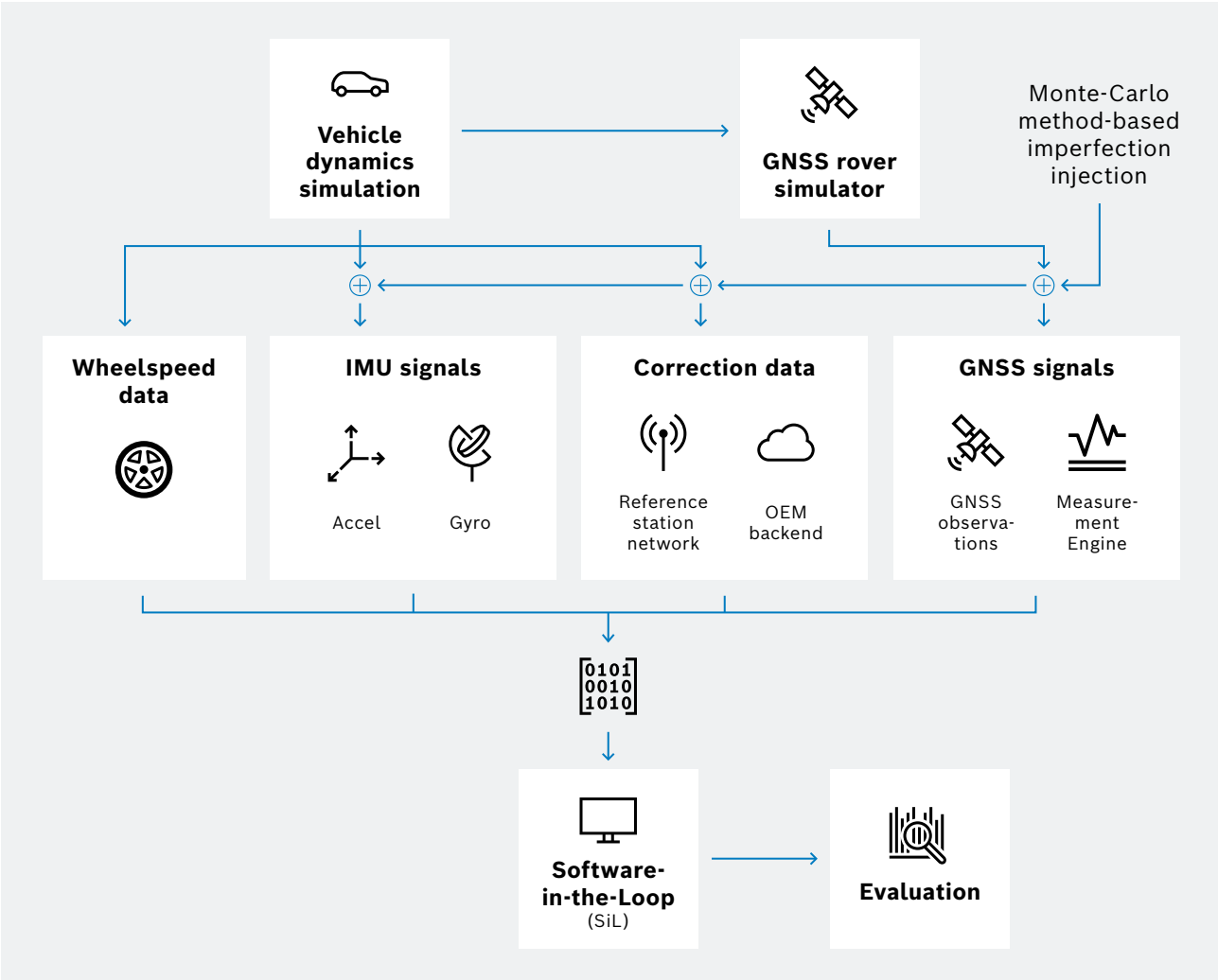


Figure 8: Model-in-the-Loop simulation environment

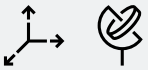
Simulation environment

A draft of the MiL simulation environment is shown in Fig. 8. Worst case driving scenarios are simulated using a vehicle dynamics simulation environment. To simulate the challenging environmental conditions in terms of GNSS, configurable synthetic observations are modelled via a so-called GNSS rover simulator. Monte-Carlo method-based imperfections can be injected onto IMU signals, correction data and GNSS signals based on the outputs of vehicle dynamics simulation environment and the GNSS rover simulator. The simulated data is processed using a Software-in-the-Loop environment based on the software to be released. The outputs of the software under test are finally evaluated against requirements where, e.g., the variation of the position error and sensitivity of the integrity parameters is analyzed.

Monte-Carlo method imperfection injection

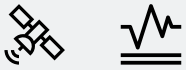
The output of the software under test is influenced by its inputs in a complex manner which does not allow to predict in advance which combination of imperfections in the measured inputs challenges the algorithm most. For this reason, a Monte-Carlo method-based simulation approach is chosen to apply the different imperfections onto the inputs of the algorithm. The idea to ensure the integrity of a complex system with this method is that the number of simulation-runs, each one with a different set of modified input parameters, is chosen large enough so that the worst-case combination of imperfections of the inputs is identified and covered with a high probability. Thus, the response of the system can be investigated under the most challenging conditions without knowing them in full detail in advance. The ranges of the different imperfections in the inputs can for instance be obtained according to statistical distributions measured in characterizations of the individual input systems.

The three components with the strongest influence on the output of the software under test are the IMU, the GNSS correction data and the raw GNSS observations as output of the GNSS receiver, all in combination with corresponding quality information.



IMU:
The inertial measurement unit consists of accelerometers and yaw rate sensors. The sensors are characterized in the lab to obtain the different possible values of the imperfections like noise or offset. The results are fitted with the appropriate distribution function to obtain its characteristic values, e.g., mean or variance. For each run of the simulation a set of imperfections of the IMU are obtained by calculating a possible realization of the imperfections according to the likelihood given by the corresponding statistic. These imperfections are added to the signals simulated with the vehicle dynamic simulation.

Correction data:
According to the specification and characterization of the correction data provided by the correction data supplier an appropriate distribution of imperfections is chosen. Similar as for the IMU, signal imperfections in each run are obtained according to the statistical likelihood. The different imperfections are then added to the correction data before they are sent to the Software-in-the-Loop environment.



GNSS:
The GNSS measurement accuracy and quality can be deteriorated by environment, e.g., due to multipath. The measurement and the corresponding quality information are altered with a Monte-Carlo method-based simulation approach to take these influences on the software into account. The statistics of the measured GNSS inaccuracies are investigated and characteristic values for the distributions for a configurable number of elevation-dependent classes are derived. The imperfections of the GNSS observations are modeled with a stationary Gauss-Markov process including the influence on the signal strength and the quality information. As for the case of the IMU and correction data, for each run of the simulation a set of input parameters for the Gauss-Markov process are calculated. These imperfections are added to the synthetic observation calculated beforehand.

Using this method of Monte-Carlo method imperfection injection, various worst case driving scenarios and challenging environmental conditions are combined with numerous imperfection variations. For each set of simulations, the system behavior and its sensitivity are verified against the SOTIF requirements. Finally, a conclusion regarding integrity risk and integrity-availability is drawn.

3.3 SOTIF-FTA verified by fault injections

The FTA method is considered as a top-down, deductive approach to analyze signal error propagations through the VMPS system, supporting the functional development and is a key element to analyze the system impact of exceptional events. The method is established but has been adapted to the VMPS SOTIF needs and therefore it is hereinafter abbreviated with SOTIF-FTA. The essential validation steps are described in Fig. 9 and will be explained in the following.

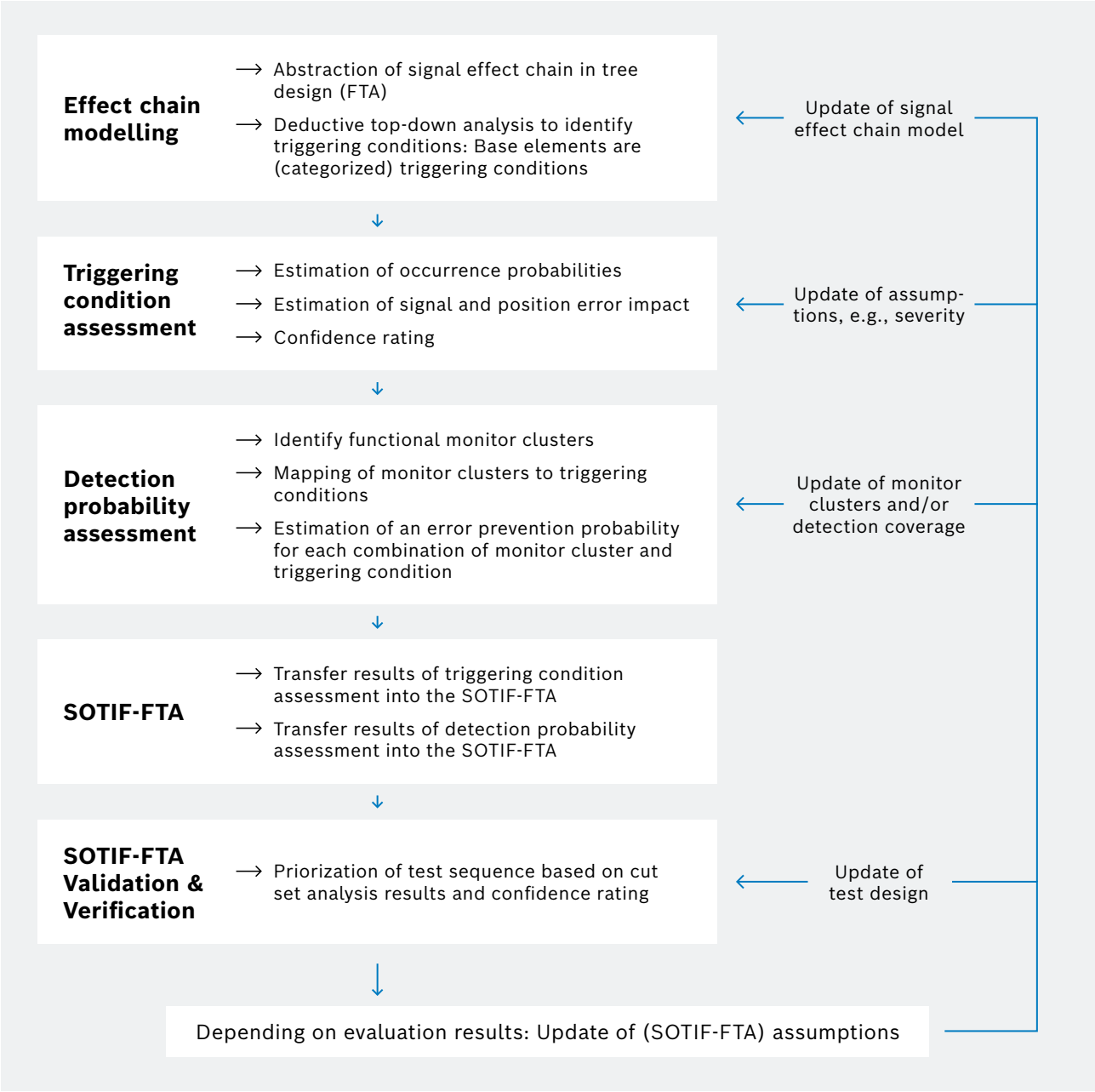


Figure 9: Essential steps in the iterative SOTIF-FTA approach

Effect chain modeling

Starting point is the SOTIF-FTA top event defined as an HMI of the VMPS sensor fusion position. The SOTIF-FTA design orients on the functional signal effect chain using a decomposition into different branches, e.g., accounting for sensor fusion, loss of GNSS reception (dead reckoning) and single, multi- and constellation wide GNSS faults. A draft of the SOTIF-FTA design structure is shown in Fig. 10. Only the GNSS related branches are shown but IMU and WSS signal branches are considered as well.

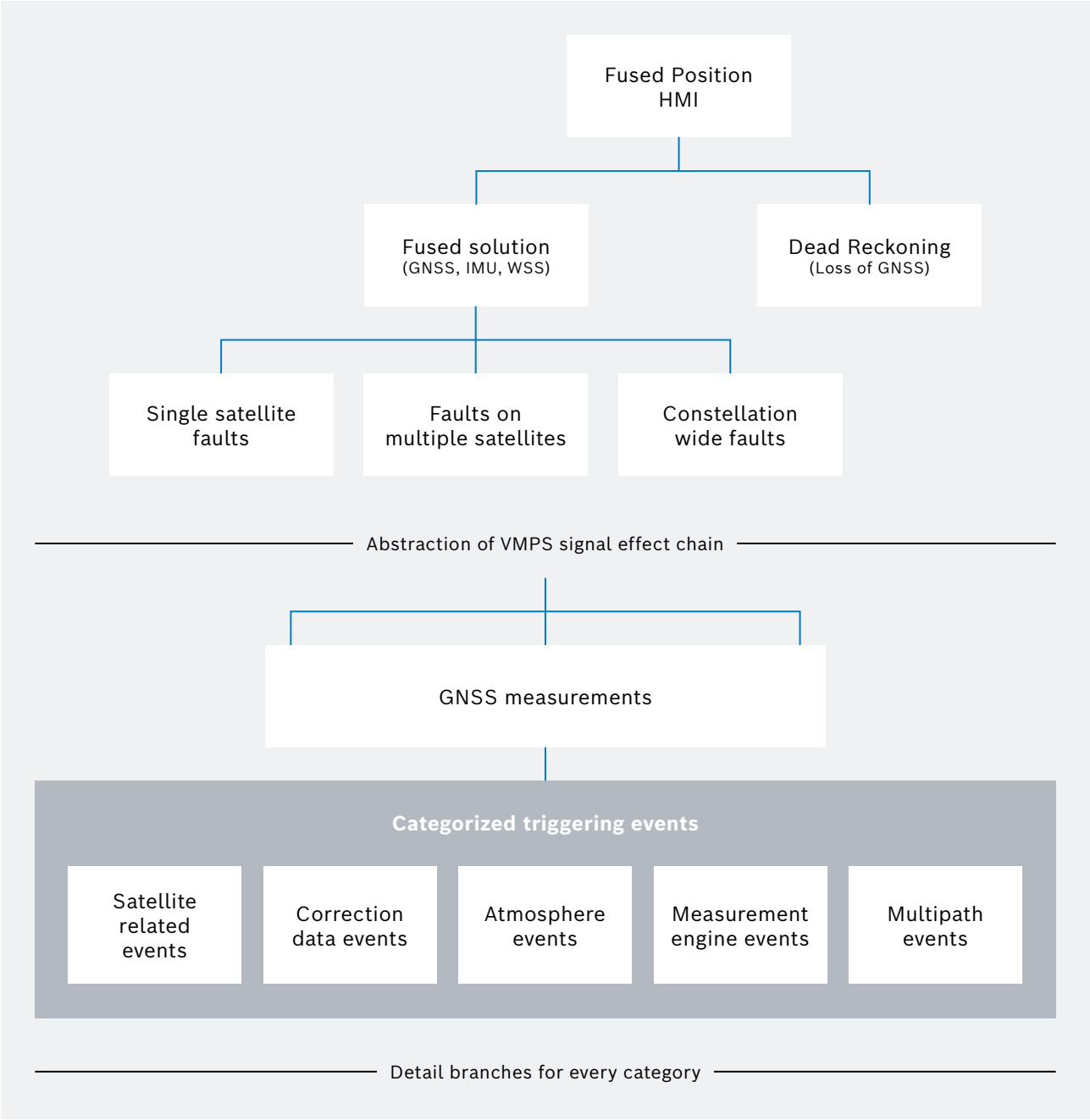


Figure 10: SOTIF-FTA design structure

Triggering condition assessment

Exceptional triggering conditions are assessed and quantitatively rated within a SOTIF triggering condition assessment. An important input source is the VC. The triggering condition assessment contains a subset of the VC though the scope of both documents differs significantly: The VC targets for a suitable mapping of triggering conditions to validation platforms whereas the triggering condition assessment aims for a quantitative rating of the potential risk caused by each triggering condition. It shall be noted that the triggering condition assessment orients on functional safety methods by applying, e.g., an exposure and severity rating for each triggering condition. Additionally, a confidence rating has been introduced to reflect how trustworthy the information and rating is. For instance, ionospheric irregularities are highly depending on solar activity and an occurrence rate has been derived by analyzing time series of geomagnetic indices and historical events. Due to the complex geophysical processes and phenomena behind this triggering condition, a reliable exposure rating is almost impossible and thus the confidence rating could be set low, increasing the need for further verification measures. The outcome of the triggering condition assessment is finally a list of characterized exceptional events, e.g., with exposure and confidence rating.

Detection probability assessment

Target of the so-called detection probability assessment is the determination of monitor clusters and allocation of a detection probability value for every cluster with respect to triggering conditions. A cluster describes a collection of integrity monitoring mechanisms or countermeasures against feared events aiming to prevent a specific triggering condition from causing an output insufficiency that could potentially lead to an HMI. The method of using functional monitoring clusters facilitates the estimation of an error prevention probability per cluster regarding specific triggering conditions.

SOTIF-FTA

Finally, the output of the preceding activities is considered as input to create and design the actual SOTIF-FTA. The effect chain model defines the tree structure, base events are the triggering conditions quantitatively described with exposure information and for every triggering condition a detection probability is allocated using the output of the detection probability assessment. Result is a quantitative SOTIF-FTA that can be used for a SOTIF triggering conditions impact analysis.

SOTIF-FTA Validation and Verification

Base events of the SOTIF-FTA are exceptional triggering conditions where most information is either derived from expert rating, literature, oriented on considerations in other GNSS-related fields like avionics or using historical data. For many identified triggering conditions, a purely analytical assessment was not considered to be sufficient, reflected for instance in the confidence rating of the triggering condition assessment. A cut set analysis is carried out to identify the most critical paths, i.e., those events which primarily impact the top-event and potentially lead to an HMI in the sensor fusion position. Based on the confidence rating of the triggering condition assessment and the result of the SOTIF-FTA cut set analysis, the most critical triggering conditions are determined and prioritized for a further validation by means of simulated fault injection tests. Target of the fault injection tests is the stimulation of functional insufficiencies by injection of single or combined triggering conditions. The behavioral response of the VMPS is recorded and afterwards evaluated to confirm or modify the SOTIF-FTA assumptions.

The testing process is further grouped into a system qualification testing and software qualification testing part focusing on the one hand on blackbox testing of the system with pass/fail criteria derived from customer or system requirements and on the other hand on whitebox testing with pass/fail criteria oriented on the expected detection and error prevention capability of the system. The results are then evaluated to conclude, e.g., on the

- fault injection stimulation and functional response;
- sequence of fault occurrence, functional insufficiency, detection, and response time;
- validity of initial assumptions in the triggering condition and detection probability assessments;
- error symptomatic and characteristic like amplitude and growth over time.

The outcome is rated and discussed by experts and might lead to the confirmation or need for adjustment of the SOTIF-FTA assumptions. The steps depicted in Fig. 9 are carried out iteratively and finally lead to a quantitative HMI probability estimation reflected in the SOTIF-FTA top event considered as another input to the SOTIF release.

4
SOTIF Release

According to Fig. 5, the evaluation results out of the three pillars test drive-based validation, Monte-Carlo simulations and SOTIF-FTA, are considered in the overall SOTIF release to argue for the fulfilment of the clauses and objectives of the ISO 21448. The validation results and argumentations are documented and considered in the decision for approval (or rejection) of the SOTIF release in accordance with clause 12 “Evaluation of the achievement of the SOTIF” of the ISO 21448. Essential inputs to the rationale are the HMI probabilities and integrity-availability results.

The release documentation is separated into different SOTIF release documents where the most important ones are depicted in Fig. 11.

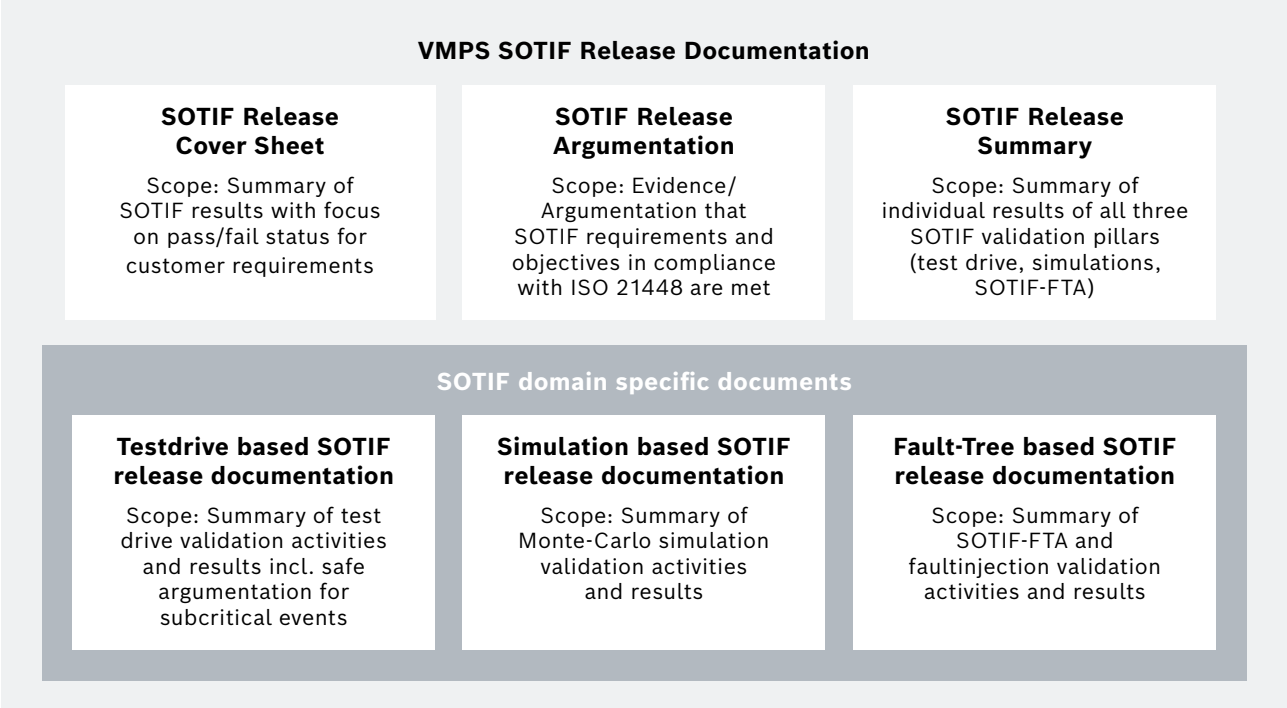


Figure 11: Example for a selection of essential SOTIF release documents

The SOTIF release cover sheet summarizes project related information, SOTIF constraints, boundary conditions and the approval or rejection decision for the SOTIF release. The SOTIF release argumentation contains responses and explanations to the objectives of the ISO 21448 with rationales and evidence why and how SOTIF for VMPS is approved. Finally, the SOTIF release summary is prepared to document the individual results of the different SOTIF validation pillars. The document landscape is completed by the domain specific documents related to the three validation pillars.

5
Summary

This article presents a systematic and structured SOTIF validation strategy. The approach was successfully applied in the series release of the VMPS, a precise and safe GNSS-based vehicle localization sensor developed at the Robert Bosch GmbH. The essential SOTIF validation activities are connected to test drive validations, Monte-Carlo simulations and Fault-Tree analysis supported by fault injection testing. In a collection of different SOTIF release documents, all activities are described, an argumentation for the achievement of the SOTIF in compliance to the ISO 21448 is provided and based on the collected results and evidence, a rationale and recommendation for approval (or rejection) of the SOTIF release is given.

Imprint

References:

[1] ISO 21448:2022

https://www.iso.org/standard/77490.html

[2] European Space Agency, Navipedia

https://gssc.esa.int/navipedia/index.php/GNSS_Performances

https://gssc.esa.int/navipedia/index.php/Integrity

Authors:

Robert Bosch GmbH
Cross-Domain Computing Solutions
Business Unit Driver Experience,
Engineering Localization

Imprint

Why Bosch?

In the future, automated vehicles will be on the road in ever increasing numbers. Precise and reliable vehicle localization is a key enabler for series introduction of safe, available and affordable automated driving.

Bosch offers a unique combination of hardware, software, and services for localization that forms a redundant system and meets the high requirements for the determination of the vehicle's position.

The vehicle motion and position sensor (VMPS) from Bosch plays a key role in this regard. It comprises high-performance satellite receivers, a correction service to enable GNSS positioning with high accuracy, inertial sensors and intelligent software for precise and reliable position calculation. With the profound knowledge regarding localization technologies Bosch contributes to the safe introduction of automated driving.

Contact us now

Do you have any questions, comments or business inquiries?

Please do not hesitate to get in touch.

Patrick Koestner

Cross-Domain Computing Solutions,
Product Manager for Localization and ADAS Market Intelligence

patrick.koestner@de.bosch.com

+49 711 811-47651

Learn more on our website
www.bosch-mobility.com

Bosch Mobility on LinkedIn
www.linkedin.com/showcase/bosch-mobility/

Robert Bosch GmbH
Robert-Bosch-Platz 1
70839 Gerlingen-Schillerhöhe,
Germany