Integrity Concept for the Safe Operation of the Swift Navigation Positioning System

DEBASHIS CHOWDHURY
SWIFT NAVIGATION

Integrity Concept for the Safe Operation of the Swift Navigation Positioning System

1. INTRODUCTION

1.1 Purpose

This document outlines the integrity concept and parameters as employed by Swift Navigation's positioning solution comprising of Starling® positioning engine and Skylark™ precise positioning service. The concept and terminology are derived from analogous concepts standardized in civil aviation industry[1].

The purpose of the integrity concept is to define a set of metrics and criteria from which safe operating conditions for Starling and Skylark can be derived.

1.2. Scope

The definitions are intended for safety-critical terrestrial applications like precise positioning of vehicles on a road and in constrained environments such as urban canyons, tunnels etc.

The integrity definitions from civil aviation industry are mapped to safety requirements for an overall Positioning system.

Based on the above, safety definitions are derived for Starling positioning engine as a safety element out-of-context, as per ISO 26262[4] standard.

2. POSITIONING PARAMETERS: ACCURACY, AVAILABILITY, CONTINUITY, INTEGRITY, TIME TO ALERT

The GNSS positions are defined in terms of the following parameters[2].

- **Accuracy:** GNSS position error **(PE)** is the difference between the estimated position and the actual position.
- **Availability:** The availability of a positioning system is defined as the ability to provide the required function and performance during the intended operation. The availability is characterized by the portion of time the system is to be used for navigation during which reliable position information is presented to integrated system.
- **Continuity:** The continuity of a system is the ability of the total system to perform its function without unscheduled interruption during the intended

operation. More specifically, continuity is the probability that the specified system performance will be maintained for the duration of a phase operation, presuming that the system was available at the beginning of that phase operation and was predicted to operate throughout the operation.

- **Integrity:** Integrity is a measure of the trust that can be placed in the correctness of the information supplied by the positioning engine. Integrity includes the ability of a system to provide timely and valid warnings to the user **(Alerts)** when the system must not be used for the intended operation. Integrity requirements are defined with four parameters:

    - **Integrity risk (P -int):** The integrity risk is the probability (per unit of time) of providing a position that is out of tolerance without warning the user within the time-to-alert.

    - **Alert limit (AL):** To ensure that the position error is acceptable, an alert limit is defined. It represents the largest position error allowable for a safe operation. The position error cannot exceed this alert limit without annunciation.

        - **The Horizontal Alert Limit (HAL)** is the radius of a circle in the horizontal plane, with its center being at the true position, that describes the region that is required to contain the indicated horizontal position with the required probability for a particular navigation mode.*

        - **The Vertical Alert Limit (VAL)** is half the length of a segment on the vertical axis, with its center being at the true position, that describes the region that is required to contain the indicated vertical position with the required probability for a particular navigation mode.

- **Time to Alert (TTA):** The TTA is the maximum allowable elapsed time from the onset of a positioning failure (position out of tolerance) until an alert is annunciated.

A fault-free positioning engine is assumed to provide position data with nominal accuracy and time-to-alert performance. Such an engine is assumed to have no failures that affect the accuracy, continuity, availability and integrity.
Integrity Failure is an integrity event that lasts for longer than the TTA and with no alarm raised within the TTA.

* HAL may be further split 'along track' and 'across track' for terrestrial/rover applications.

3. POSITIONING SYSTEM: SAFETY REQUIREMENTS

In this section, the safety requirements are derived from the integrity parameters described in the previous section, for an entire navigation system, as per the safety definitions in the ISO 26262 standard[4].

The system here consists of all components in a navigation system and illustrated

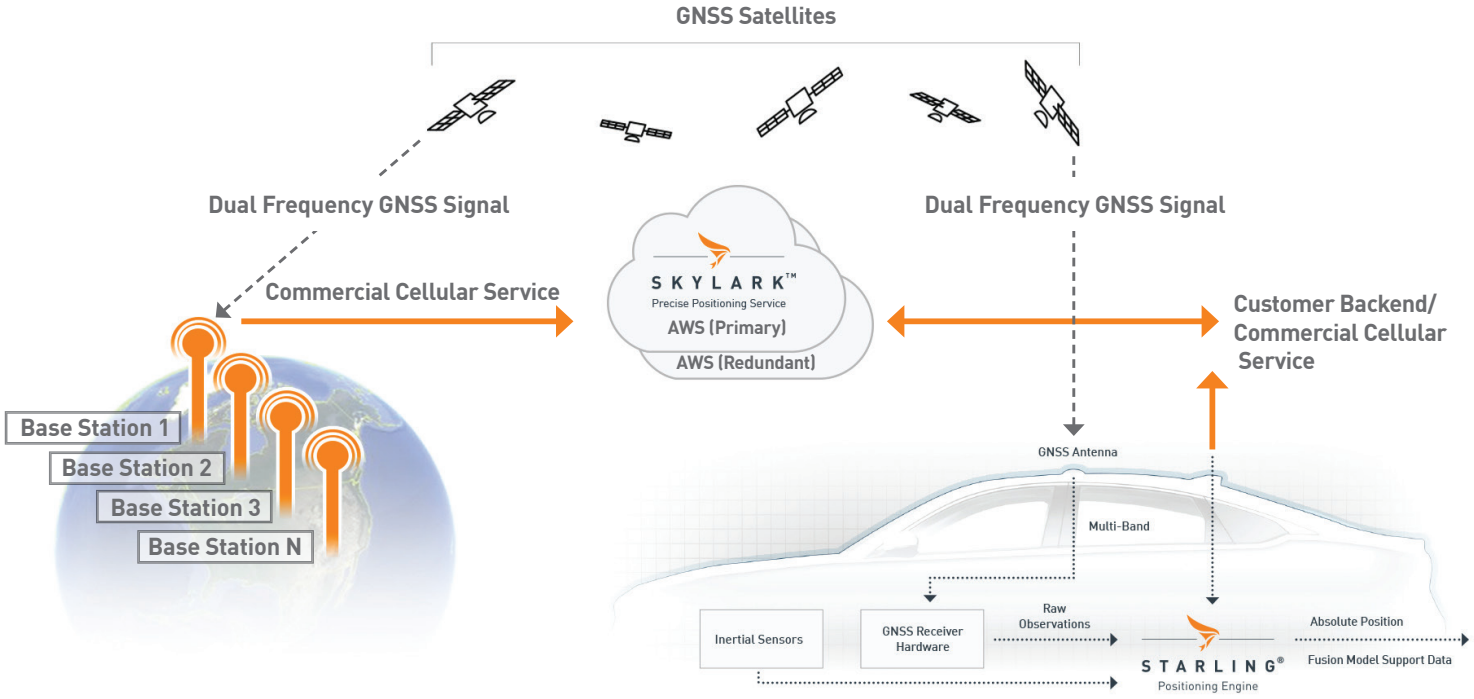

Fig. 1: Swift Navigation's positioning system concept

3.1 Safe Operation: Position Error, Alert Limit, Integrity Risk

A safe operation of a positioning system as in Fig. 1, is derived based on the parameters defined in Section 2.

- A Positioning failure is said to occur whenever the difference, PE, between the true position and the indicated position exceeds the applicable alert limit. That is,
  PE > AL

- A safe operation is thus defined as,
  PE < AL

- Probabilistic measure for a safe operation for a system, is,
  P(PE > AL) < P-int

3.2 Safety Method: Protection Limit

A positioning system maintains the integrity and safety of the GNSS navigation solution by the following **method**. For each position, since the actual PE is unknown, the positioning system computes a Protection Limit **(PL)**, which is a measure of its confidence in the positioning output. The PL is a statistical error bound computed so as to guarantee that the probability of the absolute position error exceeding the said number is smaller than or equal to the target integrity risk. An operation is deemed safe for a system when,

PL < AL, where AL is the uppermost bound of PL for safety.

Fig. 2 below shows **deemed safe** operation where horizontal and vertical **PLs < ALs**, and the green cylinder lies within the red cylinder. In aviation, this is called system availability.

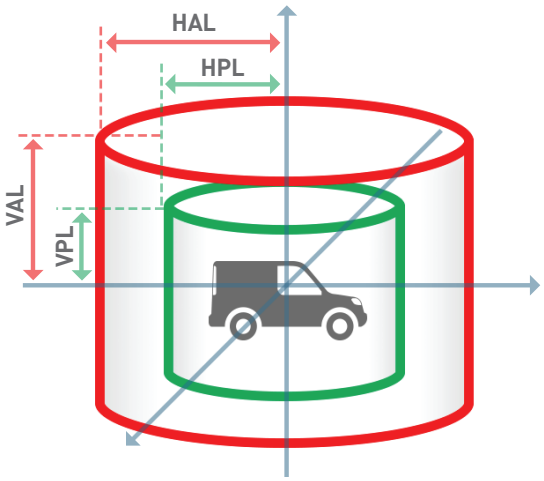

Fig. 2: Deemed Safe operation of a Positioning system

Fig. 3 below shows **deemed unsafe** operation where horizontal and vertical **PLs > ALs,** and the green cylinder lies outside the red cylinder. In aviation, this is called system unavailability.

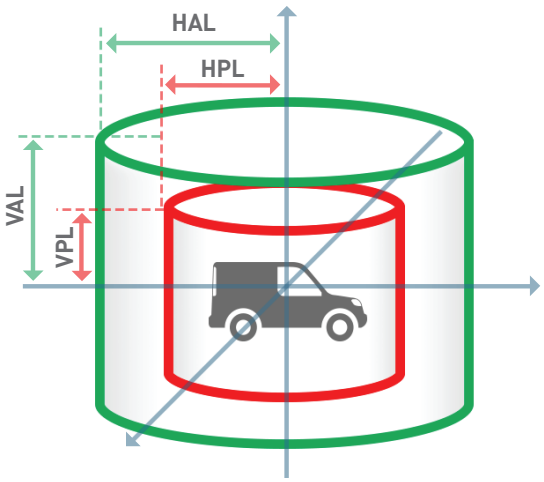

Fig. 3: Deemed Unsafe operation of Positioning system

Here, the AL is a specified limit set by the application/system and the PL is calculated for each positioning output. Since the real position error is not observable, the decision by the system to accept the positioning solution as within tolerance and raising an alert when deemed unsafe, is done by comparing the AL specified and the PL calculated, more precisely:

- If **PL > AL**, the alert triggers
- If **PL < AL**, the alert does not trigger

3.3 Positioning Failure and Safe State of a System

If a positioning failure happens as indicated by PL > AL and an alert is triggered within TTA, the positioning system is intended to reach a safe state. A safe state in the scope of ISO 26262 is defined as operating mode of an item without an unreasonable level of risk. That means the item does not show any of the already identified unintended functions that are able to lead to an identified hazardous event. Safe state thus guarantees avoidance of a potentially hazardous situation.

3.4 Relationship Between Integrity Parameters and Events

Fig. 4 below shows the relationship between Integrity Parameters and Integrity Events[3].

Misleading Information (MI) is an integrity event occurring when, the system being declared safe (and available), the position error exceeds the protection level but not the alert limit.

Hazardously Misleading Information (HMI) is an integrity event occurring when, the system being declared safe (and available), the position error exceeds the alert limit.

These are potential hazard conditions to be tested/verified for system safety compliance.

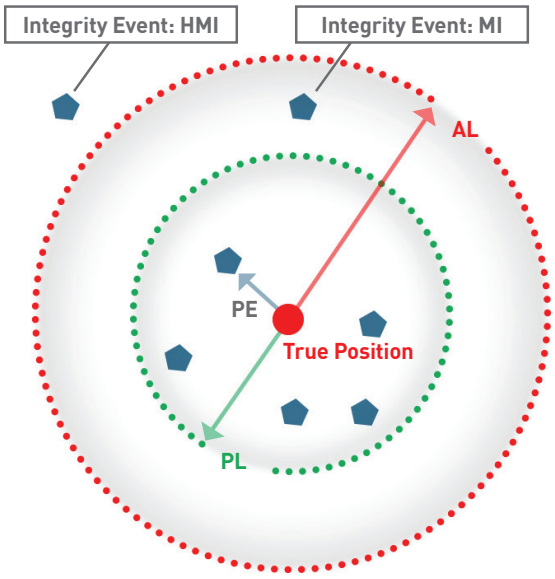

Fig. 4: Integrity Parameters and Events

4. STARLING SAFETY REQUIREMENTS: SAFETY ELEMENT OUT OF CONTEXT

Starling safety requirements are derived from overall positioning system safety requirements. Currently Starling is designed and implemented as a software Safety Element Out of Context (SEooC) as per ISO 26262 standard[4]. Therefore its safety requirements are defined and measured as a self-contained software application that will be integrated into a user's navigation system.

4.1 System-Level Assumptions/Dependencies for Starling

As noted earlier, the AL is specified/controlled by the application/navigation system and the PL is calculated by the Starling positioning engine. Starling being SEooC, is customizable to meet system level AL's and TTA's of multiple navigation systems.

Starling therefore makes its safety decisions based on its computed PL. It provides an accurate and timely estimation of the current PL to meet a given TIR (for example, TIR for Starling is $1e^{-7}$/hr for automotive solutions).

Starling's responsibility is restricted to providing a positioning output and an associated PL to the system. If it fails to do so, it reaches a safe state within a given time limit or Fault Tolerant Time Interval (FTTI).

Starling defers to the navigation system when to declare the overall system unsafe and when to trigger an alert, based on the system's AL and TTA respectively.

Starling thus assumes the following system-level requirements:

- **PL < AL**, where PL = Starling's estimated PL and AL = system specified AL
- **FTTI < TTA**, where FTTI is defined as the time interval for Starling to reach its safe state from start of failure and TTA is system's time to alert.

4.2 Starling's Safety Definitions

1. Since actual PE is not observable, based on computed PL, Starling positioning engine follows a stringent definition for its safe operation.

Starling's **safe** operation is defined as,

- **PE < PL**
- Target Integrity Risk: **P(PE > PL) < TIR**

2. Starling considers the following as **unsafe** operation:

- **PE > PL**

Fig. 5 below shows the above definitions pictorially.

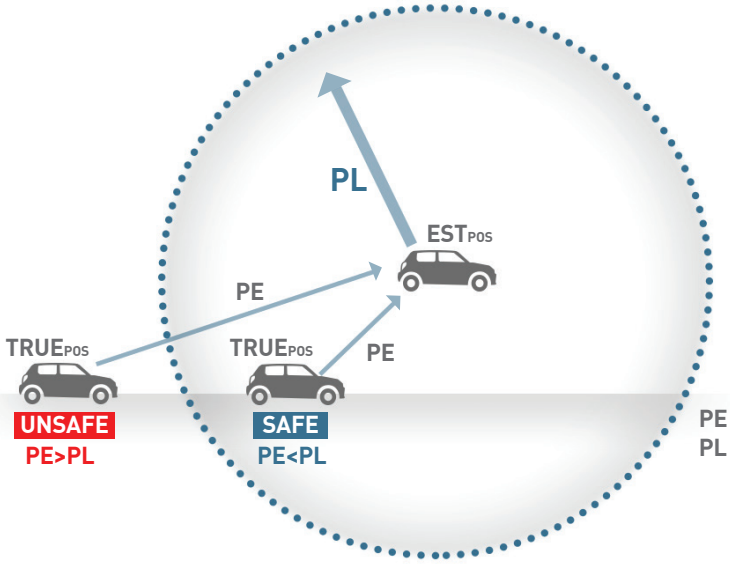

Fig. 5: Starling Positioning Engine's Safe Operation

4.3 Safe State:

If PL> AL, Starling reaches a 'safe state' within a specified FTTI (100ms target) to avoid any potential hazard. The navigation system is to consider position data unreliable in this state. Diagnosis and maintenance of a safe state is performed by a 'safe state diagnostic' functional block within Starling software. This may require further customization to comply with overall system-level requirements.

References

1. RTCA Inc., "Minimum Operational Performance Standards for Global Positioning System/Wide Area Augmentation System Airborne Equipment", RTCA DO-229D, Dec. 13, 2006.
2. Doctoral Thesis, Universite De Toulouse "Integrity monitoring for mobile users in urban environment" by Philippe Brocard, March, 2016.
3. GNSS Position Integrity in Urban Environments: A Review of Literature by Ni Zhu, Juliette Marais, David Betaille, Marion Berbineau, IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS, Feb, 2018.
4. ISO-26262, Part 10: Road Vehicles, Functional Safety, 2018