INTRODUCTION

The continuing evolution of autonomous vehicle (AV) technology, which ultimately aims to enable vehicles to drive themselves without human support or supervision, requires the use of safety-critical systems. The potential risk of AV navigation system anomalies directly affects the safety of users within the vicinity of AV operations (Kim et al., 2017; Pullen et al., 2013; Pullen & Lee, 2013). Safety assurance of navigation systems must be achieved to incorporate AVs into existing and evolving legal and regulatory frameworks.

Recent studies on AV navigation requirements have suggested that the required level of navigation integrity and continuity of safety-critical AV applications be comparable to those of civil aviation (Reid, Houts, et al., 2019; Reid, Pervez, et al., 2019). Integrity (protection against unsafe and unalerted errors) and continuity (limiting the probability of sudden loss of integrity) are known to be the two most challenging navigation requirements to satisfy and are directly related to navigation safety (ICAO, 1996). A previous study by Ford Motor Company derived the required level of integrity risk as $10^{-8}/h$ for AVs based on the desired level of road

Abstract

This study introduces a navigation integrity and continuity algorithm against an inertial measurement unit (IMU) sensor fault within a Kalman filter (KF) that ensures a high level of safety for IMU-integrated safety-critical navigation applications. A representative example of an IMU integrated navigation system is a global navigation satellite system (GNSS)/IMU system. Most previous studies have focused on GNSS faults when evaluating the integrity and continuity of a KF-based GNSS/IMU navigation system, leaving the IMU fault hypothesis unaddressed. Unlike GNSS, which is applied in the measurement update step within the KF, IMU measurements are applied in the state prediction step, which results in different fault propagation characteristics in the user state error compared with those in GNSS. This paper analytically derives the sequential IMU fault impacts on user state errors. Based on this investigation, a KF innovation-based fault detector and protection-level equations are developed, which can safely bound user state errors against sequential IMU fault impacts.

Keywords

GNSS/IMU integration, IMU failure, integrity, kalman filter, protection level
safety (Reid, Houts, et al., 2019). A report published by the United Kingdom government also claimed the need to meet tight integrity requirements for safe operation of autonomous applications from various sectors (Whitty & Walport, 2018). The report suggests an integrity risk level of $10^{-7}$ for autonomous road vehicles and automatic ship docking and $10^{-6}$ for autonomous drones, as an example. In addition to the integrity requirement, continuity requirements are also being discussed regarding the critical operations of an AV, such as lane changing by AVs, overtaking by autonomous cars, and autonomous landings of unmanned aerial systems (UASs) (Reid, Pervez, et al., 2019).

Multi-sensor navigation systems that use recursive filters for state estimation have become essential for AV applications, as operational environments are diversified and require accurate and robust navigation information from multiple sources. The Kalman filter (KF) is a widely used recursive filter for integrating multiple navigation sensors. The KF estimates filter states through two major steps at each time epoch: a state prediction and a measurement update (Welch & Bishop, 1995). Inputs from various sensors are used to estimate navigation states, including global navigation satellite systems (GNSSs), inertial measurement units (IMUs), vision sensors, barometers, magnetometers, and lidar. The KF is designed to operate under “nominal” conditions, in which sensor errors follow the probability models assigned to them; hence, the KF is vulnerable to sensor faults (errors outside these models) that affect either the state prediction or the measurement update step. Algorithms that can quantify navigation safety risks against all potential sensor faults are thus required when utilizing a KF-based multi-sensor integrated navigation system for safety-critical applications.

To develop an integrity and continuity algorithm for a KF-based multi-sensor navigation system, we leveraged concepts from existing GNSS-based safety-critical navigation systems developed over the past 30 years for civil aviation (Enge, 1999; ICAO, 1996; Lee et al., 2016, 2017; RTCA, 2001, 2017; Walter et al., 2008). These concepts include the satellite-based augmentation system (RTCA, 2001), ground-based augmentation system (RTCA, 2017), and applications of receiver autonomous integrity monitoring (RAIM) (Walter & Enge, 1995). Integrity verification within these systems is based on defining GNSS fault hypotheses, designing fault monitoring algorithms, and having users compute real-time protection levels (PLs) that bound rare-event error impacts on user position after fault monitoring. GNSS-based navigation systems utilize a nonlinear weighted least square (WLS) filter, which is a snapshot estimator that generates a navigation solution using measurements obtained at one time of interest without employing additional information on system dynamics (Enge, 1994). Thus, measurement faults present at a given time affect the solution estimated at that time only and do not influence the solution estimated at the next epoch unless they persist until that epoch. A navigation system with a snapshot filter facilitates an integrity algorithm that is straightforward compared with those based on a recursive filter. However, the snapshot filter uses less information and thus has inferior accuracy and fault-free integrity performance (Joerger & Pervan, 2013).

In contrast, a KF is a recursive estimator that sequentially incorporates both system dynamics for state predictions that create time dependency on previous states and real-time measurements (for the measurement update) to estimate navigation solutions (Groves, 2007; Brown & Hwang, 2012; Welch & Bishop, 1995). The KF generates current-time state estimates that (theoretically) maximize current-time accuracy and fault-free integrity performance (Joerger & Pervan, 2013). The KF utilizes all sensor information in addition to the current sensor outputs to determine the current state estimates. Therefore, KF position estimates are affected by
fault conditions that occurred both previously (and ended in the past) as well as current-time measurements. This fault propagation characteristic in a sequential KF must be carefully considered when designing KF-based integrity and continuity algorithms for multi-sensor navigation systems.

KF-based integrity algorithms have been actively discussed in recent publications (Bhattacharyya & Gebre-Egziabher, 2015; Brenner, 1996; Joerger & Pervan, 2013; Tanil et al., 2017; Tanil et al., 2018, 2019). These studies mainly focus on integrity against faults that occur in the GNSS measurement sequence applied in the KF measurement update. Reports by Joerger & Pervan (2013), Tanil et al. (2017), and Tanil et al. (2018, 2019) quantified the worst-case integrity risk from KF state estimates by determining the worst-case failure mode slope, which is based on the relationship between the state error and the monitor test statistics under hypothesized GNSS fault conditions. Joerger & Pervan (2013) applied the concept to precision navigation for aircraft approach and landing by using a carrier-phase GNSS measurement-based KF navigation system. Tanil et al. (2017) and Tanil et al. (2018) applied a KF-based integrity algorithm to evaluate integrity risk against GNSS spoofing within a GNSS/IMU integrated system for aircraft en route, approach, and landing operations by assuming that the IMU is always fault-free. Tanil et al. (2018) specifically enhanced computational efficiency by suggesting an analytical recursive expression of the worst-case failure mode slope, which provides a direct means of computing PLs in real time. The concept proposed by Tanil et al. (2017) and Tanil et al. (2018) was also extended and evaluated for a GNSS/IMU-based autonomous car positioning system in a study by Tanil et al. (2019). Compared with the approach of determining the worst-case failure mode slope, Bhattacharyya & Gebre-Egziabher (2015) proposed a computationally efficient approach. This approach computes a PL in real time by measuring GNSS fault impacts on KF states caused by unmitigated errors after utilizing a snapshot-based WLS RAIM monitor. The recursive impacts of the unmitigated faults determined by the snapshot-based fault monitor are upper-bounded by analytical equations derived for the recursive fault propagation of a GNSS fault vector within the KF.

One remaining problem is that sensors used in the state prediction step within the KF can also be vulnerable to faults. One of the most commonly used sensors in this class is the IMU sensor, which measures acceleration in both translational and angular dimensions. One example of an IMU failure was reported in the investigation of Qantas Airbus A330-303 flight QF72 on October 7, 2008 (Australian Transport Safety Bureau, 2011). During this flight, one of the air data inertial reference units provided erroneous data on many parameters to other aircraft systems, which led to a flight upset and serious injury to 11 passengers. Many other previous studies have tested and reported IMU failure cases. de Pasquale & Somà (2010) determined that IMUs are more prone to faults under highly vibrating environments similar to those in which an AV is likely to operate. Bhatti & Ochieng (2007) listed potential IMU sensor fault characteristics, including step faults, ramp faults, and random noise faults, and summarized the potential causes of each fault type. Researchers have also developed several IMU fault detection algorithms to mitigate IMU faults (Lu et al., 2015; Törnqvist, 2006; Zhang et al., 2018). However, these studies quantified the fault detection capability in terms of the time-to-detect without regard to the fault's impact on state estimates, thereby leaving integrity and continuity risk evaluation unaddressed.

In response, this study develops an integrity and continuity algorithm focused on sensor faults that occur within state prediction by addressing IMU sensor faults within a KF-based GNSS/IMU navigation system. GNSS/IMU integrated navigation systems are a commonly used form of a multi-sensor navigation system, as
the two sensors in this system have complementary characteristics (Groves, 2007; Brown & Hwang, 2012). In particular, IMU measurements allow a GNSS-based navigation system to output solutions at a higher update rate and to provide attitude information, as well as velocity and position data, which are required for AV control.

This study newly investigates the impact of a sequential IMU sensor fault on user state estimates within a KF. Because of the differences between fault propagation characteristics in the state prediction and measurement update steps, which are discussed in detail in this paper, the algorithms previously proposed by Bhattacharyya & Gebre-Egziabher (2015), Joerger & Pervan (2013), Tanil et al. (2017), and Tanil et al. (2018, 2019) cannot be directly applied to evaluate integrity and continuity against IMU faults. Section 2 defines IMU sensor faults and analyzes IMU fault impacts on state estimates that sequentially propagate through a KF. Section 3 introduces a new integrity and continuity algorithm for a KF-based GNSS/IMU integrated navigation system against IMU sensor faults. The integrity and continuity risks posed by this system are defined based on fault trees that incorporate the new fault hypothesis and help set the detection requirements for fault monitors. Two types of PLs, a real-time PL and a predictive PL, against IMU sensor faults are proposed to safely bound errors in the user navigation solution. This section also presents simulation results for both PLs under an example IMU fault condition when applied to UAS navigation. Finally, Section 4 gives a summary of this study.

2 | IMPACT OF IMU SENSOR FAULTS ON A KF-BASED GNSS/IMU NAVIGATION SYSTEM

2.1 | Definition of an IMU Fault Within a KF-Based GNSS/IMU Navigation System

In this section, we first define an IMU fault to investigate its impact on user navigation integrity and continuity within a KF. In a KF-based GNSS/IMU navigation system, the navigation state is predicted from a kinematic inertial navigation equation, and IMU sensor measurements are utilized as input values to these equations. Thus, a fault in the IMU sensor measurements results in a fault vector in the predicted state and sequentially affects future KF estimates through the recursive estimation process of the KF. The defined fault vector is used in the remainder of this paper to analyze fault impacts on user navigation solutions and to derive PLs that bound IMU sensor faults.

A general dynamic system model of a KF is expressed as in Equation (1):

$$\dot{x} = Fx + G_w w + G_u u$$

where $x$ is the state vector, $F$ is the state transition matrix, and $G_w$ and $G_u$ are coefficient matrices of the stochastic random noise vector ($w$) and control input vector ($u$), respectively. For a KF-based GNSS/IMU navigation system, the state vector includes the attitude ($\psi$), velocity ($v$), and position ($r$) navigation states. In addition to these states, the system also estimates the biases included in IMU measurements of an accelerometer ($b_a$) and a gyroscope ($b_g$). The GNSS receiver clock drift ($clk$) and the clock bias drift rate ($clkr$) are estimated and utilized to formulate the predicted pseudorange. The state vector is shown as in Equation (2):

$$x = [\psi \ v \ r \ b_a \ b_g \ clk \ clkr]$$
This paper uses a full-state representation to show the generalized algorithm derivation procedure for any EKF. Note that the following derivations, resulting IMU fault definition, and resulting PL equation can be applied to both full-state and error-state extended KFs (EKFs). When implementing these EKFs, the error state version has the advantage of corresponding better to the linear error assumption made as part of this derivation.

Equation (3) shows the kinematic inertial navigation model defined in the Earth-centered, Earth-fixed (ECEF) coordinate frame, which is used to formulate the dynamic system model of the KF:

\[
\begin{align*}
\psi^e_{eb} &= C^e_b \omega^i_b - \Omega^e_{ie} \psi^e_{eb} \\
\dot{v}^e_{eb} &= C^e_b f^b_{ib} - 2 \Omega^e_{ie} v^e_{eb} + g^e_b \\
\dot{r}^e_{eb} &= v^e_{eb}
\end{align*}
\] (3)

The kinematic model sequentially updates the attitude \((\psi^e_{eb})\), velocity \((v^e_{eb})\), and position \((r^e_{eb})\), where the subscript \(eb\) denotes the state of the origin of the body frame, \(b\), with respect to an ECEF frame, \(e\). The superscript \(e\) indicates that the components of the vector are represented along the axes of the ECEF frame. IMU sensor measurements are input to these equations, including the angular rate from the gyroscope \(\dot{\omega}^i_b\) and the specific force from the accelerometer \(f^b_{ib}\), where the subscript \(ib\) denotes the measurement of the origin of the IMU body frame with respect to an inertial frame \(i\). The superscript \(b\) indicates that the components of the vector are represented along the axes of the IMU body frame. The attitude \(\psi^e_{eb}\) is estimated from the measured angular rate \(\dot{\omega}^i_b\) transformed by the coordinate transformation matrix from the body frame to the Earth frame, \(C^e_b\). \(\Omega^e_{ie}\) denotes the skew-symmetric matrix of the Earth’s rotation rate. The velocity \(v^e_{eb}\) is updated using the updated attitude, specific force \(f^b_{ib}\), and acceleration due to gravity \(g^e_b\).

Finally, the position \(r^e_{eb}\) is determined by integrating the velocity.

Now, let us assume that the input IMU measurements have faults, where we denote faulty parameters using an apostrophe ('). The kinematic expression in Equation (3) is then replaced with Equation (4), which accounts for these faults. Note that faulty IMU sensor measurements \((\omega^i_b'\) and \(f^b_{ib}'\)) sequentially cause faults in the attitude \(\psi^e_{eb}'\), transformation matrix \(C^e_b\), velocity \(v^e_{eb}\), and position \(r^e_{eb}\):

\[
\begin{align*}
\psi^e_{eb}' &= C^e_b \omega^i_b' - \Omega^e_{ie} \psi^e_{eb} \\
\dot{v}^e_{eb}' &= C^e_b f^b_{ib}' - 2 \Omega^e_{ie} v^e_{eb} + g^e_b \\
\dot{r}^e_{eb}' &= v^e_{eb}'
\end{align*}
\] (4)

These faulty parameters can be expressed as follows:

\[
C^e_b' = C^e_b + \Delta C^e_b, \quad f^b_{ib}' = f^b_{ib} + \Delta f^b_{ib}, \quad \omega^i_b' = \omega^i_b + \Delta \omega^i_b, \quad v^e_{eb}' = v^e_{eb} + \Delta v^e_{eb}
\] (5)

where the quantities after \(\Delta\) indicate deviations from the nominal parameters due to faulty IMU sensor measurements. By substituting Equation (5) into Equation (4), the states under the fault condition are expressed as in Equation (6):

\[
\begin{align*}
\psi^e_{eb}' &= C^e_b \omega^i_b' - \Omega^e_{ie} \psi^e_{eb} + f^e_{eb}' \\
\dot{v}^e_{eb}' &= C^e_b f^b_{ib}' - 2 \Omega^e_{ie} v^e_{eb} + g^e_b + f^e_{eb}' \\
\dot{r}^e_{eb}' &= v^e_{eb} + f^e_{eb}'
\end{align*}
\] (6)
where \( f_{\psi b}^{\varepsilon}, f_{\psi b}^{\omega b}, \) and \( f_{\rho b}^{\varepsilon} \) are the resultant fault vectors for the equations of attitude, velocity, and position, respectively. The components of each resultant fault vector are shown in Equation (7):

\[
\begin{align*}
\dot{f}_{\psi b}^{\varepsilon} &= C_b^e \Delta \omega_{ib}^b \\
\dot{f}_{\psi b}^{\omega b} &= \Delta C_b^e \dot{f}_{ib}^b + C_b^e \Delta f_{ib}^b \\
\dot{f}_{\rho b}^{\varepsilon} &= \Delta v_{eb}^b = \Delta C_b^e f_{ib}^b + C_b^e \Delta f_{ib}^b + \Delta C_b^e f_{ib}^b
\end{align*}
\]  

(7)

In a KF, the sensor measurements of an accelerometer and a gyroscope are typically modeled as a summation of the true quantity, a constant bias, and Gaussian random noise (Groves, 2007), as in Equation (8):

\[
\begin{align*}
\dot{\omega}_{ib}^b &= \omega_{ib}^b + b_g^b + w_g^b \\
\dot{f}_{ib}^b &= f_{ib}^b + b_a^b + w_a^b
\end{align*}
\]  

(8)

where \( \omega_{ib}^b \) and \( f_{ib}^b \) represent the true angular rate and the true specific force, \( b_g^b \) and \( b_a^b \) are the biases of a gyroscope and an accelerometer, and \( w_g^b \) and \( w_a^b \) are the gyroscope and accelerometer random noise vectors, respectively. By substituting Equation (8) into Equation (6), the kinematic model under the fault condition can be expressed as functions of the KF states, control input, process noise, and fault vector, as shown in Equation (9):

\[
\begin{align*}
\dot{x}' &= -C_b^e b_g^b - \Omega_e^a \psi_{eb}^e + C_b^e \dot{\omega}_{ib}^b - C_b^e w_g^b + f_{\psi b}^{\varepsilon} \\
\dot{\psi}_{eb}^e &= -C_b^e b_a^a - 2 \Omega e \psi_{eb}^e + g_{eb}^e + C_b^e \dot{f}_{ib}^b - C_b^e w_a^a + f_{\psi b}^{\omega b} \\
\dot{\rho}_{eb}^e &= \dot{v}_{eb}^e + f_{\rho b}^{\varepsilon} \\
\dot{\bar{x}}' &= Fx \\
G_w u &= G_w w \\
f_{\bar{x}}' &= f_{\bar{x}}'
\end{align*}
\]  

(9)

In addition to the navigation states, equations for the IMU sensor biases, receiver clock drift, and clock drift rate are required to complete the system model. As explained earlier, IMU sensor biases are generally augmented in a KF state vector and are continuously estimated from the filter based on an error dynamics model. In a closed-loop KF algorithm, the estimated IMU biases for each axis are fed back and subtracted from an input IMU measurement at the next epoch. However, this bias estimation process is not sufficient to capture IMU faults because 1) IMU faults may not follow the predefined error dynamics model and 2) even if IMU faults are assumed to follow the predefined error model, there is a time delay to perfectly capture the faults. Figure 1 shows the state error of an EKF-based GNSS/IMU navigation system, where an IMU step fault (0.5 m/s\(^2\) on each axis of the accelerometer) is injected after 40 s of simulation time. The state error increases after the fault injection, but decreases over time because of the estimation and correction of the bias by the filter. It is worth noting that user integrity may be threatened by the increased state error that occurs before the fault is fully mitigated.

An IMU sensor exhibits static bias, dynamic bias, scale factor and cross-coupling error, and random noise (Groves, 2007). Well-developed models for each bias are provided in the literature (Bhatti & Ochieng, 2007; Groves, 2007; Zhiqiang & Gebre-Egziabher, 2008). IMU biases are often modeled as static biases or first-order Markov processes. In this paper, static biases are chosen for simplicity in the
presence of the requirement for rare-event error bounding, as the focus of this paper is to compute PLs against IMU faults using filter output covariances. While detailed modeling of IMU biases improves estimation accuracy, it increases system complexity by requiring additional KF states for each of the bias components and analysis of uncertain error parameters. In this study, static biases are assumed for the system model, as shown in Equation (10), and conservative variances are applied to the model to assure that the resulting PL can bound the position error:

$$E(\hat{b}_a) = 0_{3\times 1}, \ E(\hat{b}_g) = 0_{3\times 1}$$

(10)

It should be noted that for a given type of IMU sensor fault, its impacts may appear differently in user states, depending on the system model for IMU bias estimation.

The system model for the GNSS receiver clock drift and drift rate is given by Equation (11), where a constant drift rate is assumed (Groves, 2007):

$$cl\dot{k} = clkr, \ E(clkr) = 0$$

(11)

Finally, we can express the dynamic model of the KF under the IMU fault condition in a continuous form by representing Equation (11) as Equation (12). The components of this form are shown in Equation (13):

$$\dot{x}' = Fx + G_u w + G_u u + f_{\hat{x}}$$

(12)
where $f_x$ is the resultant fault vector included in the dynamic model due to faulty IMU sensor measurements. $w_g$, $w_a$, and $w_{clkr}$ are random noise vectors for the gyroscope bias, accelerometer bias, and clock drift rate.

The discrete form of Equation (12) is expressed as follows:

$$x'_k = \Phi_k x_{k-1} + \Gamma_w w_k + \Gamma_u u_k + f_{x_k}. \quad (14)$$

The discrete forms $x_k$, $\Phi_k$, $\Gamma_w$, $\Gamma_u$, $u_k$, and $f_{x_k}$ correspond to the continuous forms $x$, $F$, $G_w$, $w$, $G_u$, $u$, and $f_x$, respectively.

### 2.2 IMU Fault Propagation Through the KF

This section presents how an IMU fault (defined in the previous section) propagates within a KF. The fault propagates through the KF sequential estimation process, which includes the state prediction and measurement update, as described in Equations (15) and (16), respectively:

**State prediction:**

$$\bar{x}_k = \Phi_k \hat{x}_{k-1} + \Gamma_u u_k \quad (15)$$

**Measurement update:**

$$\hat{x}_k = \bar{x}_k + K_k (z_k - H_k \bar{x}_k) \quad (16)$$

where

- $\bar{x}_k$ is the predicted state vector at time $k$;
- $\hat{x}_k$ is the measurement-updated state vector at time $k$;
- $K_k$ is the Kalman gain matrix;
- $z_k$ is the measurement vector;
- $H_k$ is the observation matrix.

Under the IMU fault condition, the predicted state at time $k$ follows Equation (17):

$$\bar{x}'_k = \Phi_k \hat{x}_{k-1} + \Gamma_u u_k + f_{x_k} \quad (17)$$

where $f_{x_k}$ is the resultant fault vector included in the predicted state vector. Substituting Equation (17) into Equation (16) yields a measurement-updated state as follows:

$$\hat{x}'_k = \bar{x}'_k + K_k (z_k - H_k \bar{x}'_k)$$

$$= (I - K_k H_k) (\Phi_k \hat{x}_{k-1} + \Gamma_u u_k + f_{x_k}) + K_k z_k \quad (18)$$
where $K'_k$ represents the Kalman gain matrix corrupted by the faulty IMU sensor measurements. For compactness, we introduce a new matrix $L'_k = (I - K'_k H_k)$. Subsequently, Equation (18) is simplified as follows:

$$\hat{x}'_k = L'_k \Phi_k \hat{x}_{k-1} + L'_k \Gamma_u u_k + K'_k z_k + L'_k f_{\bar{z}_k}$$

(19)

Based on the expression derived in Equation (19), the vector $L'_k f_{\bar{z}_k}$ is added because of the impact of the faulty IMU measurements at time $k$. Finally, the state error $\bar{x}_k$ is derived using the following relation:

$$\bar{x}_k = \hat{x}_k' - x_k$$

(20)

where the true state is expressed as follows:

$$x_k = \Phi_k x_{k-1} + \Gamma_u u_k + \Gamma_w w_k$$

(21)

The resulting state error equation is shown in Equation (22), where $v_k$ is the vector of measurement noise included in the GNSS measurement, $z_k = H_k x_k + v_k$. A detailed derivation of the state error is presented in Appendix A:

$$\bar{x}_k = L'_k \Phi_k \bar{x}_{k-1} - K'_k v_k - L'_k \Gamma_u w_k + L'_k f_{\bar{z}_k}$$

(22)

The derived state error equation indicates that IMU sensor faults sequentially affect the state error. In addition to the current-time fault vector $(f_{\bar{z}_k})$, it is observed that the past-time fault vectors $(f_{\bar{z}_k}, f_{\bar{z}_k-1}, ..., f_{\bar{z}_1})$ remain in the state error of the previous time $(\bar{x}_{k-1})$, affecting the current-time state error $(\bar{x}_k')$, although their effect degrades over time. The design of an integrity and continuity algorithm should consider these sequential fault impacts to properly assure user navigation safety against IMU fault conditions.

3 | INTEGRITY AND CONTINUITY ALGORITHMS OF A KF-BASED GNSS/IMU NAVIGATION SYSTEM

This section presents an integrity and continuity algorithm for a tightly coupled EKF-based GNSS/IMU navigation system. Figure 2 shows an overview of the algorithm architecture. The tightly coupled EKF-based GNSS/IMU navigation system uses GNSS pseudorange and pseudorange rate measurements to estimate the navigation states together with GNSS receiver clock offsets and IMU biases, as opposed to the loosely coupled EKF, which applies position and velocity solutions as input measurements to the filter. The structure of the algorithm includes three essential steps: (a) defining integrity and continuity risks under the IMU fault hypothesis, as described in Section 3.1, (b) developing KF innovation-based IMU fault detectors considering that an IMU fault simultaneously affects all KF innovations, as described in Section 3.2, and (c) deriving PLs that can bound user state errors against sequential fault impacts, as described in Section 3.3.

3.1 | Integrity and Continuity of a KF-Based GNSS/IMU Navigation System

In this section, we review the concept of integrity and continuity assurance for navigation systems and apply this concept to a KF-based GNSS/IMU navigation
system against all sensor fault hypotheses, with an emphasis on the IMU sensor fault hypothesis. Note that prior works on a GNSS/IMU integrated system reported by Bhattacharyya & Gebre-Egziabher (2015), Brenner (1996), Joerger & Pervan (2013), Tanil et al. (2017), Tanil et al. (2018, 2019) assumed that an IMU sensor is fault-free (or that its failure rate is small enough to be negligible) and focused on GNSS fault hypotheses only. However, this assumption is generally untrue, especially for AV applications that utilize low-cost IMU sensors.

Figure 3 shows the integrity and continuity requirements that define the potential risks of the GNSS/IMU navigation system. The left branch represents events that create integrity risk ($I_{GNSS/IMU}$). This branch defines the fault hypotheses of the navigation system, which include the nominal condition ($I_{nominal}$), where faults occur in neither the GNSS nor the IMU, the GNSS fault condition ($I_{GNSS}$), and the IMU sensor fault condition ($I_{IMU}$). We assumed that the probability of a simultaneous sensor fault occurring in both the GNSS and the IMU is sufficiently low compared with the total integrity risk requirement, which allows us to neglect the integrity risk of a simultaneous fault condition.

The allocated integrity risk for each hypothesis is achieved by designing the risk in the integrity algorithms, including fault monitors and PL calculations (or, equivalently, integrity risk probability quantification). Integrity algorithms under a hypothesis $A$ are designed to achieve a missed detection probability ($P_{md,A}$), which is approximately determined by dividing the allocated risk ($I_A$) by the prior probability of fault hypothesis $A$ ($P_A$). Detailed algorithms for monitor design and PL calculation under the IMU sensor fault hypothesis are described in the following section.
Loss of integrity (LOI) of the integrated navigation system occurs when LOI takes place in any fault hypothesis, given that the solution of the integrated navigation system is computed by fusing GNSS and IMU measurements. In other words, given that the total integrity requirement of a navigation system is fixed, the requirement allocated to each sensor becomes tighter by including the IMU sensor when compared with a GNSS-only navigation system. This tightened integrity risk does not necessarily indicate availability loss. Generally, a tighter integrity risk allocation leads to a larger minimum detectable error (MDE) of a monitor, which may increase PLs and lead to availability loss. However, the benefit of adding a sensor is likely to compensate for the tighter integrity risk allocations to each sensor that result from dividing the overall integrity risk requirement into smaller pieces. In the ideal case, integration of an additional sensor makes the system noise level very small, such that the overall MDE decreases even though the tightened integrity allocation to each sensor is smaller. Therefore, additional analyses on various factors that depend on sensor quality, including nominal noise level, fault monitoring performance, and continuity performance after sensor integration, are required to elucidate the impact of additional sensors on system availability. Availability analysis is beyond the scope of this paper, as the main focus here is the introduction of a new algorithm for integrity and continuity evaluation against IMU sensor faults.

In addition to integrity, continuity assurance is also important for AV applications. Continuity is a measure of the capability to continuously generate navigation solutions during operation without unexpected interruptions (ICAO, 1996). Previous work on requirements for autonomous cars has shown that continuity assurance is required during critical operations, including lane changes and overtaking (Reid, Pervez, et al., 2019). For drones, critical operations include landing and flight close to infrastructure. For the use of an integrated navigation system in a safety-critical AV application, an algorithm that protects integrity while simultaneously meeting the allocations to each component of continuity risk should be designed to meet the required level of continuity for each AV application.
The right branch in Figure 3 shows a continuity risk event tree \( C_{\text{GNSS/IMU}} \) of the GNSS/IMU navigation system. Loss of continuity (LOC) of the integrated navigation system is allocated into LOC due to GNSS faults \( C_{\text{GNSS}} \) and LOC due to IMU faults \( C_{\text{IMU}} \). There are two ways to define the total LOC given a LOC event in any single sensor depending on the system design approach: “series” or “parallel.” In the “series” approach, the total LOC is defined as the probability of any sensor losing its continuity. In other words, integrated system continuity is maintained only when both GNSS and IMU sensors maintain their individual continuity. Assuming that the total continuity requirement for the application of interest is known, the division of the total continuity budget between the two sensors results in a stricter continuity allocation for each sensor compared with the case in which only a single sensor is used. This approach is conservative by limiting the condition that satisfies total system continuity to the case in which both sensors are properly functioning.

In contrast, in the “parallel” approach to continuity of the integrated navigation system, continuity is satisfied when either of the sensors is working. For a fixed continuity risk of each sensor, this approach significantly reduces the total continuity risk of the integrated navigation system. This lowered continuity risk can be seen as an increase in system robustness, which is one of the key advantages of using multiple sensors. Note that if GNSS is integrated with multiple IMUs of which only one IMU needs to work, the IMU function would be in parallel, and the work in this paper can be extended to that case. However, in this paper, we will make the most conservative assumption and assume that the sensors are in series, meaning that the target application requires both GNSS and IMU sensors to be functional during the entire period of operation.

LOC of a sensor can be caused either by a true alert \( P_{\text{t.a}} \) or a false alert \( P_{\text{f.a}} \), as shown in Figure 3. LOC due to a true alert occurs when a monitor detects actual sensor faults or the fault makes itself apparent (e.g., when the sensor stops providing measurements). LOC due to a false (or “fault-free”) alert takes place when no fault occurs but a monitor issues an erroneous alert leading to exclusion of that sensor from use in navigation. The required (or sub-allocated) false alert probability can be met by adjusting the monitor detection threshold.

As explained in the previous paragraph, a true alert is dependent on the prior probability of the actual sensor faults used for AVs. Thus, the continuity risk of a true alert becomes a fixed (albeit not precisely known) value once the sensor is chosen. The prior probability of GNSS faults has been extensively investigated in previous studies (Department of Defense, 2020). For example, advanced RAIM assumes the prior probability of faults as \( 10^{-5} \)/h/satellite for a global positioning system (GPS) satellite (FAA, 2021). In contrast, the prior probability of IMU sensor faults is not as well understood and is highly dependent on IMU sensor quality. This risk can be roughly estimated from the mean time between failures (MTBF) in the datasheets released by IMU manufacturers. For example, a datasheet of a tactical-grade IMU provides the MTBF as 1 failure per 100,000 h (EMCORE, n.d.). This value can be converted to \( 10^{-5} \) failures per hour. However, the use of these values for assuring system continuity is limited because most of the published datasheets provide data derived under idealized test conditions and do not reflect the actual operating conditions of AVs. Further investigations are required before we can confidently apply these failure rates to a certified continuity algorithm. However, for this study, the probability of LOC of an IMU sensor caused by a true alert is pre-allocated based on the MTBF specification provided by the IMU manufacturer, as described above.

In contrast, the false alert probability can be controlled by adjusting the monitor threshold. The false alert probability decreases as the monitor threshold is
increased, which leads to larger PLs if the same missed detection probability is maintained for integrity assurance. An IMU fault monitoring algorithm is designed to assure the false alert probability allocated to the IMU fault hypothesis \( P_{fa,IMU} \).

The remainder of this paper focuses on the false alert continuity risk, assuming that the risk due to true alerts \( P_{ta,IMU} \) is known and pre-allocated. The following section introduces the IMU fault monitoring algorithm designed in this study.

### 3.2 KF Innovation-Based IMU Fault Monitor

This study proposes utilizing a KF innovation vector to detect IMU sensor faults. Innovation vectors have been widely used for GNSS fault monitoring within a KF. Previous studies (Crespillo et al., 2017; Tanil et al., 2017; Tanil et al., 2018, 2019), addressed earlier in Section 1, developed GNSS fault monitoring and integrity risk evaluation algorithms using KF innovations. In the case of a KF-based GNSS fault monitor, a GNSS fault can occur in either a single pseudorange or multiple pseudorange measurements. Thus, a KF innovation monitor accordingly assumes either a single fault (Crespillo et al., 2017) or multiple simultaneous faults (Tanil et al., 2017; Tanil et al., 2018, 2019) in its test statistics. These assumptions are valid because the faulty subset of GNSS measurements only affects corresponding KF innovations computed based on the subset.

In contrast, an IMU sensor fault simultaneously corrupts all KF innovation vectors because each KF innovation is formulated using the common erroneous predicted state determined by the faulty IMU sensor measurements. In response, the IMU fault monitor is developed based on the fact that every innovation is affected by the IMU sensor fault.

Figure 4 illustrates the KF-based IMU fault monitoring algorithm. The KF innovation under nominal conditions for the \( j \)-th GNSS measurement at epoch \( k \), \( q_{k,j|H_0} \), is as follows:

\[
q_{k,j|H_0} = z_{k,j} - H_{k,j} \bar{x}_k
\]

\[
= -H_{k,j} \Phi_k \xi_{k-1} + H_{k,j} \Gamma w_k + v_{k,j} \quad j = 1, \ldots, m \tag{23}
\]

This expression is computed as the difference between the \( j \)-th GNSS measurement \( z_{k,j} \) and the \( j \)-th predicted range \( H_{k,j} \bar{x}_k \), where \( H_{k,j} \) is the \( j \)-th row of matrix \( H_k \), as shown in Equation (23). The innovation vector consists of KF innovations formulated by the total of \( m \) GNSS pseudorange measurements. Under fault-free conditions, this quantity follows a zero-mean Gaussian distribution with a variance of \( S_{jj} \):

\[
q_{k,j|H_0} \sim N(0,S_{k,j}) \quad \text{where} \quad S_{k,j} = R_{k,j} + H_{k,j} \bar{P} H_{k,j}^T
\]

where the subscript \( jj \) indicates the \( j \)-th diagonal element of the matrix. The variance is a function of the covariance matrices of GNSS measurement noise, \( R \), and the predicted state, \( \bar{P} \).

Under an IMU fault condition \( H_{IMU} \), the test statistic is assumed to follow a biased Gaussian distribution with a mean of \( \mu_{j,IMU} \):

\[
q_{k,j|H_{IMU}} = z_{k,j} - H_{j} \bar{x}_k
\]

\[
= -H_{k,j} \Phi_k \xi_{k-1} + H_{k,j} \Gamma w_k + v_{k,j} - H_{k,j} f \bar{x}_k
\]

\[
\sim N(\mu_{k,j,IMU},S_{jj}) \quad j = 1, \ldots, m \tag{25}
\]
where the mean is computed as in Equation (26), which is a function of the bias fault vector \( f_{\mathbf{x}_k} \) defined in Section 2.1:

\[
\mu_{k,j,IMU} = -H_{k,j} \Phi_k \mathbb{E}[\bar{x}_{k-1}] - H_{k,j} f_{\mathbf{x}_k} \tag{26}
\]

To monitor for an IMU sensor fault, each KF innovation must be compared with its corresponding threshold. The monitor then declares an IMU sensor fault if any innovation test statistic exceeds its threshold. Let \( T_j \) be the detection threshold of the \( j \)-th KF innovation. Under the fault-free hypothesis \( H_0 \), the false alert probability of the \( j \)-th innovation \( P_{fa,IMU j} \) is defined as the probability that the test statistic \( q_j \) exceeds the threshold \( T_j \), as shown in Equation (27):

\[
P_{fa,IMU j} = \mathbb{P}(q_j > T_j | H_0) \tilde{P}_{H_0} \quad j = 1, \ldots, m \tag{27}
\]

Note that the prior probability of the fault-free condition, \( \tilde{P}_{H_0} \), can be approximated as unity (this is slightly conservative), considering the very low prior probability of sensor failure. According to the above definition of the false alert probability in the \( j \)-th monitor, a threshold is defined as in Equation (28):

\[
T_{j,IMU} = K_{fa,IMU,j} \sqrt{S_{j,j}} \quad \text{where} \quad K_{fa,IMU,j} = Q^{-1}(1 - \tilde{P}_{fa,IMU,j} / 2) \tag{28}
\]

Here, \( Q^{-1} \) is the inverse of the unit Gaussian cumulative distribution function.

Considering the decision logic of the IMU monitor that an IMU sensor fault is declared if any innovation test statistic exceeds its threshold, a false alert occurs when any of the individual KF innovation monitors generate a false alert. Thus,
\( \tilde{P}_{f_a,IMU} \) is defined as the probability of a union of false alert events for each KF innovation, which should be less than or equal to the allocated requirement, as in Equation (29):

\[
\tilde{P}_{f_a,IMU} = P( |q_1| > T_1 \cup \ldots \cup |q_m| > T_m \mid H_0) \leq P_{f_a,IMU}
\] (29)

Figure 5 shows an example result for this KF innovation-based IMU fault monitor at one example time epoch after an arbitrary fault vector has been injected. An IMU sensor step fault (sudden change) with a magnitude of 0.5 m/s\(^2\) is injected into each axis of the accelerometer. The other simulation conditions are the same as those applied to the simulations that will be introduced in Section 3.3 and Table 1. In Figure 5, all KF innovations were simultaneously affected, with two innovations (\(q_2'\) and \(q_5'\)) exceeding their thresholds. Based on the detection logic of the monitor, the system declares an IMU fault.

### 3.3 PL Against IMU Sensor Faults

This section derives PLs against IMU sensor faults, which provide users with bounds on errors in their navigation solutions after monitoring for IMU faults. Two types of PLs are introduced, namely, a real-time PL\(_{KF,IMU}\) and a predictive PL\(_{KF,IMU}\). We use the subscript “KF, IMU” to clarify that the PL bounds the user KF state under the IMU sensor fault hypothesis. The final PL of the KF-based GNSS/IMU navigation system is determined by taking the maximum over the PLs for each fault mode, including PL\(_{KF,nominal}\), PL\(_{KF,GNSS}\), and PL\(_{KF,IMU}\). In this paper, we will focus on describing the newly suggested PL\(_{KF,IMU}\) values. Before doing so, we will first summarize related studies dedicated to formulating the other PLs.

To compute PLs, positioning uncertainty due to both nominal sensor noise and unmitigated fault effects must be quantified so that bounds can be computed at the probabilities dictated by the navigation requirements. Studies on uncertainty quantification for sequential estimators have been conducted by several researchers.
Output variances of the navigation states of interest are used for all PLs to bound navigation errors against nominal sensor noise. This is a key issue for determining PLs because bounds of KF estimate error distributions must account for uncertainties in sensor noise parameters. Previous studies have shown that the output KF covariance in a sequential estimator is bounded when both measurement and process noise covariance, which are inputs to the KF, are properly bounded. When sensor noise can be modeled by a Gaussian distribution, one can bound the input covariance matrices by utilizing existing Gaussian overbounding methods (Rife et al., 2004, 2006). A major challenge occurs when the sensor noise is correlated with time, such as in GNSS multipath or IMU sensor measurements in which the “white” Gaussian noise assumption is not valid. To solve this problem, researchers have developed the methods described in Khanafseh et al. (2010), Langel et al. (2021, 2019), and Langel et al. (2013) to obtain...
an overbounding distribution on the KF estimate error when the measurement and process noises are time-correlated with an uncertain time-correlation constant and variance.

In addition to nominal noise bounding, recent studies have actively discussed several approaches for bounding unmitigated fault impacts on user PL or integrity risk within a sequential KF (as noted in Section 1). Most studies have developed methods for the case of a GNSS fault, which affects the measurement update step. Based on these studies, \( \text{PL}_{KF,\text{GNSS}} \) or the worst-case integrity risk against a GNSS sensor fault can be calculated (Bhattacharyya & Gebre-Egziabher, 2015; Brenner, 1996; Joerger & Pervan, 2013; Tanil et al., 2017; Tanil et al., 2018, 2019). However, unlike GNSS sensors, which are used in the measurement update step, IMU sensors are generally used in the state prediction step within a KF. The different roles of these two sensors result in different fault propagation characteristics within a sequential KF. We derive \( \text{PL}_{KF,\text{IMU}} \) values based on the propagation characteristic of IMU faults and their impacts on user position later in this section.

Figure 6 illustrates the fundamental concept of the two types of \( \text{PL}_{KF,\text{IMU}} \) with an application to UAS operations. For AV applications, integrity bounds on position estimate errors are needed operationally to inform the user in real time whether a mission should be continued or aborted. In this example, the UAS must not exceed either the upper or lower alert limits (ALs) to avoid collision with manned aircraft or ground obstacles. The real-time \( \text{PL}_{KF,\text{IMU}} \) is utilized to bound the user position against IMU sensor faults and for comparison with the AL during operation. If a real-time \( \text{PL}_{KF,\text{IMU}} \) exceeds either AL, the UAS may initiate an emergency mode or switch to an alternative navigation system. Many AV applications also need to predict operational availability in “downstream” airspace prior to traveling within that airspace. Figure 6 illustrates an example of this situation, in which the UAS is faced with an upcoming region of airspace narrower than the current one due to tall buildings below the airspace. In such cases, the predictive \( \text{PL}_{KF,\text{IMU}} \) is utilized.
before the restricted airspace is reached to predict whether the system will remain available in that region.

The following subsections contain detailed derivations for each type of PL_{KF,IMU}.

### 3.3.1 Real-Time PL_{KF,IMU}

This section presents the mathematical development of the real-time PL in the presence of an IMU sensor failure. In this study, we show the use of KF innovations to capture IMU fault impacts on the user states in real time. Recall that the derived equation for the state error in Equation (22) is as follows:

\[
\ddot{x}_{k,p} = L_{k,p} \Phi_k \ddot{x}_{k-1} + L_{k,p} \Phi_k f_{x_k} - L_{k,p} \Gamma_k w_k + K_{k,p} \nu_k
\]  
(30)

To investigate the relationship between the state error and the KF innovation, we introduce a new matrix \( B_{k,p} \) and multiply the negative of \( B_{k,p} \) by the KF innovation in Equation (23):

\[
-B_{k,p} q_{k,j} |_{IMU} = L_{k,p} \Phi_k \ddot{x}_{k-1} + L_{k,p} \Phi_k f_{x_k} - L_{k,p} \Gamma_k w_k - B_{k,p} \nu_{k,j}
\]  
(31)

where \( B_{k,p} \) is the matrix consisting of KF parameters:

\[
B_{k,p} = L_{k,p} (H_{k,p}^T H_{k,p})^{-1} H_{k,p}^T
\]  
(32)

Note that \( H_k \) and \( K_k \) are not full-rank matrices because only a subset of the state vector is related to the input GNSS measurements. This subset includes the position and the receiver clock bias when pseudorange measurements are used. If the pseudorange rate is applied as an additional measurement, the velocity and receiver clock drift rates are also included in the subset. Because \( H_k \) is not a full-rank matrix, \((H_k^T H_k)\) becomes a singular matrix and is not invertible. By using the partial matrices of \( H_k \) and \( K_k \), denoted as \( H_{k,p} \) and \( K_{k,p} \), respectively, it is possible to convert the KF innovation from the monitor domain to the state error domain, where the subscript \( p \) indicates the partial matrices. Let \( K_k \) be a \( n \times m \) matrix and \( H_k \) be a \( m \times n \) matrix, where \( n \) is the number of KF states and \( m \) is the number of pseudorange measurements. Then, the matrix \( K_{k,p} \) can be obtained by stacking matrices \( K_{k,r} \) and \( K_{k,clk} \) as follows:

\[
K_{k,p} = \begin{bmatrix} K_{k,r} \\ K_{k,clk} \end{bmatrix}
\]  
(33)

where \( K_{k,r} \) and \( K_{k,clk} \) are constructed by extracting the rows of \( K_k \) that correspond to the position (\( r \)) and the receiver clock bias (\( clk \)) states, respectively. In the same manner, \( H_{k,p} \) can be expressed as follows:

\[
H_{k,p} = \begin{bmatrix} H_{k,r} \\ H_{k,clk} \end{bmatrix}
\]  
(34)

where \( H_{k,r} \) and \( H_{k,clk} \) are the columns of \( H_k \) corresponding to the position (\( r \)) and the receiver clock bias (\( clk \)) states, respectively.

By comparing Equations (30) and (31), one notices that the first three terms on the right side of both equations are the same. These terms include both the previous fault impacts and the current-time fault impact as well as the process noise. This comparison shows that the innovation in Equation (31) fully captures the recursive
fault impacts on the state error. The process noise term is also the same in both equations; thus, the innovation captures the real-time process noise impact as well. This observation is the starting point for the derivation of PL$_{\text{KF,IMU}}$, which enables users to directly estimate the real-time fault impacts on user state errors. The following is the state error expressed as a function of the KF innovation vector and the remaining noise terms, $B_kq_k^\prime$ and $K_k\nu_k$, that come from the KF innovation vector and the state error, respectively. Note that the effect of process noise is included in the innovation vector, which is a function of process noise as well as measurement noise, as shown in Equation (25):

$$\tilde{x}_{k,p}^\prime = -B_kq_k^\prime + B_kq_k^\prime + K_k\nu_k \quad (35)$$

The expression of the state error in terms of the innovation vector, which does not require additional knowledge of the fault vector, allows us to estimate the IMU fault impact on user state errors in real time. Based on this expression, the real-time PL$_{\text{KF,IMU}}$ is expressed as follows:

$$\text{Real-time VPL}_{\text{KF,IMU}} = -t_v B_kq_k^\prime \pm K_{md,IMU} \cdot \sigma_{(B_kq_k^\prime + K_k\nu_k)^v} \quad (36)$$

Equation (36) gives PL$_{\text{KF,IMU}}$ in the vertical position domain (vertical PL [VPL]) as an example. The first term on the right-hand side of Equation (36) represents the real-time bias estimate obtained by using the KF innovation vector, and $t_v$ is the vector used to convert the state from the ECEF frame to the local coordinate system and to extract the bias in the vertical position axis. The second term on the right-hand side is added to bound the remaining noise terms, which are functions of GNSS measurement noise. In this term, the standard deviation that bounds the noise terms in the vertical position domain $(\sigma_{(B_kq_k^\prime + K_k\nu_k)^v})$ is multiplied by the factor $K_{md,IMU}$. Note that the noise terms in the vertical position domain can be extracted from the output covariance matrix transformed from the ECEF frame to the local coordinate frame. This multiplier is applied to assure that the PL bounds the user position to the level of integrity risk that is allocated to the IMU fault hypothesis (i.e., a fraction of the total integrity risk requirement). Thus, the real-time VPL$_{\text{KF,IMU}}$ is a bound on the user vertical position error under the IMU sensor fault condition (to the allocated level of integrity risk). As bias estimates are computed in real time, it is possible to have two-sided PLs surrounding them. This results in a lower level of conservatism compared with the method of using the absolute value of the worst-case bias magnitude, as this method considers the actual magnitude of the position bias caused by potential IMU faults experienced by the navigation system in real time.

In this paper, the real-time VPL$_{\text{KF,IMU}}$ is evaluated by a simulation assuming a hovering UAS operation scenario. The simulation assumes that a dual-frequency GPS and a tactical-grade IMU sensor are integrated and included within the UAS equipage. Bounding models for each dual-frequency GPS error component are listed in Table 1. The error model for a tactical-grade IMU provided in Groves (2007) is used for the simulation and is also summarized in Table 1. The total integrity and continuity requirements are chosen to be $10^{-7}$ and $10^{-6}$ per hour for the vertical domain, respectively, based on civil aviation en route operation requirements (ICAO, 1996). These requirements are likely to vary for different UAS applications.

Figure 7 shows the simulated real-time VPL$_{\text{IMU,KF}}$ based on the derived expression in Equation (36). An IMU sensor step fault (sudden change) with a magnitude of 0.5 m/s$^2$ is injected into each axis of the accelerometer for a duration of 80 s, starting at $t = 40$ s, as shown in Figure 7(a). The thin solid lines in the left
(Figure 7(b)) and right (Figure 7(c)) figures at the bottom represent the true state errors, which indicate vertical position errors in this example. The dotted curve represents the estimated bias based on the KF innovation, which is the first term on the right-hand side of Equation (36). This result indicates that the KF innovation captures the recursive IMU sensor fault impact, from IMU faults on previous epochs as well as the current-time fault, on the user KF state error. The thick curves in the right figure show the two-sided real-time VPL_{IMU,KF}, including the additional noise-bounding term (i.e., the second term on the right-hand side of Equation (36)). The real-time VPL_{IMU,KF} bounds the user state error both under nominal and IMU sensor fault conditions. By utilizing the real-time VPL_{IMU,KF}, the user can assure that their navigation solution meets the level of integrity requirement allocation against IMU sensor faults.

Utilizing this real-time PL is less conservative than the conventional method of computing PLs based upon the worst-case user position bias caused by remaining errors after fault monitoring. However, the worst-case approach can be taken for cases in which it is not possible to estimate the actual magnitude of the bias in real time. As an example, estimation of the sequential bias is not possible under a GNSS fault condition. In Appendix B, we show that the method for estimating the bias in real time using the KF innovation is not valid under a GNSS fault condition.

3.3.2 Predictive PL_{KF,IMU}

Although the real-time PL_{KF,IMU} can bound the state error in real time without applying much conservatism, a prediction of the system availability prior to operation is required in many applications. For this purpose, navigation safety assurance systems have implemented a concept of a predictive PL for availability prediction against GNSS faults (Blanch et al., 2010; Joerger et al., 2020). Note that a predictive
PL can be designed for each system by taking into account the tradeoff between safety and availability, as it is applied prior to operation for availability evaluation. The following presents the predictive PL designed for a GNSS/IMU navigation system against IMU faults.

Because the actual measurements of KF innovations required for computing the real-time PL_{KF,IMU} are unknown in advance, an upper bound of the KF innovations is predicted for a specified probability, labeled $P_{fa,IMU}$, in Figure 3, assuming fault-free conditions. This upper bound is then applied to predict availability. We denote the predictive bound against IMU sensor faults as the predictive PL_{KF,IMU}. This section provides a detailed derivation of this predictive PL_{KF,IMU}.

Instead of utilizing the KF innovation vector, which is only available in real time, an upper bound on the KF innovation that meets the false alert probability requirement is derived from the distribution of KF innovations. By definition, this upper bound is given by the thresholds introduced in Equation (28). The threshold vector is then converted into position bias using the relationship between the KF innovation vector and the state vector introduced in Equation (31). The vertical position bias is expressed as Equation (37):

$$b_{IMU,v} = -t_v B_p \begin{bmatrix} T_{1,IMU} & T_{2,IMU} & \cdots & T_{m,IMU} \end{bmatrix}^T$$

(37)

As stated earlier in Section 3.2, the threshold magnitude depends on the allocated probability of a false alert. In this study, the false alert probability is optimally allocated in a way to minimize the vertical position bias while meeting the false alert probability requirement as expressed in Equation (38), where we denote the optimized vertical position bias ($\hat{b}_{IMU,v}$) as the minimum bounding bias:

$$\hat{b}_{IMU,v} = \arg \min_{P_{fa,IMU,j}} b_{IMU,v}, \text{ subject to } P_{fa,IMU,j} \leq P_{fa,IMU}$$

(38)

To simplify the calculation of the optimization in Equation (38), we compute an upper bound for $P_{fa,IMU}$ (given in Equation (29)) by taking the sum of individual $P_{fa,IMU,j}$ terms, as shown in Equation (39):

$$P_{fa,IMU} = P(q_1 > T_1 \cup \cdots \cup |q_m| > T_m | H_0) \leq \sum_{j=1}^{m} P_{fa,IMU,j} \leq P_{fa,IMU}$$

(39)

Finally, a predictive PL against IMU faults is determined by the sum of the minimum bounding bias ($\hat{b}_{IMU,v}$) and the remaining uncertainty due to nominal sensor noise. The output standard deviation of the vertical position state error, $\sigma_{\hat{x},v}$ (or equivalently $\sqrt{P_{\hat{v}v}}$), is multiplied by the factor $K_{md,IMU}$. The final predictive VPL_{KF,IMU} is expressed as Equation (40):

$$\text{Predictive VPL}_{KF,IMU} = \hat{b}_{IMU,v} + K_{md,IMU} \cdot \sigma_{\hat{x},v}$$

(40)

The predictive HPL_{KF,IMU} can be expressed as Equation (41):

$$\text{Predictive HPL}_{KF,IMU} = \hat{b}_{IMU,h} + K_{md,IMU} \cdot \sqrt{\sigma_{\hat{x},n}^2 + \sigma_{\hat{x},e}^2}$$

(41)

where $\sigma_{\hat{x},n}$ and $\sigma_{\hat{x},e}$ are the north and east components of the KF output covariance and $\hat{b}_{IMU,h}$ can be computed in the same way as $\hat{b}_{IMU,v}$. Note that additional
Consideration is required for the allocation of integrity and continuity risk between vertical and horizontal directions when computing both the VPL and horizontal PL (HPL) together. In this paper, only the VPL is simulated by allocating all integrity and continuity risk to the vertical components.

Figure 8 shows the predictive VPL$_{KF,IMU}$ simulated with the same conditions presented in Table 1. The predictive VPL$_{KF,IMU}$ depends on the monitor performance and is likely to be larger than the real-time VPL$_{KF,IMU}$ when the fault magnitude is less than the MDE. As discussed earlier, a key purpose of the predictive PL$_{KF,IMU}$ is to evaluate availability prior to operation. However, for comparison, the predictive VPL$_{KF,IMU}$ (the thickest solid curve) is plotted along with the state error and the real-time VPL$_{KF,IMU}$ in this figure. The circles indicate epochs when the fault is detected by the monitor. Before the monitor detects the injected IMU fault, both the state error and the real-time VPL$_{KF,IMU}$ are well below the predictive PL$_{KF,IMU}$. Users can utilize the real-time VPL$_{KF,IMU}$, which is valid even after detection, as a means of providing navigation safety before the system reaches an AL.

The proposed PL can be applied to any type of IMU error condition to ensure user position error. Appendix C contains examples of the proposed PL simulated under the assumption of other IMU fault modes, including an accelerometer ramp fault, a gyroscope step fault, and a gyroscope ramp fault. Future work will investigate system availability under different IMU fault modes as well as IMU sensor quality by applying the proposed PLs against IMU faults.

**FIGURE 8** Simulation results for the predictive VPL$_{KF,IMU}$
This study has introduced an integrity and continuity assurance algorithm for a tightly coupled KF-based GNSS/IMU system against potential IMU sensor faults. As the IMU sensor is used in the state prediction step within the KF, an IMU fault vector is defined in the domain of the predicted state. The recursive impacts of this fault vector on user states within a sequential KF are analyzed, and algorithms are developed to assure that integrity and continuity requirements are met in the presence of a fault vector. First, example integrity and continuity risk allocations were defined under IMU sensor faults. Based on these definitions, a fault monitoring algorithm that exploits the KF innovation vector was developed, considering that every KF innovation is simultaneously affected by the IMU sensor fault. Lastly, two types of $PL_{KF,IMU}$ were defined. The real-time $PL_{KF,IMU}$ employs real-time KF innovation measurements to estimate potential user state errors under IMU sensor faults. The derivation of this parameter is based on the key finding in this study that the KF innovation provides direct estimates of the recursive fault impact on user state errors under the IMU fault condition. The real-time $PL_{KF,IMU}$ can only be computed when actual KF innovation measurements are available, but it allows a rapid response (e.g., degrading to a less-demanding operation) if the PL grows beyond tolerable safety limits. A predictive $PL_{KF,IMU}$ is also derived, which is an upper bound on the real-time $PL_{KF,IMU}$ to a specified false alert probability. This parameter can be used to predict system availability prior to beginning an operation.

This study assumed a navigation system with a single IMU for simplicity in terms of presenting the main concept of the proposed algorithm. Incorporation of multiple IMUs in this algorithm will be conducted in our future work, because redundant IMU sensors will likely be needed to meet the strictest integrity and continuity requirements for AV applications. This work can be extended to other KF-based multi-sensor navigation systems and opens the possibility of utilizing KF-based multi-sensor navigation systems in a wide range of AV applications with demanding safety requirements.

**ACKNOWLEDGMENTS**

This paper is a revised version of proceedings previously published in the ION GNSS+ 2018 and ION GNSS+ 2019 conferences. The authors would like to acknowledge the support received from the National Research Foundation of Korea (NRF) grant (No. 2020R1A2C1011745) funded by the Korean government (MSIT), as well as the Unmanned Vehicles Advanced Core Technology Research and Development Program through the National Research Foundation of Korea (NRF) Unmanned Vehicle Advanced Research Center (UVARC), funded by the Ministry of Science and ICT, the Republic of Korea (No. 2020M3C1C1A01086407).

**REFERENCES**


APPENDICES

APPENDIX A

The state error under the IMU sensor fault condition is derived via the following steps:

1) Multiply $L_k'x_k$ by $x_k$:

$$ L_k'x_k = L_k'\Phi_kx_{k-1} + L_k'T_uu_k + L_k'T_ww_k $$

(42)

2) Subtract $L_k'x_k$ from $\hat{x}_k$:

$$ \hat{x}_k' - L_k'x_k = L_k'\Phi_k\hat{x}_{k-1} + K_k'z_k + L_k'f_{\pi} - L_k'T_ww_k $$

(43)

3) Insert $z_k = H_kx_k + v_k$ into Equation (43):

$$ \hat{x}_k' - L_k'x_k = L_k'\Phi_k\hat{x}_{k-1} + K_k'H_kx_k + K_k'v_k + L_k'f_{\pi} - L_k'T_ww_k $$

(44)

4) Rearrange Equation (44):

$$ \hat{x}_k' = L_k'\Phi_k\hat{x}_{k-1} + K_k'v_k - L_k'T_ww_k + L_k'f_{\pi} $$

(45)

APPENDIX B

The following shows that the method introduced in Section 3.3 for estimating the bias in real time using the KF innovation is not valid under the GNSS fault condition. Equations (46) and (47) give the state error and the KF innovation vector, respectively, under a GNSS fault condition in which $f_{\pi,\text{GNSS}}$ is the fault defined in the predicted state due to sensor faults in GNSS:

$$ \hat{x}_{k,p}' = L_{k,p}'\Phi_k\hat{x}_{k-1} - L_{k,p}'T_ww_k + K_{k,p}'f_{\pi,\text{GNSS}} + K_{k,p}'v_k $$

(46)

$$ -B_{k,p}q_{k,j}' = L_{k,p}'\Phi_k\hat{x}_{k-1} - L_{k,p}'T_ww_k - B_{k,p}f_{\pi,\text{GNSS}} - B_{k,p}v_{k,j} $$

(47)

If we take the same approach of utilizing the KF innovation to estimate the state error, we find that the state error is expressed not only with the KF innovation vector (and noise terms) but also with the terms relating to the fault vector. In other words, information regarding the fault vector is also required to estimate the state error. Because the user does not have knowledge of the fault vector in real time, it is not possible to estimate the state error in real time based on Equation (48):

$$ \hat{x}_{k,p}' = -B_{k,p}q_{k}' + B_{k,p}v_k + K_{k,p}'v_k + (K_{k,p} + B_{k,p})f_{\pi,\text{GNSS}} $$

(48)

APPENDIX C

Figure 9 shows simulated results for VPL$_{KF,IMU}$ under an accelerometer ramp fault. When the accelerometer ramp fault is injected, the error does not converge by the IMU bias estimation of the filter and continues to increase throughout the
FIGURE 9  Simulation results for the predictive VPL\textsubscript{KF,IMU} under an accelerometer ramp fault

FIGURE 10  Simulation results for the predictive VPL\textsubscript{KF,IMU} under a gyroscope step fault
simulation period, as opposed to the simulation results obtained when the step fault is injected.

Figure 10 and Figure 11 present simulation results for $VPL_{KF,IMU}$ under a gyroscope step fault and a ramp fault, respectively. Because the gyroscope has a more indirect impact on the position compared to the accelerometer, the position error and the PL are kept small in the initial stage of fault detection, even after the gyroscope fault is detected. Further simulations and investigations of errors and PL characteristics in different IMU error modes will be performed in future work.