Preliminary Integrity Assessment of the LDACS Navigation Function

Brandon Weaver, Gianluca Zampieri, Michael Meurer, *German Aerospace Center (DLR)*
Okuary Osechas, *Center for Aviation at Zurich University of Applied Sciences (ZHAW)*
Gary McGraw, *Genova Technologies*

BIOGRAPHY

Brandon Weaver is a researcher at the German Aerospace Center (DLR) as part of the Alternative Navigation Systems group within the Institute of Communications and Navigation. He joined DLR in 2020 after graduating from Tufts University with a Master of Science in Mechanical Engineering. Before attending Tufts, he worked at the Charles Stark Draper Laboratory, Inc. testing and evaluating GPS receivers for high-performance applications. His current research activities focus on non-GNSS integrity for civil aviation.

Gianluca Zampieri received a Master degree in Electronics and Telecommunications Engineering from University of Trento, Italy in 2019. After graduation, he joined the Alternative Navigation Systems Group at the Institute for Communication and Navigation of the German Aerospace Centre (DLR). He is currently involved in research activities on Alternative PNT, focusing on the design and analysis of system architectures. In addition, he is currently pursuing his Ph.D degree at the RWTH Aachen University.

Okuary Osechas is a researcher with the Center for Aviation at Zurich University of Applied Sciences. He has also worked for the German Aerospace Center (DLR) and the Mitsubishi Electric Research Lab. He received a Diploma in Electrical Engineering from Karlsruhe University and a Ph.D. in Electrical Engineering from Tufts University.

Michael Meurer received the diploma in electrical engineering and the Ph.D. degree from the University of Kaiserslautern, Germany. After graduation, he joined the Research Group for Radio Communications at the Technical University of Kaiserslautern, Germany, as a senior key researcher, where he was involved in various international and national projects in the field of communications and navigation both as project coordinator and as technical contributor. From 2003 till 2013, Dr. Meurer was active as a senior lecturer and Associate Professor (PD) at the same university. Since 2006 Dr. Meurer is with the German Aerospace Centre (DLR), Institute of Communications and Navigation, where he is the director of the Department of Navigation and of the center of excellence for satellite navigation. In addition, since 2013 he is a professor of electrical engineering and director of the Chair of Navigation at the RWTH Aachen University. His current research interests include GNSS signals, GNSS receivers, interference and spoofing mitigation and navigation for safety-critical applications.

Gary McGraw is a PNT and systems engineering consultant with Genova Technologies. Gary is retired from Collins Aerospace where he was a Technical Fellow in Navigation Systems in the Advanced Technology Center. While at Collins, Gary led the development of several high accuracy and high integrity navigation systems for both civil aviation and military applications. He received the B.S. degree in Electrical Engineering and Mathematics from Iowa State University, and the M.S. and Ph.D. degrees in Electrical Engineering from the University of California, Los Angeles. Gary is a Fellow of the Institute of Navigation (ION) and is a Senior Member of the IEEE. He serves the ION as an Associate Editor of the NAVIGATION journal, is the ION Executive Vice President, and was the recipient of the 2011 Johannes Kepler Award.

ABSTRACT

Various trade studies and analyses have been conducted to evolve the LDACS-NAV concept to meet certain performance requirements so that an LDACS implementation can be used by civil aircraft for navigation purposes. This paper continues this series of analyses by focusing on integrity requirements. A general LDACS architecture complying with an expected LDACS-NAV specification is assessed for its feasibility in meeting integrity requirements specified for position sources enabling ADS-B Out messages. The assessment is intended to guide the design of LDACS-NAV as it progresses through the standards-making process by identifying high-level integrity failure modes using fault tree analysis.

https://doi.org/10.33012/2024.19516

1. INTRODUCTION

The L-band Digital Aeronautical Communications System (LDACS) is an upcoming data-link technology standard envisioned for future communications infrastructure for civil aviation (DLR, n.d.). LDACS-NAV refers to the navigation functionality of the standard and is envisioned to specify an alternative position, navigation, and timing (APNT) service for civil airspace users. Any system used for navigation onboard civil aircraft must meet specific requirements corresponding to the operations and applications for which the aircraft type is intended. These requirements include but are not limited to certain performance requirements placed on the estimated aircraft position such as accuracy, integrity, etc.

Various trade studies and analyses have been conducted to evolve the LDACS-NAV concept to meet such performance requirements so that an LDACS implementation can be used by civil aircraft for navigation purposes. These previous LDACS-NAV analyses have investigated possible architectures and augmentations such that accuracy requirements specified for position sources enabling ADS-B Out messages can be feasibly met (McGraw, et al., 2023), (Zampieri, et al., 2023). This paper continues this series of analyses but instead focuses on the integrity aspect of navigation requirements. A general LDACS architecture complying with an expected LDACS-NAV specification is assessed for its feasibility in meeting integrity requirements specified for position sources enabling ADS-B Out messages. The assessment is intended to guide the design of LDACS-NAV as it progresses through the standards-making process.

To accomplish this assessment, a general LDACS architecture is described at a high-level and the fundamental measurements enabling LDACS-NAV are described. This system description then supports a fault tree analysis (FTA), which systematically identifies modes of failure within the assumed system contributing to some top-level event. In this paper, this top-level event is a loss of position integrity when using LDACS-NAV. The FTA presented here is primarily a qualitative analysis, as the intent is to identify integrity risks in the envisioned LDACS-NAV specification. A quantitative FTA, which includes data-supported fault occurrence probability computations, is more appropriate for a planned LDACS implementation or at a minimum a more mature LDACS-NAV specification and is therefore not performed here.

The paper is organized as follows. First, the target integrity requirements and the rationale for their targeting are discussed. Next, an overview of LDACS-NAV, including a measurement model for the information used to compute an aircraft position, is described. Third, the FTA is presented based on the described system which assesses qualitatively whether LDACS-NAV can feasibly meet the target integrity requirements. The analysis outcome is a set of identified failure modes contributing to a loss of integrity. Potential mitigations of the more severe modes are discussed, followed by a concluding section summarizing the paper.

2. TARGET INTEGRITY REQUIREMENTS

Navigation integrity requirements are composed of three specified parameters: an alert limit, time-to-alert, and a risk probability. The alert limit defines the allowable amount a position estimate can deviate from the true position before an alert should be raised. The time-to-alert specifies the maximum interval of time between when a position deviation exceeds the alert limit and when an alert is provided. The risk specifies the maximum probability of a loss of integrity, i.e. the occurrence of a position deviation without an accompanying alert within the time-to-alert. The particular values for these parameters depend on the application enabled by the navigation system.

LDACS-NAV is envisioned to support an APNT service for airspace applications that currently rely on GPS/GNSS. One such application, the Automatic Dependent Surveillance – Broadcast (ADS-B) system, depends on a position source meeting the navigation requirements listed in 14 CFR §91.227. Specifically, a position source requires a Navigation Integrity Category (NIC) less than 0.2 nm and a Source Integrity Level (SIL) of 3. These requirements can be decoded using AC 20-165B to mean an alert limit of 0.2 nm and a probability of 10^{-7} per flight hour or sample (Federal Aviation Administration, 2015). As ADS-B Out capability is mandated for all aircraft flying in certain classes of U.S. airspace, having a non-GNSS position source meeting such requirements enables continuing operations where ADS-B Out is required during GNSS unavailabililty.

When one considers that *tolerance* according to Fischer (2011) relates to the specified amount a feature (i.e. position estimate) is allowed to vary from nominal (i.e. actual position), describing a position deviation greater than the alert limit as an out-of-tolerance (OOT) position estimate offers a convenient shorthand to refer to this situation. Based on this, a position tolerance of 0.2 nm (370.4 m) is assumed for an envisioned LDACS-NAV implementation.

We emphasize that the fault tree analysis in this paper is solely a qualitative analysis, such that the identified fault/failure events are *not* used to compute the probability of the top-level event for direct comparison to the 10^{-7} probability requirement. Any numbers that appear are only to support the qualitative analysis.

3. LDACS-NAV

This section provides an overview of LDACS, including a description of the LDACS-NAV component. A mathematical model for the basic LDACS-NAV measurement is then presented, followed by a high-level architecture of a general LDACS-NAV implementation.

3.1. LDACS-NAV Overview

As the name implies, LDACS is primarily an aviation communications system. Specifically, LDACS is a data-link technology consisting of ground stations (GSs) and airborne stations (ASs) with bidirectional communication channels that are frequency duplexed within the L-band allocated for aeronautical applications. The LDACS GSs are ideally synchronized to some common reference time which we call LDACS System Time (LST). Multiple GSs use an FDMA scheme to transmit simultaneously and continuously without interference, with multiple ASs on a single channel using a TDMA scheme for interference-free transmissions to the controlling GS. LDACS transmissions additionally use orthogonal frequency-division multiplexing (OFDM) to avoid intersymbol interference in a bandwidth-efficient manner. The channels used for ground-to-air communication are called the Forward Link (FL) channels, with channels used for air-to-ground communication called the Reverse Link (RL) channels.

To support proper symbol decoding of the received signal, the FL signals periodically transmit a synchronization sequence allowing correlation by the AS to a replica sequence. The synchronization sequence can also be used by the AS to construct a pseudorange measurement for the transmitting GS. A single Super-Frame contains 39 such sequences, three within the Broadcast (BC) Frame and one beginning each of the following 36 frames, as shown in Figure 1 below.

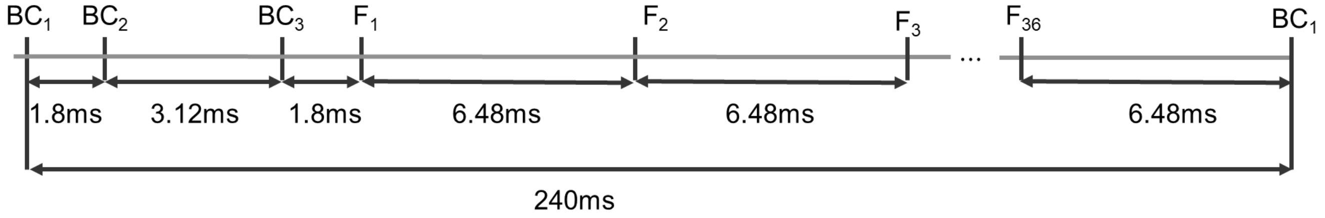

FIGURE 1 – Scheduled LDACS FL synchronization sequences within one Super-Frame.

A pseudorange measurement is constructed by differencing the time-of-arrival (TOA) measured at the AS and the time-of-transmit (TOT) determined from uplinked data and multiplying by the signal propagation speed, c. Positioning proceeds as follows. The equation relating a single pseudorange to AS position is expressed as

$$\rho_i = c(TOA - TOT) = \sqrt{(x_i - x_u)^2 + (y_i - y_u)^2 + (z_i - z_u)^2} + b \qquad (1)$$

where (x_i, y_i, z_i) and (x_u, y_u, z_u) are the GS and AS position coordinates, respectively, and b is the AS clock offset common to all (synchronized) GSs. With GS coordinates available to the AS, the AS coordinates and AS clock offset are the four unknown parameters to be estimated. Having four unknowns, the pseudoranges to at least four different GSs are required to compute a position solution if no other navigation information is used. The position coordinates and AS clock offset can then be found using a least-squares estimation algorithm, as is used in GPS positioning. This is the basic concept for LDACS-NAV. Previous analyses have investigated positioning using both the RL and FL channels to construct two-way ranges (McGraw, et al., 2023), (Zampieri, et al., 2023) but that is outside this paper's scope.

A high-level block diagram representing a functional architecture for LDACS-NAV is shown below.

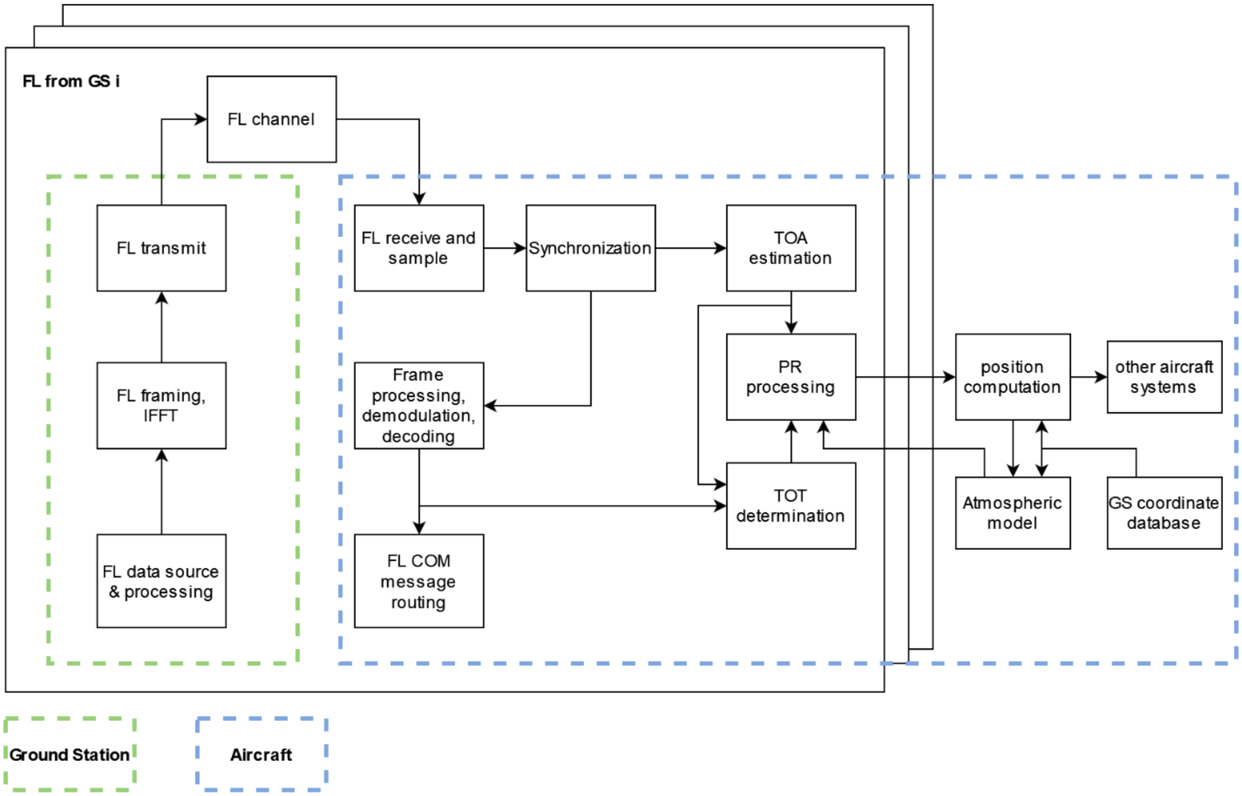

FIGURE 2 - High-level LDACS-NAV functional architecture

How the above functions are mapped to specific hardware components depends on the particular implementation of the LDACS-NAV specification, but a general grouping of functions within the GS or AS can be assumed as shown in Figure 2. The pages distinguish the separate FL signals from different GSs.

An aircraft uses the pseudorange relationship expressed in (1) along with known GS coordinates to compute a position estimate, which can be sent to other aircraft systems requiring navigation. The next section describes the pseudorange construction using the TOT and TOA of an identifiable feature of the LDACS FL signal in more detail. The remaining blocks pertain to functions required for communication functionality, showing how LDACS-NAV fits within the broader LDACS specification. This high-level diagram and the model of the constructed pseudoranges serve as the basis of an assumed implementation of LDACS-NAV which we subject to a fault tree analysis, as presented in the next section.

3.2. Constructing LDACS-NAV Pseudoranges

This section describes how LDACS-NAV pseudoranges are constructed using notation intended to support the later fault tree analysis.

First, to avoid an abundance of notation, let any practical value (measurement, estimate, assumption, etc.) intended to represent some quantity x as $\hat{x}$. The deviation between this practical value and the true value is denoted δx such that $\hat{x} = x + \delta x$. If specificity is necessary, the agent i realizing $\hat{x}$ is denoted by $\hat{x}|_i$.

Next, we include notation to distinguish between different time scales. Let t represent time within some common reference time scale, i.e. LDACS System Time (LST). A local clock, i, can be represented by a function mapping t to the local time $C_i(t)$. The occurrence of an event A can be specified in LST as t_A. The time an event A occurs is often practically realized by some system component corresponding to a local clock i, specified as $C_i(\hat{t}_A)$ in LST, Note that this is different than saying a system component measures an event time as $C_i(t_A)$, as this would actually by an exact determination of when event A occurs but represented in the local time scale. Figure 3 provides a graphical representation of the notation discussed thus far.

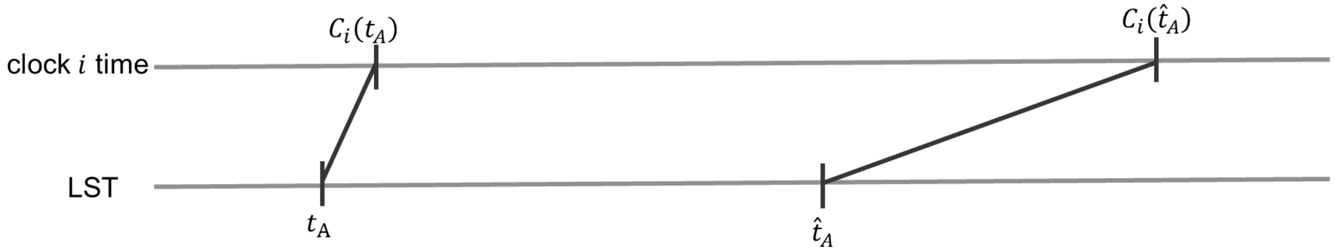

FIGURE 3 – Time scale notation

To account for the various discrepancies, let $\delta t_A = \hat{t}_A - t_A$ represent the deviation of the realized time of a particular event A. Additionally, let a local clock's offset from LST at time t be represented by $\delta C_i(t) = C_i(t) - t$. We can then express the estimated time an event A occurs in a local clock scale C_i as

$$C_i(\hat{t}_A) = \hat{t}_A + \delta C_i(\hat{t}_A) = t_A + \delta t_A + \delta C_i(\hat{t}_A) \tag{2}$$

Now we apply the above notation to LDACS-NAV pseudoranges. Let C_{AS} and C_{GS} represent the local clocks of an AS and GS, respectively. For example, if a GS is initially offset from LST by 500 ms and drifts at a rate of 1ms/s, its local time scale would be $C_{GS}(t) = 1.001t + 0.5$ if t is given in seconds, i.e $\delta C_{GS}(t) = 0.001t + 05$. If at some point the GS starts correcting for the 500 ms offset through its estimate of LST, the local time scale would then be $C_{GS}(t) = 1.001t$, i.e. $\delta C_{GS}(t) = 0.001t$. Therefore, the error of any estimated clock terms can be lumped into the $\delta C_i(t)$ term.

A pseudorange measurement is constructed from an observed transit time, $\hat{\tau}$, multiplied by its assumed speed of propagation, $\hat{c}$, nominally taken to be the speed of light in a vacuum. A pseudorange measurement can then be expressed as

$$\hat{\rho} = \hat{c}\hat{\tau} = (c + \delta c)(\tau + \delta\tau) \tag{3}$$

where c represents the true signal speed and τ the true transit time. Two very important events for determining a transit time are the moment a signal is transmitted by a GS and the moment it arrives at the AS. The times of the events are generally referred to as time-of-transmission (TOT) and time-of-arrival (TOA). In our notation, these are denoted in LST as t_{OT} and t_{OA}, respectively, such that the true transit time is expressed as $\tau = t_{OA} - t_{OT}$.

As discussed, the true t_{OT} and t_{OA} are practically realized by the system. The realized $\hat{t}_{OT}$ and $\hat{t}_{OA}$ values play an important role and are usually represented in a different time scale. For the TOA, the AS will estimate an arrival time of the signal and measure it according to its local clock, i.e. $C_{AS}(\hat{t}_{OA}|_{AS})$. Implementation aspects such as coherent integration intervals, delay lock loop bandwidth, etc., will dictate the point in received transmissions when the TOA is valid. The TOT is more complex and can be realized in various ways. Here we assume the AS knows the transmission schedule for the synchronization sequences in the FL, and the GS provides its clock model estimates via the data-link, enabling the AS to determine the TOT corresponding to the place in the transmission where the TOA is valid. This situation is somewhat subtle, as discussed in more detail below.

An LDACS GS would ideally transmit its frames according to some predetermined schedule, such that $C_{GS}(\hat{t}_{OT,k}|_{GS})$ corresponds to, for example, the scheduled transmission time of the beginning of frame k. This same schedule would be known by the AS, such that $C_{AS}(\hat{t}_{OT,k}|_{AS})$ likewise would correspond to frame k's scheduled transmission time. Assuming a frame is T_F seconds long, transmission begins at some initial zero-time, and the GS and AS use the same predefined schedule, the situation would resemble that shown in Table 1 below.

TABLE 1

Scheduled Transmission Times Across Components

Frame	Scheduled Time	$C_{GS}(\hat{t}_{OT,k}\|_{GS})$	$C_{AS}(\hat{t}_{OT,k}\|_{AS})$
0	0	0	0
1	T_F	T_F	T_F
2	$2T_F$	$2T_F$	$2T_F$

Since $C_{AS}\left(\hat{t}_{OT,k}|_{AS}\right) = C_{GS}\left(\hat{t}_{OT,k}|_{GS}\right)$ and $t_{OT,k}$ is the same in both terms, then by (2) the identity

$$\delta t_{OT,k}|_{AS} + \delta C_{AS}\left(\hat{t}_{OT,k}|_{AS}\right) = \delta t_{OT,k}|_{GS} + \delta C_{GS}\left(\hat{t}_{OT,k}|_{GS}\right) \tag{4}$$

can be used to express $C_{AS}\left(\hat{t}_{OT,k}|_{AS}\right)$, referenced to the AS, in terms of GS error components.

For example, if a GS's time scale is equivalent to LST and correctly transmits frames according to the scheduled times such that $\delta t_{OT,k}|_{GS} = \delta C_{GS}\left(\hat{t}_{OT,k}|_{GS}\right) = 0$, then $C_{GS}\left(\hat{t}_{OT,k}|_{GS}\right) = t_{OT,k} = C_{AS}\left(\hat{t}_{OT,k}|_{AS}\right)$ for every frame and using (2) it can be shown that $\delta t_{OT,k} = -\delta C_{AS}\left(\hat{t}_{OT,k}|_{AS}\right)$. As long as the correct scheduled time is assumed, the deviations in $C_{AS}\left(\hat{t}_{OT,k}|_{AS}\right)$ cancel so that (4) holds. Referencing Figure 1, we can determine how far a synchronization sequence has traveled by the time the next sequence is transmitted. The interval between any two non-BC frames is 6.48ms which corresponds to around 1000 nautical miles (nmi). As an AS is unlikely to receive FL signals from any GS more than 200 nmi away, there is no ambiguity about a received sequence's scheduled time.

Of course, it is unlikely a GS can perfectly transmit frames according to a predefined schedule in LST. Not only will there be some offset between the GS time scale and LST, but the GS might transmit a frame at a different instant than intended. In this case, (4) still holds so that the observed transit time can be expressed using (2) as

$$\hat{\tau} = \tau + \delta t_{OA}|_{AS} - \delta t_{OT}|_{GS} + \delta C_{AS}(\hat{t}_{OA}|_{AS}) - \delta C_{GS}(\hat{t}_{OT}|_{GS}) \tag{5}$$

Combining (3) and (5), we can express the constructed pseudorange with expanded deviation terms as

$$\hat{\rho} = \hat{c}\hat{\tau} = (c + \delta c)\left(\tau + \delta t_{OA}|_{AS} - \delta t_{OT}|_{GS} + \delta C_{AS}(\hat{t}_{OA}|_{AS}) - \delta C_{GS}(\hat{t}_{OT}|_{GS})\right) \tag{6}$$

with the deviation terms summarized in Table 2 below.

TABLE 2

Pseudorange Deviation Terms

Deviation term	Description
δc	Deviation between actual signal speed, c, and assumed speed, $\hat{c}$
$\delta t_{OA}\|_{AS}$	AS TOA error
$\delta t_{OT}\|_{GS}$	GS TOT error
$\delta C_{AS}(\hat{t}_{OA}\|_{AS})$	AS time scale offset relative to LST at realized TOA instant
$\delta C_{GS}(\hat{t}_{OT}\|_{GS})$	GS time scale offset relative to LST at realized TOT instant

The developed pseudorange model, combined with the system block diagram in Figure 2, is used to support the fault tree analysis described next.

4. FAULT TREE ANALYSIS

This section presents the main contribution of the paper: a fault tree analysis (FTA) of a generalized implementation of LDACS-NAV to qualitatively assess the integrity performance. First, a brief introduction to fault trees and FTA is described, followed by the FTA for an assumed LDACS-NAV implementation.

4.1. FTA Introduction

The information in this section is taken from Vesely, et al. (1981), SAE (1996), and NASA (2002). Fault tree analysis is a systematic way of identifying the causes to some top-level undesired event. The sequence and combinations of factors resulting in a top-level event can be represented graphically in a fault tree as event blocks connected with logic gates. Guidance material for FTA often recommend certain techniques to aid fault tree construction thereby avoiding common pitfalls. System block diagrams work well with one such technique: identifying the minimum immediate, necessary, and sufficient (INS) causes of an undesired event. An example provided in NASA (2002) is the situation that no water flows from a faucet when turned on. One might begin to consider all possible causes this is occurring: water is shut off, pipe has burst, etc. In FTA, however, you only consider the minimum INS causes. For the faucet situation, this would be that either the faucet has plugged or that no water is reaching the faucet.

This approach works well for systems described using block diagrams, as the general example below shows.

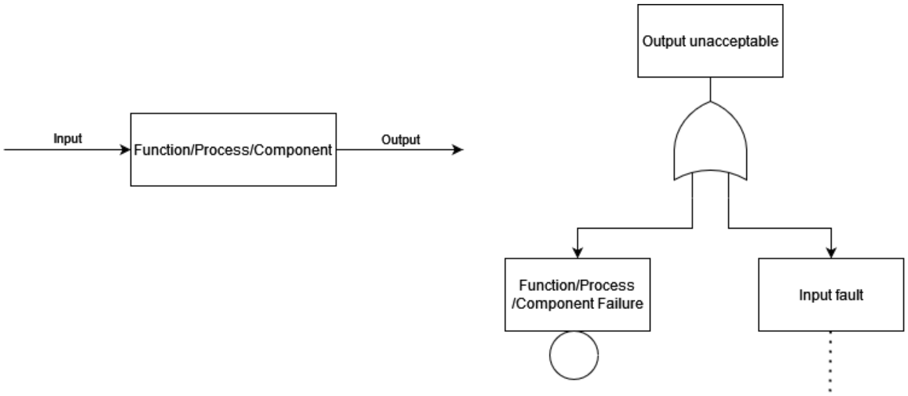
Input
Function/Process/Component
Output
Output unacceptable
Function/Process /Component Failure
Input fault

FIGURE 4 - System block diagram and corresponding fault tree

Starting from an undesired event, "Output unacceptable", the INS technique limits possible causes to either the component itself failing or the component receiving faulted inputs. The faulted inputs can then be traced to another component block, where the same possible causes (component itself or inputs) are hypothesized. This basic idea can then be repeated for the entire system, thus providing a systematic way of considering contributing factors to a top-level undesired event. The fault tree, once it reaches a sufficient level of depth, can then be simplified with Boolean algebra to determine the set of failure modes that individual cause the top-level event. A given mode can be a combination of multiple basic failure events in the fault tree, with the full set called the minimal cut set.

4.2. LDACS-NAV FTA

The LDACS-NAV fault tree construction begins with identifying the objective of the FTA: the qualitative assessment of LDACS-NAV to meet target integrity requirements. As described in Sec. 2, integrity requirements can be considered to be a tolerance on the position estimate with associated alerting requirements. Any position estimate exceeding this tolerance without annunciation can therefore be classified as out-of-tolerance (OOT) and results in a loss of integrity.

The top-level undesired event serves as the root of the fault tree. To assess how the LDACS-NAV implementation can result in a loss of integrity, we define the top-level undesired event as "an OOT position estimate occurs without annunciation" which corresponds to the output of the "position computation" box in Figure 2. When identifying contributing factors, we may rely on the numerical values associated with the ADS-B position source integrity requirements, i.e. the probability that a position estimate deviates from the true position by greater than 0.2 nmi without annunciation is less than 10^{-7} per flight hour. Use of these values are not intended to represent a quantitative FTA, but are simply to support qualitative objectives. Lower level events are often characterized using the out-of-tolerance concept, with the particular tolerance flowing down from the position estimate tolerance.

Using the block diagram in Figure 2 combined with the INS technique described in the previous section, an initial fault tree level can be constructed as shown below:

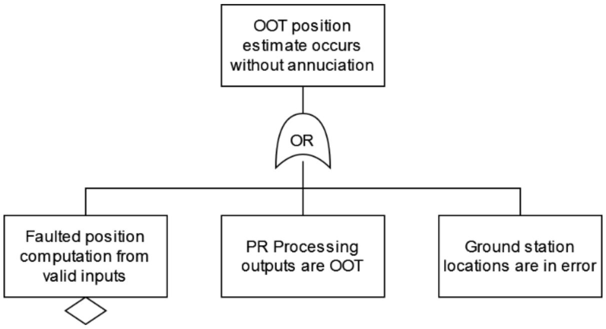
OOT position estimate occurs without annuciation
OR
Faulted position computation from valid inputs
PR Processing outputs are OOT
Ground station locations are in error

FIGURE 5 - Initial fault tree level

The diamond under the left-most block in Figure 5 designates an event that is not developed further due, in this case, to its perceived inconsequential nature. We present an example of the reasoning used to construct the full fault tree by developing the "PR processing outputs are OOT" block further. The first step is determining an approximate tolerance for the pseudorange error, beyond which results in the top-level event. The position error resulting from a pseudorange error depends on a number of factors such as ground station geometry, measurement weighting, and the algorithm used to compute a position. The pseudorange error budgets outlined in Zampieri, et al. (2023) derive an RSS error of 15-40 m depending on certain ground network and airborne measurement processing assumptions. As this corresponds to accuracy, with integrity tolerances being larger, taking this range as the approximate pseudorange tolerance is an acceptable simplification for the qualitative analysis.

Due to the nature of communications, the pseudorange constructed from the controlling GS FL signal is considered separately from pseudoranges constructed from other GS FL signals, although we focus on the controlling GS in our discussion. The pseudorange branch can then be developed further as shown in the left diagram of Figure 6 below.

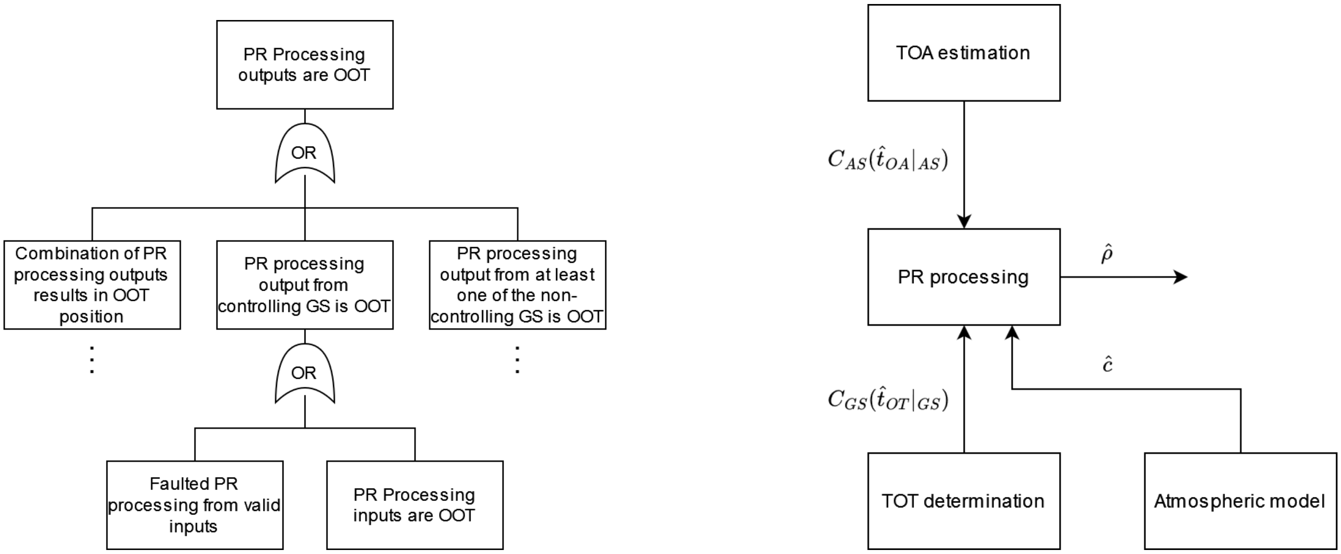
PR Processing outputs are OOT
OR
Combination of PR processing outputs results in OOT position
PR processing output from controlling GS is OOT
PR processing output from at least one of the non-controlling GS is OOT
OR
Faulted PR processing from valid inputs
PR Processing inputs are OOT
TOA estimation
$C_{AS}(\hat{t}_{OA}|_{AS})$
PR processing
$\hat{\rho}$
$\hat{c}$
$C_{GS}(\hat{t}_{OT}|_{GS})$
TOT determination
Atmospheric model

FIGURE 6 – Left: Further developed branch for OOT pseudoranges; Right: Detailed input/output of PR Processing block

Next, we need to consider the nature of the PR processing block in Figure 2. The block can be shown in more detail using the pseudorange notation developed earlier, as shown in the right diagram in Figure 6 above. Applying the INS technique, an OOT PR processing output can be caused by invalid PR processing inputs or a fault internal to PR processing. As the PR processing block is highly dependent on the airborne implementation of LDACS-NAV, it is difficult to conceive of faults internal to PR processing without additional information. As such, we mark the block with a diamond to designate no further development, in this case due to lack of necessary information.

We then continue to the inputs, focusing now on the atmospheric model output being OOT. The assumed speed $\hat{c}$ includes the correction of the tropospheric delay using atmospheric weather models and the assumed GS and aircraft locations If the inputs, i.e. the AS and GS coordinates, are valid, then an OOT model output is solely due to the model not matching the actual tropospheric delay. This can occur because an inappropriate model for the application is used or an anomalous weather event occurs. The developed branch is then represented as shown in Figure 7 below, where the shaded diamond refers to an event considered elsewhere in the fault tree and the remaining unshaded diamonds designating events not further developed.

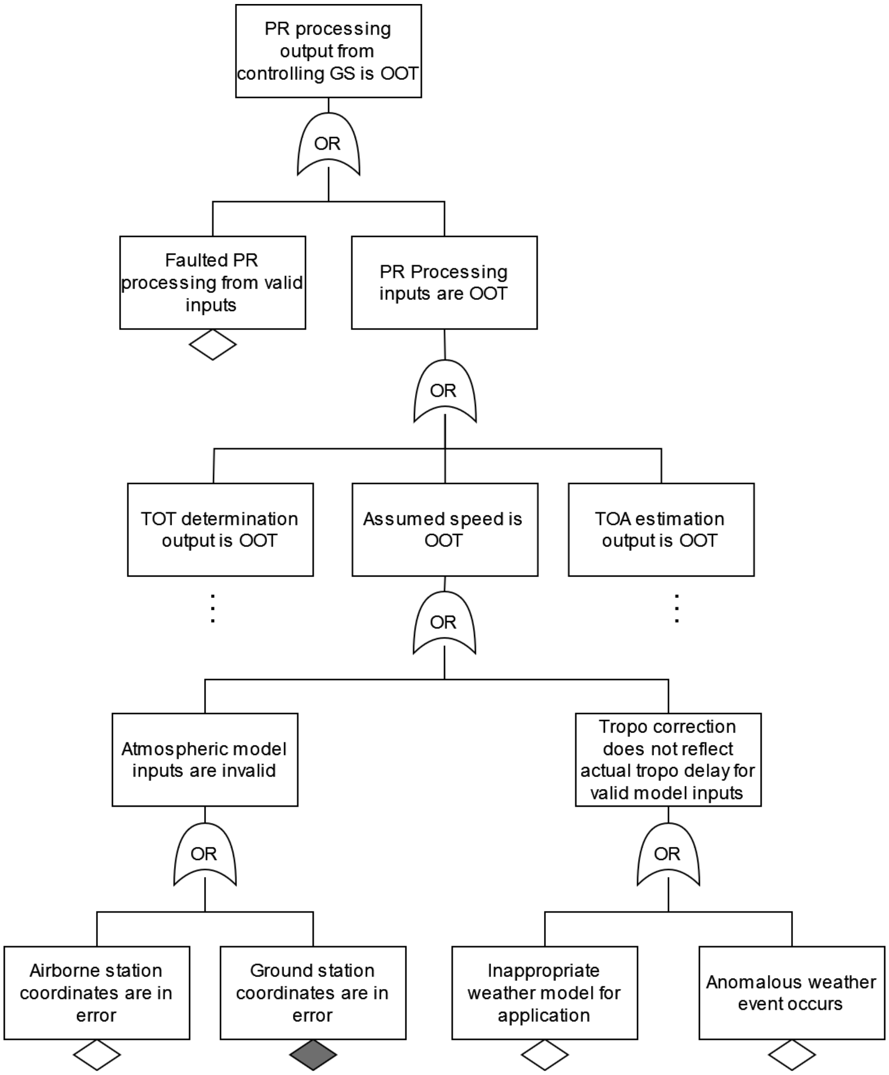
PR processing output from controlling GS is OOT
OR
Faulted PR processing from valid inputs
PR Processing inputs are OOT
OR
TOT determination output is OOT
Assumed speed is OOT
TOA estimation output is OOT
OR
Atmospheric model inputs are invalid
Tropo correction does not reflect actual tropo delay for valid model inputs
OR
OR
Airborne station coordinates are in error
Ground station coordinates are in error
Inappropriate weather model for application
Anomalous weather event occurs

FIGURE 7 - Developing the fault tree

As a final step, these events can be given an approximate severity rating based on a typical tropospheric delay correction residual magnitude and approximate likelihood of occurrence. Assuming an extreme example of inappropriate weather model, i.e. none whatsoever, tropospheric delays on the order of 30-50 m are possible (Narayanan, 2023), which is of concern based on the 15-40m approximate pseudorange tolerance. It is reasonable to expect that an implementation of LDACS-NAV would use an appropriate tropospheric delay compensation model such that this event is unlikely to occur and therefore has a low severity. Anomalous weather conditions are a more likely occurrence, with frequent phenomenon known as tropospheric ducting capable of resulting in 5 m of error in the worst case after tropospheric delay correction (Narayanan, 2023). As this could be bounded by a conservative error model without unduly affecting accuracy performance for the target applications, this event likewise has a low severity.

Using the same reasoning, the full fault tree is constructed where the leaves of the tree, or those events with no further development, serve as failure modes contributing to the top-level loss of position integrity event. These modes are given a severity rating based on a first impression of its likelihood and resulting impact on the position error, as presented in Table 3 below.

TABLE 3

Possible LDACS-NAV Integrity Failure Modes

Fault mode	**Severity**	**Reason**
Faulted position computation from valid inputs	Low	SW developed to appropriate assurance level
GS coordinates correspond to different GS	Low	Frequencies assigned to specific GS, BC frames additionally contain GS coordinates
Faulted PR processing from valid inputs	Unrated	Requires more implementation detail
Map-shift caused by published station coordinates being in error	Low	Techniques used to correct DME ground station coordinates can be adopted for LDACS
Change in transmitting antenna location	Medium	Transmissions switching to separate antenna on tower for backup/maintenance related reasons causes range error
Uncompensated receive delay	Medium	HW/FW/SW developed to appropriate assurance level
Implementation-specific inputs to atmospheric model e.g. meteorological inputs are invalid	Unrated	Requires more implementation detail
Inappropriate atmospheric model	Low	Model for terrestrial propagation should be used
Anomalous weather event occurs	Low	Mitigated by uncorrected tropo error over-bounding
GS time scale not synchronized to LST	High	Each microsecond offset results in ~300m pseudorange error
Uncompensated transmit delay	High	Each microsecond delay results in ~300m pseudorange error
Faulted FL reception/sampling of valid sync sequence	Low	HW/FW/SW developed to appropriate assurance level
Sync sequence thought to be from controlling GS taken from spoofed signal	Low	Authentication during cell-entry reduces likelihood
Sync sequence thought to be from non-controlling GS taken from spoofed signal	Unrated	Requires more investigation
Transmitted FL sync sequence is invalid	Low	Class of faults where COM remains functional but the sync sequence distortion results in pseudorange errors assumed to be small
Received sync sequence affected by free-space channel effects	High	Multipath-induced delay of sync sequence can result in hundreds of meters of pseudorange error
TOT-related info provided by spoofed signal	Low	AS checks authenticity of received messages using encrypted key
Received TOT-related info corrupted by free-space channel effects	Low	Decoded data integrity checks likely to preclude use of erroneous data

The above severity ratings should not be taken as definitive, but rather a first impression on which failure modes are challenging to mitigate. For example, *received sync sequence affected by free-space channel effects* is given a high severity rating as this occurrence requires residual monitoring which requires careful tradeoffs between detection and false alert probabilities. Previous work has proposed using carrier phase smoothing to mitigate this mode, but doing so is a specific implementation for PR Processing and would require further fault tree development. Carrier phase smoothing, for example, can result in cycle slips impacting the pseudorange error. Another aspect to consider is that the hardware, software, and firmware is developed to the appropriate assurance level for *navigation* and not just communication.

5. CONCLUSION

This paper created an initial list of high-level failure modes resulting in a loss of position integrity for the LDACS-NAV function. The methodology to produce the list was fault tree analysis, a standard tool in safety-oriented system design and assessment. The identified failure modes were assigned a severity rating based on the expected likelihood of occurrence and impact on position error. Many of the failure modes are expected to be of low concern due to the built-in safeguards of any typical implementation, whereas other modes may require targeted approaches to reduce their likelihood and/or impact on position error. The latter set are the areas of focus for future work.

The depth of the analysis was limited by the lack of implementation detail inherent to standards/specifications. Future work focusing on a subset of the identified failure modes can make many more assumptions to allow further development of the corresponding fault tree branches. With a more detailed design or implemented system, quantitative fault tree analysis can be conducted to assess whether the top-level event occurs within the probability specified by the integrity risk.

6. REFERENCES

DLR: Institut für Kommunikation und Navigation. (n.d.). *About LDACS*. Retrieved 2023, from ldacs.com: https://www.ldacs.com/

Federal Aviation Administration. (2015). *Advisory Circular 20-165B, Airworthiness Approbal of Automatic Dependent Surveillance - Broadcast OUT Systems.*

Fischer, B. R. (2011). *Mechanical Tolerance Stackup and Analysis* (2nd ed.). CRC Press.

McGraw, G., Zampieri, G., Osechas, O., Meurer, M., & Kalyanaraman, S. (2023). LDACS APNT Protocol and Measurement Signal Processing Architecture. *Proceedings of the 2023 International Technical Meeting of The Institute of Navigation.* Long Beach, CA.

Narayanan, S. (2023). *Atmospheric error modeling for alternative position navigation and timing systems.* [Doctoral Thesis, Technische Universität Berlin].

NASA. (2002). *Fault Tree Handbook with Aerospace Applications.* NASA Office of Safety and Mission Assurance.

SAE. (1996). *ARP 4761 - Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment.* Society of Automotive Engineers, Inc.

Vesely, W. E., Goldberg, F. F., Roberts, N. H., & Haasl, D. F. (1981). *NUREG-0492, Fault Tree Handbook.* U.S. Nuclear Regulatory Commission.

Zampieri, G., McGraw, G. A., Osechas, O., Weaver, B., & Meurer, M. (2023). LDACS APNT Service Area Analysis with Barometric Altimeter Augmentation and Ground Station Selection Constraints. *Proceedings of the 36th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2023).* Denver, CO.