Reengineering DME/N Integrity to Support PBN

Gerhard E. Berz
Senior Expert Navigation and Spectrum
EUROCONTROL
Brussels, Belgium
Tel: +32 2 729 3734
E-mail: gerhard.berz@eurocontrol.int

Luca Saini
Safety Authority
Thales Airspace Mobility Solutions, Navigation
Gorgonzola, Italy
Tel: +39 02 95095 507
E-mail: luca.saini@thalesgroup.com

INTRODUCTION

The number of GPS outages likely caused by radio frequency interference reported by aircraft operators in the European region has reached a historic high in 2018 and 2019. The issue continues in 2020 / 2021 despite a reduced numbers of flights (and subsequently also a reduced number of reports) [1]. While various efforts are underway to counteract this trend, the most suitable back-up navigation infrastructure to maintain Performance Based Navigation (PBN) operations currently is DME/DME area navigation. This can be referred to as "short term A-PNT" (Alternate Positioning, Navigation and Timing), where the long-term variant deals with researching the introduction of new A-PNT technology [2].

PBN specifications make a distinction between RNAV and RNP specifications, where the latter provide on-board performance monitoring and alerting, which implies a recognized level of integrity. While DME/DME can support RNAV5 and RNAV1 applications, the support of RNP1 is subject to State approval. EUROCAE Working Group 107, "DME Infrastructure supporting PBN Positioning", was created in 2018. The deliverables of the group are to update EUROCAE Document ED-57 [3], Minimum Operational Performance Standard for DME (Ground Equipment), and to write a new MASPS. This Multi-DME-focused Minimum Aviation System Performance Standard will be consistent with the RNP/RNAV MASPS (ED75 / RTCA DO236, covering aircraft avionics and just completing an update which strengthens DME provisions [4]) and provide a basis for States to approve DME infrastructure for PBN as described in the ICAO PBN Manual [5]. This will enable a more robust RNP service in locations where this is required. In other locations where RNAV applications are used, it will improve the reliability of DME-based RNAV1 service as well. This is desirable because with increasing use of GPS, aircraft will only rarely navigate using DME. Therefore, these measures ensure that when DME/DME service is needed due to a GPS outage, the expected performance can be provided.

Conventional navigation aids were standardized prior to the development of the performance requirement elements of accuracy, availability, continuity and integrity, which are commonplace in GNSS. While the current ICAO Annex 10 places such requirements on DME, they are generally not directly specified using those terms. Especially with respect to integrity, no formal requirement is present, while prescribed monitoring systems do provide some level of integrity – which is difficult to quantify. Furthermore, due to its association with ILS and developments related to MLS and DME/P, currently installed ground transponders often do meet a specific level of integrity, as determined by the system manufacturer. Similarly, the use of DME by Flight Management Systems (FMS) includes a number of on-board reasonableness checks to prevent misleading outputs in the area navigation position solution.

EUROCAE WG107 seeks to formalize these existing integrity elements into a consistent framework, expressed in a requirements structure usable by PBN. This encompasses ground, propagation and aircraft elements. This paper gives an overview of the envisaged systems approach, primarily discussing the ground transponder elements. However, their further interactions with the other elements, including aircraft performance and operational context will be explained also. It will show the aspects being considered to derive a new, system level integrity requirement for DME/DME supporting PBN (including RNP specifications), and its allocation to the system components, including setting a requirement for transponder integrity performance.

A key element for the transponder integrity requirement is the agreement of a common transponder integrity demonstration methodology in the updated ED-57A MOPS. The method is built on existing ILS and MLS principles but seeks to clarify a variety of aspects, which have not been so clear in ICAO documentation [6]. It is the expectation that all recent DME transponders will be able to use the method in a consistent and comparable manner and meet the new integrity requirement. This will allow ANSP to qualify their DME/DME service to support RNP. It is also expected that this can be declared in updated AIP provisions. At this stage it is not yet known whether this will lead to modified or additional flight inspection requirements for DME, but this continues to be a possibility especially for terminal area procedures (SID and STAR).

INTEGRITY FOR PBN

Integrity is navigation's most important safety parameter. It ensures the absence of hazardously misleading information in aircraft navigation. GNSS integrity schemes were introduced because GNSS satellites serve multiple user segments and can therefore not include executive monitors, which shut down the satellite signal if there is a deviation from aviation requirements. There are also some complexities arising from the fact that satellites are orbiting the earth at a large distance from earth, so installing something like a far-field monitor is not practicable. Consequently, augmentation services have been developed which implement "user-level integrity", i.e., an integrity level derived and applicable to the aircraft navigation receiver output. A key advantage is the GNSS propagation path, where apart from disturbances linked to the ionosphere, multipath is very benign. Differential GNSS augmentation systems (GBAS, SBAS) eliminate the ionosphere errors, whereas in ABAS/RAIM systems, the single frequency correction works well enough to meet requirements for en-route and terminal applications (and future dual-frequency GNSS systems will also eliminate ionosphere-related errors).

When considering terrestrial navigation systems, integrity monitoring is implemented directly at the ground facility. However, this leaves the propagation path unprotected, which includes troposphere propagation and multipath as principal error sources. In ILS, critical and sensitive areas are implemented to limit propagation-related errors, in particular as they arise from airport movements of aircraft and airport vehicles. Some level of multipath protection is achieved also for VOR and DME from site safeguarding practices, such as the implementation of so-called "Building Restricted Areas" [7]. Furthermore, flight inspection of the associated conventional procedures essentially implements propagation quality monitoring while assuming that such propagation issues are, for the most part, stationary. In the use of DME for PBN however, DME ranges are used at a large variety of geometries, which may not have been discovered by flight inspection, since it would be prohibitive to inspect every possible radial or orbit at all possible distances and altitudes. Past experience does not suggest that DME propagation issues are relevant for area navigation (first area navigation standards and certifications dating back to the 1980's). However, given the attempt to introduce a formal integrity level for DME support to PBN and the limitations inherent in ground - aircraft paths compared to space to aircraft signal paths, maintaining integrity during propagation is one of the key challenges. A related paper to this IFIS will cover propagation aspects (multipath) in more detail (considering DME troposphere delays to be negligible for the envisaged accuracy performance levels [8]).

The most prominent integrity issue for DME has actually been the map-shift, linked to errors in ground facility coordinates. This is essentially the same as an ephemeris error in GNSS. Note that further, more detailed aspects are discussed in [9]. Recent advances in aeronautical data integrity, introduced to support PBN implementation, have largely eliminated this error source. ANSP deciding to support RNP procedures with DME area navigation can easily implement rigorous checking of such coordinates, and once established as being correct, can maintain this as well through a process, which is a lot simpler than ephemeris monitoring in GNSS.

Continuing from the bad news (propagation) to the better news (station coordinates) and finally the best news, the well-established monitoring architectures for navigation aids do represent a significant advantage for achieving integrity at the level where the signal leaves the transmit antenna compared to space vehicles. Nonetheless, some challenges remain. The first challenge is that all the work on MLS and ILS integrity, which has been extended to the associated DME's is on a per approach basis. PBN requires integrity on the basis of a flight hour. The second challenge is that an individual facility

integrity level needs to be linked to a service level integrity for PBN, where multiple DME facilities contribute to a position solution similar to what is done in GNSS. While the first challenge will be addressed later in the paper, some first ideas of how to address the second challenge are presented here. They do not represent any level of consensus. These ideas are meant to be instructive for the professional community operating conventional navigation aids on how DME service provision aspects and associated facility requirements may evolve in the future.

LINKING SERVICE LEVEL TO FACILITY LEVEL INTEGRITY

Again it is useful to compare to how integrity performance levels have been derived for GNSS. Annex 10 Vol I requires an integrity of $1 - 1 \times 10^{-7}$ / per hour for the GNSS signal in space supporting typical operations of en-route, terminal, departure as well as initial, intermediate and non-precision approach (Table 3.7.2.4-1). However, individual PBN approvals to navigation specifications supporting non-precision approach only require two orders of magnitude less:

> *Integrity. Malfunction of the aircraft navigation equipment is classified as a Major failure condition under airworthiness regulations (i.e. 1×10^{-5} per hour). [5, Volume 2, Part C, Chapter 5].*

The two orders of magnitude more for GNSS to support PBN were chosen based on the rationale that GNSS support multiple aircraft. In line with this, GPS RAIM algorithms were designed based on the following assumptions:

> *Individual satellite fault rate: 1×10^{-5} per hour*
>
> *Number of satellites used in a position solution: 10*
>
> *Resulting possible fault rate at the positioning level: 1×10^{-4} per hour*
>
> *Required missed detection probability to meet the 10^{-7} requirement: 1×10^{-3} per hour*

For DME, we take no a priori credit for the performance of airborne algorithms conducting reasonableness checks, since their performance is unquantified. We could consider however, similar to what is done for ILS, a ratio between faults which would lead to a simple unavailability (such as a large step which cannot be tracked) versus those which would actually compromise the position solution in a non-obvious way. A half-half ratio would seem to be quite conservative.

RNAV avionics capable of tracking multiple DME ranges normally track either two or four DME. Some do an “all in view” solution, but they are not very widespread yet. So assuming 4 DME ranges tracked for a position solution would be a conservative equivalent of the 10 satellites above. Given that equipment is typically dual redundant but that FMS selection logic would normally be identical for both multi-DME interrogators, it is assumed that on average the same set of 4 DME is tracked.

While Annex 10 does have a requirement that an individual DME should be able to handle 100 aircraft, it would lead us directly to a 10^{-7} requirement as is used for GNSS, whereas it is clear that a given set of DME supports a lot less aircraft than GNSS does. So some scaling down seems appropriate. Figure 1 shows the number of aircraft in a 130NM circle near Europe’s 50 busiest terminal airspaces at a peak traffic level, and the associated number of DME facilities within those same circles.

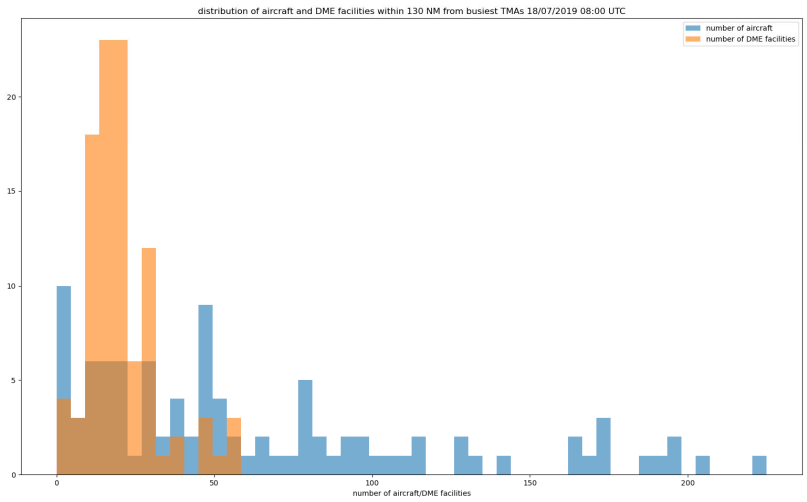

Figure 1: Number of Aircraft (blue) and DME (orange) within 130NM

during Peak Traffic near Multiple Major European Airports

The corresponding mean values are 62.7 aircraft for 20 DME facilities. Aircraft tracking 4 facilities would multiply the number of aircraft in a "single DME sense" to 250. Splitting this traffic load evenly over the available DME's (which is not conservative), we end up with 12.5 aircraft served per DME transponder. Increasing this number a bit for conservatism and then reducing it again to take into account the ratio of integrity-relevant to non-relevant aircraft positioning faults, **we can easily justify a transponder integrity requirement of 1 – 1 x 10^{-6} per hour to support PBN; one order of magnitude less than for GNSS**. A concern that remains is that this paper napkin type of analysis is geared to a DME-facility-rich environment. In light of recent crisis situations, there is an increased motivation to withdraw facilities – having a given DME transponder support only 10 aircraft (in an integrity relevant way; otherwise it would be 20) does seem like quite a luxury when the station handling capability is much higher. Current rationalization efforts focus on NDB and VOR, and often leave any colocated DME facility in place. Nonetheless, in a GNSS outage situation we would also have to consider supporting aircraft in a DME-sparse environment. However, going up to the 100 aircraft SARPs number for PBN support is considered infeasible when having to achieve suitable station geometry at lower altitudes. For the time being, it is assumed that this analysis would scale down accordingly, whereas future improvements in DME range processing by FMS would contribute further to maintaining the balance.

Having set a requirement for DME ground facility integrity performance, we can now turn to analyzing if current monitoring architectures are able to meet such a requirement.

DME/N INTEGRITY METHODOLOGY

As part of equipment design approval, the System Safety Assessment (SSA) is the verification that the implemented design meets both the qualitative and quantitative safety objectives. The allocated integrity level is the main safety objective to be assessed as achievable.

This section summarizes the guidelines available for the derivation of an integrity level based on the specific design of a DME ground transponder. The presented content is an extraction of the work performed within EUROCAE WG107 which aims at the ED57 (DME MOPS) update. A more complete version is available in [10].

Background

Relevant formulas for ground facility integrity risk calculations are present in several documents:

- ICAO Annex 10 Vol I (7th Edition, July 2018, including Amendment 92), Attachment G section 11.2.4 provides a relationship for the calculation of the integrity risk of an MLS system
- ICAO Annex 10 Vol I Attachment C, section 2.8.2.4 provides a similar formula for the calculation of the integrity risk of an ILS system
- EUROCAE ED57 section 2.3.4 proposes, for a DME/P, a derivation of the integrity failure probability which is also similar

However, these equations address only a system architecture composed by one transmission and one monitor function and do not give any guidance on how to derive integrity performance for a specific integrity monitoring architecture.

More details are given within the ICAO EUR DOC 016 [11]. Appendix E of the document provides integrity assessment examples applied to different system architectures. Integrity risks are calculated using a risk case analysis methodology which attributes quantitative hazardous failure rates to all relevant components of the system.

The given examples consider:

- The redundancy of the monitors (only the OR control decision logic is considered)
- The separation between the monitor and the control execution functions
- The case where an automatic monitor integrity test is added with dedicated resources
- The case where an automatic end-to-end test is added with dedicated resources.

The newly proposed methodology still relies on a risk case analysis and extends the applicability to commonly deployed system monitoring architectures. In addition, it derives methods for accounting of integrity risk reduction factors due to detectable component failure sequences and for calculating the integrity risk when expressed per unit time i.e. per system operational hour.

Risk Analysis

The usual way to derive system integrity risk can be structured by applying the steps as reported in the following sections.

System Decomposition of Architectural Elements

This activity consists in identifying the system architectural elements that affect the generation of a signal-in-Space (SiS) integrity violation, its detection and the relevant decision actions that need to be taken to avoid its transmission. These elements are usually identified in the transmission, monitoring, control decision and control actuation (shutdown path) functions. If the monitor function is at the same time monitored for its intended behaviour by a monitor integrity check, also the resources used to implement them need to be accounted for. Other factors that play an important role in the overall system integrity risk evaluation include:

- The presence of redundant elements in the monitoring and control functions. Note that the transmission redundancy does not play a significant role in the integrity risk reduction as the SiS integrity failure occurs when the corrupted transmitted signal is either not detected or detected but not removed.
- The control logic setting between AND/OR
- The detailed path of the shutdown from control decision to control application to transmission

- The need to periodically perform an End-To-End (ETE) test, of duration T_{ETE}, capable to detect any residual (latent) undetected fault. Note that the execution of an ETE test must include a real transmission shutdown and is usually set between 6 to 12 months.

The quantification process relies on a failure rate estimation of each element. For this aim, it is necessary to identify only those failures that affect the integrity of the transmitted signal, the monitor capability to detect and the impossibility to remove it. This activity is part of what it is defined as Failure Mode and Effect Analysis (FMEA). The results are hazardous failure rates (λ) associated to each single element.

For any item, the proposed methodology assumes that the probability $P_b(t)$ for an element to be in healthy state at time t is $P_b(t) = P_{OK}(t) = e^{-\lambda t}$ As the product λt is almost always $<< 1$ for any time $t \leq T_{ETE}$, the previous relationship can be approximated as $P_{OK}(t) \approx 1 - \lambda t$ and, consequently, $P_{NOK}(t) \approx \lambda t$.

Quantification of Cumulative Integrity Risk

Let's consider a very simple case of a system architecture composed by one transmitter and one monitor, and let be λ_T and λ_M their hazardous failure rates respectively. The risk analysis is reported in ***Table 1***.

Table 1: Risk Case Analysis for a Simplified Non-Redundant System

Risk case number	Transmitter (TR) status	Monitor status	Integrity risk	Probability integrity failure for $t < T_{ETE}$
1	OK	OK	NO	0
2	OK	NOK	NO	0
3	NOK	OK	YES (between two TR checks)	$< \lambda_T T_M \times (1-\lambda_M t)$
4	NOK	NOK	YES	$\lambda_T t \times \lambda_M t$

The total integrity risk I(t) is given by the sum of risk cases 3 and 4. I(t) is an ever-increasing function of time t. It reaches its maximum value when $t=T_{ETE}$ i.e. just before the execution of the end-to-end test. After that, I(t) is reset to 0 because, if this test is successful no integrity failure condition is present, if unsuccessful the integrity violation becomes detected and removed by maintenance. Within risk #3, the T_M parameter represents the interval time between two transmitter checks performed by the monitor. In practical current implementations, its value is on the order of very few seconds and the contribution to the integrity risk due to case #3 is always negligible, as λ_T and λ_M values are of the order of 10^{-6} failures per hour. Therefore, for times $t >> T_M$ but still $<< T_{ETE}$, the only accountable contribution is given by risk case #4 such that $I(t) \approx \lambda_T t * \lambda_M t$ and $Imax \approx I(t= T_{ETE})$. This relationship is equivalent to the ones currently present within ICAO Annex Vol 1 and ED57 when time T is equal to the end-to-end test time.

A similar approach as reported in ***Table 1*** can be followed for deriving integrity risk of more complex system architectures. Risk cases represent specific system states where a single system state is the result of a combination of single element states that assume a binary value between OK or NOK (Not OK). For a system composed of N elements there are 2^N system states that need to be analysed for determining if an integrity failure condition is present. If retained, a quantitative risk case probability evaluation is provided by multiplying the single element state probabilities. Then the overall integrity risk is given by summing up all identified hazardous system states. This process is a generalisation of a Fault Tree Analysis (FTA).

Figure 2 provides the calculated integrity risk for a fully dual system architecture composed of transmitters, monitors, monitor integrity checks, control units and shutdown paths and for different control logic voting setting between AND/OR, using hazardous failure rates representative of current designs.

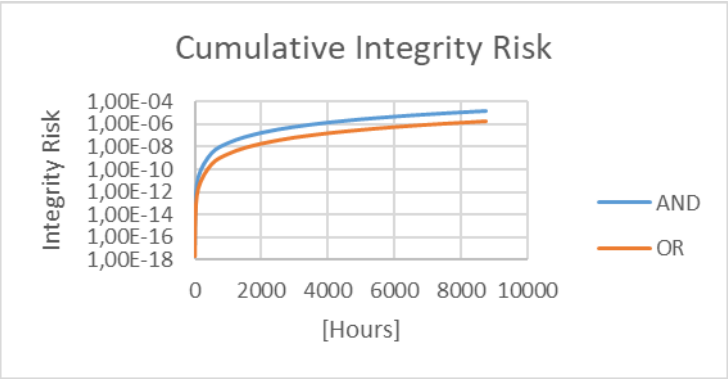

Figure 2: Integrity Cumulative Risk for a Fully Dual-Redundant Architecture

As expected, the OR setting is providing a better integrity as a transmitter shutdown decision is taken even in cases when only one monitor is alarmed, while for AND setting both monitors need to be activated. The cumulative integrity risk function is used to define the minimum intervention period of end-to-end test execution. Once an Integrity Safety Objective (ISO) is given in terms of cumulative probability, the T_{ETE} is derived as that period for which $I(T_{ETE}) \leq ISO$.

Failure Sequence Integrity Risk Reduction Factor

The cumulative integrity risk estimation as described above, is based on probabilities that certain architectural elements of a system are in failed state at a defined time t.

For example, in an architecture formed by one transmitter and one monitor and control elements, the system is in integrity signal failed state when both the transmitter and the monitor and control elements are failed i.e. when the transmitter generates a non-integer signal-on-air and the monitor and control element is not cable to detect or to remove it. However, if the two elements are independent, the real integrity violation occurs only when the monitor and control element fails before the transmitter. The opposite failure sequence is not producing an integrity failure because if the transmitter fails first, the monitor and control element is capable to shut it down.

The above rationale suggests that the integrity risk, as estimated previously, is overly conservative. The quantitative estimation consists in the determination of failure sequence reduction factors, $\alpha < 1$, defined by:

$Ir(t) = \alpha\, I(t)$ where, Ir(t) is the reduced integrity risk and I(t) is the unreduced integrity risk (without considering failure sequence)

The sequence reduction factor α is shown to be dependent on the specific equipment architecture, on their constituting element failure rates and on time t.

In a simple case, let S_{AB} be a system composed of two independent elements A and B with failure rates λ_A and λ_B respectively. Let be $P_{AB}(t) = P_A(t) \times P_B(t)$, the cumulative probability at time t for of the system where both elements are failed. We want to know which is the fraction $\alpha_{AB}(t)$ of $P_{AB}(t)$ due to the one of two possible failure sequences when A fails before B. It can be shown that:

$$\alpha_{AB}(t) = \frac{\left(1 - e^{-\lambda_B t}\right) - \frac{\lambda_B}{\lambda_A + \lambda_B}\left(1 - e^{-(\lambda_A + \lambda_B)t}\right)}{(1 - e^{-\lambda_A t})(1 - e^{-\lambda_B t})}$$

The above relationship can be approximated under the following conditions:

1) For $\lambda_A\, t$ and $\lambda_B\, t << 1$, $\alpha_{AB}(t) = 1/2$
2) For $t \rightarrow \infty$, $\alpha_{AB}(t) \rightarrow \lambda_A / (\lambda_A + \lambda_B)$

If the system is representative of a real DME system composed by monitor (A) and a transmitter (B), the SiS integrity failure condition is given when both elements are failed such that the monitor has (silently) failed before the transmitter. The opposite sequence failure would be detectable. For DME systems which are currently in operation, the condition 1) above defined is always verified for times $t < T_{ETE}$. Therefore, the cumulative integrity risk can be reduced by 50% and results in $I(t) \approx 0.5 \times \lambda_A \lambda_B t^2$, i.e. half of the value as reported in current ED57 for DME/P.

For systems having N independent elements, the number of all possible failure sequences is shown to be N!. If condition 1) above is satisfied for all elements then it can be shown that the reduction factor α is equal to $\alpha = N_i/N!$, where N_i is the number of all failure sequences that lead to a defined condition like an integrity failure. **Table 2** lists the calculated failure sequence integrity risk reduction factors for different system monitoring architectures (MIT stands for monitor integrity test, i.e., additional circuitry which checks the functioning of the monitors).

Table 2: Sequence Failure Reduction Factors for Different System Monitoring Architectures

System monitoring architecture	Number of total failure sequences	Number of total integrity failure sequences	Reduction Factor
TX-Single MON	2	1	1/2
TX- Dual MON (OR)	6	2	2/6 or 1/3
TX- Dual MON (AND)	6	4	4/6 or 2/3
TX-Single MON-MIT	6	1	1/6
TX-Dual MON-MIT (OR)	120	6	6/120 or 1/20
TX-Dual MON-MIT (AND)	120	42	42/120 or 7/20

Derivation of Integrity Risk per Operational Hour

The above integrity risk derivation is expressed in terms of a cumulative probability distribution. It represents the probability to have a signal integrity failure condition present at a time t, which has not been automatically removed by the system and regardless of when it occurred. The time t represents the time elapsed since the execution of the last end-to-end scheduled check. In absence of any other means to detect a failure occurrence and remove the corrupted signal, the cumulative distribution is also representative of the probability of having an integrity failure condition present at a specific moment in time. However, when the Integrity Safety Objective is provided per operational hour, the cumulative risk is overly conservative.

The integrity risk per operational hour is defined as the probability of having an integrity failure condition within the period [t; t+h], where t can take any value between 0 and T_{ETE} . The overall probability can be split in two components:

- The probability that the integrity failure happens in the interval [t, t+h];
- The probability that the integrity failure appeared in the interval [0; t] and was either not detected, or detected but not removed.

Therefore, a general formulation representing the integrity probability failure condition in the interval [t, t+h] is given as follows: $I_{tot}(t) = I_h(t) + I_r(t)$

Where: $I_h(t)$ represents the probability to have an integrity failure occurrence within the period [t, t+h] and $I_r(t)$ represents the probability that an integrity failure already exists at time t.

Derivation of $I_h(t)$: For the calculation of $I_h(t)$ it is observed that the probability I_h to have an integrity failure event occurrence within the time interval h can be intuitively expressed by $I_h(t) = I(t+h)-I(t)$ where I(t) is the cumulative integrity

risk at time t. Under the case where h << t, I(t+h) can be approximated by $I(t+h) \approx I(t) + I'(t)\ h$ where I'(t) is the first derivative of the function I(t). Therefore, we can write $I_h(t) \approx I'(t)\ h$.

Derivation of $I_r(t)$: In order to derive this contribution, we need to start from a high-level overview of the possible sequence of failures of the major functional blocks of a DME transponder. These functional blocks are:

- Transmitter – TX
- Monitor – MON
- Control Unit – CU and
- Shut-Down path – SD

In this approach, MON covers only the TX failure detection while CU and SD cover the controlling part, namely the execution of the transmitter shut-down. The possible failure sequences of these functional blocks are as follows:

Table 3: Failure Sequence Cases

Case	1st failure	2nd failure
A	TX	MON/CU/SD
B	CU/SD	TX
C	MON	TX

Case A: Case A occurs when the transmission fails before the monitoring and control functions. Therefore, the integrity failure condition is detected by the executive monitoring, making the equipment unserviceable.

Case B: Case B is applicable when the first failure occurs before time t and affects only the control part i.e. the control logic and/or the shutdown path. In such a case, when the transmitter fails, the monitor raises an alarm reported to the maintenance monitoring function up to the maintenance operator and possibly to an air traffic controller. Under this case, the equipment is made manually (by human-in-the-loop) unserviceable following the execution of maintenance procedures. Therefore, the contribution to the integrity risk depends on the logistic time period elapsing between the monitor detection and the transponder manual shutdown.

A quantitative relationship representing this contribution is given by the following relationship $I_B(t,h) = (\lambda_T\ N\ h)\ (\lambda_C \times t)$. Where: $\lambda_C \times t$ is the probability to have the CU/SD silently failed at time t, and $\lambda_T\ N\ h$ is the probability that the transmitter fails $N \times h$-times before t. $N \times h$ can be considered as the maximum intervention time for maintenance to remove the failure condition.

Case C: A completely silent integrity failure condition was pre-existing i.e. the integrity failure occurred before time t due to a first failure of the monitoring function (excluding the control and shutdown path part) followed by a transmission fault. Differently from case B, the case C introduces a risk that tends to accumulate over time, i.e. where a cumulative probability distribution becomes justified in evaluating the probability of having an integrity failure condition. However, case C requires that the monitor fails before the transmitter, which means that this risk can be reduced by considering the failure sequence factor. This contribution can be expressed by $I_C(t) = \alpha\ I_M(t)$ where $I_M(t)$ is the cumulative integrity risk of the system limited to only the monitoring part.

The total integrity risk within interval time [t; t+h] can therefore be derived from cumulative integrity risk-derived functions and be represented by $I_{tot}(t) \approx I'(t)\ h + (\lambda_T\ N\ h)\ (\lambda_C \times t) + \alpha\ I_M(t)$.

Figure 3 depicts a comparison between a cumulative and per operational hour integrity risk. The assumed system architecture is a dual monitor with MIT with a dual control unit and shutdown path. Control unit voting logic is assumed to be "OR". The integrity risk per operational hour accounts for the sequence failure reduction factor and assumes a maintenance intervention time of 12 hours.

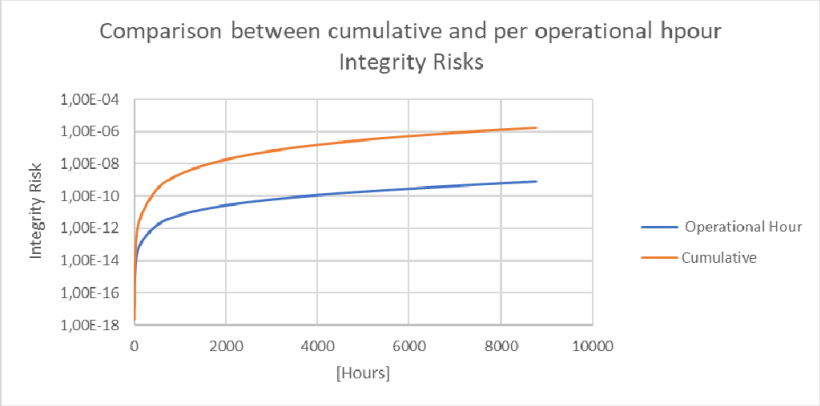

Figure 3: Comparison between Cumulative and per Operational Hour Integrity Risk

Implications for Air Navigation Service Providers (ANSP)

The integrity risk analysis has shown that two time parameters linked to service provision practicalities have an impact on the achievable facility integrity level. The first one is the intervention time, i.e., the time required between a maintenance alert and an associated maintenance action (stopping transmission). This is closely linked to the maintenance interface operated by the ANSP, including its reliability (which has not been considered here – given that these are fully independent systems with a generally high level of reliability, the impact is likely quite limited). The second one is the end-to-end test interval, which normally requires a maintenance crew to go on-site and execute an equipment shutdown. Many ANSP do this on an annual basis (8760 hours), and do not wish to increase this. An additional consideration is the choice of redundant monitoring logic, which optimizes either integrity or continuity. ANSP choosing an AND logic to optimize continuity will typically wish to continue to do so.

Here it is necessary to recall the context of PBN: RNP capable aircraft represent a more modern generation of aircraft, while RNP applications are foreseen for medium to high-density terminal areas where strategic deconfliction between arrival and departure routes requires associated path containment. In other words, qualifying DME/N for supporting RNP navigation applications is not something for remote areas with limited infrastructure and possibly associated long intervention times. This is something for network-relevant airports where normally, ANSP maintenance crews are present, while the impact of a large scale GNSS-outage could cause serious impact and therefore, a modest investment to ensure that RNP aircraft capable of multi-DME navigation can continue operations without limitations. This is not meant to leave behind business sectors such as general aviation: ensuring that the majority of network traffic can continue without contingency measures also helps in maintaining some Air Traffic Control (ATC) resources able to help a limited subset of traffic, which may require navigation assistance.

Several DME transponder manufacturers participate in EUROCAE WG107. Each of them had slightly different approaches to analyzing integrity. The integrity risk methodology developed in WG107 provides a consistent framework extendable to all possible monitoring architectures, which means that declared integrity performance becomes comparable (between various manufacturers). This is essential to achieve a harmonized level of performance for PBN. The method was applied to a Thales system commonly installed around the world. The resulting integrity performance, as a function of the two “ANSP variables” intervention time and end-to-end test time is shown in figure 4.

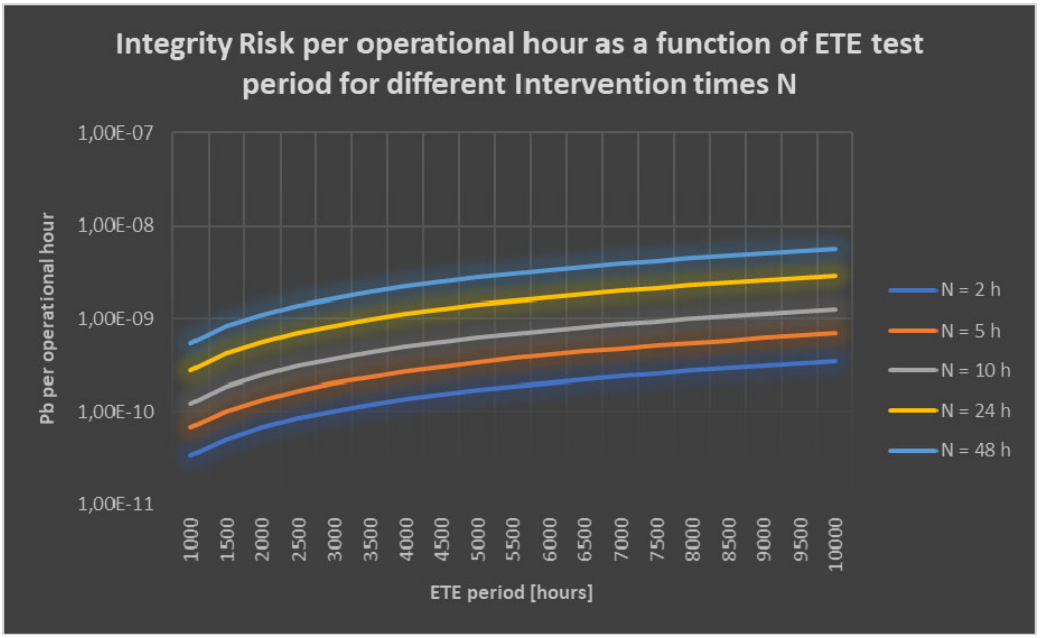

Figure 4: Integrity Performance of a Commonly Installed Thales DME Transponder

It can be seen from figure 4 that a 10^{-6} integrity risk performance is clearly achievable, even for quite generous intervention times and ETE test execution periods longer than one year. The margin shrinks for an AND configuration, but remains positive. Further work in WG107 shows that a good variety of commonly implemented architectures (even with single monitors) can meet a 10^{-6} per hour integrity risk requirement.

CONCLUSIONS

Most GNSS interference is "man-made" and therefore difficult to quantify in terms of its probability of occurrence, frequency of occurrence and area of impact. As explained in the GNSS Manual RFI Mitigation Plan [12], in this case there is a link between risk severity and probability of occurrence: if a large operational impact can be created with a relatively minor effort, this increases the probability of occurrence. The provision of an infrastructure which can maintain the large majority of air transport operations even in demanding traffic environments (further supported by inertial navigation capabilities) ensures that any intentional motivation to interrupt air traffic remains limited. Furthermore, it also guards against unintentional GNSS RFI cases. These are rare, but have occurred and certainly remain possible. The advanced PBN navigation applications which require RNP are an enabler for efficient operations which minimize noise, fuel burn and emissions.

The relevant portion of the work of EUROCAE WG107 was summarized in this paper and has the goal to provide a "means of compliance" for States to authorize RNP operations, initially to the RNP1 level, based on DME infrastructure. The foreseen target environment are terminal areas with relevant levels of traffic which justify such measures. A key ingredient for this is the provision of a DME network where individual facilities provide a $1 - 1 \times 10^{-6}$ per hour integrity level. Based on the analysis conducted so far, this appears feasible with current equipment. The associated requirements for intervention time and end-to-end shutdown test execution are also in line with current ANSP maintenance practices. The removal of faulted DME signals from transmission is a key advantage compared to GNSS, because it eliminates the need to remove the ranging source through detection by an algorithm.

Additional requirements to ensure the provision of such a high-integrity DME network for PBN were discussed earlier in this paper and include tight control of the aeronautical publication of the DME facility coordinates and elevation. The role of flight inspection is to help preserve the integrity provided by the transponder facility by detecting propagation anomalies such as multipath.

RECOMMENDATIONS

While the work of EUROCAE WG107 will not be completed before 2023, we already recommend ANSP to consider the approaches developed by WG107, in particular for DME transponder integrity. The WG107 methodology can be referred to in calls for tender, and a requirement to meet a 10^{-6} per hour integrity risk level is recommended for such procurement actions to support PBN implementation and GNSS resilience.

For the flight inspection community, we highlight its important role in preserving facility integrity in the signal in space. This is a potentially new and expanding role, considering that "multipath protection" so far mainly applies to ILS. However, for such efforts to be conducted in an efficient manner, this will likely require a cooperative approach taking into account the result of simulation tools to identify potential problem areas.

FUTURE WORK

As explained in the main body of the paper, the derivation of a DME facility integrity performance requirement has not been formally agreed. EUROCAE WG107 will further consolidate the explained approaches and remains open to further comments on the integrity risk assessment method itself, as well as its implications for service provision. This work is expected to conclude in 2023. Implementation could follow immediately as it is expected that the associated requirements will not pose any undue burdens on ground facility manufacturers, ANSP or flight inspection providers.

REFERENCES

[1] EUROCONTROL Stakeholder Forum on GNSS Radio Frequency Interference and Think Paper #9, accessed at EUROCONTROL Stakeholder Forum on GNSS | EUROCONTROL

[2] Vitan et al, Research on Alternate Positioning, Navigation and Timing in Europe, Integrated Communications, Navigation, Surveillance Conference, Herndon VA, USA, April 2018

[3] ED-57, Minimum Performance Specification for Distance Measuring Equipment (DME/N and DME/P), (ground equipment), EUROCAE, Paris, October 1992

[4] RTCA DO-236C, Minimum Aviation System Performance Standards: Required Navigation Performance for Area Navigation, RTCA, Washington DC, 2013

[5] DOC 9613, Performance Based Navigation Manual, 4th Edition, ICAO Montreal, 2013

[6] Annex 10 Volume I, Radio Navigation Aids, 7th edition incorporating amendment 92, ICAO Montreal, July 2018

[7] EUR DOC 015, European Guidance Material on Building Restricted Areas, ICAO Paris, November 2015

[8] Shrivathsan, Impact of Tropospheric Anomalies on Ground-to-Air Radio Navigation Systems, Proceedings of ION GNSS+, Miami FL, USA, September 2019

[9] Berz et al, Can Current DME Support PBN with Integrity?, Proceedings of ION GNSS+, Nashville TN, USA, September 2013

[10] Working Paper 2, DME Transponder Integrity, ICAO Navigation Systems Panel, 2nd Conventional Navigation Aids and Testing Working Group Meeting, online meeting, December 2020

[11] EUR DOC 016, European Guidance Material on Integrity Demonstration in Support of Certification of ILS and MLS Systems, 2nd Edition, ICAO Paris, November 2019

[12] DOC 9849, GNSS Manual, Advance 3rd Edition, ICAO Montreal, 2017