DOI: 10.13009/EUCASS2022-7320
9TH EUROPEAN CONFERENCE FOR AERONAUTICS AND SPACE SCIENCES (EUCASS)

# Robust FDIR approach for the future hybrid navigation system for VEGA-C

*S. Ramirez*, R. Polonio*, S. de la Riva*, C. Fernandez*, S. Diaz*, L. Favilli**, G. Mattei**, G. Curti****
**SENER Aeroespacial, C. de Severo Ochoa, 4, 28760 Tres Cantos, Madrid, Spain,*
sergio.ramirez@aeroespacial.sener; rafael.polonio@aeroespacial.sener, santiago.delariva@aeroespacial.sener, cesar.fernandez@aeroespacial.sener, silvia.diaz@aeroespacial.sener

***AVIO S.p.A., 00034 Colleferro, Metropolitan City of Rome, Italy*
leonardo.favilli@avio.com, giovanni.mattei@avio.com,

****ESA ESRIN, Via Galileo Galilei, 1, 00044 Frascati RM, Italy*
gianluca.curti@esa.int

## Abstract
NAVIGA is a navigation unit designed for its use in future space transportation systems, initially for launcher applications. This unit hybridises the data coming from two different sensors, a IMU and a GNSS, that could suffer from specific failures or degradation during its operational life, due to multiple types of causes. The unit is designed to have a high reliability, so it can be used without redundancy in critical applications, while operating in a harsh environment. One of the unit main contributors for its high reliability, is the FDIR (Failure Detection Identification and Recovery) function design. There are several types of failures (e.g. saturations, sensor degradation), that the unit needs to identify and isolate, and if necessary, to perform the necessary recovery actions. For safety-critical missions, where even a high-reliability is not enough, the unit provides the capability to detect and isolate failures, avoiding the propagation of any failure to the GNC system, and also the mechanisms to perform a warm reset to recover the unit operation. The present paper presents the FDIR design that has been selected for the NAVIGA unit, and the trade-off performed to justify it. The NAVIGA unit is currently under development, close to concluding the Phase C, with an EM available for testing the unit functionality, including the FDIR in the following months.

## Abbreviations and Symbols
In order to facilitate the lecture for the reader, the abbreviations and symbols used within the document are listed below.

| Symbol | Description |
|---|---|
| CUSUM | Cumulative Sum Test |
| DR | Detection Rate |
| FAR | False Alarm Rate |
| FDIR | Fault Detection Isolation and Recovery |
| ICST | Innovation Chi-Square Test |
| IM | Innovation Monitoring Test |
| IMU | Inertial Measurement Unit |
| MDR | Miss Detection Rate |
| SEC | Size-Effect Compensation |
| $S_k$ | Innovation cov. matrix at instant k |
| $v_k$ | Filter innovation at instant k |
| $g_k$ | CUSUM test statistic at instant k |
| $s_k$ | CUSUM distance measure at instant k |
| $d_{CUSUM}$ | CUSUM drift |

| Symbol | Description |
|---|---|
| $h_{CUSUM}$ | CUSUM threshold |
| $\gamma_k$ | ICST test statistic at instant k |
| $h_{ICST}$ | ICST threshold |
| $\hat{\sigma}_S$ | Covariance square root given by the INS solution |
| $h_{IM}$ | IM threshold |
| $i_{1,n}$ | Vector with n unitary elements |
| $n_{GNSS}$ | Number of GNSS measurements |
| $t$ | Current time (s) |
| $t_0$ | Time when the error was activated (s) |
| $e(t)$ | Error injected at instant $t$ |
| $b$ | Bias of the error injected |
| $s$ | Scale factor of the error injected |
| $N$ | White noise of the error injected |

DOI: 10.13009/EUCASS2022-7320



## 1. Introduction

NAVIGA, also named VEGA-C Navigation Equipment (VNE), is an electronic sensing/processing unit providing a navigation solution to be originally integrated in the GNC subsystem of the VEGA-C launcher. The unit is devoted to generating a complete set of reliable navigation data consistent with the GNC subsystem needs for the different phases of the associated missions [1].

The unit integrates the information coming from two subsystems: an Inertial Measurement Unit (IMU) and a Global Navigation Satellite System (GNSS) receiver. The generation of the navigation solution is carried out by the Data Fusion function that fuses the stand-alone solutions coming from the two sources, providing a robust hybrid navigation solution:

- the IMU, which provides high frequency but drifting measurements; and;
- the GNSS measurement, which provides low frequency but bounded measurements.

This joint solution assures the compliance with the system navigation needs in the different phases of the launcher lifecycle, especially at critical events following long inertial phases, like orbit injection after long ballistic phases, or after blackout exit, guaranteeing a landing accuracy requirement.

NAVIGA, as a navigation unit, will be a critical element for the GNC subsystem and consequently to the whole space vehicle. One example of this criticality is the issue accounted within the EXOMARS 2016. On 19 October of 2016, ESA's Entry, Descent and Landing Demonstrator Module (EDM) failed to land on the Mars surface due to an error sensor saturation in its inertial measurement unit (IMU). The reasons for the crash were, among other, to be blamed on the IMU, and on the GNC and fault detection, isolation, and recovery (FDIR) algorithms. Literally, according to the official report [2], two of the reasons were:

1. an “Inadequate persistence time of the IMU saturation and inadequate handling of IMU saturation by the GNC” and
2. an “Insufficient approach to FDIR and design robustness."

This example and several others, motivate the need of having a robust FDIR design for the NAVIGA unit, which needs to operate continuously, even in the presence of degraded or faulty measurement from its sensing elements, the IMU and the GNSS. This paper is centred in the definition and justification of the FDIR element that detects, identifies and removes, and even recovers from, the measurement errors of the motion sensors that constitute the VNE navigation system. It is divided into an introduction of the project context; a description of the high-level architecture of the unit and the FDIR function; the presentation of the achieved results and conclusions from them.

## 2. VNE Context and Purpose

NAVIGA combines two key elements for future space transportation systems: cost competitiveness and versatility. The design of a unit capable of achieving the same performances than similar space navigation units with a reduced cost has been possible by combining the knowledge and experience in space navigation solutions together with the know-how in developing high-precision harsh-environment aviation products. The three strategies applied to the project to reduce the unit recurrent cost, maintaining the required performances, are

- the use of sensors hybridization techniques to provide a robust navigation solution, combined with FDIR algorithms to improve the unit reliability by means of SW
- the inclusion of radiation tolerant (new space) and automotive parts, and
- the adoption of the military manufacturing processes for the production of the unit.

The second key element, versatility, is achieved by the modular and flexible design that permits having a complete qualified unit that can be adapted, with minor modification and delta tests, to other environments and space transportation missions in a short time. Advantages of this versatility are significant in the current market that is increasingly demanding new products in less time and with lower development costs. The two key elements are complemented by a third one: NAVIGA is a fully European unit that ensures the non-dependability from ITAR restriction nor from third party rights and obligations.

The purpose of the VNE development is to respond to the market need, within the VEGA-C context by:

- Producing the most cost-competitive product with very good performances.
- Adopting the state-of-the-art GNSS and IMU components and a robust hybridization scheme.
- Using, whenever possible, EU parts and avoiding ITAR restricted nor from any one with third party rights and obligations.

DOI: 10.13009/EUCASS2022-7320



- Providing a configurable and versatile unit that could be easily adapted to different missions, in a short time and with limited effort.

NAVIGA development activities are part of the VEga Consolidation and Evolution Preparation Programme (VECEP), an optional Programme of the European Space Agency, subscribed by several European countries. The program is driven by AVIO (IT), as the VEGA Launcher System Prime Contractor. The development is carried out by a consortium with a very suitable and efficient combination of skills and background experience, currently formed by DEIMOS (ES and RO), Civitanavi (IT), Innalabs (IE) ATOS (CZ) and SENER Aeroespacial (ES), being the latter also leading the activity.
NAVIGA development is currently near to complete the Phase C, with an EM available within the 2022 (see Figure 1). The Critical Design Review will be held on September 2022 and the Qualification Review within the 2023. Then, after the in-flight qualification phase, NAVIGA unit will be ready for exploitation.

## 3. Unit Design and Architecture

The NAVIGA unit follows a modular architecture, both from a functional and a physical point of view. These features allow the NAVIGA to be adapted, with a limited effort, to work in different missions. Following list includes the main elements and functions integrated in the NAVIGA unit, which are described below:

1. **GNSS board**. Based on a radiation tolerant device with a LEON2FT processor that also incorporates a GNSS core capable of processing modernized GPS and Galileo signals. This block comprises the RF Front-End and the GNSS core contained in the AGGA-4.
2. **Processing board**, managing the complete unit and communicating with the IMU and GNSS board. It integrates the data from the IMU and GNSS to provide the required output data to the OBC. It also contains the Data Fusion processing SW. This block also includes a complementary FW solution in order to optimize the resources available and to provide the best performing solution for each of the functions considered.
3. **IMU**. It provides measurements to calculate attitude, angular rates, linear velocity and position relative to the reference frame based on a set of accelerometers and gyroscopes.
4. **OBSW**: This element is in charge of the complete management of the unit and the generation of a valid navigation function. It is divided in three main blocks concerning the management of the unit itself, the GNSS processing SW, and the data fusion function where the data provided by the IMU and the GNSS are combined within a Kalman Filter (KF) that determines the final navigation solution.
5. **DC/DC board**. It receives the primary power from the unregulated power bus and provides conditioned power supplies to the VNE unit and the IMU.

The modularity in the VNE allows for different operating modes, depending on the navigation solution required: IMU only, GNSS only or hybrid. This modularity allows the unit to cover a wide range of cost and performance levels, as demanded by the project or mission. Other features and growth capabilities make the VNE a versatile unit able to operate in a wide range of missions and environments:

- Interchangeable IMU. The IMU could improve its performances either by upgrading the gyroscopes (adding fibre length) or the accelerometers, being both potential upgrades FFF compatible.
- Possible connection to additional sensors inputs (e.g. a Star Tracker).
- Configurable output rate for the navigation solution.
- The GNSS receiver has provisions to process two different frequencies or processing the signals coming from two different antennae, and then selecting the optimal source.

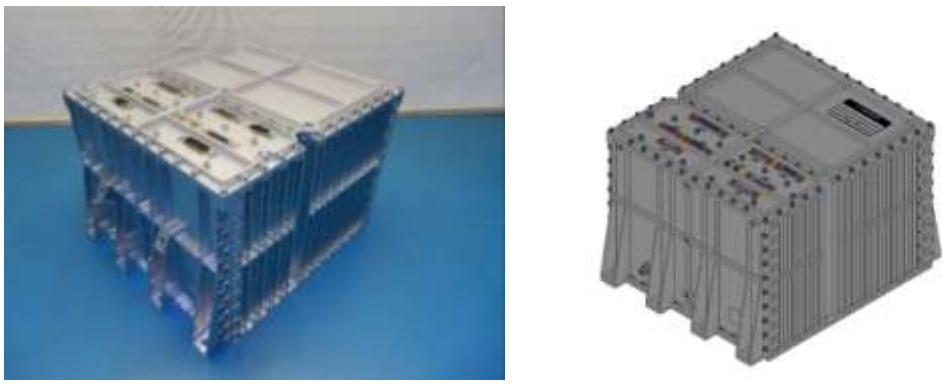

Figure 1: NAVIGA EM Model (left) and CAD Model (right)

DOI: 10.13009/EUCASS2022-7320



# 4. FDIR Design

## 4.1 General Unit FDIR

The FDIR function is a critical part of the NAVIGA unit. In general terms, the FDIR of the unit will acquire and check data coming from sensors (IMU and GNSS) and DC/DC, it monitors internal parameters produced and NAVIGA normal operation. In case this monitorization/checks detects a condition out of limit, unexpected response or situation, an event will be generated, and the recovery action (if any) would be executed. Basically, the SW implements the unit monitorization function to check its own status and to provide FDIR capability over it. The unit FDIR will perform Continuous Built-In test checks that are executed in parallel to the basic system functions. The Monitoring function is implemented via periodic checking of NAVIGA internal status variables such as:

- Analog sensors acquired (temperature and voltages)
- IMU measurements reading
- GNSS data provided,
- Data Fusion monitoring, and
- Timing/synchronization functions
- Internal memory checks performed thought the memory scrubbing

The checks will apply filtering and limits in order to avoid false triggers. The intention is that transient or spurious error will not provoke alarm reporting or recovery action execution.

The complete NAVIGA FDIR function is implemented at different acquisition and processing levels, following the hierarchical nominal dataflow of the different sensors data. Each of these levels is characterised by specific recovery actions:

- U0 – Sensor/FPGA Level
- U1 – MGMT SW Level
- U2 – DF SW Level

Each level can detect a subset of errors and perform specific recovery actions. If the level cannot perform the recovery action, or only partially, it will send the indication to the following level, to trigger the subsequent recovery action. Figure 2 provides a scheme of the NAVIGA FDIR, and the main task included in these three levels.

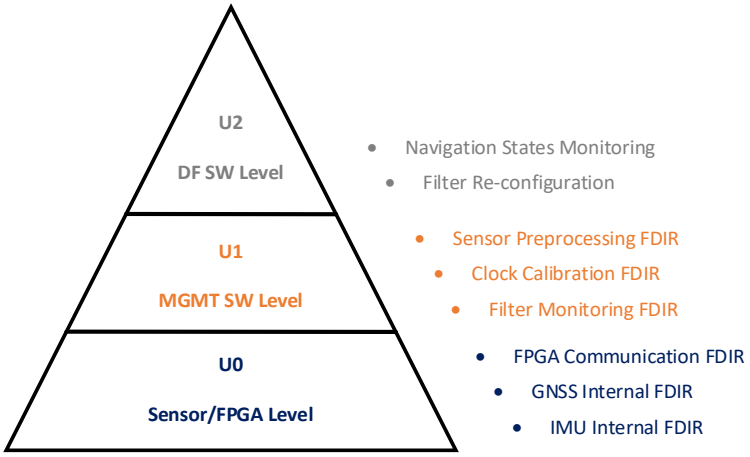


Figure 2: NAVIGA FDIR Detection/Recovery Levels

The NAVIGA FDIR will detect and manage different types of errors events, coming from the detection levels depicted in Figure 2, for which a unique identifier will be associated. Two types of error events will be provided:

- **Low severity events (LSE).** If a Low Severity event is detected the unit signals the corresponding event report in the 1553 TM and to continue with the normal operation, so it will remain in the same mode. LSE checks are split into three groups:
  - *GNSS Sensor checks. For the LSEs related to the GNSS board and/or SW.*
  - *IMU Sensor checks. For the LSEs related to the IMU sensor.*
  - *Management and DF checks. For those LSEs related to events not directly related to the sensor management and data processing.*

DOI: 10.13009/EUCASS2022-7320



- **High severity events (HSE).** If a HSE is detected in any operating mode, except for the Flight Mode, the unit will enter the Failure mode, from which it can only exit by a hard reset. If in Flight Mode, the unit is in Flight mode, the unit will try to continue in Flight Mode, carrying on its tasks, data processing and functionality according to "last survivor policy". In any case, the system will be informed by the generation of a death report, with all the details of the error, subsequently the assertion of the specified TLM line and the generation of an event TM indication the failure reason. The NAVIGA high severity events are the following:
  - *WCET (worst case execution time) violation*
  - *Unexpected SW errors*
  - *Arithmetic exceptions both in IU and FPU*
  - *Processor unexpected and unmasked exceptions (data abort, undefined instruction)*
  - *Microcontroller unmasked exceptions (managed thru the Error Signalling Module)*
  - *Watchdog time-out*
  - *EDAC double memory error*
  - *Processor board IBIT*

These errors are notified to the OBC through the 1553 bus and/or through a dedicated TLM line (depending on the concrete error event).

The NAVIGA unit does not present any internal redundancy at sensor level, thus, in Flight Mode, it needs to follow the "last survivor policy". This means that once a failure is detected, it needs to inform the System about it and to try to recover it and continue its operation. Externally, the host vehicle can switch between the redundant units, if any, in case an LSE or HSE is reported. In case the unit is not in Flight Mode, the Failure Mode will be entered if any failure is detected, to avoid the operation with a faulty unit.

## 4.2 IMU FDIR

The IMU FDIR strategy is active at different levels. The main level is the IMU processing software (U1). At this level, different actions of recovery are performed depending on the failure nature. The information about the failure is propagated, so at the U2 level, it can also execute the proper recovery depending on the situation encountered, to preserve DF performances. The main functions are included at low-level (U0) within the IMU:

- Saturation detection
- Communications check
- Temperature FDIR in case of unavailability for the thermal compensation algorithm

The main action to propagate the information upwards is to raise the IMU invalidity flags, so the following FDIR levels (U1 and U2) can interpret the information and act consequently. From the IMU status at Level U0, there are only three possible scenarios:

- **IMU degraded:** The recovery action depends on the nature of the failure:
  - In case of accelerometer failure or saturation to set the accelerometer data to 0, and to increase the IMU data noises inside the DF.
  - In the rest of the cases (mainly due to thermal probes failures and loss of sync), there is no associated recovery action, and the data coming from the accelerometers and gyroscopes is used as it is within the DF, without performing any recovery action.
- **IMU loss:** The recovery action has been concluded to set the IMU data to 0 and to increase the IMU data noises inside the DF. Note that a gyroscope failure would lead to IMU loss condition.
- **Valid measurements:** Nominal operation of the unit.

Note that at U2 level, there are further FDIR functions implemented which take the proper action at DF level, in order to try to acknowledge for the lack of inertial information received. The FTA (Fault Tree Analysis) for the IMU FDIR is presented in Figure 3.

Note that to decide the best recovery action for the IMU saturation event, a trade-off between different methods was carried out. The recovery modes considered were:

- **Method 1:** Set current measurement to 0.
- **Method 2:** Use last valid measurement as the current measurement.

Even though method 2 proved to perform better in scenarios with a constant manoeuvre rate, it also showed a less robust behaviour in periods of high dynamics. Taking into account that robustness is a key factor in the NAVIGA design, it was decided to use the Method 1 (i.e. set the measurements to zero), thus, the GNC system can decide to whether or not stop the manoeuvre when a failure is detected.

DOI: 10.13009/EUCASS2022-7320



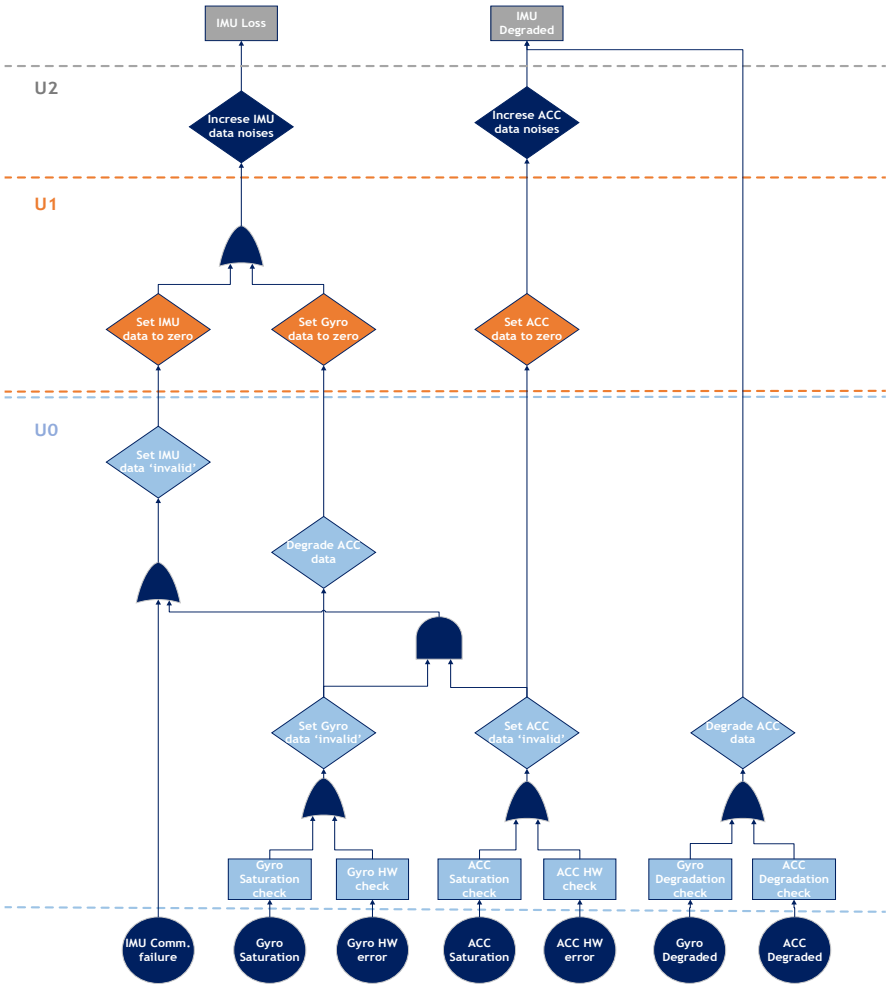


Figure 3: FTA for the IMU FDIR

### 4.3 GNSS FDIR

The navigation function of NAVIGA is designed based on an inertial propagation using IMU data, and a periodic correction of the solution by means of a loosely coupled data fusion. Aiming to improve the robustness of the navigation, the FDIR must prevent the navigation to execute the update whenever a wrong GNSS measurement is detected. Hence, the wrong measurement detected will be discarded consequently, and the navigation continues its execution as if the GNSS measurement was not available, solely relying in the IMU propagation till the GNSS is again valid. This can be graphically represented by the fault tree diagram in Figure 4. It can also be observed, how all the situations lead to a unique failure event and a nominal degraded functioning:

- IMU Only propagation (GNSS Loss): The propagation continues with the data coming from the IMU
- Nominal Operation (GNSS Degraded)

This is extremely important, since the wrong acquired GNSS solution will deteriorate the performances of the whole data fusion and could propagate the errors to the System Level.

At the GNSS sensor and FPGA (level U0), a first layer of the GNSS FDIR is implemented. The functions implemented can be summarized in five main groups:

- RF Front End Module Checks
- GNSS Electronic Checks
- Interfaces Checks
- Navigation Solution Monitoring
- RF Signal (External) Checks

DOI: 10.13009/EUCASS2022-7320



Although complete, this failure list might lead to some undetected events and for that reason, it is essential to extend the FDIR at levels U1 and U2 to avoid using a measurement that should have been discarded for the navigation solution. The aim of these GNSS FDIR functions at higher level would be to

- Monitor sudden changes in the navigation solution, or sudden differences between GNSS and DF navigation solutions beyond a defined threshold.
- Detect unexpected lack of GNSS signal.

From the GNSS status, there are only three possible scenarios at DF level:

- **GNSS loss:** No recovery strategy is envisaged. In case of GNSS failure detection, the measurement will be discarded. The navigation solution could still be provided since the IMU could propagate the state while the GNSS is unavailable (IMU only propagation).
- **GNSS degraded:** In case of using doppler or detecting a high jerk, a specific measurements noises should be used within the DF. Thus, the GNSS measurement is still used but considering a higher expected error.
- **Valid measurements:** Nominal operation of the unit.

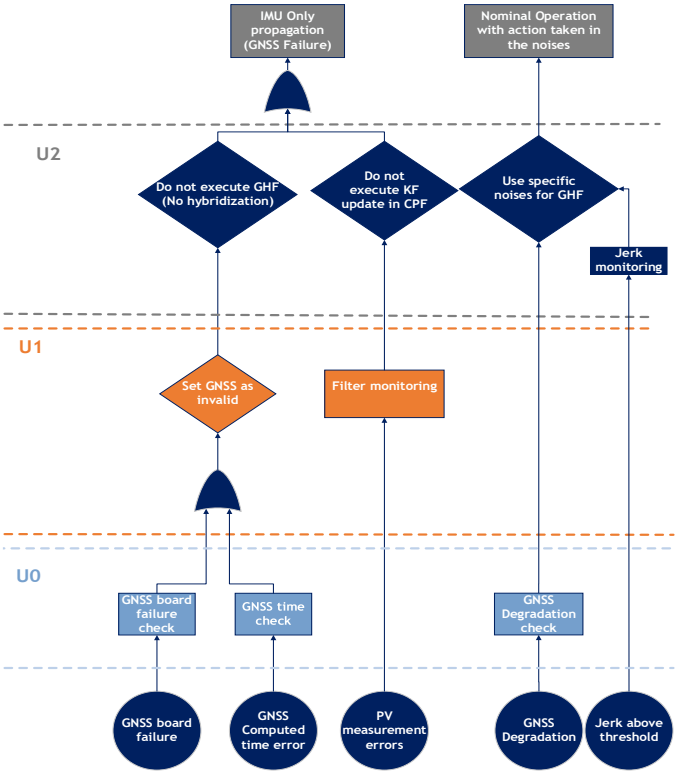


Figure 4: FTA GNSS FDIR

The first objective of the GNSS FDIR at level U1 and U2, to monitor differences between GNSS and DF solution, is the most complex one, since there is none straightforward algorithm and architecture able to differentiate between failures coming from the GNSS or the IMU propagation. The typical algorithms are based on the statistics between the predicted data from the propagation and the innovations of the filter implemented within the Data Fusion. Several algorithms are described below and later tested in Section §5.2.

## Filter Monitoring

This check is devoted to detecting any inconsistency in the Kalman filter behaviour, which will be identified as an error in the processed measurement. The filter monitoring checks are based on statistical methods, that analyse the residuals or innovations of the filter. In case of misbehaviour of the measurement, the innovation for example would exceed its associated covariance, which basically means that the difference between the measurement with respect to the navigation solution is higher than approximately the measurement covariance plus the navigation covariance. Put another way, the measurement is out of the expected range of values. In the following section a trade-off between the most common filter monitoring algorithms is presented. The considered algorithms are:

DOI: 10.13009/EUCASS2022-7320



- **Cumulative sum (CUSUM)**: The functioning of the algorithm is simple; it computes the cumulative sum of the distance measurement given as an input. The distance measurement is defined as the normalized innovation (innovation divided by the innovation standard deviation). This distance measurement is the input for the stopping rule of the method which is defined using thresholds. For a further description of the CUSUM algorithm see [3].
  To prevent possible drifts, two actions are taken:
  - Subtract a small drift term ($d$) at each time step term to prevent false alarms preventing positive drifts.
  - To prevent a negative drift, which will increase the time detection after a change is occurring, the test statistic is reset when it becomes smaller than 0

  The distance measure is computed as:

$$s_k = \frac{1}{\sqrt{n_{GNSS}}}\, i_{1,n_{GNSS}}^T\, \boldsymbol{S}_k^{-\frac{1}{2}}\, \nu_k \tag{1}$$

  And the algorithms can be written as:

$$\begin{cases} g_k = g_{k-1} + s_k - d_{CUSUM} \\ H_0 \colon g_k < 0 \rightarrow g_k = 0 \rightarrow \ Normal\ Scenario \\ H_1 \colon g_k > h_{CUSUM} > 0 \rightarrow g_k = 0 \rightarrow \ Failure\ detected \end{cases} \tag{2}$$

- **Innovation Chi-Square Test (ICST):** This test relies on the chi-square detection method, for a broader description on this topic see [4]. The failure detection based on the innovation chi-square test is normally implemented by filtering the innovation at a single epoch. Thus, the statistic is usually built as the weighted norm of the current time t innovation vector, that is:

$$\gamma_k = \nu_k^T\, \boldsymbol{S_k^{-1}}\, \nu_k \tag{3}$$

  In case there is no failure, the test statistic ($\gamma_k$), follows a central chi-square distribution with $n$ degrees of freedom, being $n$ the number of measurements at time $k$: $\gamma_k \sim \chi_n^2$
  The threshold $h_{ICST}$ to determine the existence of failure or not is computed using the inverse chi-square cumulative distribution for a certain probability of false alarm ( $P_f$ ) and a fixed degrees of freedom value $n$

$$\begin{cases} H_0 \colon\ \gamma_k < h_{ICST} & \rightarrow \ Normal\ Scenario \\ H_1 \colon\ \gamma_k \geq h_{ICST} & \rightarrow \ Fault\ Scenario \end{cases} \tag{4}$$

- **Innovation Monitoring (IM):** This algorithm explodes the benefits of using a navigation hybrid solution, it is equivalent to check internally the correct execution of the filter estimation, since it compares the innovation with the covariance of the innovation, and it checks it is not beyond a threshold. The algorithm can be summarized as:

$$\begin{cases} H_0 \colon & |\nu| < h_{IM} \cdot \hat{\sigma}_S \rightarrow \ Normal\ Scenario \\ H_1 \colon & |\nu| \geq h_{IM} \cdot \hat{\sigma}_S \rightarrow \ Fault\ Scenario \end{cases} \tag{5}$$

DOI: 10.13009/EUCASS2022-7320



### KF Reset

In the filter monitoring algorithms, it is detected that there are outliers where the GNSS FDIR algorithm discards the solution for long periods, leading to a notorious degradation of the performance. This is caused because a miss estimation of the IMU parameter occurs (due to a miss detection of a GNSS PV error), leading to:

- High values of the innovation since the propagated solution drifts promptly due to a miss estimation of the IMU parameters
- Low values of the innovation covariance since it is considered that the IMU parameters are correctly estimated

All the filter monitoring algorithms rely on comparing the innovation to its covariance; therefore, all three algorithms would discard the GNSS solution in that scenario. To solve this issue, it was decided to implement a filter reset mode. This mode will be entered when the GNSS FDIR flag is active for a long period and the following actions will be carried out:

- To reset the IMU parameters and the covariance associated to the IMU parameters. As commented before, this malfunction of the filter is caused by a misestimation of the IMU parameters, therefore, to avoid this scenario we reset these values.
- To force the hybridization of the next GNSS measurement but only hybridizing position, velocity and attitude. We are not able to detect if the GNSS measurement is faulty, therefore, it is more robust to only hybridize position, velocity and attitude to avoid the misestimation of the IMU parameters.

The performance obtained by this FDIR implementation is presented in Section §5.2.

## 5. Filter Monitoring Performance Analysis

In this section we will describe the trade-off analyses to decide which FDIR algorithm suits better to our problem. The proposed parametrization for the algorithms is shown in following table:

Table 1: Filter monitoring algorithm's parameters

| | **CUSUM** | **ICST** | **IM** |
|---|---|---|---|
| Threshold | 4 | 16.81 | 3.5 |
| Drift | 2 | - | - |

### 5.1 Test Cases

For all the analyses an in-house simulator of the VNE unit has been used. In order to test the FDIR performance, we have considered a VEGA-C trajectory where several PV errors have been inserted along the trajectory. The error's model is defined as:

$$e(t) = b + s * (t - t_0) + N \quad \textbf{(6)}$$

A more detailed description of each simulation carried out is presented in Table 2.

Table 2: PV Errors: Simulation setup

| **ID** | **Injection time[s]** | **Duration [s]** | **Bias ($3\sigma$)** | **Scale Factor ($3\sigma$)** | **Noise Power (max)** | **Figures** |
|---|---|---|---|---|---|---|
| 01 | 1 each 1000 seconds | 15-100 | P: 600 m<br>V: 27 m/s | P: 3 m/s<br>V: 0.07 m/s$^2$ | P: 10 $m^2 \cdot Hz^{-1}$<br>V: 0.1 $(m/s)^2 \cdot Hz^{-1}$<br>Sample Time: 0.5 ms | Figure 5, Figure 6 |
| 02 | Same set-up as ID-01. In this case, the FDIR active is the ICST algorithm. | | | | | Figure 5, Figure 6 |
| 03 | Same set-up as ID-01. In this case, the FDIR active is the IM algorithm. | | | | | Figure 5, Figure 6 |
| 04 | Same set-up as ID-01. In this case, the KF reset mode is included. | | | | | Figure 7, Figure 8 |
| 05 | Same set-up as ID-02. In this case, the KF reset mode is included | | | | | Figure 7, Figure 8 |
| 06 | Same set-up as ID-03. In this case, the KF reset mode is included | | | | | Figure 7, Figure 8 |

DOI: 10.13009/EUCASS2022-7320



### 5.2 Results

To demonstrate the performances of the FDIR algorithms, several figures of merit are calculated for each of them. The most important ones are:

- Detection Rate: It is the percentage of failures detected by the FDIR

$$DR\ [\%] = \frac{Failures_{detected}}{Failures_{injected}} \cdot 100 \tag{7}$$

- Miss Detection Rate: It is the complementary of the latter, that is the percentage of failures not detected by the FDIR

$$MDR\ [\%] = \frac{Failures_{notDetected}}{Failures_{injected}} \cdot 100 \tag{8}$$

$MDR = 1 - DR.$

- False Alarm Rate: It is the percentage of time that the FDIR is active when there is no failure injected.

$$FAR\ [\%] = \frac{t_{FDIR_{FlagActive}}}{t_{T,FDIR_{FlagActive}}} \cdot 100 \tag{9}$$

Where $t_{T,FDIR_{FlagActive}}$ stands for the total time in which the FDIR flag is activated along the simulation.

An ideal FDIR will present a 100% of detections and a 0% of false alarm rate. In this way, tuning the FDIR thresholds is a compromise between the false alarm rate achieved and the detection rate.

The computation of these FOM for the different FDIR algorithms have been collected in a histogram which correlates the probability of encountering a miss detection or false alarm with respect to the number of MC shots, also, it shows the Gaussian distribution exhibited in the MC:

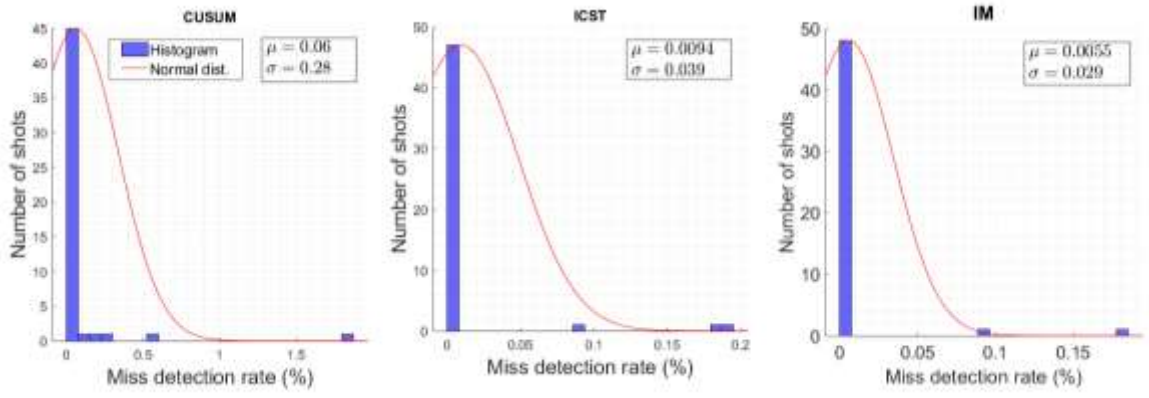


Figure 5: PV Errors trade-off - Miss detection performance without KF reset mode

DOI: 10.13009/EUCASS2022-7320



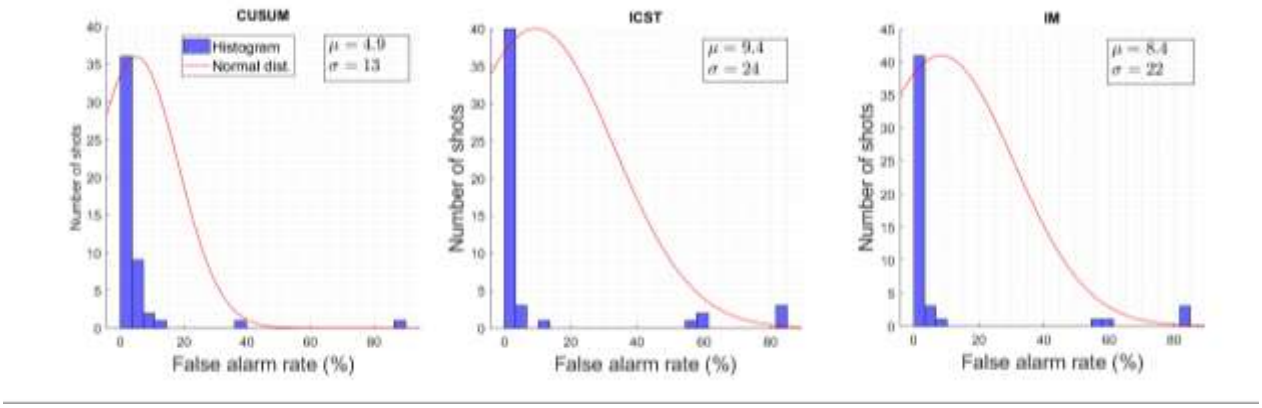


Figure 6: PV Errors trade-off - False alarm rate performance without KF reset mode

The following conclusions can be extracted from Figure 5 and Figure 6:

- IM achieves the best miss detection rate performance, followed closely by the ICST algorithm.
- CUSUM algorithm stands out in terms of false alarm rate performance but also shows the worst miss detection rate performance

In all the algorithms it is detected that there are outliers where the false alarm rate is greater than 50%. These outliers are explained by the scenario presented above. These outliers present error of the order of magnitude of 100 km in position and 500 m/s in velocity. To test the efficiency of the KF reset mode proposed, we carry out the same analysis but with the KF reset mode implemented. The results obtained are presented in Figure 7 and Figure 8.

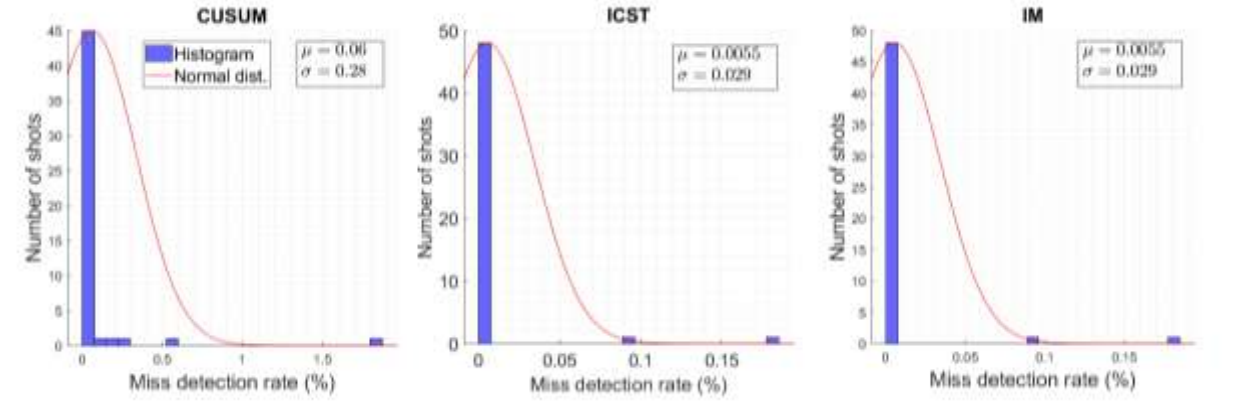


Figure 7: PV Errors trade-off - Miss detection rate performance with KF reset mode

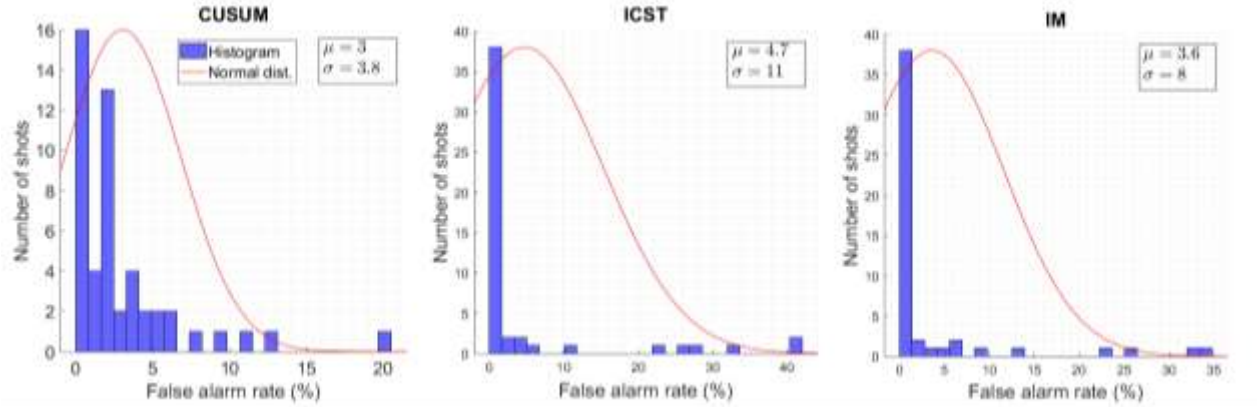


Figure 8: PV Errors trade-off - False alarm rate performance with KF reset mode

DOI: 10.13009/EUCASS2022-7320



As it can be appreciated, the outliers have been eliminated reducing the false alarm rate notoriously. Note that the miss detection rate has not been affected since the modification implemented only affects cases where a miss detection occurs.
The three algorithms show similar performance in terms of position and velocity: velocity error < 1 m/s $3\sigma$ and position error <200 m $3\sigma$ for most of the trajectory. This result shows how the robust FDIR implemented allows to achieve continuous acceptable performances even in an environment of GNSS faults.
Since the three algorithms show the same performance, it was decided to implement the Innovation Monitoring given its simplicity compared to the other two algorithms. Note that since all algorithms rely on the monitoring of the innovation, it is reasonable that they show similar performance.

## 6. Conclusions

The FDIR function is a critical element of any complex autonomous system. For the NAVIGA unit, this element is especially critical in order to maintain a high reliability. In case of detected errors at sensor level, the FDIR strategy is always simple and robust, but for the case of undetected errors, the FDIR design becomes a great challenge. This is particularly paramount for the GNSS sensor, which is the accurate sensor that corrects the propagation drifts, and that can suffer from failures difficult to detect (e.g. measurement spikes, jamming, spoofing). The main idea behind the FDIR design for the NAVIGA unit, is to detect and isolate the failure as soon as possible, and to try to continue the operation following the “last survivor policy”. The decision is then passed to the GNC system to whether continue the operation, abort it, or switch to the redundant chain. This paper has presented the specific design for the FDIR of the NAVIGA unit, and how it behaves against different “undetected” GNSS errors.

## Acknowledgments

This work has been carried out in the frame of the VECEP and VNE programme of the European Space Agency with AVIO as Costumer for the NAVIGA unit. In this context, SENER is the lead contractor for the development of the VNE. NAVIGA (VNE) is a joint effort of many individuals and organisations during several years. We would like to thank to:

- All current and previous NAVIGA team members at SENER, AVIO, ESA/ESRIN (Frascati, Italy) and different partners from industry that worked hard during all this time to reach current state of the project.
- All States and Delegations supporting the ESA VEGA development programme, and in particular the Italian and Spanish delegation, who have believed in and firmly committed to the project.

## References

[1] S. Diaz, C. P. Fernandez, et al. 2020. NAVIGA: A Modular Low-Cost Space Navigation Unit for Space Transportation. *71st International Astronautical Congress (IAC)*
[2] Toni Tolker-Nielsen 2017. ESA. EXOMARS 2016 - Schiaparelli Anomaly Inquiry. Tech. rep. DG-I/2017/546/TTN. *European Space Agency (ESA), May 2017, p. 28*
[3] I. Nikiforov, V. Varavva, V. Kireichikov, 1993, Application of statistical fault detection algorithms to navigation systems monitoring, *Automatica Volume 29, Issue 5 Pages 1275-1290,*
[4] B. Brumback and M. Srinath June 1987, "A Chi-square test for fault-detection in Kalman filters," in *IEEE Transactions on Automatic Control, vol. 32, no. 6, pp. 552-554,*