

Integrity Investigations Within the European Galileo System Test Bed (GSTB)

Wolfgang Werner, Norbert Lemke, Ingrid Deuster, Udo Rossbach

IfEN Gesellschaft für Satellitennavigation mbH (IfEN GmbH), D-85586 Poing, Germany

BIOGRAPHIES

Wolfgang Werner received a diploma in Computer Science from the University of Technology in Munich in 1994. He worked as a research associate at the Institute of Geodesy and Navigation (IfEN) in the field of high-precision differential GPS (DGPS), ambiguity resolution and airport pseudolite (APL) research. In 2000 he received his Ph. D. from the University FAF Munich. Since 1999 he is Technical Director of IfEN GmbH. Having been responsible for the EGNOS Independent Check Set algorithm development, he is currently working on Galileo integrity algorithms.

Norbert Lemke is a project manager and senior systems engineer for navigation applications and receiver development at IfEN GmbH. He holds a diploma (MSc) in Aerospace Engineering from Berlin University of Technology. Currently he works in the field of navigation, integrity, receiver development and telematics.

Ingrid Deuster holds a diploma in Geodesy from the University of Stuttgart. In 1998/1999 she worked as a research associate at the Institute of Photogrammetry and Cartography of the University FAF Munich. She joined IfEN in 1999 as a systems engineer and has worked since then in the field of satellite navigation integrity. She was involved in the EGNOS Check Set algorithm development and in the Galileo Integrity Performance Assessment (GIPA) early trials. Currently she is working for the GSTB project.

Udo Rossbach holds a Ph. D. in surveying engineering from the University of Federal Armed Forces Munich, Germany. Since 1999 he is working as a systems engineer with IfEN GmbH. There he is involved in the development of GPS / GLONASS / EGNOS / Galileo algorithms and software.

ABSTRACT

The European Galileo System Test Bed V1 (GSTB-V1) main goal is to reduce major risks inherent with Galileo system design activities and algorithm developments. One important issue hereby is to investigate the Galileo system with respect to achievable performances and to select the final set of orbit determination, time synchronisation (OD&TS) and integrity algorithms out of a set of candidate system algorithms. One of the major aspects is focussed on system integrity analyses. GSTB makes use of GPS data monitored by a worldwide network of ground stations. These data are gathered at the GSTB processing centre (GPC) and fed into a chain of processing facilities, providing OD&TS algorithms as well as signal-in-space accuracy (SISA) and integrity algorithms. Analysis results will be extrapolated to Galileo signal structures and frequencies.

The GSTB element that provides the capability to investigate integrity issues is called Experimental Integrity Processing Facility (E-IPF). It is designed to allow for flexible data evaluation and experimentations. Integrity performances will be estimated based on the OD&TS computation results and "truth references" (precise orbits and clocks) taken from the International GPS Service (IGS).

Two different possibilities are foreseen how the E-IPF can be exploited:

On the one hand, there is a routine data processing that works in a (more or less) continuous way. The raw measurement data coming from the ground stations network are gathered at the Data Server Facility (DSF) and forwarded together with SISA data to E-IPF for this standard data processing. The produced data are integrity flags, false alarm and missed-detection rates and several other types of

statistics and useful integrity-related information. All these data will be made freely available through the worldwide web (WWW).

The second way to use the E-IPF is through specialised integrity experimentation. Here the E-IPF can be configured in a very flexible way to output relevant integrity-related diagnostic data and statistics. This way of usage, however, requires expert knowledge and is restricted to authorised users only.

The first part of the paper presents the context and overall design of the E-IPF together with the core products that are generated by the E-IPF. There will be five main components in the E-IPF: interface server, processing kernel, configuration tool, monitoring agent and long-term statistics generator. Each of these components, their functionalities and interrelations are described in detail.

The second part of the paper describes the implemented Galileo baseline algorithms as well as several alternate candidate core integrity algorithms and the possibilities for integrity test case experimenting. Furthermore, simulation and manipulation algorithms that are used to contaminate the raw measurement data with different types of feared events as well as the necessary analysing algorithms are presented. As the operational phase of the GSTB processing centre and the routine data processing is about starting, some early results are also provided.

EXPERIMENTAL IPF ARCHITECTURE

The following figure 1 shows the architecture of the E-IPF:

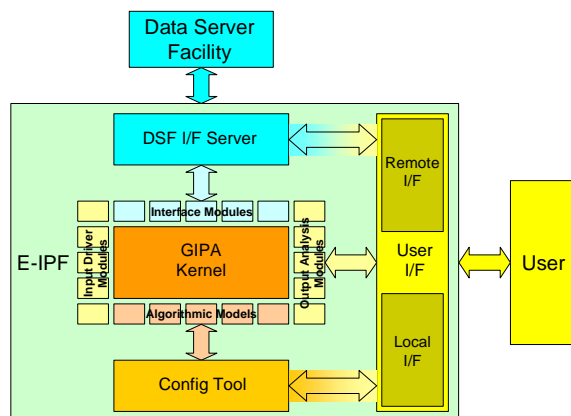


Figure 1: Experimental IPF architecture

The E-IPF SW has been developed as platform-independent as possible, making use of Trolltech's Qt library.

The heart of the E-IPF SW is the processing kernel. The processing kernel has integrated a set of around 230 algorithmic modules that perform all required processing tasks. Among these modules are: earth tidal correction, tropospheric and ionospheric correction, station synchronisation, carrier-phase smoothing, satellite anomaly detection, the integrity check modules, and quite a number of basic modules for low-level data transformation tasks or graphical displays. Also available are modules for data input and output as well as a certain set of simulation and statistical analysis modules.

All the available modules can be inserted in a configuration and linked together as needed. This allows for a very high flexibility in experimenting with the algorithms.

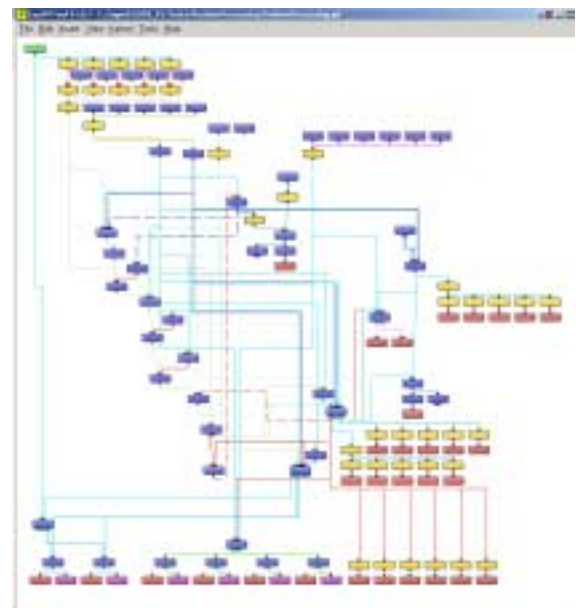


Figure 2: ExpIPFTool screen-shot (PC platform)

The price to pay for this high flexibility is the complexity of the configurations. One complex configuration (which is used for the routine processing of the E-IPF) is shown in figure 2. For an easier configuration of the E-IPF, two different features have been implemented: a configuration tool that allows to graphically configuring the system, and a simplified configuration possibility that makes use of a simplified configuration file of a different format together with a "frozen" configuration file template.

The following figure 3 shows the E-IPF SW components. These components are stand-alone executables that have a well-defined interface with each other and with the DSF, which is the central data archive and storage element of the GSTB-V1.

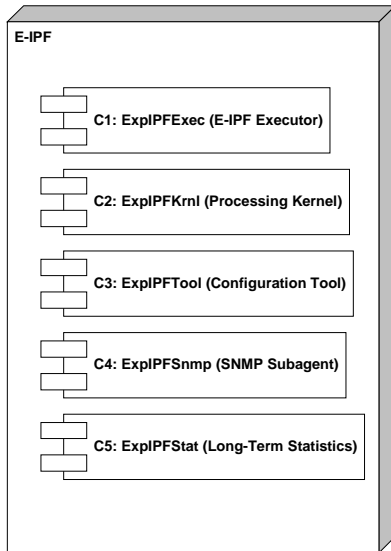


Figure 3: Experimental IPF breakdown

The E-IPF SW is divided into the following five components:

- E-IPF Executor
- Processing Kernel
- Configuration Tool
- SNMP Demon
- Long-term statistics

Each of these is briefly described in the following.

Executor Component

The E-IPF Executor is the SW component that realises the E-IPF operator interface for the routine data processing or for test case experiments, where monitoring and control capabilities have to be used. It is the SW component that will be called by the routine operator for performing the routine operations.

The main functionalities of this SW component are:

- Transfer E-IPF input data (via FTP) from DSF to the E-IPF session directory
- Step through the multi-session file (see below) provided by the operator
- Start the E-IPF kernel or statistics component with the appropriate configuration for each individual session
- Transfer E-IPF output data (via FTP) back to DSF

Dependent on the type of input configuration file, the executor either prepares a session for kernel processing, for long-term statistics computation or performs a "merge" between a simplified routine processing configuration file and the E-IPF resident "frozen" configuration file. The output of this

"merge" process is a standard kernel configuration file that may be passed directly to the kernel component.

An execution of the E-IPF is triggered via a system-level defined multi-session approach: A filename of a multi-session file is passed to the executor component. This multi-session file contains the filenames of a certain number of session files. Each session file defines a clear task for the E-IPF. In this way, the E-IPF can be used within a pre-defined regular processing schedule or even for some kind of backlog processing. This is a necessary feature, because after a change in the baseline algorithms or in the tuning of parameters for these baseline algorithms, all relevant processing has to be repeated, when consolidated long-term statistics must be evaluated.

Finally, the executor component also performs all data housekeeping activities that are related to the E-IPF platform itself. Especially in cases, when there is insufficient disk space available, the GPC operator has to be warned.

Kernel Component

The kernel is the heart of E-IPF processing. It integrates a slim scheduling mechanism with a flexible linker mechanism and the full set of algorithmic modules. These modules are also included in the configuration tool component. This modular architecture allows easy expansion of the system via integration of new modules. The E-IPF allows also an integration of external modules that can be configured and, hence, included in the scheduling scheme.

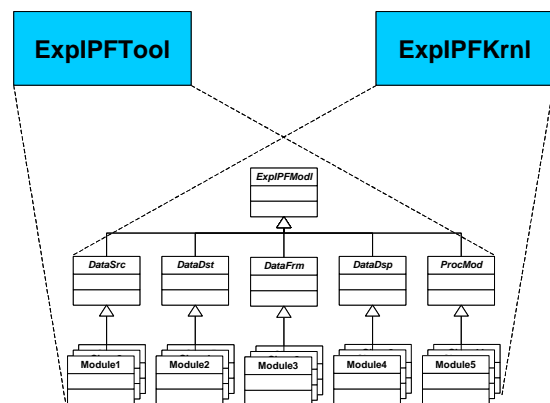


Figure 4: Algorithmic modules E-IPF components

However, the interfaces of the modules as used by the kernel are different from the interfaces as used by the configuration tool. While the kernel mainly uses three virtual functions, called "Init", "Exec" and "Exit", the configuration tool uses a module

interface that provides information about the syntactical specification and the configuration parameters of each module.

Once the kernel component has read its configuration, it sets its starting and end processing times and steps through the processing via a pre-defined epoch interval (normally set to one second). During each second each modules' "Exec" function is called in a pre-defined sequence that respects all data dependencies.

The kernel, thus, works through the configuration of modules once per processing epoch. No screen output is performed by the kernel itself. Screen outputs can, however, be generated by usage of the display type modules, when a certain key parameter is set.

Nevertheless, the kernel run can be monitored via an E-IPF specific SNMP MIB-tree (management information base tree) extension, or may even be stopped via a further call of the executor component.

Tool Component

The objective of the configuration tool is to allow an easy configurability of the E-IPF kernel. Due to the flexibility of linking different modules together as needed, setting up a complex configuration is not an easy task. For this reason, the tool allows to do the configuration graphically by just inserting the modules from a menu and linking them by clicking their input and output data sockets.

The figure 5 below shows a screen shot of the running E-IPF SW (the tool window in the middle right place) and a few graphical display modules that have been configured for a short analysis.

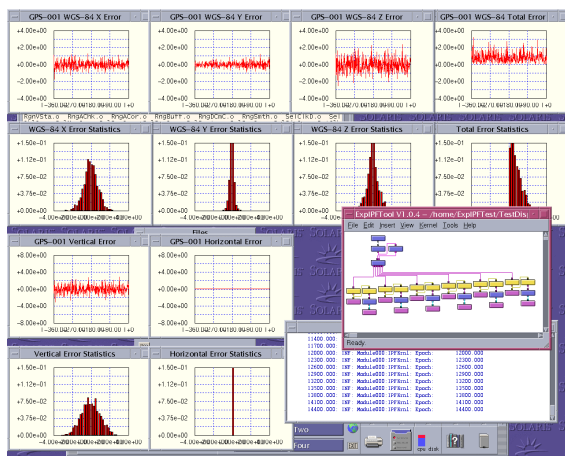


Figure 5: E-IPF in action (Solaris platform)

SNMP Component

This component is a minor component that is realising the SNMP protocol interface to the DSF (or any other monitoring element).

The SNMP private part for the E-IPF provides information on the E-IPF internal health status, memory consumption and session and multi-session processing status. This information is normally retrieved (monitored) at a regular basis by the DSF.

Long-term Statistics Component

The objective of the statistics component is to build long-term statistics over a configured time-interval based on the results of individual kernel processing runs.

The kernel normally generates the core products and all statistics based on its processing of batches of 24 hours of data. As the kernel does only work with data that are available in this time window, no long-term statistics can be generated by itself. For this reason, the statistics component receives in input a set of 24-hour-statistics (e.g. from a single week) and accumulates all relevant data. Moreover, it is possible to accumulate e.g. an already accumulated one-week statistic with additional ones. As the file formats are identical, the period may be chosen as desired by the experimenter and/or GPC operator.

The long-term statistics accumulation is required, because the extremely low figures that are involved in satellite navigation integrity processing (false alarm or missed-detection rates) require a huge amount of samples that in real-data processing will only be available after a long time of experimenting. To arrive at consolidated figures for the important risks (and hence budgets that have to be allocated to individual events in GPS/Galileo) a very long time of data processing is needed.

Nevertheless care must be used, as no baseline algorithm or parameter change should have been performed during this time.

ROUTINE PROCESSING

The E-IPF is capable of producing a wealth of integrity-related core products. In the following a brief overview of the main core products that are produced within the routine processing is provided:

- IF (Integrity Flag) Mean Update Rate Statistic (Probability of False Alarm)

- Time Synchronisation Error Statistics at Sensor Stations
- IF false alarm/ miss detection rate statistics vs. number of observing sensor stations
- VPL/HPL vs. true error Stanford graphics obtained with GPS data
- Availability graphics for GPS VPL < 20 m using high density stations network for Global coverage
- Availability graphics for GPS VPL < 12 m using high density stations network for Global coverage
- Estimated SISE (signal in space error) at WUL (worst user location) per satellite
- Integrity flag per satellite
- Integrity Check reference data: true SISE per satellite
- Sigma check per satellite

There are several more core products that may be generated by use of the E-IPF, but the above listed products are generated on a day-by-day basis in routine processing. Long-term products are also built from some of these to obtain system level performance results.

Among the additional products that are available in experimentation are:

- Availability graphics for GPS VPL < 20 m using high density stations network for European coverage
- Availability graphics for GPS VPL < 12 m using high density stations network for European coverage
- Estimated satellite/plane error per satellite
- Integrity Check reference data: true satellite error
- Sigma-check maps (quality figure for accuracy of satellite error estimation)
- Generic time series data and one- or two dimensional histogram data

For the routine processing a set of baseline algorithms and their related baseline parameters have been or are just on the way of being fixed. Currently the following key algorithms are used for the baseline integrity processing:

- Raw data validation: The raw pseudo-range is compared to the computed pseudo-range. The difference between these two ranges is compared with a configured threshold.
- Frequency crosscheck: The differences between the measurements on both L1 and L2 frequency are compared and checked via a further configurable threshold.

- Range-variation check: The raw pseudo-ranges of the current epoch and of the previous epochs are compared. If the variation exceeds a certain limit, the ranges are discarded.
- Tropospheric model: The tropospheric model from ESA (*ESA, 2003*) is used. Standard values are used to evaluate the model instead of using real measurements. However, there is an integrity experiment foreseen that uses real measurements as an input.
- Cycle-slip detection: The cycle-slip detection and repair is based on a combination of a third order time difference and a second order polynomial fit.
- Multipath detection and removal: An algorithm is used that is based on a set of digital filter coefficients working on code minus carrier observables.
- Ionospheric delay correction: No ionospheric correction is used, because the dual-frequency iono-free combination is used as an input to the integrity check algorithm.
- Sagnac effect: Earth rotation effect during signal travel time is corrected.
- Solid earth tides: The sensor station position displacement due to the solid earth tides is corrected.
- Modified Hatch filter: Code range measurements are smoothed using carrier-phase measurements and a configurable smoothing time constant.
- Clock estimation for sensor stations: The residual measurements are averaged and outliers are detected and excluded. The averaged values are band-pass filtered.
- Clock jump / drift detection: The current measurement is compared against an expected value, computed with the help of previous measurements based on an extrapolated polynomial fit. Clock drifts are identified by analysing the polynomial coefficients.
- Satellite and station failures: These types of failures are identified via majority crosschecks.
- SISE estimation according to Galileo B2 phase. The worst user SISE is estimated through an estimation of the satellite position error (satellite level) based on a three parameters approach. The estimated position error is projected to all potential users in the satellite footprint.
- Integrity check algorithm according to Galileo B2 phase. This algorithm considers

the probability of false alarm as well as the probability of missed detection.

- Integrity flag representation is two bits. The associated values can be "monitored", "not monitored" or "don't use".
- Protection level computation is performed according to the MOPS (minimum operational performance standards, *RTCA, 1999*) HPL/VPL equations. The term for flight-technical errors ($\sigma\text{-flt}$) is replaced by the SISA. The other components of the weight for the least-squares estimation are unchanged.

Several alternative algorithms have also been implemented (e.g. GIPA integrity algorithm, see *Werner, 2002* and *Werner et al., 2001*) and comparable tests between the different choices of algorithms can be performed in the experimentation.

INTEGRITY EXPERIMENTATION

The Integrity Test Case experimentation makes extensive use of the E-IPF platform. The experimentation is decomposed in the eight categories A to H according to the following logic:

Category A: Allocation

The aim of this category is to clarify integrity architectural related issues. Within this category there are two test cases:

- ITC-A.1: Integrity System Allocation deals with different SISA/IF concepts and the impact of these concepts for the integrity tree including the integrity risk for the user segment. It will also describe how the results of other elementary test cases are linked to a certain set of design drivers and how the decision of the best concept will be evaluated.
- ITC-A.2: Pre-Processing Function Performance and FE (feared event) Definition describe the allocation of the different pre-processing functionalities. It also addresses feared events, which will be considered within the integrity test cases. For some feared events it is necessary to specify different magnitudes and durations of the feared events. This is done within this test case as well.

Category B: Pre-Processing

The aim of these tests is to specify a baseline pre-processing. For this category 3 elementary test cases are defined. The first one addresses mainly the overall performance of the pre-processing were as

the other three test cases deals with some specific pre-processing functionalities.

- ITC-B.1: Pre-Processing Performance.
- ITC-B.2: Time Synchronisation Errors
- ITC-B.4: Meteorological Sensors

The elevation angle at the sensor station is one of the key parameter for the pre-processing performance and is addressed in this category.

Category C: IF Algorithm Assessment

The aim of these tests is to select one integrity check / IF representation which is analysed by the tests of the remaining categories (D to H). For this category three elementary test cases are defined:

- ITC-C.1: Integrity Flag Performance
- ITC-C.2: Integrity Flag Representation.
- ITC-C.3: BW and Processing Time Assessment

The decision, which is the algorithm that will be chosen for final implementation in Galileo, is mainly based on the sigma check value (accuracy of the check) and the misdetection probability. The other key parameters for the integrity check algorithm are evaluated during the sensitivity analysis in category D.

For the selection of the "best integrity check" a reference scenario with a global sensor station network and a fixed ground station elevation angle is used.

Category D: Sensitivity Analysis of Integrity Check and Pre-Processing

The aim of this category is to evaluate the selected integrity check and the baseline pre-processing in detail. To do so the remaining key parameter of the integrity check and the pre-processing are addressed in the elementary test cases:

- ITC-D.1: Sensitivity to Measurement Characteristic after Pre-Processing
- ITC-D.2: Sensitivity to Number of Observation
- ITC-D.3: Sensitivity to Elevation Angle

Category E: Sensitivity Analysis for the User

Based on the selected integrity check and IF representation the user algorithms are evaluated in detail. Within this category two elementary test cases are defined:

- ITC-E.1: Sensitivity of User to Elevation Angle
- ITC-E.2: Sensitivity of User to Noise

Category F: System Performance

The aim of this category is to evaluate the continuity and availability of the selected SISA/IF concept.

Two elementary test cases are defined:

- ITC-F.1: Continuity and Availability for Normal Condition
- ITC-F.2: Continuity and Availability for Degraded Conditions

Both test cases addresses availability and continuity at user level as well as GIC (ground integrity channel) level. The degraded conditions are defined within the elementary test cases of category A.

Category G: Feared Events

The defined feared events of category A are evaluated here. This category contains three test cases:

- ITC-G.1: Sensitivity of integrity check to Sensor Station Failures
- ITC-G.2: SIS Feared Event Effects
- ITC-G.3: OD&TS and IF Correlation

For some feared event it is necessary to define the magnitude and duration of the feared event. This is done in the category A. Within this category G the feasibility of detection of the feared events is mainly addressed.

Category H: Others

Within this category the comparison between the SBAS/UDRE (space-based augmentation system, user differential range error) and the selected SISA/IF concept is evaluated.

Most of the experimentations and trade-off will consider only a global network, but some system performances assessment will be made on regional configurations.

The general data flow for integrity processing is depicted in figure 6.

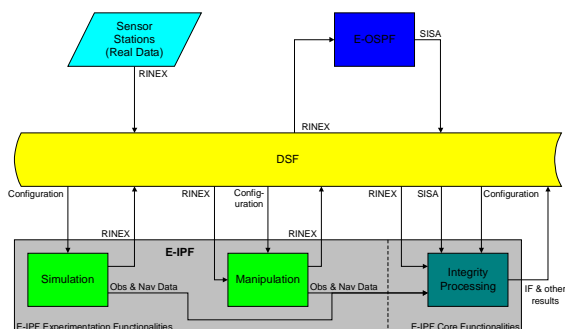


Figure 6: Experimentation data flow

Recorded sensor station measurement (observation and navigation) data are stored in the DSF in RINEX format. For experimentation purposes, measurement data may also be simulated by the E-IPF and stored in the DSF. Stored data (preferably recorded data) may be manipulated by the E-IPF for experimentation purposes. The manipulated data are then also stored in the DSF.

The E-OSPF obtains its measurement data from the DSF and writes the created SISA values back to the DSF. The E-IPF Integrity Processing obtains its measurement data and SISA values from the DSF. The measurement data for E-OSPF and E-IPF Integrity Processing are not necessarily identical. In fact, there are tests, where E-OSPF and E-IPF shall work on different data.

When E-OSPF functionalities are not needed for a particular test case. Simulated or manipulated observation and navigation data (in an E-IPF internal format) can be directly used by the integrity processing, without intermediate storage in the DSF.

E-IPF output routinely will be the integrity flags, but depending on the test case, there will be additional or alternative output as well. Mostly, this will be information on IF availability, false-alarm rate and misdetection probability. But there will also be test cases that work with e.g. only the pre-processing part of the E-IPF, producing pre-processed pseudoranges or information on the quality of tropospheric models as output.

CORE PRODUCT EXAMPLES

Here are some first examples of graphical core products. The main core products are just data in XML format, but the E-IPF is also able to produce graphical outputs where relevant.

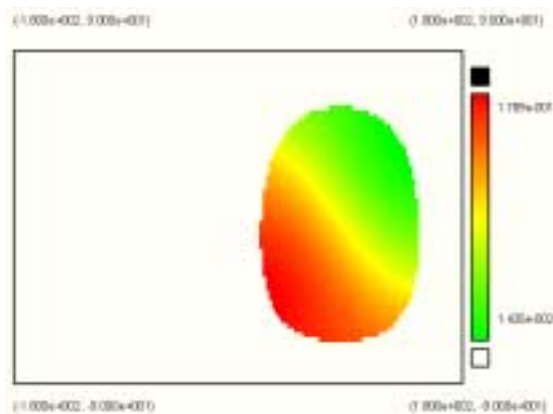


Figure 7: Estimated SISE over satellite footprint

Figure 7 shows a snapshot of an estimated SISE over the satellite footprint. The bounding rectangle

is equivalent to a world-map (units are in degrees and metres). This core product was generated based on simulated data.

Figure 8 shows the estimated SISE over satellite ground-track. The graphic is obtained by an accumulation over the processing period of 24 hours (data rate 300 seconds). Again the rectangle corresponds to a world map.

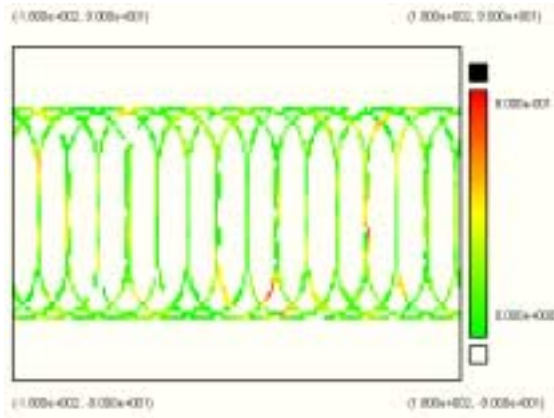


Figure 8: Estimated worst-user SISE over satellite ground-track

Figure 9 shows a histogram over the difference between true and estimated worst-user SISE accumulated for all satellites over the simulation period. The estimation algorithm used was the Galileo B2 phase baseline algorithm (estimation of satellite position error based on three parameters).

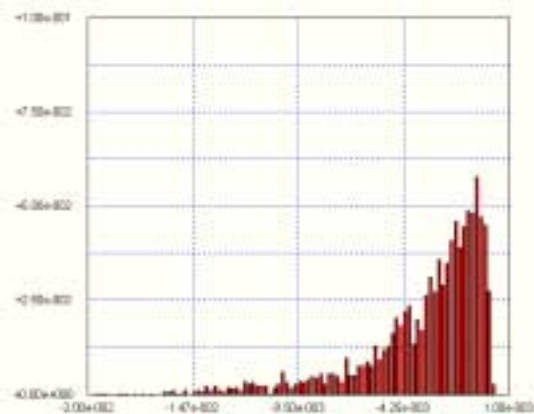


Figure 9: Difference between true and estimated worst-user SISE values (units are [m])

Figure 10 shows a classical Stanford triangle plot (*Stanford University, 1999*). Depicted is the vertical protection level versus vertical position error. The plot has been generated using data across all sensor stations within the same simulation.

Figure 11 shows a user-level availability map based on vertical protection level of 12 m. The protection level has been computed according to WAAS

MOPS (*RTCA, 1999*, adapted for Galileo). The bounding rectangle again corresponds to a world-map.

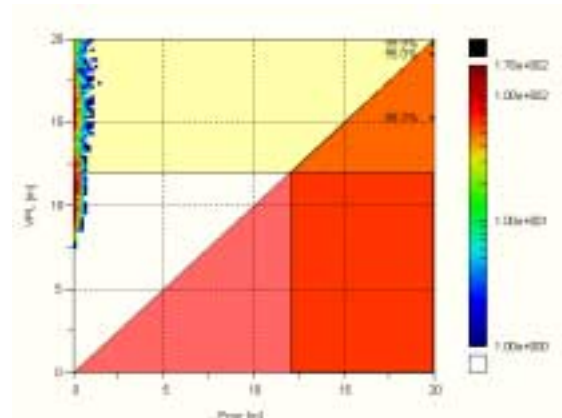


Figure 10: Vertical Stanford plot

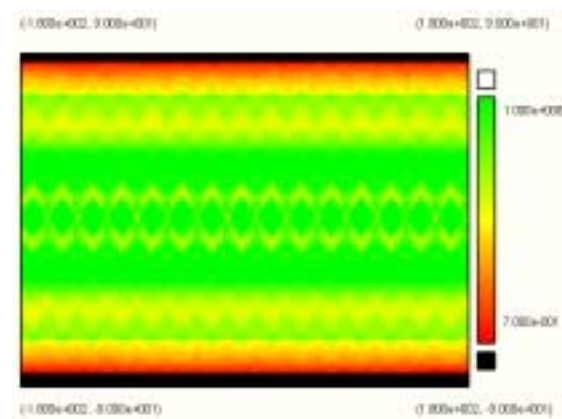


Figure 11: Availability map based on vertical protection level (12 m)

Note that these example products have been generated by simulations. No real data have been used here. However, experimentations with real data are about to begin and first results will be available soon.

CONCLUSIONS AND WAY FORWARD

Major effort has been spent on development of the E-IPF platform. The E-IPF is the central processing utility for integrity related experimentations with GPS and/or Galileo within GSTB-V1. Its components allow for a wide range of integrity-related experimentations.

The development is now in its final stage and testcase experimentations as well as routine experimentation is expected to start in a few weeks from now. All important core products are made available through a web-interface by the GPC.

Still a few algorithms have to be completed and tuning of baseline parameters must be performed before the processing may start on a daily basis. Integration of the E-IPF with other GSTB-V1 elements like E-OSPF or DSF is foreseen for early October.

The E-IPF SW is an open platform for easy integration of additional algorithms. This feature is important not only during the early phases of processing, when algorithms are changing frequently, but also later, when additional new ideas and algorithms need to be tested.

The integrity experimentation plan has been presented covering a huge set of activities and experiments with the objective of supporting the decision for the choice of a final algorithm baseline and appropriate tuning parameters.

As currently, the real data processing is based on real GPS measurements only, it is foreseen to upgrade the E-IPF to Galileo-like signal structures and the Galileo IOV (initial operational validation) scenario within the next stage of the project, which will be started soon.

ACKNOWLEDGEMENTS

The GSTB-V1 project is funded by the European Space Agency as an experimentation platform to mitigate algorithm-related development risks.

REFERENCES

ESA (2003). *Galileo Reference Troposphere Model for the User Receiver*, European Space Agency, ESTEC, Noordwijk, June 30, 2003.

RTCA (1999). *Minimum Operational Performance Standards For Global Positioning System/Wide Area Augmentation System Airborne Equipment*, RTCA Document No.: RTCA/DO-229B, Prepared by RTCA Special Committee 159 (RTCA SC-159), RTCA, Inc., Washington, D.C., October 6, 1999.

Stanford University (1999).
<http://waas.stanford.edu/metrics.html>.

Werner, W.; Zink, T.; Löhnert, E.; Pielmeier, J. (2001). *GALILEO Integrity Performance Assessment (GIPA)*, Proceedings of the 14th International Technical Meeting of the Satellite Division of The Institute of Navigation, ION GPS 2001, Salt Lake City, Utah, September 11-14, 2001, pp. 1838-1849.

Werner, W.; Zink, T.; Hahn, J. (2002). *GALILEO Integrity Performance Assessment Results And Recommendations*, Proceedings ION GPS 2002, Oregon Convention Centre, Portland, Oregon, September 24-27, 2002, pp. 2185-2195.