JOANNEUM RESEARCH DIGITAL
Institute for Digital Technologies

ESR EXECUTIVE SUMMARY

Analysis of GNSS Spaceborne Resilience

Author:

Thomas Prechtl

with contributions from the project consortium:

Hermann Katz
Günther Obertaxer
Harald Schlemmer
Sascha Bartl
Patrick Schmidt
Hannes Filippi
Franz Zangerl

Contract No. 4000133305/20/NL/CRS/hh

Final version 1.0 ***June 2023***

ESA STUDY CONTRACT REPORT – SPECIMEN

ESA Contract No:	SUBJECT:	CONTRACTOR:
4000133305/20/NL/CRS/hh	**Analysis of GNSS Spaceborne Resilience** **ESR Executive Summary Report**	JOANNEUM RESEARCH
ESA CR( )No:	No. of Volumes: **1** This is Volume No: **1**	CONTRACTOR'S REFERENCE: Space GNSS Resilience

ABSTRACT:

This Report summarises the findings of the Contract.

Name of author:

Thomas Prechtl (JOANNEUM RESEARCH)

NAME OF ESA STUDY MANAGER:	ESA BUDGET HEADING:
Pietro Giordano, Miguel Cordero Limón, Technical Officers ESTEC, TEC-ESN Christophe Seynaeve, Hendriline Hertzog, Contract Officers ESTEC, IPL--PTE	E/0901-01-K-30-01 (TDE WP19-20, T106-602ES)

Reference	ESR_Analysis_of_GNSS_Spaceborne_resilience_Executive_Summary.docx
Version	1.0
Status	Final
Date	2023-06-12

Version	**Date**	**Author**	**Versions / changes**
Final V1.0	2023-06-12	Thomas Prechtl	

Name	**Contact**	
Thomas Prechtl	Email:	thomas.prechtl@joanneum.at
	Phone:	+43 (316) 876 – 2514
	Mobile:	+43 (664602) 876 – 2514
	Pers. Fax:	+43 (316) 876 – 9 2514
Michael Schönhuber	Email:	michael.schoenhuber@joanneum.at
	Phone:	+43 (316) 876 – 2511
	Mobile:	+43 (664602) 876 – 2511
	Pers. Fax:	+43 (316) 876 – 9 2511
Name	**Contact**	
Pietro Giordano	Email:	Pietro.Giordano@esa.int
	Phone:	+31 71 565 3003
Miguel Cordero Limón	Email:	Miguel.Cordero.Limon@esa.int
	Phone:	+31 71 565 4507

Objectives of the activity

The activity aims to perform a comprehensive quantitative radio frequency interference (RFI) risk assessment for spaceborne GNSS receivers and derived products following the standards ISO 31000:2018 and ISO/IEC 27005:2018 as well as to investigate on RFI mitigation techniques appropriate for such systems, and considering different types of missions and scenarios.

Risk assessment for typical scenarios/missions

Three factors have been identified as relevant for generation of a so-called risk a risk priority number (RPN), determining the specific risk for a mission/scenario: GNSS dependency of a mission, RFI exposure of spacecraft in orbit, and RFI criticality. Each factor has an assessment between 1 and 10 and so the max. $\mathrm{RPN} = 10 \times 10 \times 10 = 1000$. The following table displays the category thresholds and the assessment for a sample mission:

Risk categories	LOW	MEDIUM	SEVERE	EXTREME	FATAL
RPN from	0	176	501	751	1000
RPN till	175	500	750	999	> 1000

Mission	Orbit	GNSS dependency	exposure, likelihood (intentional)	exposure, likelihood (non-intentional)	criticality	RPN intentional interf.	RPN non-intentional interf.
CHAMP	LEO (454 km)	10	7	7	8	560	560

Each scenario was evaluated regarding GNSS setup, overall mission setup/constraints, expected exposure to RFI and a final evaluation providing the weighting numbers:

GNSS dependency: this describes how much the evaluated application scenario depends on GNSS measurements for correct functionality and is mainly depending on the availability of backup/supplementary sensors.

RFI exposure: this describes the expected exposure to RFI for the evaluated application scenario, which is mainly depending on the orbit, direction of GNSS antenna and existence of other, potentially RFI-generating, equipment on-board the space vehicle.

RFI criticality: this describes how critical RFI is for the application scenario or overall mission given that the interference is severe enough to cause a GNSS malfunction in terms of jamming (denial-of-service) or spoofing (receiver misdirection).

The following scenarios have been identified for evaluation within the activity:

- Attitude and orbit control system (AOCS)
- Time referencing/synchronization
- Launch
- Re-entry
- Rendezvous or formation flying
- Precise orbit determination (POD)
- Precise on-board orbit determination (P2OD)
- GNSS reflectometry
- Radio occultation

For mission/scenario risk assessment, the following criterions were considered:

Mission objective, use of GNSS, requirements on GNSS, location and orientation of antenna(s), observations, processing, latency, orbit (altitude, time of visibility), mission phases, backup/supplementary sensors, RFI exposure and spoofing related risk, and the worst-case impact of RFI/Spoofing.

Table 1: Structured overview on identified GNSS scenarios with RPN values

Scenario	Orbit / configuration	Differing characteristics	Common characteristics	Typical accuracy	Tolerable error	GNSS dependency	RFI exposure	RFI criticality	RPN
AOCS	LEO	Zenith	RT NAV PR SF / MF	1-2 m / 1°	10-20 m	**5**	**5**	**5**	**125**
	GEO	Nadir + conical		1-2 m / 1°	10-20 m	**5**	**8**	**5**	**200**
Timing	LEO	Zenith	RT NAV PR SF / MF	< 10 ns	20 ns	**9**	**5**	**7**	**315**
	GEO	Nadir + conical			20 ns	**9**	**8**	**7**	**504**
Launch	GNC Large Launchers		Omni RT NAV PR SF	5-10 m / 0.1-0.5 m/s	20 m 1 m/s	**1**	**8**	**3**	**24**
	GNC Micro launchers			5-10 m / 0.1-0.5 m/s	20 m 1 m/s	**6**	**8**	**6**	**288**
	Safeguard			5-10 m / 0.1-0.5 m/s	20 m 1 m/s	**4**	**8**	**7**	**224**
Re-entry			Omni RT NAV PR SF / MF	5-10 m / 0.1-0.5 m/s	10 m / 0.5 m/s	**1**	**8**	**3**	**24**
Rendezvous / formation	LEO	Omni / zenith	RT NAV PR + CP MF	< 1m	1 m	**6**	**5**	**6**	**180**
	GEO	Omni / nadir / conical		< 1m	1 m	**6**	**8**	**6**	**288**
POD	LEO		Zenith NRT No NAV PR + CP MF	< 5 cm	10 cm	**8**	**7**	**6**	**336**
P2OD	LEO		Zenith RT NAV PR + CP MF	< 5 cm	10 cm	**9**	**7**	**8**	**504**
GNSS-R	LEO		Nadir (reflected) NRT No NAV Amp SF / MF	0.1 dB	0.1-0.2 dB	**10**	**7**	**8**	**560**
GNSS-RO	LEO		Limb NRT No NAV CP SF / MF	< 10 cm	20 cm	**10**	**7**	**8**	**560**

Abbreviations: Requirements: RT (real-time), NRT (non-real-time)
Observations: AMP (amplitude), PR (Pseudorange), CP (carrier phase)
GNSS configuration: SF (single-), MF (multi-frequency)

Note: If not stated otherwise nadir-pointing and conical antennas mostly receive second lobe signals instead of direct signals, which reduces the signal amplitude.

Scenarios of RFI sources

From literature research and the consortium's own experience the possible types of RFI were collected and in consideration of their transmission parameters (frequency, bandwidth, power, modulation, antenna type) the most critical unintentional RFI sources identified:

- Primary and secondary flight surveillance RADARs,
- DME (Distance Measuring Equipment) /TACAN (TACtical Air Navigation system),
- JDITS/MIDS (NATO Joint Tactical/Multifunctional Information Distribution System).

(Different types of) jamming and spoofing as intentional RFI sources.

Impact of RF interference and Spoofing

The impact of RF interference on the GNSS signals and measurements can be expressed and theoretically simulated by utilization of the Spectral Separation Coefficient (SSC).
The SSC is used to calculate the loss in C/N_0 of GNSS signals caused by a certain type of interference, which is the main effect seen in the case of RF interference. The C/N_0 is degraded depending on the SSC and the received power of interference signals. The C/N_0 degradation leads to the following effects within the receiver:

- Increased correlation and measurements noise
- Increased bit error rate (BER)
- Increased PVT noise
- Loss of PVT availability
- Loss of tracking

The impact of spoofing signals on the authentic signals is strictly similar to the impact of RFI in the sense that spoofing signals cause a C/N_0 degradation of the authentic signals. But the is different since the spoofing signals cannot be straightforward distinguished from the authentic signals within the receiver. This means that the acquisition and tracking modules of the receiver are either tracking authentic or spoofed signals and cannot determined which is the case without dedicated spoofing detection algorithms.

Simulation of signals and receiver tests

Within the activity, the impact of RFI on two different types of spaceborne GNSS receivers were tested:

- PRETTY EM (Passive REflecTomeTry and dosimetry) mock-up of a Low Earth Orbit (LEO) cube sat performing slant geometry GNSS reflectometry from in orbit as well as radiation measurements, and
- PODRIX EQM, a multi constellation, GPS and Galileo receiver for Precise Orbit Determination (POD).

The signals for the tests were generated by different means:

- Standard GNSS signals were simulated using Spirent GSS simulators;
- Jamming RFI (chirp and white noise type) were artificially computed and played out by a GIPSIE RTX signal generator;
- DME/TACAN RFI computer generated simulation of the nine frequency relevant stations at the European hotspot around Frankfurt/Main/Germany also played out by the signal generator;
- Spoofing signals by GIPSIE AJ+S advance jamming and spoofing system with signals played out by the signal generator;
- Spirent GSS simulator for highly synchronised and long duration spoofing.

The hardware tests were carried out in the laboratories of Beyond Gravity in Vienna, the external generation of RFI and spoofing signals was contributed by JOANNEUM RESEARCH and OHB Digital Solutions.

Reflectometry tests

Figure 1 shows a photograph of the PRETTY EM test setup in the Beyond Gravity laboratory while Figure 2 provides the test setup block diagram.

The average DME/TACAN power level of -62.65 dBm at the PRETTY receiver input had a noticeable effect on the reflectometer results. The reflectometer has to find most signal energy for the delays corresponding to the path difference between direct and reflected signal. A clear identification of the actual reflected signal is only possible in the period with low interference power. An increased noise on the correlation results was observed for most of the time. The calculated signal power level in other delay taps than the actual reflected signal reach about the same levels as the wanted signal.

Figure 1: Beyond Gravity PRETTY EM test lab setup.

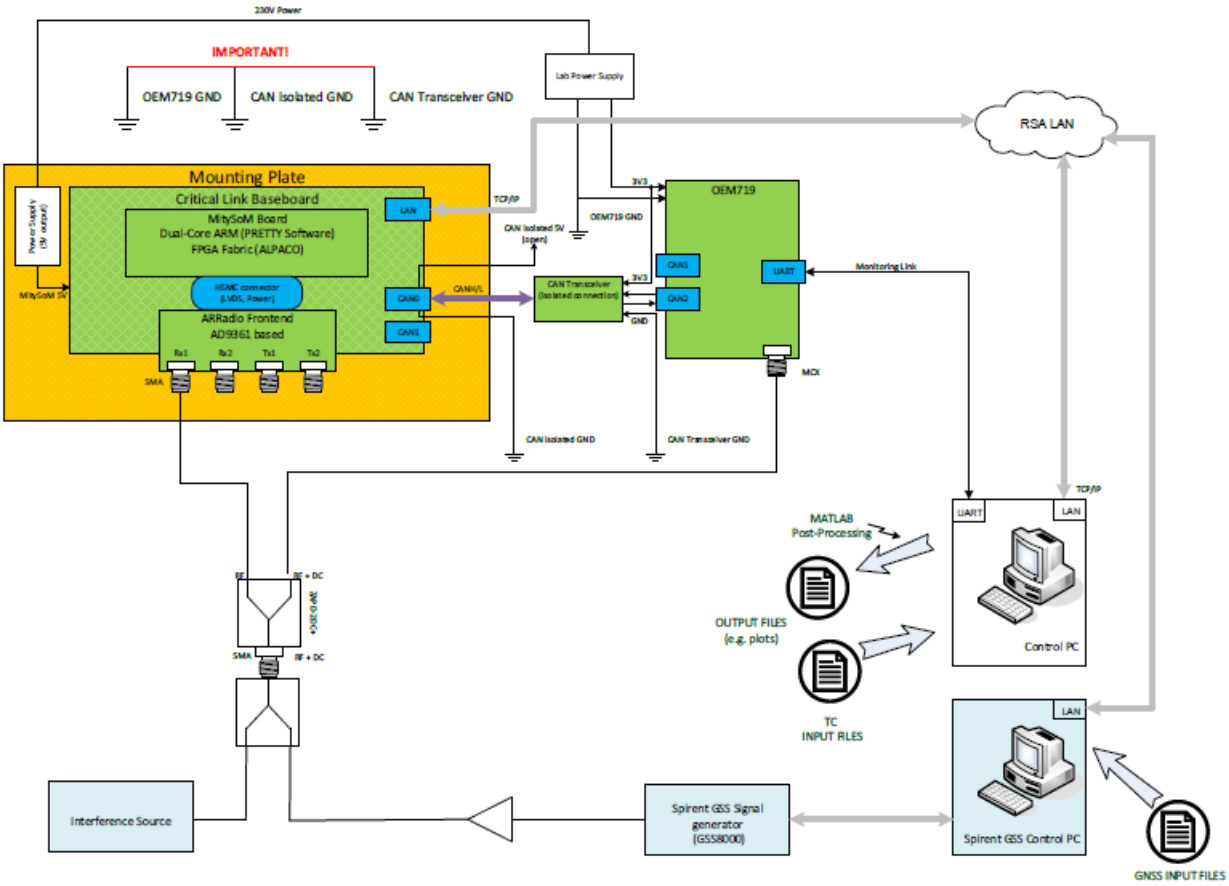

Figure 2: Beyond Gravity standard PRETTY test setup.

At interference power peaks the reflectometer results were completely disturbed, i.e. the reflectometer is not able to produce useful measurements.

Interference from DME/TACAN resulted in a degradation of the correlation results, as expected. The impact of the cyclical behaviour of the DME/TACAN pulses is clearly visible in the correlation results.

The aim of PRETTY is to measure height (e.g. of ice) relative to the earth ellipsoid. The increased noise due to interference reduces the measurement precision. High interference power levels lead to a complete loss of measurements.

The power levels of a single DME/TACAN signal are received at power level below -62.65dBm. However, taking into account that multiple DME/TACAN signals may be imposed and that the reflectometer will be equipped with a medium to high gain antenna, it is concluded that DME/TACAN signals are a threat for GNSS based reflectometry.

Tests of Precise real-time navigation (PPP) in LEO

Figure 3 depicts the standard setup for GNSS receiver system test. shows the specific test setup for the Precise Real-Time Navigation (PPP) tests with PODRIX EQM while Figure 4 shows a photograph of the test setup.

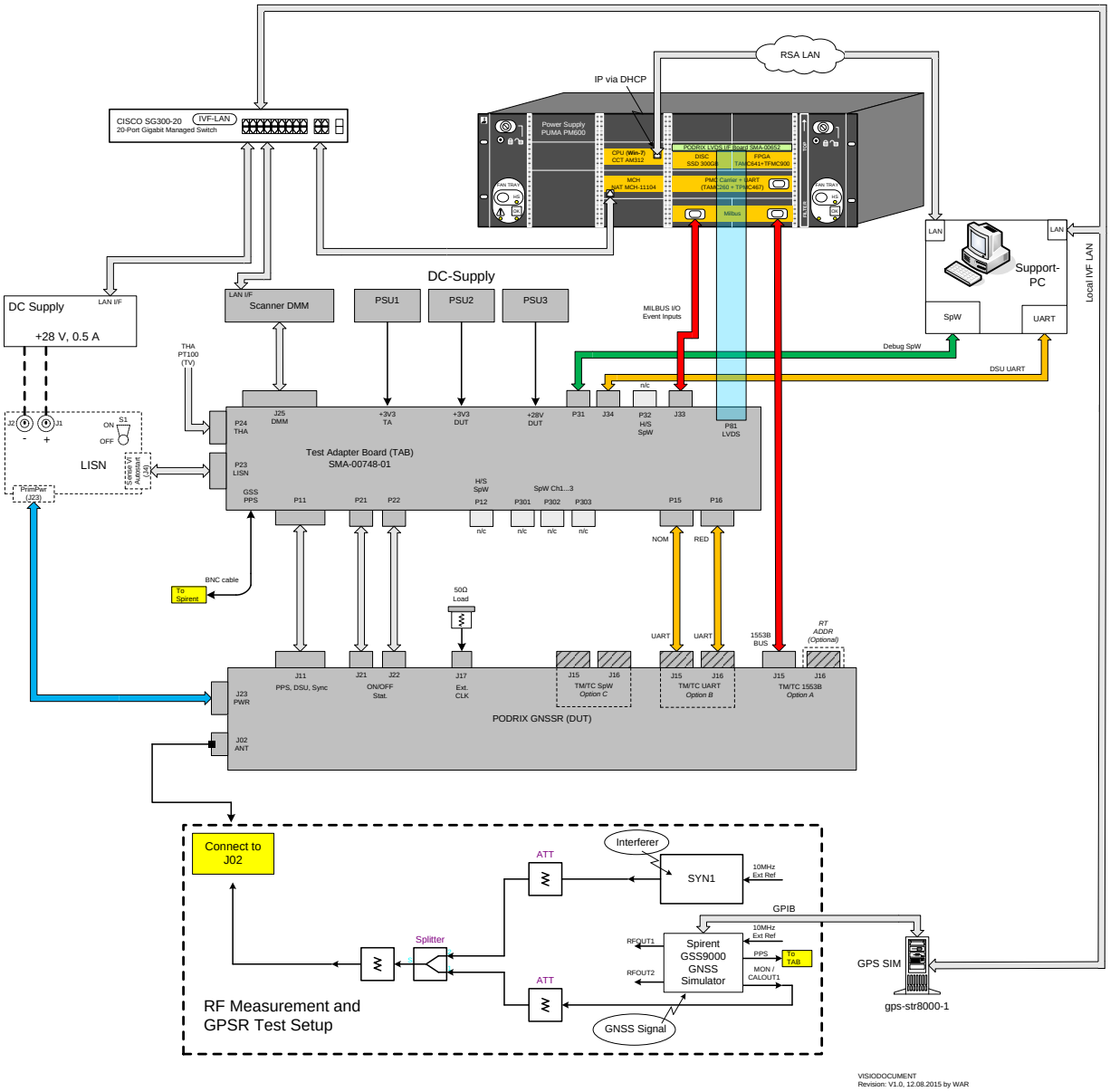

Figure 3: Beyond Gravity standard GNSS receiver test setup.

Figure 4: PPP test setup at Beyond Gravity cleanroom.

The tests applied jamming on L5. Jamming on L1 is expected to have a worse impact on the GNSS receiver performance, because of the narrower bandwidth with respect to L5.

Jamming on L5 was tested with gradually increasing power levels to assess the (increasing) impact on the GNSS receiver performance. The result of jamming is primarily a degradation in tracked C/N_0. As the jamming signal power was increased, tracked signals were lost, and the NavSol position/velocity performance was impacted. Generally, the GNSS receiver was able to recover nominal performance quickly after the jamming signal stopped, even after a signal outage (NavSol PVT propagated).

Jamming on L1 is expected to have a worse impact on the GNSS receiver performance, because of the narrower bandwidth with respect to L5. From the calculation of achievable power levels for different orbits with standard equipment we conclude that malicious interference by means of ground-based transmitters with chirp or CW signals is feasible especially for antenna orientations tilted with respect to zenith direction.

The jamming tests conducted in this study used mainly white noise signals. It is assumed that jamming with continuous-wave (CW) signals is the worst case. Interference with continuous wave signals is used in the frame of EMC RFC tests. The standard PODRIX EMC RFC tests use continuous-wave signals. Experience shows a rapid degradation with increasing signal power.

DME/TACAN: A significant impact on the GNSS receiver performance was observed only for power levels exceeding the actual power levels expected in orbit. Therefore, disturbances are expected only in case of positive

antenna gains in direction of the DME/TACAN transmitters. Therefore, GNS receivers with zenith-pointing antennas are considered not to be affected by DME/TACAN.

Spoofing: The receiver did not react on the unsynchronised spoofing by changing its position estimates but experienced the spoofing attack as jamming attack.

The spoofing simulations using the Spirent GSS as source of spoofing signals demonstrated that spoofing is feasible at least for perfect synchronisation. PODRIX did not detect the spoofing attack. At least the filtered navigation mitigated the effect of spoofing in the sense that it did not exactly follow the spoofed trajectory.

The simulated power levels were some dB higher than the actual GNSS signals. As these signals are received at rather low levels (lower than about -110dBm), it is considered as feasible to generate on-ground effective spoofing signal power levels.

On Signal-to-Noise levels

In L*EO* GNSS receivers receive GNSS main lobe signals. The associated power levels are high enough in order to provide some C/N0 margin. A C/N_0 degradation of about 5 dB is considered as limit. The performance of a filtered navigation solution is insignificantly affected by this amount of C/N_0 degradation. For unfiltered navigation solutions, a C/N_0 decrease is associated with corresponding PVT error increases. The acceptable degradation depends on the actual requirements.

In Geostationary Earth Orbit (GEO), already the nominal C/N_0 values are challenging. Therefore, the C/N_0 margin is below 2dB. The rather small margins identify interference as a potential threat for spaceborne GNSS receivers.

Beyond Gravity's experience with navigation receivers in LEO indicated that for zenith-pointing antennas currently observed unintentional interference from ground is sufficiently small such that alarming threats are not observed. Nevertheless, impacts from ground surveillance RADARs can be observed

Earth observation GNSS sensors like radio occultation or scatterometer are known to be disturbed by unintentional interference such as DME/TACAN or L2 surveillance radar. This could also be seen by the tests with PRETTY. Significant disturbances of the results were observed for an average power level of -82.7dBm at the antenna port. For the envisaged antenna gain of 14dBi, this corresponds to -96.7dBm at the antenna. Such levels are reached by the DME/TACAN signals at all LEO altitudes.

As unintentional interference from ground is already of concern and needs to be considered for applications with antenna orientations towards earth, intentional jamming of spaceborne is judged feasible and has to be considered as threat.

Assessment of mitigation approaches

Table 2 lists the technological pathways that were explored for this activity. Many of the discussed jamming and spoofing detection and mitigation approaches are feasible for space receivers.

The well predictable movement of a satellite in orbit eases spoofing detection and enables bridging short periods of jamming. Plausibility checks of measurement and the monitoring of Kalman filter states can reveal spoofing attacks. Such checks are rather easy to implement. It is recommended to give higher attention to spoofing and jamming detection in future GNSS receiver developments.

Table 2: Categories of RFI detection and detection/mitigation techniques

Group	Approach	
Antenna defences	Direction of arrival (DoA)	Interference or jamming signals are detected by means of identifying the direction of arrival and mitigating by minimising the antenna gain direction.
	Direction of interference (DoI)	
	Null-steering	
	Beamforming	
At Frontend	Automatic Gain Control (AGC)	Analyses of the received signal allow for the detection of jamming
	Sample distribution	
	Spectral analysis	
	Artificial Intelligence (AI) techniques	
Pre-correlation	Spatial filtering	The processing of the digital data in front of the GNSS channel processing shall mitigate radio frequency (RF) interference
	Pulse blanking	
	Adaptive notch filtering	
	Frequency domain adaptive filtering (FDAF)	
	Wavelet packet transform (WPT)	
	Eigenvalue decomposition	
Post-correlation	Array processing beamforming	The processing of the digital data at the output of the GNSS channel processing shall detect and mitigate RF interference
	Transformed domain excision	
Measurement level	Plausibility checks	Sanity checks of GNSS measurements shall detect jamming and spoofing attacks.
	Code/carrier cross check	
	Different frequency bands	
	C/N_0 monitoring	
	Step detection	
	Drift monitoring	
Hybridisation	Inertial Measurement Unit (IMU)	Combination of GNSS navigation with other sensor or sources of information shall assess the plausibility of the GNSS navigation solution in order to detect spoofing attacks.
	Kalman filter internals	
Cryptographic techniques	PRS, OSNMA, Spread spectrum security codes	Encrypted navigations allow authorised users to validate the received GNSS signals.
Other approaches	Vector tracking	Techniques which make more robust the GNSS signal tracking.
	IMU	

For spaceborne GNSS receivers, the authentication approaches are considered as more appropriate for spoofing detection than encrypted signals. To our knowledge, secure modules for the reception of PRS signals need to be tamper-proof. The realisation of tamper-proofness for a space receiver is considered as very complicated and demanding.

For jamming mitigation, the approaches suppressing the interference in front of the actual GNSS channel processing are considered as preferred, i.e. spatial filtering and pre-correlation techniques.

Spatial filtering may require enough space for accommodating antenna arrays on the satellite or dedicated antenna developments. The advantage of spatial filtering is that it can mitigate jamming and spoofing signals. Dedicated spatial filters in front of the GNSS receiver box would have the advantage that this technique could be applied to protect existing GNSS receiver designs. Except for pulse blanking, all pre-correlation techniques require a linear frontend, i.e. the amplifiers must not saturate, and the ADC must not clip in the presence of the interfering signal. Therefore, multi-bit ADCs are necessary. Modern FGPA provide the necessary processing power to implement the discussed techniques (probably with the exception of the Eigenvalue decomposition) in spaceborne GNSS receivers. As dedicated GNSS receiver chips often have a limited resolution, it is important to decide on the necessary jamming mitigation capabilities already at the architectural design level.

Conclusions from simulations and Outlook

The most promising mitigation techniques were simulated by Beyond Gravity with MATLAB™ to examine the possibility for implementation in a spaceborne GNSS receiver by determining their complexity, amount of necessary processing power, and processing delay.

All simulated interference mitigation approaches are sensitive to the characteristics of the jamming signal.

For spaceborne GNSS receivers, the authentication approaches are considered as more appropriate for spoofing detection than encrypted signals. To our knowledge, secure modules for the reception of PRS signals need to be tamper-proof. The realisation of tamper-resilience for a space receiver is considered as very complicated and demanding.

For jamming mitigation, the approaches suppressing the interference in front of the actual GNSS channel processing are considered as preferred, i.e. spatial filtering and pre-correlation techniques. The former can mitigate jamming and spoofing and can be applied to existing GNSS receiver designs. Nevertheless, some pre-requisites must be fulfilled: linear amplifiers must not saturate, multi-bit ADCs are necessary.

The adaptive notch filter is suited for the mitigation of narrow-band signals with constant or changing frequency (like chirps). It is not adequate for pulsed signals or the superimposition of pulses at different frequencies like DME/TACAN signals. In order to adapt to chirps with high sweep rates, a wide notch filter is required. Such a filter eliminates significant parts of the signal. Therefore, even for weak interference a signal loss has to be accepted. On the other hand, the adaptive notch filter showed the most reliable operation of all simulated approaches at high sweep rates. As an active adaptive notch filter causes a signal loss even in absence of an interfering signal, the notch filter shall only be enabled in case interference has been detected. The notch filter suppresses the interfering signal. This suppression in dB is independent of the signal amplitude - the residuals are proportional to the amplitude of the jammer.

The frequency domain adaptive filter is known to be suited for the suppression of pulsed interference. It can also be applied for mitigating continuous wave and chirp signals. The effectivity of the approach depends on the ratio of the window length of the inputs to the FFT and the sweep period of the chirp. In case the FFT-spectrum of the chirps covers large parts of the signal spectrum, eliminating the chirps also mitigates the signal. For example, a sweep rate of 10^{12} Hz/s made impossible proper operation of the emulated receiver. In case FDAF is adequate for the characteristic of the interfering signal, an advantage of this technique is its weak dependency on the amplitude of the interfering signal. This is explained by the fact that all spectral contributions above the threshold are eliminated no matter how far they exceed the threshold.

The adaptive predictor of the Wavelet Packet Transform (WPT) approach only works for real signals. For a properly defined threshold in the denoiser, the approach does not cause a significant loss in absence of the jammer. The approach is suited for the mitigation of narrow-band signals with constant or changing frequency (like chirps). The mitigation performance is appealing for low to moderate sweep rates. As the interfering signal is suppressed by means of subtracting an estimate of it, the residual errors are proportional to the jammer amplitude. An alternative WPT-based mitigation approach is the elimination of outliers in the transformed domain. As no adaptive predictor is involved, this approach can be applied to complex signals. Compared with the approach with the adaptive predictor, this approach is a bit more effective for high jammer amplitudes. In principle, this approach could be used to eliminate pulsed signals. However, it is considered as difficult to find

the optimum time and frequency resolution. Increasing the number of WPT-levels enhances the frequency resolution but reduces the time resolution.

All assessed mitigation approaches struggle with high chirp sweep rates. A potential countermeasure is the increase of the sampling rate. For the adaptive notch filter the update rate of the estimator would increase and the bandwidth gets wider for the same parameter values. The FDAF window period would get shorter for the same number of FFT-points, i.e. a smaller spectral portion of the chirp's frequency range would be covered. This would reduce the loss of signal due the elimination of the spectral outliers. The situation is more complicated for the Wavelet Packet Transform (WPT). As shown in section 5.3.5, the WPT rather coarsely divides the spectrum into regions. For example, in order to obtain the same frequency resolution with twice of the sampling frequency, an additional WPT level needs to be introduced. As a result, also the time resolution of the WPT is the same as for the lower sampling frequency. Only the adaptive predictor would profit from the higher sampling rate, as the update rate of its adjustment process is increased.

Not assessed in the present document, but worth to mention: A high sampling rate can also be used to implement steep digital filters mitigating the interfering signals outside the GNSS bands.

A major improvement with respect to robustness against interferences is the use of multi-frequency receivers and antennas. For bigger spacecrafts with nadir pointing antennas the implementation of array antennas would open the possibility of several additional detection and mitigation techniques.

JOANNEUM RESEARCH
Forschungsgesellschaft mbH

Leonhardstraße 59
8010 Graz

Phone +43 316 876-0
Fax +43 316 876-1181

prm@joanneum.at
www.joanneum.at