H2020 STRIKE3: Standardization of Interference Threat Monitoring and Receiver Testing - Significant Achievements and Impact

M. Z. H. Bhuiyan1, N. G. Ferrara2, S. Thombre3, A. Hashemi4, M. Pattinson5, M. Dumville6, M. Alexandersson7, E. Axell1, P. Eliardsson2, M. Pölösky6, V. Manikundalam5, S. Lee6, J. Reyes Gonzalez2

1Finnish Geospatial Research Institute, National Land Survey of Finland, Finland
2Nottingham Scientific Ltd, UK
3Swedish Defence Research Agency (FOI), Sweden
4Automotive & Rail Innovation Center (ARIC) of AGIT mbH, Germany
5GNSS Labs, India
6ETRI, Republic of Korea
7European GNSS Agency (GSA)
(1zahidul.bhuiyan)@nls.fi

Abstract — The H2020 project STRIKE3 contributes enormously for lifting EU industry and institutions to the premier position in the global market for GNSS interference monitoring, detection, reporting, receiver standardization, applications and services. This has been achieved over the last three years through the deployment and operation of an international GNSS interference monitoring network to capture the scale and state of the problem, and through work with international GNSS partners to develop, negotiate, promote and implement standards for GNSS threat reporting and GNSS receiver testing. The achievements of STRIKE3 are based on the following cornerstones: i. STRIKE3 global interference monitoring network, ii. A draft interference reporting standard, iii. A draft receiver testing standard against interference, and iv. International knowledge sharing and awareness building against interference among key GNSS stakeholders across public and private sectors. All these aspects will be presented herein with greater details.

Keywords — GNSS, interference, standards, receiver testing.

I. INTRODUCTION

The H2020 project STRIKE3 is a European initiative that supports the increasing use of GNSS within safety, security, governmental and regulated applications. The project is sponsored by the European GNSS Agency (GSA) as part of the European Commission’s H2020 Framework Programme for Research and Development. The aim of STRIKE3 is to develop international standards in the specific area of GNSS threat reporting and GNSS receiver testing. This has been achieved through the deployment and operation of an international GNSS interference monitoring network to capture the scale and state of the problem, and through work with international GNSS partners to develop, negotiate, promote and implement standards for GNSS threat reporting and GNSS receiver testing. International partnership with countries, international organizations and agencies is a fundamental aspect to the ultimate success of the STRIKE3 project. The project altogether includes over 40 international partners who participate in the international GNSS interference monitoring network and provide their valuable reviews into ensuring that the STRIKE3 standards are relevant to their business interests in GNSS.

The STRIKE3 project started in February 2016 with the deployment of the international monitoring network. Since then, the network has grown enormously and at the present time almost 50 sites have contributed to autonomous, persistent monitoring of the GNSS spectrum as well as detecting, characterising and reporting of any interference threats to GNSS signals. The monitoring of the signal spectrum within the STRIKE3 network only considers GPS L1/Galileo E1 signal band at 1575.42 MHz frequency. The project has so far assembled a database of over 500,000 threat signatures which have been collected and analysed. These threat signatures include about 60,000 GNSS jammer signatures. The database will help in future to ensure that the forthcoming GNSS receivers and applications are hardened to the threats that are present in the real-world. An example of such an attempt can be found in [1], where an adaptive interference mitigation technique is proposed to counteract unintentional Narrow-Band Interference (NBI) within the GNSS spectrum.

II. STRIKE3 MONITORING RESULTS

Across the STRIKE3 project as a whole there have been 48 monitoring sites across 21 different countries. The sites have been chosen to cover different countries, to cover different types of location with different local interference environment (e.g. city areas, major roads, etc.), and to include sites with different uses (e.g. timing, airports, power grids, etc.) in order to cover different types of infrastructure and engage with different potential stakeholders. Some sites have had continuous monitoring for over 2+ years, whilst others have been in place for just a short time, sometimes being moved around to other sites in order to build up a bigger picture.

Three types of equipment have been used for the monitoring, including Detector V0 and GSS100D (from Nottingham Scientific Limited (NSL)) and RF Oculus (from Swedish Defence Research Agency (FOI)). All equipment detect interference in the L1 spectrum, as well as providing additional information about the nature of the signal.

Completing long-term monitoring on such a wide scale has a number of benefits. Having such a large dataset has allowed
the consortium to obtain some good evidence for the real-world level of interference that exists and how widespread jammers are. Additionally, the results for specific sites are useful for the hosts to assess specific risks, patterns of activity, etc. Some of the general conclusions from the analysis of the database are presented below.

Firstly, the monitoring has shown there is a lot of interference – even more than was expected at the start of the project. Also, it has been determined that interference – both unintentional and intentional – affects every site that has been monitored, i.e. none of the sites monitored have been completely ‘clean’. However, there is of course a wide variation in activity between sites depending on the type of infrastructure, the local environment, and also the country in which it is located. Fig. 1 compares the average monthly number of events detected at a selection of sites. It can be seen that there is a huge variation in activity at different sites.

![Fig. 1. Average Monthly Number of Detected Events at Selected Sites](image)

In general, those sites that are the busiest in terms of human activity and traffic (city centres and city motorways) are affected most by interference (both unintentional and intentional from in-vehicle jammers) whereas more remote sites have fewer events.

Despite the very high numbers of events that are detected, the vast majority of interference events were detected with low power and short duration which do not cause any noticeable impact on GNSS tracking. We also see much more unintentional than intentional interference. It is difficult to see a real pattern in these unintentional events, although generally there are more during daytime than night, and more on weekdays, so they still seem to be linked to human activity.

Although many events have no impact, we still see tens of thousands at a power level that may cause some impact at the monitoring sites and many hundreds that cause a complete loss of GNSS positioning at the receiver. However, it should be noted that the COTS receiver in the monitoring equipment is a particular type and not representative for all users and so impact may be more (or less) for different equipment at the same locations. It is also noted that the events that have been detected in STRIKE3, whether unintentional or intentional, are not directed specifically at the infrastructure where the detection equipment is located – it is incidental interference that is being detected. Therefore, it is perhaps not surprising (although reassuring) that the impact is usually low, even if the probability of such interference occurring is high. However, some of the highest power events do illustrate the sort of disruption that could be caused if there was a directed attack specifically on a target, in which case the impact would be much higher although the probability of occurrence is very low.

In terms of the signals themselves, the monitoring has also built up a huge database of many different types of signal (both jammers and unintentional events) that are found in the real-world. This has given a valuable insight into those signals that pose the greatest threat, i.e. those that are most widespread and hence will be most commonly encountered by receivers in the real world. The most common interference signal type detected at different STRIKE3 monitoring sites is shown in Fig. 2. It also allows us to see some emerging trends, such as new types of jammers (e.g. the ‘tick’ signal), differences in the type of jammers that are common in different countries, and how people’s use of jammers could be changing (e.g. use of two separate jammers at the same time). Such knowledge has fed into the receiver testing to test receivers against those threats.

![Fig. 2. Example Spectrum and Spectrogram of Most Common Signal Type (wide sweep fast)](image)

III. STRIKE3 INTERFERENCE REPORTING STANDARD

The STRIKE3 project has produced two draft standards. The first draft standard relates to the needs for GNSS interference detection, monitoring and reporting. The motivation for this standard is that there is a growing understanding that the threat scene is changing and in order to ensure that GNSS technologies remain robust, there is a need to share experiences and events at a global level. The monitoring results show the benefits of wide-scale monitoring, but even having 50 sites is just scratching the surface of what is out there. The motivation behind the proposed draft reporting standards is to allow a mechanism for different types of equipment to identify and report on interference events in a standard way. This allows consistency in the results from different types of equipment so that wider analysis can be performed to get a better idea of the general level of activity. Clearly, there are a number of GNSS interference monitoring and reporting systems that work in a different way and report different information. To enable as many different types of equipment as possible to report, and to address concerns over data security and confidentiality, the standards consist of several parts. Firstly, there is a standard event definition to ensure that only detected events that meet certain criteria are reported. This acts to filter out low-level noise and consider only significant events, and helps to ensure that different equipment will report the same events. Secondly, a minimum reporting message has been proposed which includes mandatory reporting information (i.e., identifier, equipment type, event definition, frequency band,
geographic region, date, etc.) [2], [3]. This ensures that all equipment reports the same basic level of information to allow coherent analysis, but without requiring sensitive information on exact site location (for example) to be shared. In addition, there are a series of optional information which can also be included in the message if a manufacturer wishes to provide within their products (e.g., event start time, event duration, GNSS fix lost (yes/no), spectrum, C/N0, etc.) [2], [3].

IV. STRIKE3 RECEIVER TESTING STANDARD

The second draft standard which has been developed within the STRIKE3 project relates to the testing of GNSS receivers when subjected to interference and other threats [3], [4]. A thorough receiver test standard against real world interference has been drafted within the STRIKE project. The motivation for proposing this test standard is to ensure that the market has access to a test specification that can be used to assess the performance of different GNSS receivers under a range of typical interferences which have been detected in the “real world”. This will provide the market an opportunity to protect its GNSS applications and ensure that the market does not opt for the lowest cost solution but selects the most appropriate technology to meet the needs of the intended applications. The GNSS receiver test standard has been developed based on a generic series of threats as detected during the GNSS interference monitoring campaign phase. The test standard can also evolve to accommodate new threats as they are being detected and reported.

The GNSS receiver test standard has been developed based on a generic series of threats as detected during the GNSS interference monitoring campaign phase. The test standard can also evolve to accommodate new threats as they are detected and reported. The draft receiver test standard makes reference to the following items which are essential to support receiver testing.

**Test Architecture:** it defines the test system architecture utilized to assess the performance of GNSS receivers in the presence of interference signals derived from the STRIKE3 database. The following GNSS receiver types are considered within the test architecture:

1. Professional receivers,
2. Mass-market receivers,
3. Integrated receivers (i.e., antenna and receiver in an integrated device), and
4. Timing receivers.

**Performance Metrics:** it considers how interference impacts a GNSS receiver and which performance metrics should be logged and observed to assess the impact of the threat on the receiver electronics. It also suggests suitable levels of performance. The draft standard recommends a set of performance metrics to be utilized for each test case depending on the type of the receiver.

An example test set-up for both mass market and professional grade receivers is shown in Fig. 3. The clean GNSS signal is generated from a multi-constellation, multi-frequency Spectracom GSG-6 hardware simulator, whereas the threat signature is generated using a Keysight Vector Signal Generator (VSG) through the replay of raw I/Q (In-phase/Quad-phase) sample data. Raw I/Q data captured in the field for a real-world event is used as input to the VSG which then re-creates the detected threat by continuously replaying the data in a loop.

Both the GNSS signal simulator and the VSG are controlled via software in order to automate the testing process. The automation script is used to control these devices remotely and to limit human intervention. The script also provides synchronization between the two instruments in order to ensure repeatability of the tests and reliability of the results. A laptop is used to record and analyze the performance of the receiver against the different threat signals. The analysis is performed using a MATLAB-based script that processes the NMEA output messages from the Receiver Under Test (RUT).

V. RECEIVER TESTING RESULTS ANALYSIS

As a part of the STRIKE3 project, a receiver test campaign has been recently completed in order to analyze the impact on different real-world threats on different GNSS receivers. In this paper, the authors briefly highlights the key findings of some of the test results. Tests have been carried out for four different grade receivers mentioned in Section IV. Each RUT is tested against different types of real world interference threats (wide swept frequency with fast repeat rate, narrow band signal, triangular wave, etc.) in different test scenarios. Example test results obtained with mass-market receiver and professional grade receivers are shown in the following.

Fig. 4 shows the impact of a multi-peak interference power profile on the mass-market receiver. A triangular wave
interference signature was selected to be reproduced by VSG in accordance with the receiver test platform shown in Fig. 3. The introduced Jamming-to-Signal power ratio (J/S) can be seen on the right-hand vertical axis, whereas the East-North-Up (ENU) position error can be seen on the left-hand vertical axis. The default receiver settings were used for the analysis, meaning that the receiver decides its own parameters for C/No masking and elevation masking for PVT computation. As can be seen from the Fig. 4, the mass-market RUT prioritizes the availability of the position solution over its accuracy. During the interference interval, there are only a few epochs at which the receiver does not yield a position solution, but this high yield comes with degraded positioning accuracy. The position fix availability during the interference interval for the mass-market receiver is high (97.91%) at the expense of position accuracy (i.e., both maximum horizontal and maximum vertical errors are 78.8 m and 167.4 m, respectively).

On the other hand, the professional grade RUT behaves differently for the same multi-peak sensitivity test case. As shown in Fig. 5, the professional-grade RUT preserves the position accuracy at the expense of solution availability (58.58%). It does not offer the position solution as often during the interference interval, but when it does the position errors are minor (i.e., both maximum horizontal and vertical errors are 0.72 m and 0.78 m, respectively). The test duration for both the cases was exactly one hour. At the beginning of the tests, both receivers were in cold start mode. The inaccurate position solution, especially in the vertical component, computed by the receivers in the beginning of the test was due to the cold start and the resulting unavailability of ionospheric parameters, and to the convergence of the navigation filter.

An extensive summary of the receiver test results obtained within STRIKE3 project can be found in [5]. The extensive results analysis showed that all receiver categories are impacted ominously by the interference threats. More specifically, it is observed that the mass market RUT was capable of recovering from a highly-powered jamming event much faster than the professional grade RUT resulting in a much higher availability for mass market RUT than that of a professional grade RUT. On the contrary, in terms of performance accuracy, the professional grade RUT is instead performing better than the mass-market RUT. However, when a C/N0 mask of 25 dB-Hz is applied at PVT computation stage for both receiver categories, they tend to behave almost similarly against interference threats, i.e. both receivers exhibit similar availability against same kind of interference threat. In case of timing receivers, it was observed that all the interference signatures were able to degrade the performance of the timing receiver. The PPS signal generated by the timing RUT once exposed to interference differed from the one under nominal conditions. Moreover, the interference caused the RUT to violate the ITU requirements for timing devices to be used as primary reference clocks.

VI. CONCLUSIONS

STRIKE3 successfully addresses the concerns of government departments, transport operators, critical infrastructure operators, service providers and law enforcement agencies across Europe and globally, that are concerned about GNSS denial of service attacks. It has achieved its goal through establishing a global GNSS interference monitoring and reporting network and via international knowledge exchange among key GNSS stakeholders. STRIKE3 offered a draft GNSS threat monitoring and reporting standard, which would help the GNSS community to receive consistent reports of events that have some impact on GNSS services. In addition to the reporting standard, STRIKE3 also successfully produced a draft receiver testing standard against interference. The availability of threats and test standards is very critical to developing the next generation of receiver technologies to support the wider use of GNSS in safety and liability critical high-value applications. Some key findings with the receiver test results were also briefly presented. The impact of real word jamming on different grade receivers were analyzed following the guidelines mentioned in the draft receiver testing standard. The results in general imply the severity of the real world jamming on the normal operation of different grade GNSS receivers.

Fig. 5. East-North-Up position for professional-grade multi-peak sensitivity test in the static case

ACKNOWLEDGMENT

This work has been co-funded by the EU H2020 project entitled “Standardization of GNSS Threat reporting and Receiver testing through International Knowledge Exchange, Experimentation and Exploitation (STRIKE3)” – grant agreement number 687329.

REFERENCES


