Standardization of GNSS Threat reporting and Receiver testing through International Knowledge Exchange, Experimentation and Exploitation [STRIKE3]

- Draft Standards for Receiver Testing -

Michael Pattinson[1], Mark Dumville[1], Yeqiu Ying[1], Dimitrios Fryganiotis[1], Zahidul Bhuiyan[2], Sarang Thombre[2] , Åsa Waern[3], Patrik Eliardsson[3], Martin Pölöskey[4], Steve Hill[5], Venkatesh Manikundalam[6], Sanguk Lee[7], Joaquin Reyes Gonzalez[8]

Nottingham Scientific Ltd[1], Finnish Geospatial Research Institute, National Land Survey of Finland[2], Swedish Defence Research Agency (FOI)[3], Automotive & Rail Innovation Center (ARIC) of AGIT mbH[4], Satellite Applications Catapult Limited[5], GNSS Labs[6], ETRI[7], European GNSS Agency (GSA)[8]

Summary

STRIKE3 is a European initiative to support the increasing use of GNSS within safety, security, governmental and regulated applications. STRIKE3 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. To do this STRIKE3 persistently monitors the international GNSS threat scene to capture the scale and dynamics of the problem and works with international GNSS partners to develop, negotiate, promote and implement standards for threat reporting and receiver testing. This is being achieved through the deployment and operation of an international GNSS interference monitoring network to monitor for interference on a global scale and to capture real-world threats for testing GNSS receiver resilience.

This paper presents a proposed methodology to rigorously test receivers against interference threats, along with a selection of common real-world signatures that have been detected.

Motivation

GNSS is being used for an ever expanding range of safety, security, business and policy critical applications. GNSS functionality is being embedded into many parts of critical infrastructures and European economies are now dependent on uninterrupted access to GNSS positioning, navigation and timing services. At the same time, GNSS vulnerabilities are being exposed and threats to denial of GNSS service are increasing. Reports of events of loss of GNSS services are commonplace. To ensure GNSS is protected, there is now a need to respond at an international level to ensure that there is

- a common standard for GNSS threat monitoring and reporting, and
- a global standard for assessing the performance of GNSS receivers and applications under threat.

This will ensure the dominance of GNSS as the backbone to our positioning, navigation and timing needs.

STRIKE3 Approach

To achieve these goals the STRIKE3 project has been structured in three main parts:

a. **STRIKE3 International Monitoring and Reporting Network**
To gain sophisticated technical information about the threats, i.e. the signals which cause interferences on GNSS, a monitoring network is being built up on an international basis. The various sensors detect interference signals if they appear and report these into a centralized database.

In order to get this possible a common monitoring and reporting standard must be available. The generation of a draft version of this document is one of the main outcomes of STRIKE3 project.

b. **STRIKE3 Threat Database**
All identified and recorded signals from all monitoring stations are being uploaded into a central threat data base. There these ten-thousands of signals can be analysed and compared extensively.

c. **STRIKE3 Threat Testing Standard**
Based on the knowledge gained from the manifold recorded and analysed interference signals, receiver can be tested on their robustness against interferences. To get comparable results out of such test campaigns, these tests must be standardized. Hence, the generation of a draft version of a threat testing standard is another main outcome of STRIKE3 project.

The overall project structure has been depicted in the following figure 1.

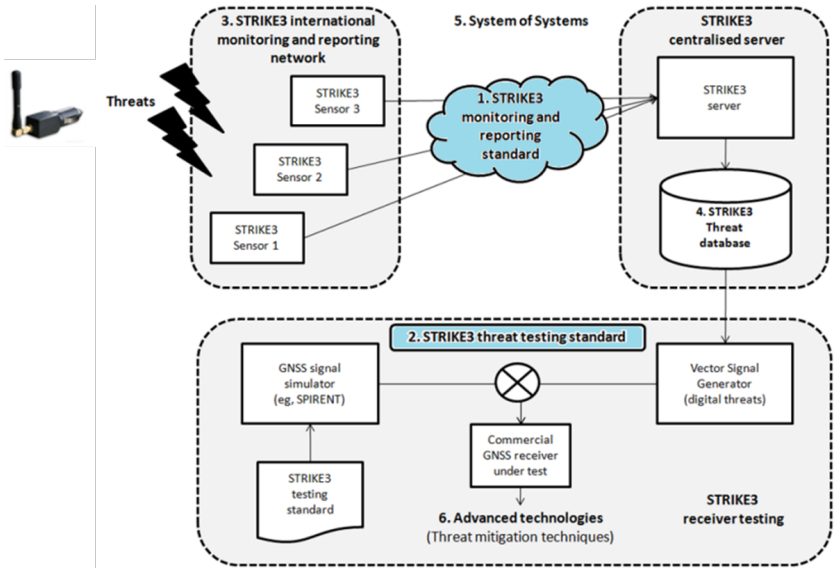

Figure 1: Structure of STRIKE3 project

Monitoring and Threats

Over the course of the past year, STRIKE3 has built up a network of about 30 interference monitoring sites in 23 different countries around the World (see Fig. 2). This provides a valuable resource for determining the level of interferences and types of signals that affect real-world installations at a variety of locations (see Fig. 3 and Fig. 4). Such knowledge enables STRIKE3 to assess the incidence of deliberate jamming vs. unintentional interference to be estimated, as well as comparisons of the

most common types of interferences at different types of location. This helps to understand the real-world threat to GNSS. In addition, detailed information about the interference signals is collected and used in the creation of test standards.

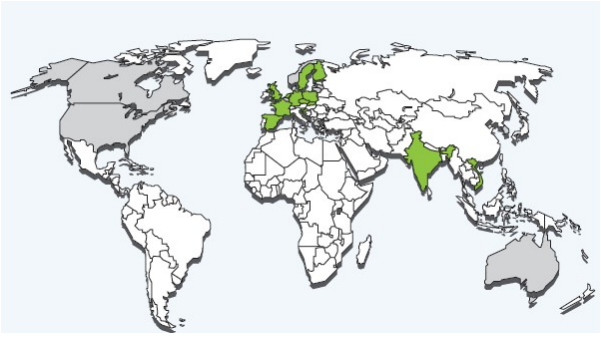

Figure 2: Summary of Countries Included in STRIKE3 International Monitoring

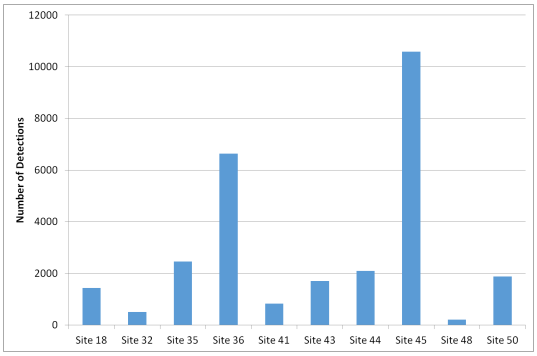

Figure 3: Summary of Total Number of Detected Interference Events at Different Sites in Q4 2016

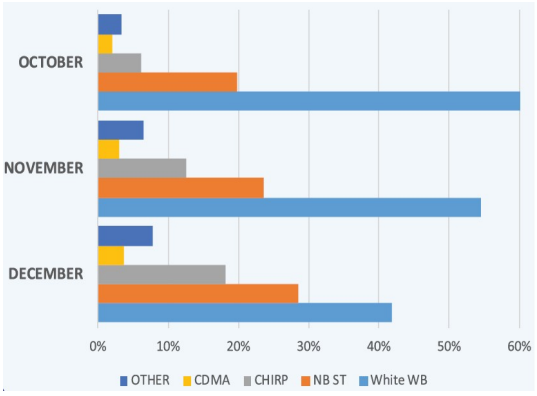

Figure 4: Summary of Number of Detected Interference Events of Different Signal Types in Q4 2016

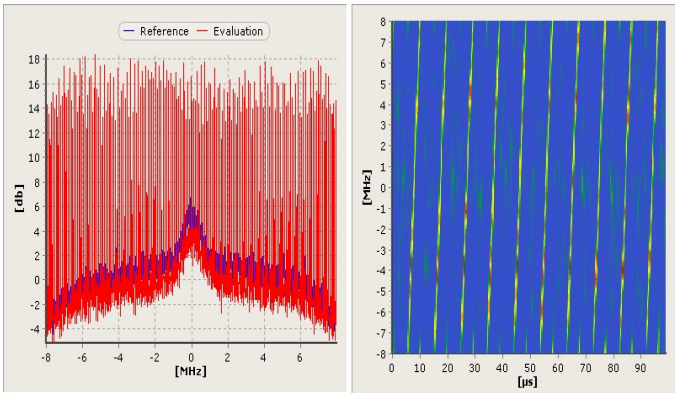

Figure 5: Example of Interference Signal Detected by STRIKE3 Monitoring Network

STRIKE3 Threats Database

The database provides a lot of information and insights about recorded real live interferences and disturbances on GNSS. Hence, it is the core for developing strategies and procedures for mitigation and defence of these threats ("know your enemy"). To get the most valuable results out of the data base, all collected signals shall be described and stored by using the identical data formats, which must be described in an official document. Hence, the "Draft Standards for Threat Monitoring and Reporting"-document, is a key deliverable of STRIKE3 project and is available through STRIKE3 website for public. It contains definitions on events, events messages and system information messages and their corresponding data formats. The signals and the knowledge about these interferences will be used to improve the robustness of receivers and systems as described in the following.

The draft version of the document shall be the basis to be reviewed and discussed within the international standardizing committees to become once a worldwide standardizing document.

Testing Receiver Robustness

The robustness of receivers against interferences is another major criteria to choose the suitable device, as important as its performance on accuracy and speed. A standard methodology to test receivers against selected threats shall be proposed, becoming a framework and instructions for performing these tests.

It is also to define a standard set of threats to be used for testing, based on the interference signals observed in the field, and to propose a method to identify and select new threats for testing in the future.

The set-up of the test equipment, the architecture and test-processes shall be defined to make the results comparable and repeatable. A draft standard test document is being evolved. In order to validate the defined tests being practicable and representative a number of receivers will be tested on robustness by using various threat signals within the project.

The resulting test standards will then envisage as a guideline for standard bodies, application developers, receiver manufacturers, etc. Expected values of metrics and pass/fail criteria shall be defined by the relevant authority based on requirements.

Draft Test Standards

One of the core objectives of the STRIKE3 project is the development of a proposal for these test standards. The standards deliver a framework based around a number of key considerations necessary to describe a comprehensive set of tests. The user can then tailor the testing to suit the performance needs of their application and the capabilities (robustness) of the type of receivers against threats used therein. The standards are formed around following aspects of receiver performance assessment.

- ***Test Architecture:*** The test system architecture utilised to assess the performance of GNSS receivers in the presence of interference signals derived from the STRIKE3 database.
- ***Performance Metrics***: How interference impacts a GNSS receiver and which metrics should be logged and observed to assess that impact. Suitable levels of performance are also suggested.
- ***Test methodology*****:** The method for carrying out the testing against the proposed standard.
- ***Criteria and Procedure for Selecting Threats.*** The basis for how threats should be selected from the STRIKE3 database for addition to the standard and how the threats can be parameterised for utilisation within the test system with repeatability.
- ***Application of Proposed Test Standards.*** How the user would utilise the standard to assess the performance of their GNSS receiver equipment and the associated systems.

One of the key aspects of these test standards is the link to real-world threats from the threat database populated by the monitoring network (as seen in Fig. 5). Unlike other standards where the definitions of interference test signals are fixed, the goal of these standards is for the tests to reflect real-world threats that the receiver is likely to encounter, and for the tests to evolve as new threats are identified.

The STRIKE3 standards will include a baseline set of threats based on the existing interference signals and include a methodology for identifying and selecting new threats. The generic process on testing receivers' robustness is shown in the following picture (6):

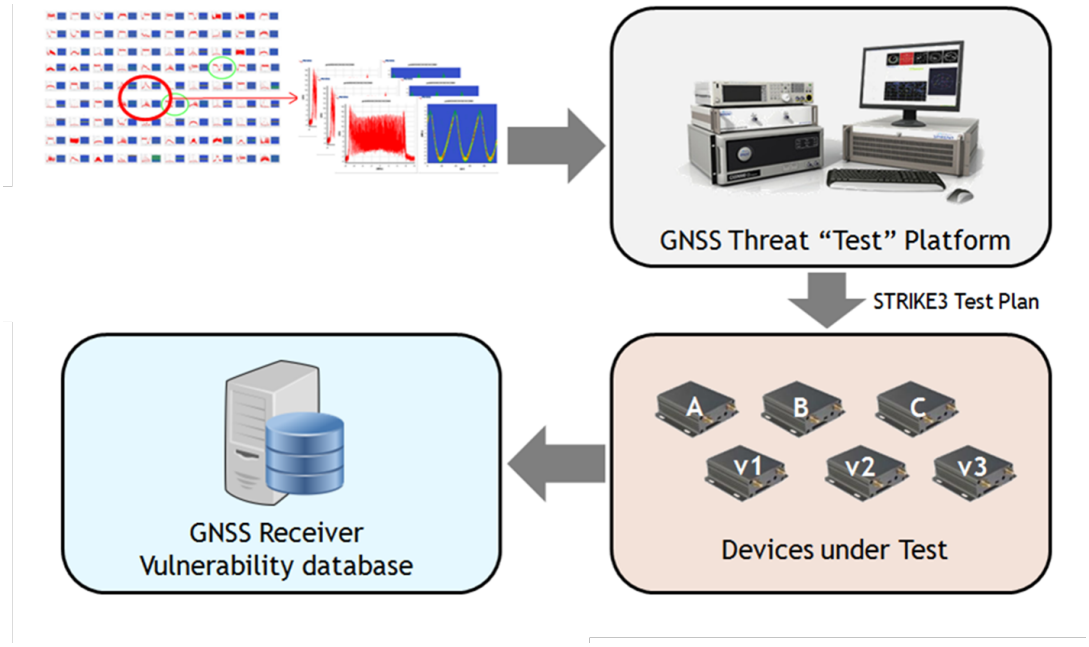

Figure 6: Process on Receiver Testing

Threat selection

The test standards will focus on real threats from STRIKE3 event database. Due to the international monitoring stations ten-thousands of events are available already, which can be grouped according to their signatures, i.e. chirp signals (CS), single tone (ST), narrow band (NB), wide band (WB), etc. The initial threat selection considering signals from each category will be done within the project. These threats will be prepared and tested during the project as well as some unusual signals which are anticipated to be difficult to mitigate.

To generate the test signals there are two approaches under consideration:

- Replay of raw data samples as described above
- Generation of synthetic signals (based on properties of real signals detected in the field) by using an Interference Signal Generation

Both will be defined and tested in STRIKE3 and the best approach will be proposed and published. Final recommendation will produce a baseline set of threats. The focus in STRIKE3 lays on GPS L1 interference, future standards can be extended to cover other frequencies, though.

Test Architecture

The proposed test architecture is shown in figure 7. It considers the use of real threat signals out of the threat data base as well as synthesised interference signals generated by a vector signal generator (see "real data path" and "synthesis path" in picture 7). The pure GNSS signal is provided through a GNSS

constellation simulator. This avoids any error or deviation due to environmental influences which might influence the tests under open sky conditions, like changing open sky views, reflections and shadowing, changes in satellite constellations and many others. The proposed architecture will provide repeatable and valid testing results.

For validation reason it is proposed to use two identical device under test, one will receive the clean GNSS signal only (baseline performance) and the other one will receive the GNSS signal modulated by the interference threat signal (interference performance) additionally.

Finally, the tests with all metrics and the results will be completely recorded and documented within a storage device.

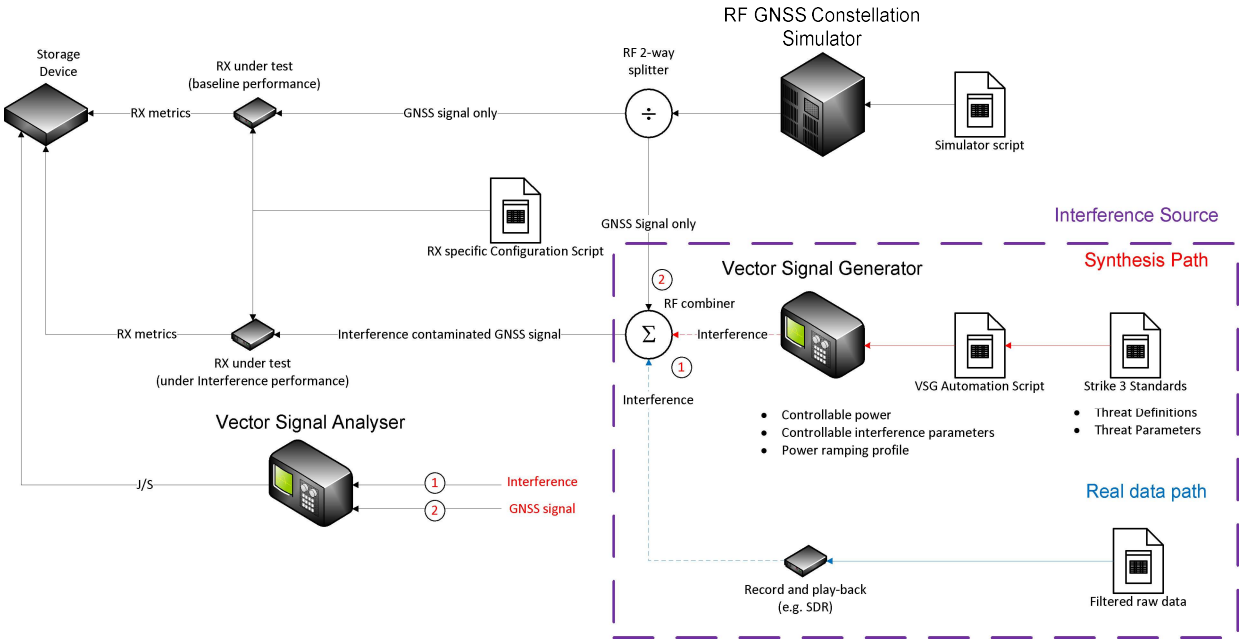

Figure 7: Receiver Test Architecture

Test Cases and Criteria

Beside the finger prints of the utilized threat signals, the intensity of interference must be considered as well. So tests will be performed by varying the ramp-up /ramp-down rates, i.e. changes in the height of the power steps, their duration and the number of these steps (Fig. 8). Dependant on the results and experiences made by these real tests, recommendations will be given in the draft test standard.

The test shall start in initial conditions for receiver (e.g. receiver in stable mode tracking all satellites). Variables to be evaluated within the tests are:

- Test times and durations
- Times of test case events (e.g. start of interference, increase in power level, etc.)
- Interference power levels at each time

Within the frame of STRIKE3 various receivers will be selected, i.e. from mass-market, professional, integrated devices and timing receivers and then get tested by the following draft test specification.

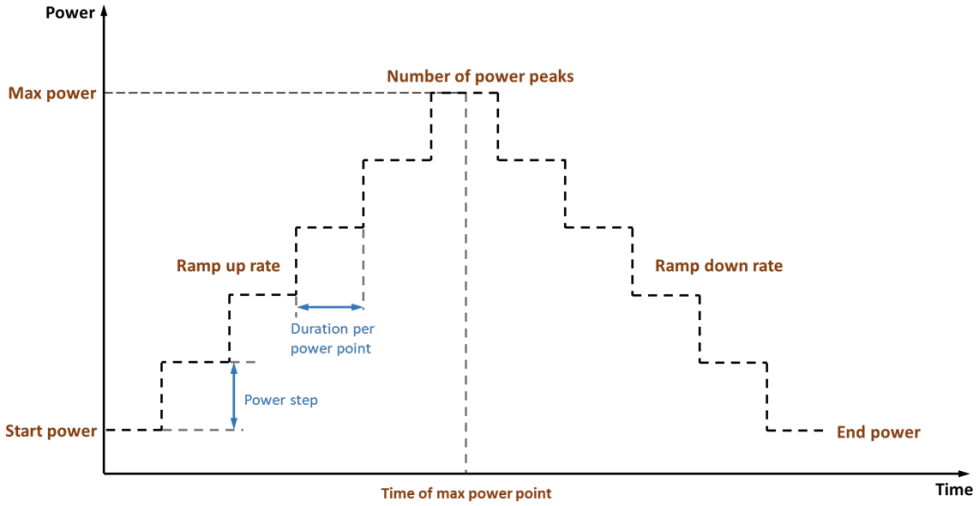

Figure 8: Ramp signal for receiver testing

Measurements and assessments can be made on:

- Time To First Fix (TTFF): assess time taken for receiver to recover after strong interference event. This can be compared with TTFF after a cold / warm start.
- Acquisition and tracking sensitivity (single peak and multi-peak ramp)
- Behaviour of static receiver as interference level increases, including impact on position error, point at which tracking is lost and point at which re-acquisition occurs
- Behaviour of dynamic receiver as interference level increases, in particular impact on position error
- Behaviour of timing receiver as the impact of interferences on performance of their timing output

Outlook

The Test Standards Document is being prepared and will be available soon for public. To review the feasibility of these testing standards, practical receiver tests will be performed accordingly. Starting in fourth quarter of 2017 this will lead to a consolidated draft test standards on receiver testing in 2018. (As result of the physical test, an anonymous overview of the receiver performances will be submitted after the end of the test campaign.

In future, beyond STRIKE3 project, all these activities shall lead to improved mitigation and resilience of the receivers against the threats.

The monitoring and analysis on threats and interferences will continue, quarterly score cards of the results will be issued through STRIKE3 web page.

The draft standard on Threat Monitoring & Reporting is available for public to be downloaded at STRIKE3 website.

STRIKE3 website can get reached at www.gnss-strike3.eu, where further information on STRIKE3 project and various documents and articles can be found for download, too.

Acknowledgements

This work has been co-funded under the European H2020 research programme through the European GNSS Agency (GSA)

Contact

Martin Pölöskey
Automotive & Rail Innovation Center
Friedrich-List-Allee 11
D-41844 Wegberg-Wildenrath, Germany
Tel.: +49-2432-93376-11
Mail: martin.poloskey@aric-research.de