GNSS Research: Summary of STRIKE3's first year

July 20, 2017 - By Michael Pattinson, Mark Dumville, Yeqiu Ying, Dimitrios Fryganiotis, Zahidul Bhuiyan, Sarang Thombre, Åsa Waern, Patrik Eliardsson, Martin Pölöskey, Steve Hill, Venkatesh Manikundalam, Sanguk Lee, Joaquin Reyes Gonzalez and GPS World Staff

Est. reading time: 1 minute

Example of unusual detected signal type likely to have an impact on GNSS performance. (Figures courtesy of Nottingham Scientific Ltd.)

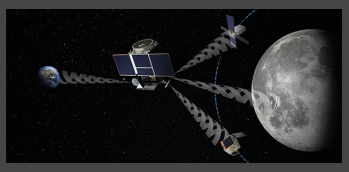
Presented at the European Navigation Conference, Switzerland, May 2017

This paper summarizes major findings from the first year of monitoring by the International Knowledge Exchange, Experimentation and Exploitation (STRIKE3), a new European initiative to support the increasing use of GNSS within safety, security, governmental and regulated applications and addressing concerns about GNSS denial of service attacks. STRIKE3 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 through an international GNSS interference monitoring network.

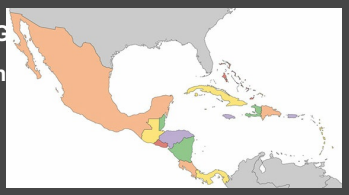
European economies are now dependent on uninterrupted access to GNSS services. At the same time, GNSS vulnerabilities are being exposed, and threats to denial of GNSS service are increasing. We must ensure that there is a common standard for GNSS threat monitoring and reporting, and a global standard 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 has built a network of more than 20 interference monitoring sites in 14 countries. This enables STRIKE3 to assess the incidence of deliberate jamming versus unintentional interference to be estimated, as well as comparisons of the most common types of interference at different types of location. Detailed data about the interference signals is collected and used in the creation of test standards. Common signal types as well as unusual ones that are likely to have a major impact on GNSS performance are extracted from the database and added to a test methodology. These will be used to test different types of receivers to better understand impact and help improve mitigation, finally leading to an international test specification.

You May Also Like



GSA



This article is tagged with denial of service, International Knowledge Exchange Experimentation and Exploitation research, STRIKE3 and posted in GNSS

Comments are currently closed.