GNSS System

GNSS Vulnerabilities Conference Discusses Solutions to Jamming, Interference

September 8, 2009
By: David Last

Conference Report

GNSS is vulnerable to space weather, unintentional interference, jamming, and multipath propagation. The second conference on GNSS Vulnerabilities and Solutions, held September 2-5, focused on these issues.

The conference was held at Baska, on Krk Island off the Adriatic coast of Croatia, and was a joint venture by the Royal Institute of Navigation, London, and Nottingham University's Institute of Engineering Surveying and Space Geodesy. This idyllic location attracted 64 delegates from 21 countries. Most came from Europe, with unusually strong representation from the former eastern bloc.

Nearly half the papers focussed on space weather and ionospheric and tropospheric propagation, taking in long-term and short-term solar effects, scintillation, signal attenuation, tropospheric delay variations, meteorological influences and even gravity waves. Bruno Zolesi of the Italian National Institute for Geophysics and Vulcanology summarized two decades of research across 35 countries, driven by the European COST (Cooperation in the Field of Scientific and Technical Research) program. Jan Lastovicka of the Czech Republic reviewed the science, including the ionospheric effects of planetary waves, tides, gravity waves, and even cold fronts. The approach of the physicists was: Understand these things and maybe you can mitigate your vulnerability to them.

GNSS vulnerability can threaten safety critical and mission critical systems, including navigation in the air, maritime automatic identification systems, and the transportation of nuclear waste and other dangerous materials on land. Mitigations include EGNOS (the European WAAS) and GBAS (Ground Based Augmentation Systems).

An unexpectedly hot topic was the enthusiasm of European governments to deploy road user charging schemes based largely on GNSS technology. Road pricing is a rare and novel case of GNSS users who are hostile to the technology and seeking to exploit its vulnerability to the maximum. To enforce charges through the legal system may require levels of integrity approaching those of aircraft instrument approach systems! Peter Vermaat of the UK's TRL Limited reviewed the contribution that non-GNSS technologies such as number-plate recognition can make to ensuring the overall integrity of the charging system.

David Last reported on the appearance of low-cost jammers capable of blocking the L1 and L2 frequencies of GPS and Galileo, plus mobile phones. Criminals are now using these devices to defeat tracking and security systems. He predicted that spoofing devices would follow jammers. Suggestions for weapons to defend GNSS came mostly from Germany: Ulrich Engel and Angelika Hirrle proposed exciting new mathematical techniques to help separate GNSS signals from noise and interference, whilst Michael Felux sought refuge in low-cost inertial systems.

The Last presentation on criminal jamming will appear as the Expert Advice column in the October issue of *GPS World* magazine, and be available online via the magazine Digital Edition and to website visitors by the second week of that month.

Hank Skalski of the U.S. Department of Transportation laid out U.S. government plans to detect and track down sources of GPS jamming. The SETS (Space Event Tracking System) will deploy aircraft, vans, fixed base units, and trained technicians. From Russia, Grigory Stupak and Mark Shmulevich reported their nation's plans to restore a full GLONASS constellation of 30 space vehicles, laying out a road map leading to full interoperability with GPS. They envisaged a world orbited by 117 navigation satellites, with GLONASS operating alongside GPS, Galileo, and China's COMPASS — supported by a further 29 augmentation satellites. That would certainly mitigate many of the vulnerabilities of GNSS due to propagation effects — but not those due to interference in the frequency bands they will all share.