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

Michael Pattinson

European Global Navigation Satellite Systems Agency
GNSS Benefits

• Freely available signals, 24/7, all weather
• Position, precise timing
• Used in wide range of domains and industries
  – Consumer
  – Commercial
  – Safety
  – Security
  – Transactions
  – Liability
  – Governmental
GNSS Limitations

• Weak signals
  – Difficult to track indoors and in obstructed areas
  – Susceptible to interference
Radio Frequency Interference

• Unintentional
  – Mis-tuned or faulty equipment, Space Weather

• Intentional
  – Jamming, Spoofing, Meaconing

• Impacts of Interference
  – Receiver
    • Degraded solution
    • No solution (position, timing)
  – Services
    • Small nuisance
    • Economic impact
    • Safety impact
Counter Measures

- Legislation (Supply, Possession, Use)
- Education
- Enforcement
  - Detect and remove
  - Direct or indirect
- Equipment
  - Antenna
  - Receiver
  - Hybridisation
- Procedure/process
Counter Measures

- Legislation (Supply, Possession, Use)
- Education
- Enforcement
  - Detect and remove
  - Direct or indirect
- Equipment
  - Antenna
  - Receiver
  - Hybridisation
- Procedure/process

All dependent on understanding the threat
Understanding the Threat

• Interference Monitoring and Reporting
  – What threats are out there?
  – Focus on jamming (STRIKE3)

• Receiver Response to Threats
  – Are we protected?
  – If not, how can we improve?
State of the Art

• Previous studies
  – DETECTOR, SENTINEL, PROTECTOR, etc.

• Existing systems
  – GSS100D Detector
  – Signal Sentry 1000
  – N6841A RF Sensor

• Why STRIKE3?
STRIKE3 Rationale 1

- Site 1
  - 1436 events
  - 37 Chirp

- Site 2
  - 250 events
  - 11 chirp (different signatures)

- To monitor single site – one sensor
- To understand wider threat environment – monitoring network required (regulators, government, users)
Monitoring network deployment
- Limited if deploy own network with single type of sensor
- Larger network and more data if allow reports from different systems
- Are results compatible?
• Monitoring useful – understand the threat environment

• So what? - Countermeasures
  – Legislation (Supply, Possession, Use)
  – Education
  – Enforcement
    • Detect and remove
    • Direct or indirect
  – Equipment
    • Antenna
    • Receiver
    • Hybridisation
  – Procedure/process
STRIKE3 and Interference Monitoring

- Development of Reporting Standard for Interference Events
  - Consistency of reporting
  - System independent
  - Help creation of networks and threat database

- Implement reporting standards
  - Modify existing systems
  - Testing, validation of standards
STRIKE3 and Interference Monitoring

• Deploy international network of sensors
  – Range of countries and types of site
  – Populate database:
    • Analysis and understanding of threat
    • Threat signatures / types of threat
STRIKE3 and Receiver Testing

• Development of Testing Standard
  – Check receiver resilience against threats
    • Based on identified threats (from database)
  – Consistent approach to testing and analysis
  – Receiver independent
STRIKE3 and Receiver Testing

• Validation of Testing Standard
  – Test different receivers and algorithms
  – Response to real events
  – Test against emerging threats
  – Improved mitigation

1st June 2016, ENC2016, Helsinki
STRIKE3 Current Status

• KO Feb 2016

• Current activities
  – State of the art review
    • Stakeholders, existing systems, previous projects, current work on standardisation, etc.
  – International threat collection exercise
    • 10 sensors deployed in 5 countries
      – Building up data base of events
    • More deployments planned in coming months

1st June 2016, ENC2016, Helsinki
STRIKE3 Current Sensor Network

• Countries
  – UK, Sweden, Poland, Slovakia, Czech Republic, Finland, India

• Types of site
  – Environment (city, suburban, motorway)
  – Site use (CORS, timing, power grid, airport)

• Types of Sensor
  – Detector (NSL), RF Oculus (FOI), GEMNet (SAC)
  – Some co-location to compare results
STRIKE3 Initial Results

• Variation in activity between sites
  – < 5 events per day, low power
  – 100+ events per day, many different signals

• Different sensors detect same events
  – Compare results

• Impact on GNSS
  – Many events no impact
  – GNSS tracking can be affected – signal power and type
STRIKE3 Future Activities

• Analysis of threat collection results
• Development of draft Standards (Jan 2017)
• Implement reporting Standards and develop test environment (Oct 2017)
• Long term threat Monitoring and Receiver Testing (2018)

• www.gnss-strike3.eu – coming soon!
Thank You for Your Attention!

The work presented in this paper has been co-funded under the H2020 programme through the European GNSS Agency (GSA)