UN ICG Experts Meeting: GNSS Services

Vienna, Austria, 14 – 18 December, 2015

Methods and techniques for improvement of GNSS resilience against jamming-spoofing-meaconing attacks at the open sea

Renato Filjar, SERDJO KOS

Faculty of Maritime Studies, University of Rijeka, Croatia

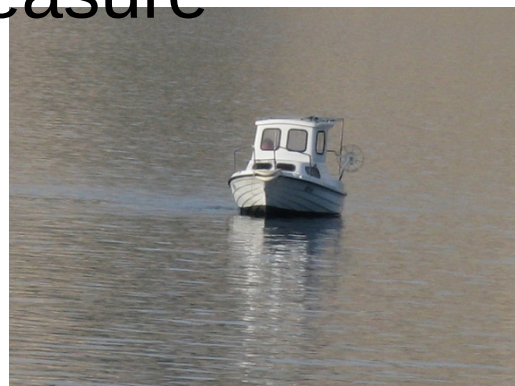
UN ICG Experts Meeting: GNSS Services

Methods and techniques for improvement of GNSS resilience against jamming-spoofing-meaconing attacks at the open sea

Full Professor Serdjo Kos, FRIN

- Introduction and motivation

- Increasing volume of maritime transport emphasises vulnerabilities of GNSS operation at the open sea
- Crew, vessel and goods may be at danger as the result of provision of engineered GNSS signals and navigation data
- Lack of supporting ICT infrastructure at the open sea
- A process for JSM-resilient GNSS operation at the open sea is proposed as a JSM counter-measure
- Anti-JSM effort as a risk-reduction process

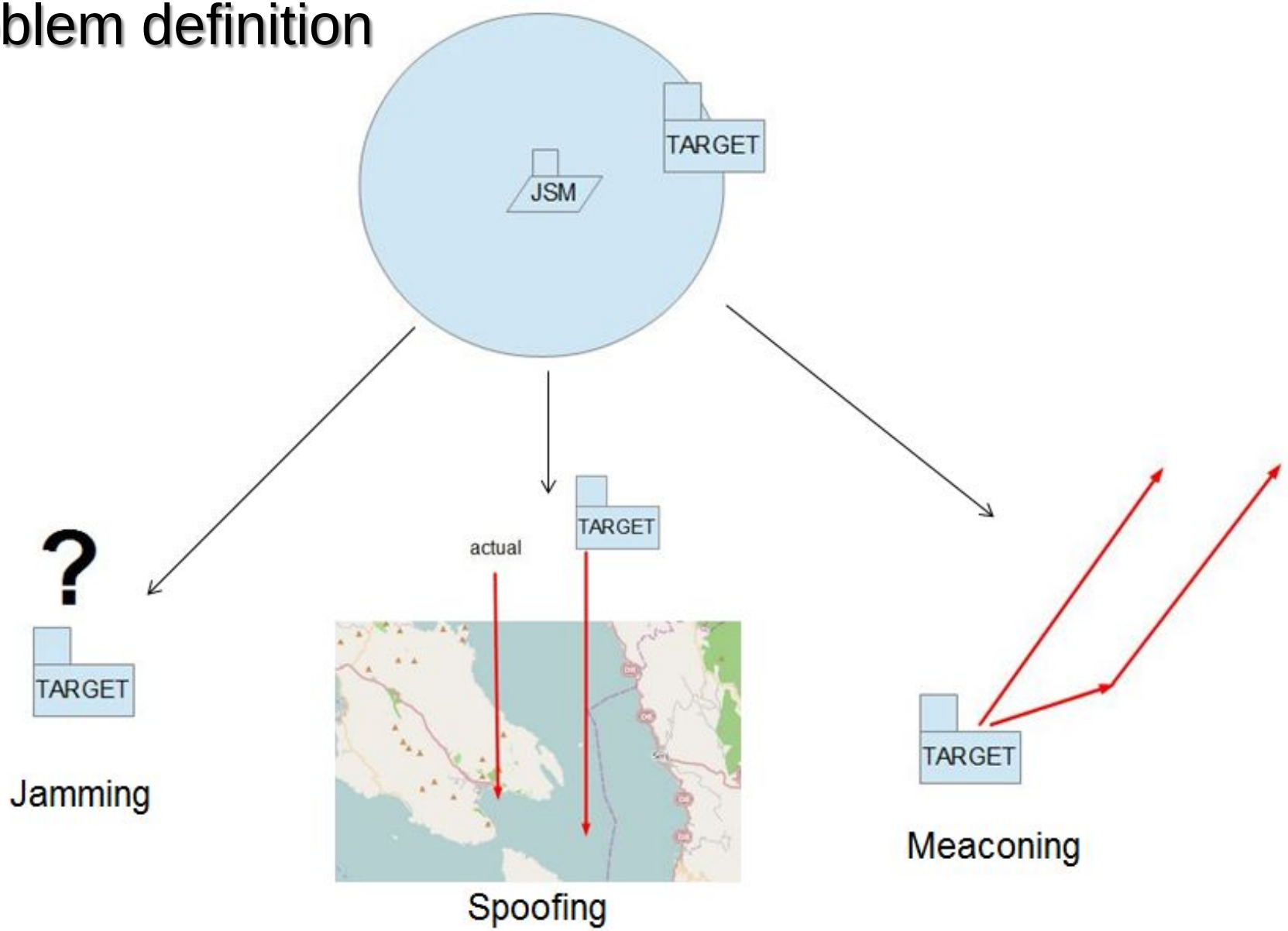


UN ICG Experts Meeting: GNSS Services

Methods and techniques for improvement of GNSS resilience against jamming-spoofing-meaconing attacks at the open sea

Full Professor Serdjo Kos, FRIN

- Problem definition



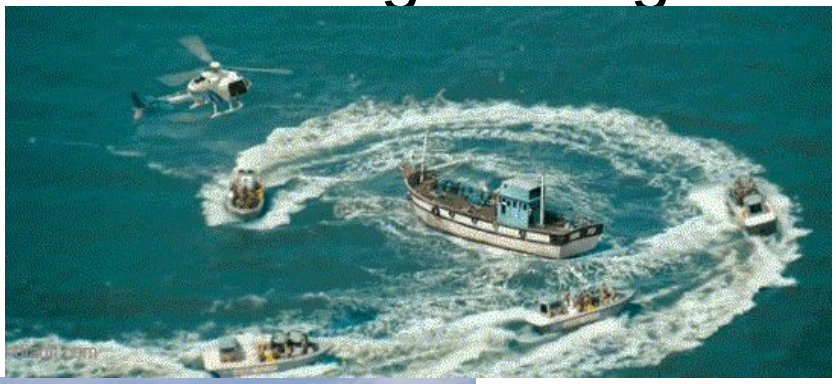
UN ICG Experts Meeting: GNSS Services

Methods and techniques for improvement of GNSS resilience against jamming-spoofing-meaconing attacks at the open sea

Full Professor Serdjo Kos, FRIN

- Evil intent behind JSM operation

- Potential targets:
- Load (intentionally grounding the vessel and grabbing what remains of her load)
- Crew (kidnapping for ransom)
- Vessel (take-over, hijacking)



UN ICG Experts Meeting: GNSS Services

Methods and techniques for improvement of GNSS resilience against jamming-spoofing-meaconing attacks at the open sea

Full Professor Serdjo Kos, FRIN

- Evil intent behind JSM operation at the open sea – risk assessment

- Grounding – less probable
- Take-over – highly probable
- Crew kidnapping – moderately to highly probable

UN ICG Experts Meeting: GNSS Services

Methods and techniques for improvement of GNSS resilience against jamming-spoofing-meaconing attacks at the open sea

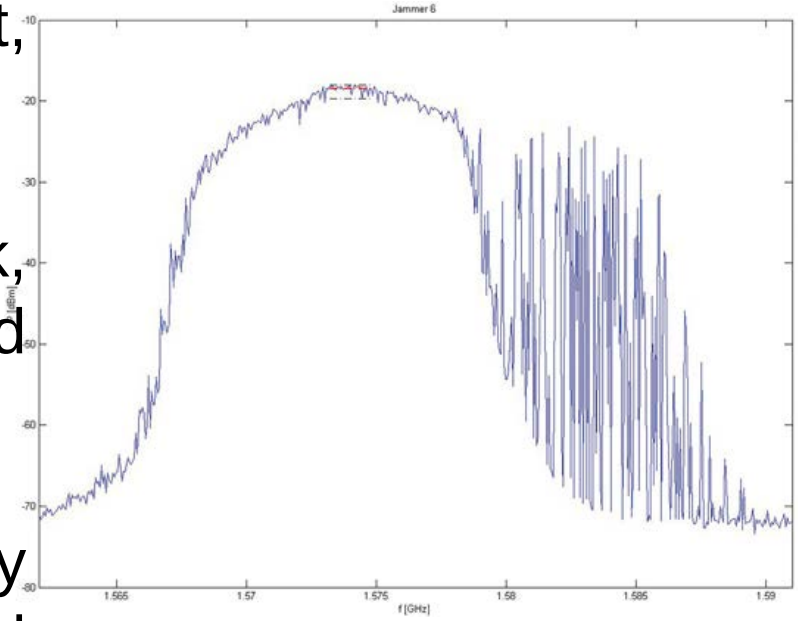
Full Professor Serdjo Kos, FRIN

- The nature of a JSM attack

- Jamming – simple and cheap equipment, not highly sophisticated attack

- Spoofing – a highly sophisticated attack, requires targeted education, skills and experience

- Meaconing – moderately to highly sophisticated attack, may be conducted by less-experienced personnel equipped with highly sophisticated equipment

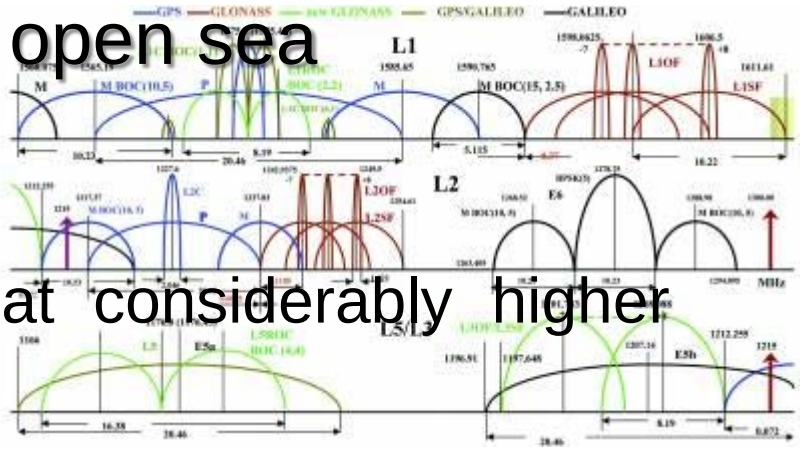


UN ICG Experts Meeting: GNSS Services

Methods and techniques for improvement of GNSS resilience against jamming-spoofing-meaconing attacks at the open sea

Full Professor Serdjo Kos, FRIN

- Developing JSM resilience at the open sea
- Signatures of JSM in operation



  - Received satellite signal strength at considerably higher levels than usual
  - Rapid change of satellite signal strength at the moment of the start of JSM operation
  - Increasing discrepancy with other positioning sensors
  - Apparent discrepancy in relative signal power of different GNSS signals (for instance: GPS L1 vs GPS L2)
  - Discrepancy between satellite ephemeris and almanac data

UN ICG Experts Meeting: GNSS Services

Methods and techniques for improvement of GNSS resilience against jamming-spoofing-meaconing attacks at the open sea

Full Professor Serdjo Kos, FRIN

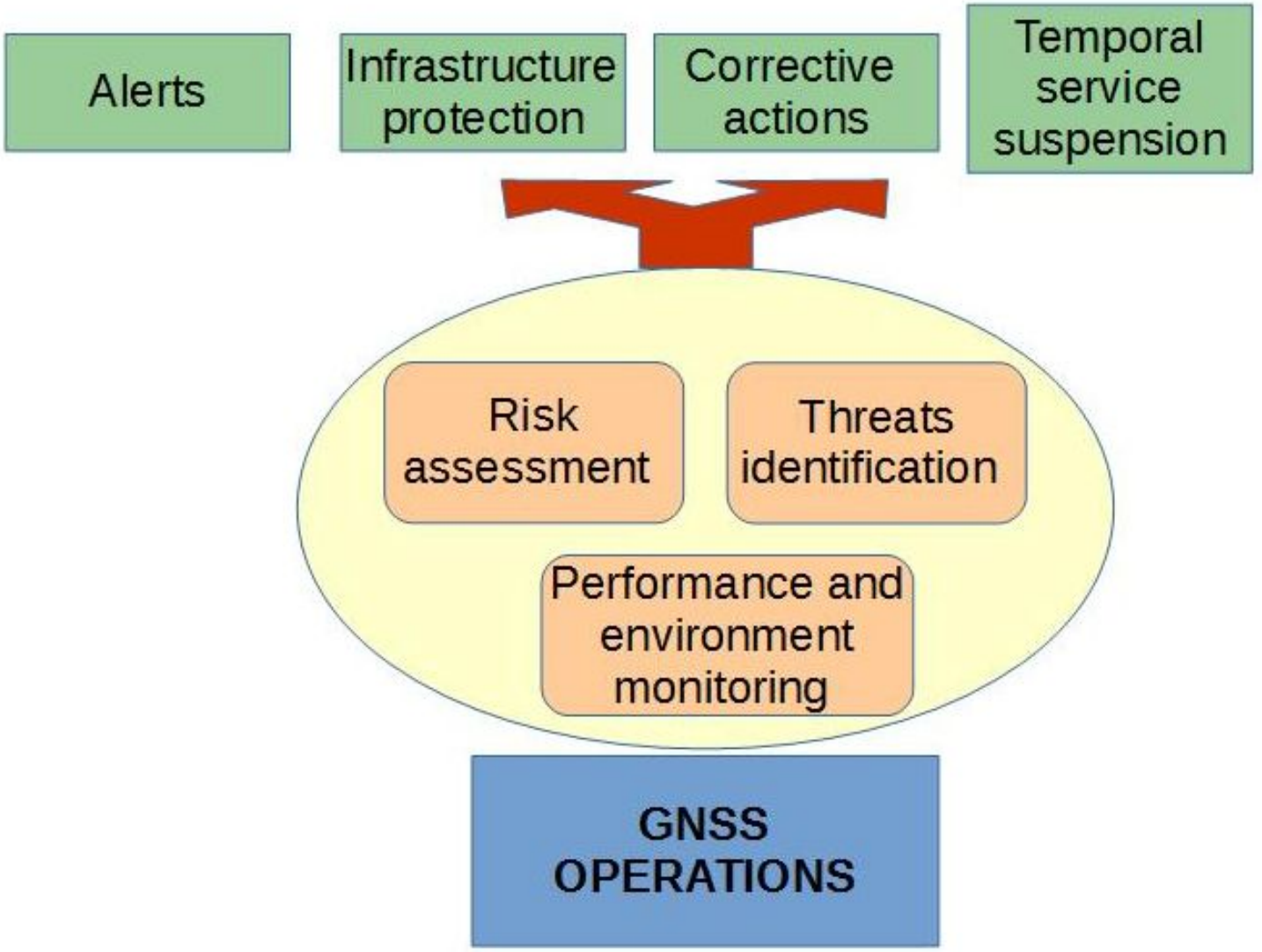
- Recommendations for development of JSM resilience at the open sea
- Continuous monitoring of GNSS performance both on vessel's bridge and regionally/globally
- Looking for signatures of JSM operations (manually – the crew, or automatically – specially designed GNSS receiver)

UN ICG Experts Meeting: GNSS Services

Methods and techniques for improvement of GNSS resilience against jamming-spoofing-meaconing attacks at the open sea

Full Professor Serdjo Kos, FRIN

- GNSS JSM resilience scheme at the open sea



UN ICG Experts Meeting: GNSS Services

Methods and techniques for improvement of GNSS resilience against jamming-spoofing-meaconing attacks at the open sea

Full Professor Serdjo Kos, FRIN

- GNSS JSM resilience scheme at the open sea

- Threats identification – risk assessment of reasonably possible threats
- Risk assessment for processes – include the assesssment of risk to navigation process (what are the effects of GNSS failure for navigation?) and how to overcome them
- GNSS performance and operation, and positioning environment monitoring – sudden and unexplained changes in GNSS receiver readings, spectrum observation – manual or automatic?

UN ICG Experts Meeting: GNSS Services

Methods and techniques for improvement of GNSS resilience against jamming-spoofing-meaconing attacks at the open sea

Full Professor Serdjo Kos, FRIN

- GNSS JSM resilience scheme at the open sea

- Alerts – internal (within a vessel) and external (JSM operation report to international monitoring authorities)
- Infrastructure protection – cannot be done by vessel's crew – who will act on that?
- Corrective actions – temporal suspension of GNSS usage, swithch to alternative positioning resources, informing the authorities
- Restriction or temporal suspension of services – AIS and similar services

UN ICG Experts Meeting: GNSS Services

Methods and techniques for improvement of GNSS resilience against jamming-spoofing-meaconing attacks at the open sea

Full Professor Serdjo Kos, FRIN

- Disucssion
- JMS in operation is identifiable
- Modern state-of-the-art in electronic navigation focuses on system integration -> an officer on bridge cannot easily inspect the performace of a particular positioning sensor
- Additional education required in understanding the GNSS vulnerabilities
- A novel deisgn of GNSS equipment is needed, that allows for easy inspection of GNSS performance, or that comprises advanced algorithms for JMS operation
- Collation of observed GNSS JSM operations on a global scale recommended

UN ICG Experts Meeting: GNSS Services

Methods and techniques for improvement of GNSS resilience against jamming-spoofing-meaconing attacks at the open sea

Full Professor Serdjo Kos, FRIN

- Conclusion
- The main causes of vulnerabilities
  - Over-reliance on GNSS
  - System integration in electronic navigation
  - Crew do not develop the required skills and knowledge
- Proposed process for development of JSM-resilient GNSS operation at the open sea
- Call for international co-operation on combating JSM
- Call for the crew's additional professional education
- Call for GNSS receiver design with embedded algorithms for GNSS JSM operation assessment
- Future work will concentrate on improvements in GNSS SDR equipment design, and JSM-resilient GNSS operation process development

UN ICG Experts Meeting: GNSS Services

Methods and techniques for improvement of GNSS resilience against jamming-spoofing-meaconing attacks at the open sea

Full Professor Serdjo Kos, FRIN

- ## Reference

- Borio, D. (2013). Spectral and Spatial Characterization of GNSS Jammers. Proc of 7 th GNSS Vulnerabilities and Solutions Conference. Baška, Krk Island, Croatia.
- Crane, R. (2012). Radio Frequency Interference and Cybersecurity Framework. 8th Annual Baska GNSS Conference. Baska, Krk Island, Croatia. Available on-line at: http://www.gps.gov/news/2012/05/croatia/, courtesy of the US National Coordination Office for Space-Based Positioning, Navigation and Timing.
- Filjar, R, Brčić, D, and Kos, S. (2014). Jamming-Spoofing-Meaconing-Resilient GNSS Performance at the Open Sea. Proc of 8th Annual Baska GNSS Conference (5 pages). Baska, Krk Island, Croatia
- Filjar, R., D. Huljenić. (2012). The importance of mitigation of GNSS vulnerabilities and risks. Coordinates, 8(5), 14 - 16.
- Grant, A. (2013). Resilient PNT: making way through rough waters. Proc of 7 th GNSS Vulnerabilities and Solutions Conference. Baška, Krk Island, Croatia.
- Kroener, U, and Dimc, F. (2010). Hardenning of civilian GNSS trackers. Proc of 3 rd GNSS Vulnerabilitiesand Solutions Conference (on CD). Baška, Krk Island, Croatia.
- O'Hamlon, B W et al. (2013). Real-Time GPS Spoofing Detection via Correllation of Encrypted Signals. Navigation, 60($), 267-278.
- Petrovski, I G, and Tsujii, T. (2012). Digital Satellite Navigation and Geophysics: A Practical Guide withGNSS Signal Simulator and Receiver Laboratory. Cambridge University Press. Cambridge, UK.

UN ICG Experts Meeting: GNSS Services

Methods and techniques for improvement of GNSS resilience against jamming-spoofing-meaconing attacks at the open sea

Full Professor Serdjo Kos, FRIN

- ## Reference

- Sheridan, K. (2013). GNSS Interference Detection and Characterisation using a Software Receiver – The DETECTOR Project. Proc of 7 th GNSS Vulnerabilities and Solutions Conference. Baška, Krk Island, Croatia.
- Sanz Subirana, J, Juan Zornoza, J M, and Hernandez-Pajares, M. (2013). GNSS Data Processing – Vol. I: Fundamentals and Algorithms. European Space Agency. Noordwijk, the Netherlands.
- Thomas et al. (2011). Global Navigation Space Systems: reliance and vulnerabilities. Royal Academy of Engineering.London, UK.
- Williams, P, Hargreaves, C, Last, J D, and Ward, N. (2013). eLoran – the route to resilience? Proc of 7 th GNSS Vulnerabilities and Solutions Conference. Baška, Krk Island, Croatia.

UN ICG Experts Meeting: GNSS Services

Methods and techniques for improvement of GNSS resilience against jamming-spoofing-meaconing attacks at the open sea

Full Professor Serdjo Kos, FRIN

- **Traceability**

This lecture is based on the paper presented at the 8th Annual Baska GNSS Conference (Baska, Krk Island, Croatia), a meeting point for scientists, engineers, strategists, advisors, policy-makers, technology- and business-developers, regulators, end-users and the other interesting parties.

The Annual Baska GNSS Conference addresses the latest developments in:

- GNSS core and advanced PNT,
- development of resilient GNSS (especially against space weather, ionospheric and jamming effects),
- signal processing for GNSS receiver design,
- GNSS alternatives, and
- GNSS PNT navigation and non-navigation applications (incl. intelligent transport systems, GNSS-R, location-based services, space weather and ionospheric monitoring, timing and synchronisation applications, forestry, and agriculture).

Invitation to 10th Annual Baska GNSS Conference to be held in Baska, Krk Island, Croatia
8 – 10 May, 2016

THANK YOU FOR YOUR ATTENTION !

Full Professor Serdjo Kos, FRIN
Member of Council, The Royal Institute of Navigation, London, UK
Faculty of Maritime Studies,
University of Rijeka, Croatia

E-mail:skos@pfri.hr