A PROPOSAL FOR A GNSS FAILURE LEGAL LIABILITIES SCHEME

Renato Filjar, Axel Luttenberger, Serdjo Kos
Faculty of Maritime Studies, University of Rijeka, Rijeka, Croatia
E-mail: renato.filjar@gmail.com

Abstract: *The proper scheme of legal liability scheme for the management of legal consequences of a GNSS failure has become an important GNSS utilisation issue for some time. As the GNSS has become both the enabling and the underlying foundation to a growing number of systems and services, the quest of legal liability emerges as an important component of the establishment of the GNSS business environment. Considering the current state of the art, the GNSS should be considered a component of the national infrastructure, along with the systems such as those for power distribution or the national airspace.*
Here we present a proposal for a legal liability scheme in the case of the GNSS failure, which is based on the spatial, technology and business environment shared liability. Reflecting the GNSS utilisation from the service proviso perspective, this proposal requests the GNSS risks assessment, and mitigation plan to be prepared by the GNSS business environment stakeholders. Under the proposed scheme, the national regulatory agency and the service providers should take a portion of legal responsibility for provision of the guaranteed level of the GNSS positioning and timing service, thus allowing for sustained provision of the GNSS performance and the quality of GNSS-based services.

KEY WORDS

1. GNSS failure 2. liability scheme 3. GNSS-based services 4. legal framework

1 INTRODUCTION. The widespread utilisation of the satellite navigation technologies attract more people to use GNSS either directly or embedded within complex technological and socio-economic systems. Satellite navigation applications range from navigation, through transport-, financial- and telecommunications-related services, to national security and public safety, thus establishing the GNSS as a component of national infrastructure.
The GNSS utilisation in various technological and socio-economic systems means that GNSS will be increasingly used mostly by users with poor GNSS education and interest in technology, and in challenging positioning environments with natural and artificial threats to GNSS integrity and performance. Operators of satellite navigation systems can guarantee the GNSS service performance only in favourable positioning environments that are completely opposite to the environments in which majority of GNSS users utilise the technology. The growing number of GNSS-based services ask for the establishment of the GNSS failure legal liabilities scheme for the cases of damages to property, health and life. After establishing the framework for its deployment, we propose the appropriate GNSS failure legal liability scheme based on shared responsibility between the stakeholders of GNSS-based services business environment.

2 GNSS AS A COMPONENT OF NATIONAL INFRASTRUCTURE. Humanity can be considered navigation oriented, with a number of individual and common societal activities (such as economy and transport) being firmly navigation-oriented. Satellite navigation has brought unprecedented enhancement in ability to accurately and robustly estimate one's position in space. With a growing number of technology and socio-economic applications, satellite navigation systems have matured to the level of being considered a public goods. Embedded in numerous technological and socio-economic systems, GNSS has become a component of national infrastructure in a way that its performance and operation should be sustained for the benefits on the national level. While the GNSS supports provision of fundamental, regulated and commercial (private) services, the satellite navigation technology can be found in national, as well as in regulated and commercial (private)

infrastructure. GNSS failure, caused by either operational failure, or a failure to sustain the expected positioning, navigation and timing (PNT) performance will inevitably lead to considerable deterioration or even temporal suspension of a wide variety of services.

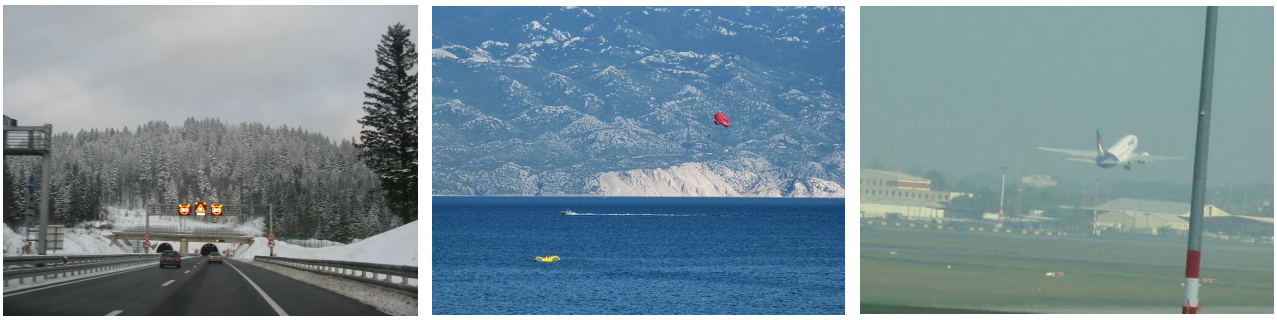

Fig 1 GNSS improves services and processes in various segments of transport (in the air, on the sea and on land), but increasingly extends its reach to non-navigation disciplines

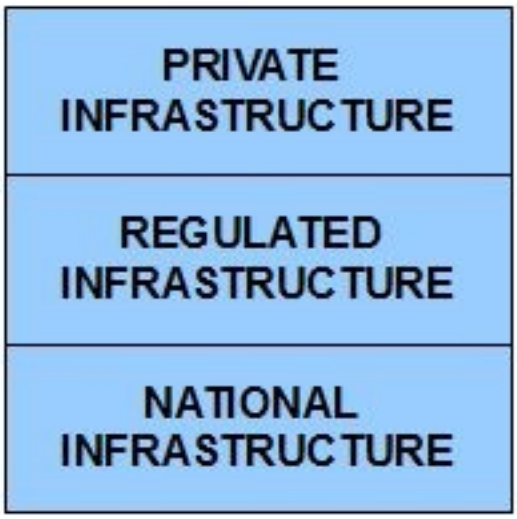

Fig 2 All three layers of infrastructure in support of a wide variety of services available nation-wide utilise GNSS

Sustained PNT GNSS services provision is therefore essential for economic growth, safety and security, and receives the nation-wide sustainability and protection priority. This applies to both navigation-related and non-navigation applications of GNSS.

3 CORE GNSS VULNERABILITIES AND RISKS arise as the effects of both natural and artificial (man-made) sources. Those can ignite the GNSS vulnerabilities and risks by either affecting the positioning estimation errors, or reducing the availability of the PNT services. The vulnerabilities and risks of satellite navigation systems' usage emerge as result of the core nature of the GNSS operation, its architecture, and the environment in which the GNSS operations are performed, as depicted on Fig 3.
Comprising four essential components, the GNSS architecture does not allow for complete control of the system's operation and performance by any single stakeholder (system's operator, regulator, end-user or any other). Thus online a limited assurances can be offered in regard to the quality of

system performance and operation, although it is kept at every high level.

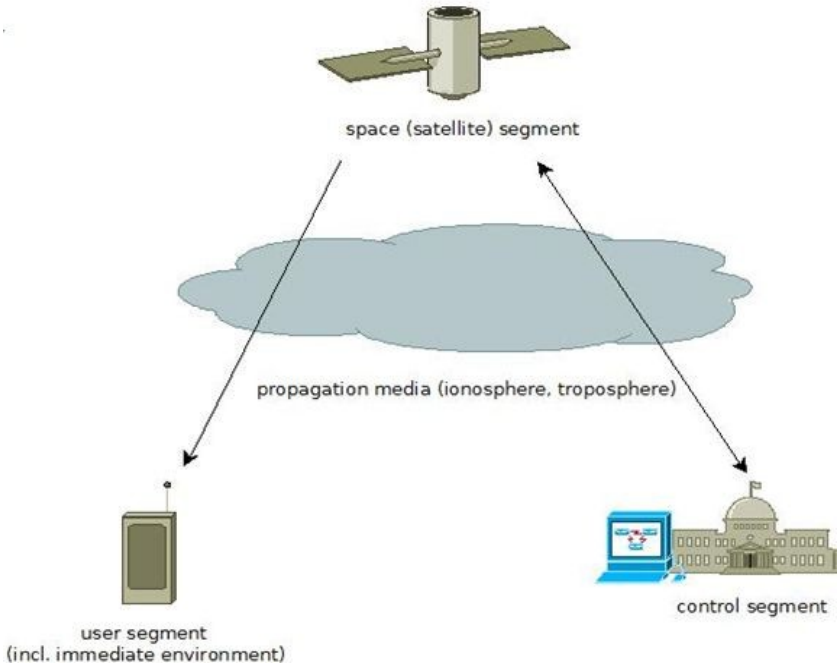

Fig 3 Architecture of a GNSS

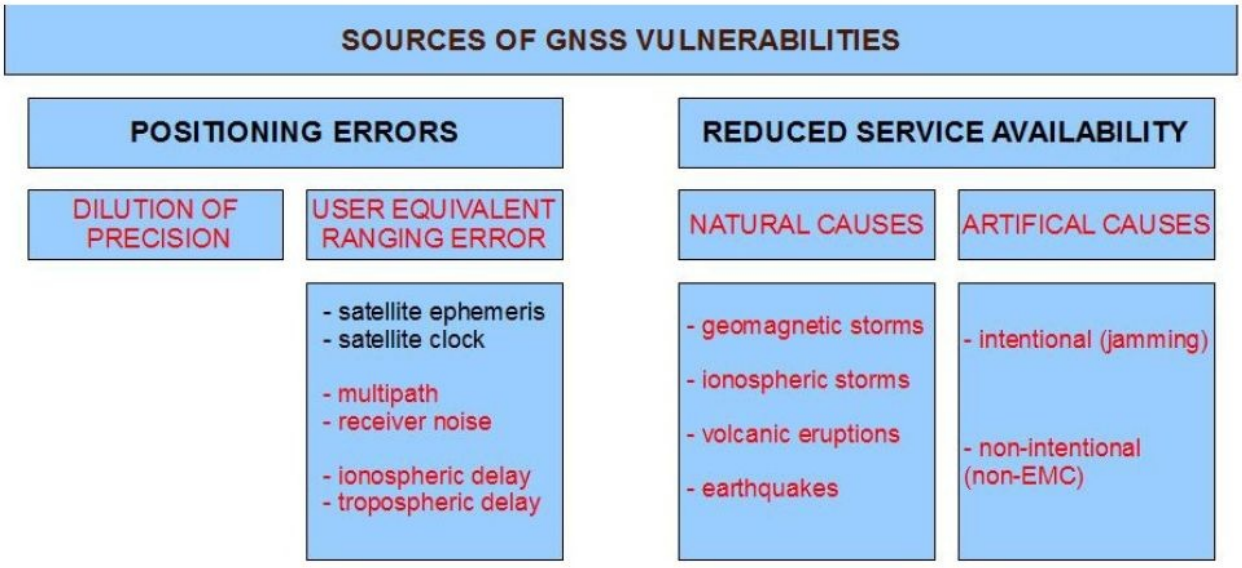

Fig 4 Sources of GNSS vulnerabilities

The errors in positioning estimation result in combined effects of Dilution of Precision (DOP) and User Equivalent Ranging Errors (UERE), where the ionospheric delay and multipath emerge as the most influential sources. A proper modelling and forecasting of the ionospheric dynamics (for GNSS ionospheric delay) and hardware, software and operational solutions (for multipath-caused errors) can successfully mitigate the positioning errors as a source of GNSS vulnerabilities and risks for a wide range of GNSS applications, at least to a bearable levels. Mitigation of causes of reduced PNT service availability is much harder to overcome. The effects of some natural causes of GNSS vulnerabilities and risks may be identified or forecast relatively easily, but the transfer of this knowledge to community of GNSS users still seems to be a daunting task. For the rest, it is the quest for continuous monitoring of geophysical processes on the local scale and learn of the

mechanism and patterns that will lead to establishment of new prediction models related to effects on GNSS PNT performance and system's operation. On the other side, the effects of the artificial sources of disruptions and deteriorations of GNSS PNT services have become increasingly frequent and disastrous. The abundance of low-cost low-priced GNSS jamming equipment raises concerns of potentially devastating effects on GNSS-based systems and services.

4 GNSS RESILIENCE SCHEME. In its essence, satellite navigation technology was not designed to satisfy demands of modern GNSS-based systems and services. Still, the freely globally available (i. e. non-royalty) PNT service has attracted a huge attention at both commercial and non-commercial (incl. governments and science) communities, raising the quest on how to properly address the GNSS vulnerabilities and risks problems in a system with distributed (i. e. non-centralised) control.

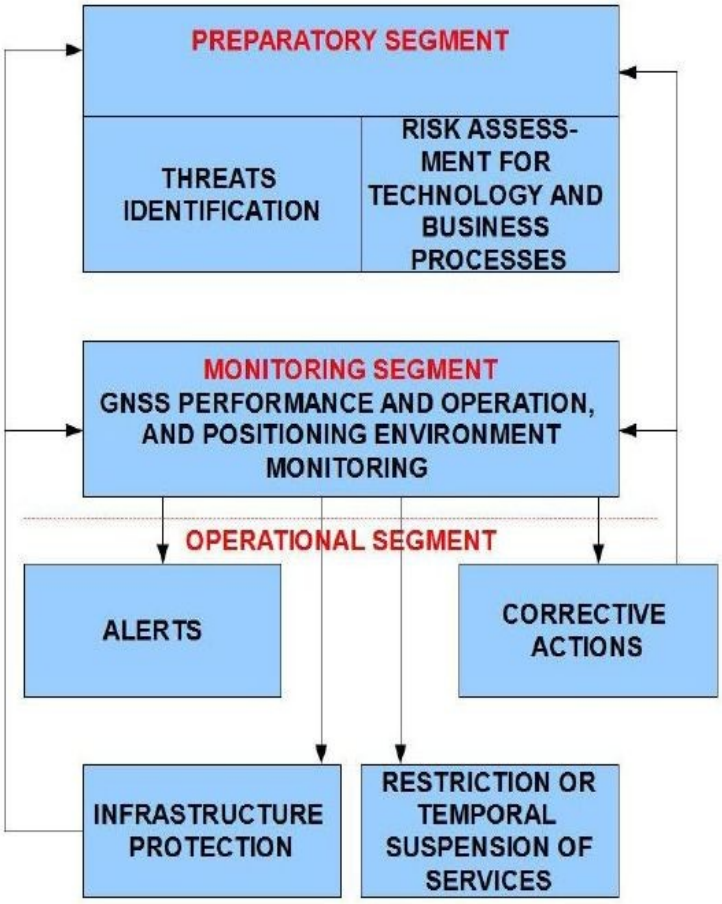

Fig 5 GNSS resilience scheme

These authors proposed a GNSS resilience scheme, depicted on Fig 5, aimed at solution of the problem of curbing the GNSS vulnerabilities and risks problem. The main actions comprised by the proposed GNSS resilience scheme include the following operation segments:

- preparatory segment (particular threats identification, individual risk assessment for every GNSS-based system or service user),
- monitoring segment (continuous monitoring of relevant parameters that indicate the time of appearance and nature of the known threats),
- operational segment (comprising activities following the identification of the threat, such as: alerting targeted group of GNSS users, corrective actions deployment, suspension of GNSS-based services and protection of the infrastructure).

5 BUSINESS ENVIRONMENT FOR GNSS-BASED SERVICES. Satellite navigation is a fundamental technology, utilised to provide a plethora of commercial and non-commercial services. End-users use services through interaction with the related applications.

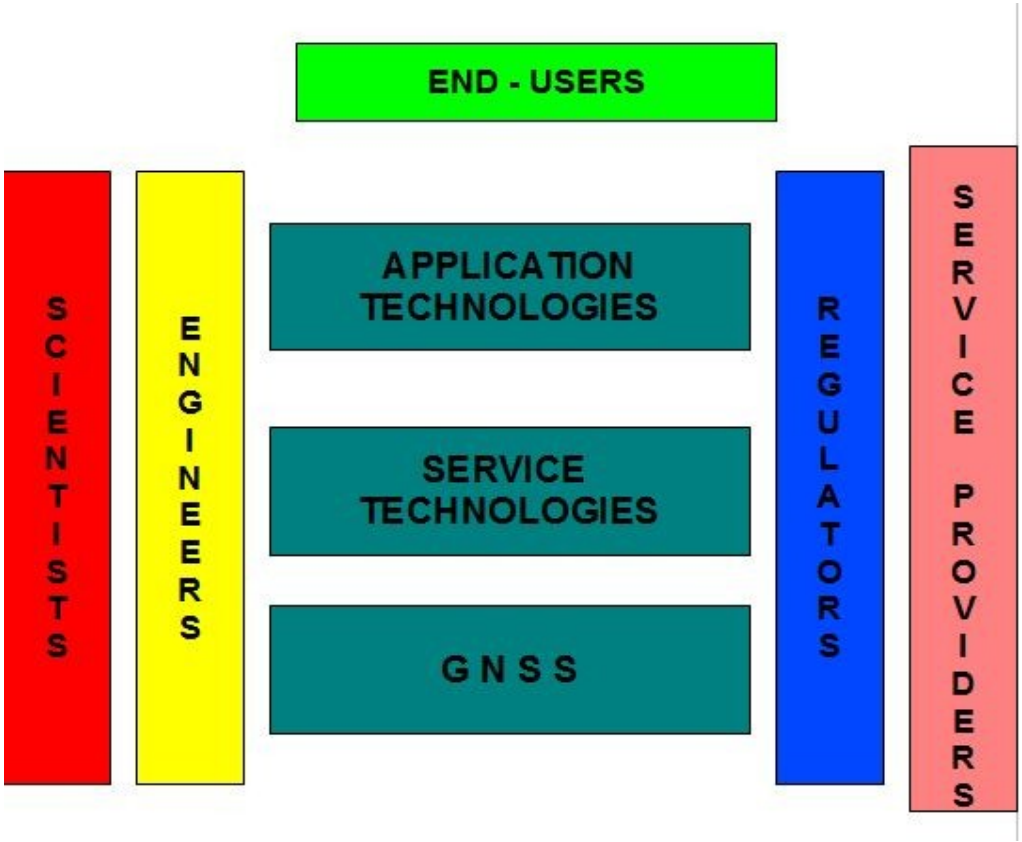

Fig 6 Business environment for GNSS-based systems and services

The establishment of technologies-services-applications hierarchy is a task conducted by a number of stakeholders (scientists, engineers, regulators, service and content providers, technology operators and en-users), as presented on Fig 6. The engagement of every stakeholder within the business environment for GNSS-based systems and services means that relations between them has been established, and that every stakeholder influences not only the business balance, but also the essential balance of system and services performance and operation.

6 PROPOSAL FOR GNSS FAILURE LEGAL LIABILITIES SCHEME. Considering the role of the GNSS within the national infrastructure (Chapter 2), the complexities of core GNSS vulnerabilities and risks (Chapter 3) and the business environment for GNSS systems and services (Chapter 5) and the need for utilisation of the GNSS resilience scheme (Chapter 4) for the purpose of curbing the GNSS vulnerabilities and risks, here we propose the scheme for identification of legal liabilities due to the GNSS failure to provide expected performance of PNT service. Assuming that in certain cases the failure in proviso of expected GNSS PNT service can lead to material and financial damage, and/or injuries or loss of life, our proposal attempts to fill in the gap of defining the legal liability for cases in question.

Our proposal for the GNSS failure legal liability scheme is based on the shared liability concept, instead of the sole liability of the GNSS operator, that comprise all stakeholders of the GNSS business environment within the limits of their effects and contributions to GNSS business and technology environment (Fig 7, Table 1).

Furthermore, our proposal calls for joint effort of all GNSS-related stakeholders in provisioning reasonable alerts of misused utilisation of satellite navigation-based systems and services, and of alerting on deteriorating conditions for GNSS utilisation.

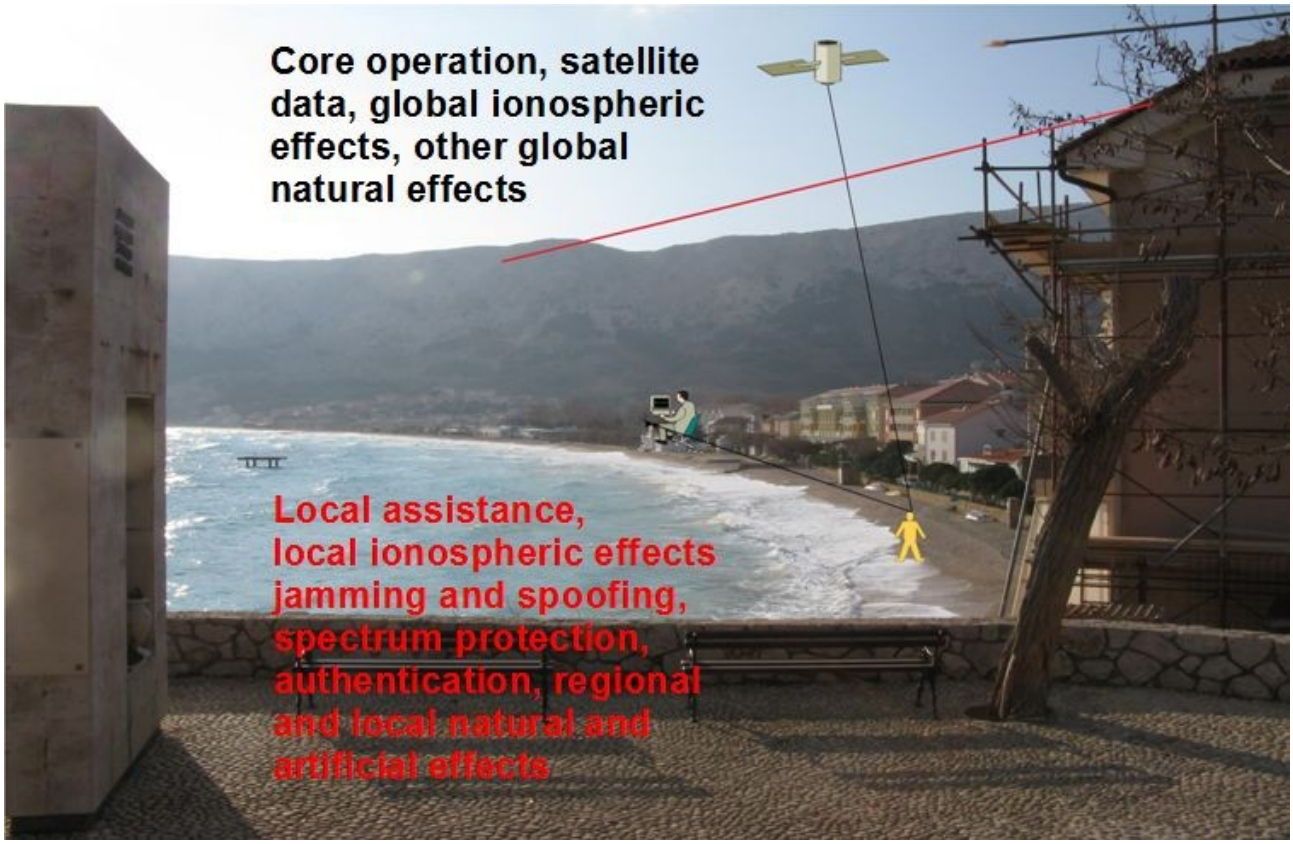

Fig 7 Concept of the shared liability for GNSS failures

Table 1

Legally liable subject	Causes of loss
GNSS operators	Core system failure, failure in global GNSS assistance and augmentation provision, failure in provision of alerts on global ionospheric and the other global natural effects
National regulators	Failure in GNSS signal and spectrum protection on national level, failure in combating local jamming and spoofing, failure in regulating GNSS-based service provisioning
GNSS-based service providers	Failure in advising and fostering the proper use of robust standardised equipment, failure in combating user-initiated jamming, failure in provision of targeted GNSS performance deterioration alerts, failure in robust provisioning of GNSS-based services, failure in conducting the risk assessment
End-users	All remaining failures, including misconducts, and equipment misuse and unlicensed modifications.

7 DISCUSSION. GNSS failure may cause loss of life, injuries, material and financial damage. Since the GNSS failure legal liability has not regulated at the international level, this paper attempts to clarify the situation and propose the shared liability concept based on the areas of reasonable impact on GNSS-based services and systems.

Present view on the problem assumes the GNSS operator's responsibility. We argue that national

regulators, service providers and end-users should be engaged in the scheme, accepting responsibilities for their actions and legal liabilities for the failures in their respective areas of operation. Within the proposed scheme, we call for proper risk assessment, preparations of corrective actions, and their operational status in case of particular threats to GNSS performance and operations.
Finally, we emphasise the request for co-ordinated efforts between GNSS operators, national authorities and service providers in establishment and operation of the GNSS resilience scheme on the national level.

8 CONCLUSION. Raising number of GNSS-based services and systems accentuate the importance of the establishment of the GNSS failure legal liability scheme. We presented a proposal for such a scheme, based on understanding of sources of GNSS vulnerabilities and risks, and GNSS applications business environment, GNSS resilience scheme, and the fact that GNSS has become a component of national infrastructure. Based on shared responsibility concept, the proposed GNSS failure legal liability scheme defines clear legal liability for every stakeholder and fosters the implementation of GNSS resilience scheme as nation-wide contribution to provision of sustained GNSS performance to the end-users.

REFERENCE

Bollweg, H-G. (2008). Initial Consiedrations regarding the Feasibility of an International UNIDROIT Instrument to Cover Liability for Damage Caused by Malfunctions in Global (Navigation) Satellite Systems. International Institute for the Unification of Private Law (UNIDROIT). Rome, Italy. Available at: http://bit.ly/s7dlb8, accessed on: 2 January, 2012.

Carbone, S M, M E De Maestri. (2009). The Rationale for an International Convention on Third Party Liability for Satellite Navigation Signals. International Institute for the Unification of Private Law (UNIDROIT). Rome, Italy. Available at: http://bit.ly/s3DfB2, accessed on 2 January, 2012.

Filjar, R, H Gold, I Markežić. (2011). GNSS – the risk of the underlying technology. *Proc of 5th GNSS Vulnerabilities and Solutions Conference*. Baska, Krk Island, Croatia.

Filjar, R, K Vidovic, P Britvic. (2011). Scenarios of critical GPS positioning performance for eCall (4 pages). *Proc of 5th GNSS Vulnerabilities and Solutions Conference*. Baska, Krk Island, Croatia.

Filjar, R, S Kos, K Vidović. (2010). Global Navigation Satellite System as a Component of National Infrastructure. *UN/Moldova/US Workshop on GNSS Applications.* Kishinev, Moldova.

Filjar, R. (2009). Satellite navigation as a component of national infrastructure. *53rd European Organization for Quality Annual Congress*. Cavtat/Dubrovnik, Croatia.

UNIDROIT Secretariat. (2010). An instrument on third party liability for Global Navigation Satellite System (GNSS) services: a preliminary study. International Institute for the Unification of Private Law (UNIDROIT). Rome, Italy. Available at: http://bit.ly/vCUJDQ, accessed on 2 January, 2012.