The SENTINEL Project

The SENTINEL project is researching and developing a service to establish the extent to which global navigation satellite systems (GNSS) – in particular GPS and Galileo and/or eLoran Positioning, Navigation and Timing (PNT) signals can be trusted by users on a 24x7 basis. The SENTINEL project is part-funded by the government-backed Technology Strategy Board.

The SENTINEL Service will be used to **detect, quantify and locate GNSS interference at point of use**, either accidental (e.g. multipath, harmonics), deliberate (e.g. criminal jammers) or natural phenomena (e.g. weather, solar flares). This will enable timely action to be taken to mitigate any adverse impact on (for example) safety, mission-critical, security or revenue generating services which are enabled by PNT signals. It will provide real-time alerts to discriminate natural events and enable the location of deliberate jamming to be detected to provide timely detection and mitigation by the appropriate agencies.

This project is critical to developing effective strategies to respond to deliberate interference attacks as well as building confidence in existing signals. Currently organisations have little knowledge about the overall threat from deliberate jamming, interference or the 24x7 reliability of signals, whilst responding to such attacks requires justification and resourcing. This is an increasing risk as PNT services are further relied upon not only in the security and emergency services but also commercially in the increasingly GNSS-enabled world.

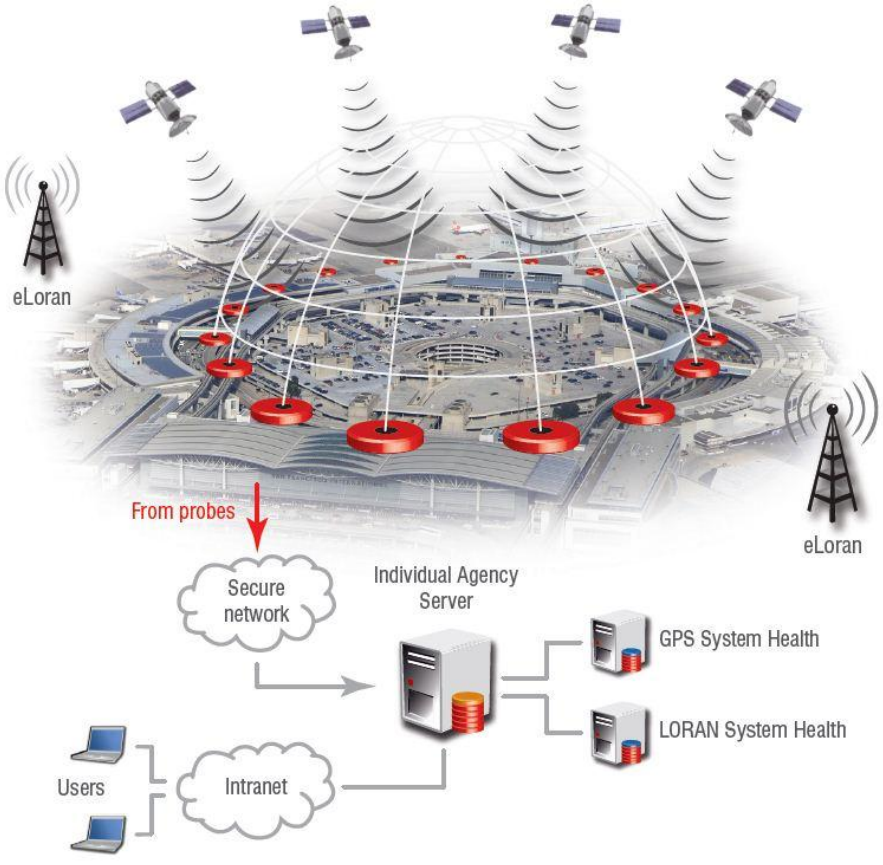

Figure 1: SENTINEL Overview

SENTINEL will deploy trial GNSS interference detection probes in a controlled manner to address the detection of deliberate or accidental signal jamming and also to detect, quantify and discriminate between low level interference such as spoofing or natural phenomena and the impact of unusual multipath in the vicinity. Simultaneously, the probes will quantify the quality of the UK eLoran signal as a complimentary PNT signal to GPS. Innovative techniques will be used to locate, quantify and detect the threat so that service providers can understand and interpret the problem and develop a more effective trusted service.

SENTINEL collaboration partners include: ACPO-ITS – The research arm of the Association of Chief Police Officers & agency partners, GLA – General Lighthouse Authorities of the UK and Ireland, OS – Ordnance Survey, NPL – National Physical Laboratory, Timing Metrology Division, UoB – University of Bath, Electronic & Electrical Engineering Faculty, Thatcham – Vehicle Security, Chronos Technology Ltd – Collaboration Leader

ACPO bring the support of key UK Government agencies including CPNI – Centre for the Protection of National Infrastructure, SOCA – Serious Organised Crime Agency, HOSDB – Home Office Scientific Development Branch and OFCOM – The Independent regulator and competition authority for the UK communications industries. ACPO together with GLA have a remit to ensure the protection of critical national infrastructure including roads, railways, harbours and airports. This will build on the current experimental GNSS UK Monitoring network developed under the Technology Strategy Board part-funded “GAARDIAN” project, and bring actual user-community deployment experience together with further R&D capability to the consortium.

SENTINEL innovation will add to the research from the GAARDIAN project and include:

- The first detailed multimodal analysis using continuous monitoring to explore the nature and extent of GNSS and eLoran interference which might compromise trusted services. This is important to fully understand and develop mitigation techniques.
- Research into techniques for real-time detection, characterisation, discrimination and location of natural and deliberate interference phenomena. The bringing together of all aspects particularly natural interference, systematic effects and location of interferers is not only a significant challenge technically but never been done before globally.
- The use of technology in this area to enable trust by ensuring system integrity is not discredited with false alarms, which is a very important requirement of a detection system such because if the system alarms too much, ‘cry wolf’ will occur and a real incident may be missed by users.

Other countries, notably the USA, are developing similar capability but analysis does clearly show the UK is a world leader in this detection technology capability and with active support from the Government this will only continue. The SENTINEL consortium is willing to work with European partners to bring this capability to a wider audience or to integrate the technology with any existing or planned systems.

Contact: Andy Proctor, Chronos technology. Andy.proctor@chronos.co.uk