Presentation to: International Committee on Global Navigation Satellite Systems (ICG)

Interference Detection and Mitigation: The SENTINEL project

Andy Proctor
Divisional Manager, Chronos Technology
Exploitation/Dissemination lead, The SENTINEL project

June 2012

Agenda

- Background and History
- Concepts
- Delivery
- Status & Findings
- Future

Inverness
Aberdeen
Perth
Dundee
Kirkcaldy
Glasgow
Edinburgh
East Kilbride
United Kingdom
Londonderry / Derry
Belfast
Craigavon
Sligo
Dundalk
Isle of Man
York
Leeds
Hull
Swords
Irish Sea
Manchester
Sheffield
Galway
Ireland
Dublin
Stoke-on-Trent
Nottingham
Limerick
Kilkenny
Birmingham
Tralee
Clonmel
Coventry
Waterford
Cork
Cloyne
Coronea
Leap
Bristol
Cardiff
Southampton
Exeter
Brighton
Plymouth
Portsmouth
St. Ives
English Channel
Amiens

What is it?

- Public-Private Consortium
- Led by Chronos Technology
- Technology Strategy Board co-funded
  - Industry
  - User
  - Academic partners
- Key aim to develop a GNSS interference detection capability
  - For CNI & Law Enforcement

Chronos Technology

Chronos Technology

Thatcham

Ordnance Survey

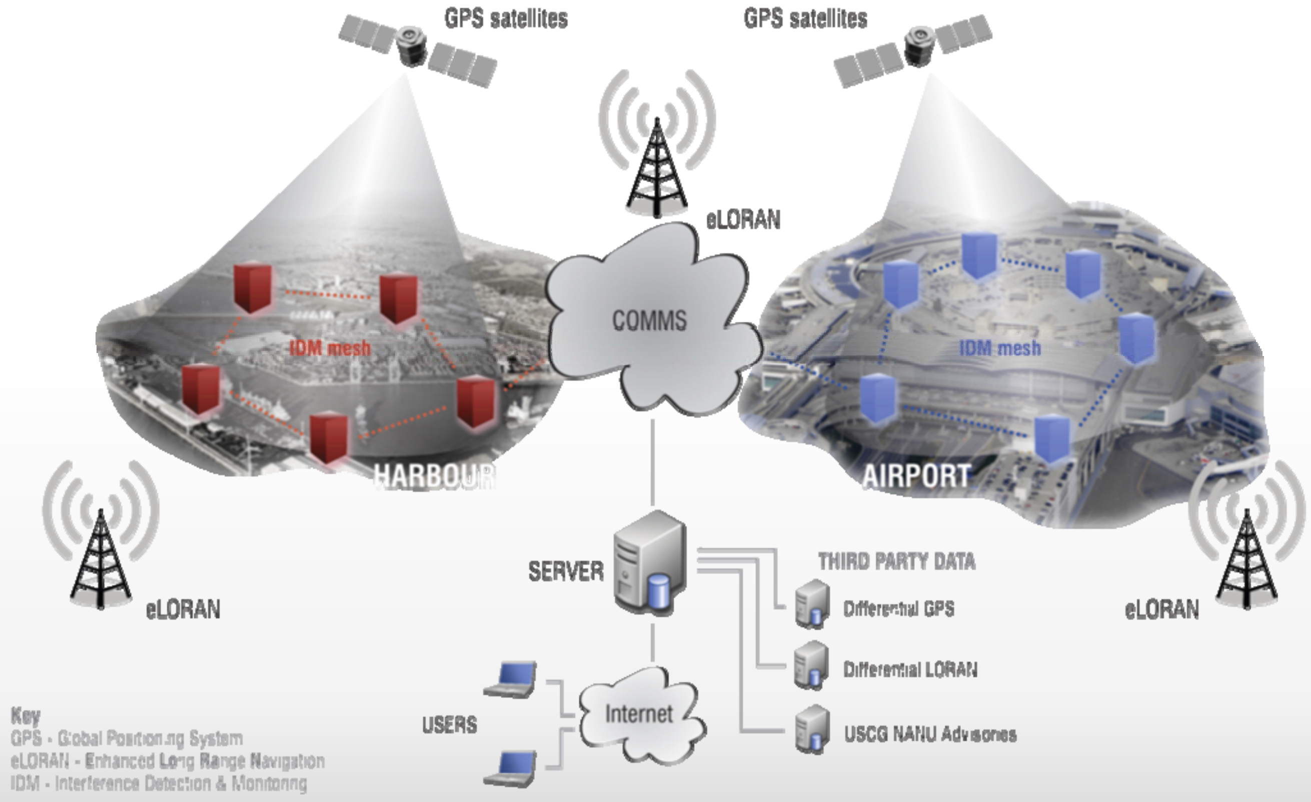
NPL

University of Bath

Research & Radionavigation
General Lighthouse Authorities
United Kingdom and Ireland

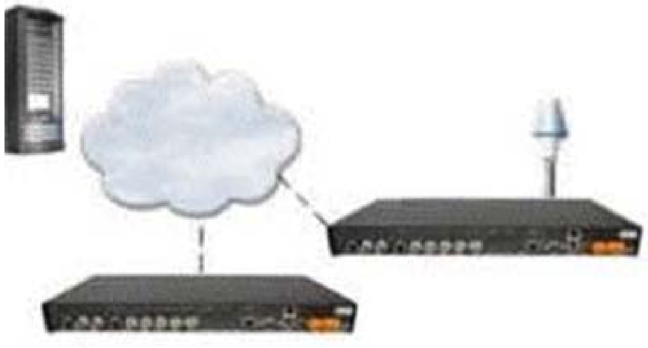
ACPO
Association of Chief Police Officers

Origins - GAARDIAN



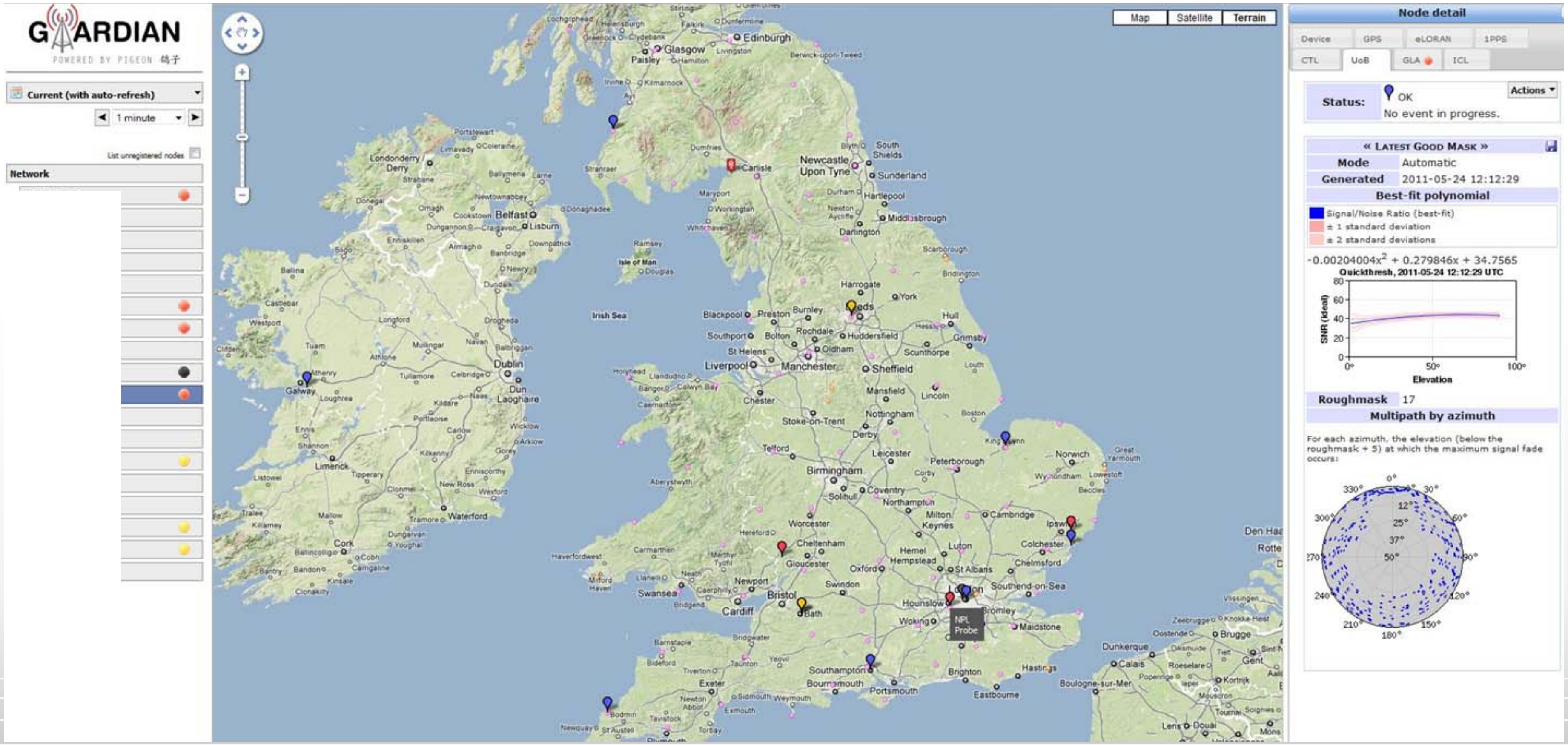
Key
GPS - Global Positioning System
eLORAN - Enhanced Long Range Navigation
IDM - Interference Detection & Monitoring

GAARDIAN Delivered



- Market/Risk Analysis
  - Across all sectors, user requirement definition
- IDM sensors
  - 24 x 7 Monitoring hardware – “Probes”
  - Can be deployed as a network in the vicinity of the user/area of interest
- UK Monitoring & detection network
  - Enabled Real-Time GPS, Galileo, Glonass or eLoran (PNT) monitoring
  - Can utilise existing infrastructure, networks of opportunity

UK Monitoring network



GUARDIAN

POWERED BY PIGEON 鸽子

Current (with auto-refresh)

1 minute

List unregistered nodes □

Network

Node detail

Device | GPS | eLORAN | 1PPS | CTL | UoB | GLA ● | ICL

Status: OK
No event in progress.

Actions ▾

« Latest Good Mask »

Mode	Automatic
Generated	2011-05-24 12:12:29

Best-fit polynomial

🟦 Signal/Noise Ratio (best-fit)
🟥 ± 1 standard deviation
🟥 ± 2 standard deviations

$-0.00204004x^2 + 0.279846x + 34.7565$

Quickthresh, 2011-05-24 12:12:29 UTC

Roughmask	17

Multipath by azimuth

For each azimuth, the elevation (below the roughmask + 5) at which the maximum signal fade occurs:

Key Results

- Capture of a jammer (2011)
- Understanding of jamming impact
- Increased awareness of problem nationally and globally

Protecting the UK Infrastructure: A System to Detect GNSS Jamming and Interference

Andy G. Proctor & Charles W. T. Curry, *Chronos Technology Ltd.*
Jenna Tong & Robert Watson, *University of Bath*
Mark Greaves & Paul Cruddace, *Ordnance Survey*

Abstract

The vulnerability of space based position navigation and timing (PNT) systems to RF interference sources is becoming well known outside of the traditional PNT sector for example, into the critical infrastructure operations area. Risk managers of organisations in this area are becoming aware of the vulnerabilities and dependencies in using space based PNT systems. This paper presents work performed and work on-going in the UK, to develop capabilities that provide detection and early warning for operators of critical infrastructure and law enforcement agencies (LEA), to the presence of RF interference in the bands associated with space based PNT. These capabilities can detect and will be able to locate source(s) of RF interference which allows infrastructure operators and LEA to take advantage of quality of service and trust concepts when applied to these space based PNT systems. This paper also presents a case study of the detection of an intentional RF interference device, which impacted upon one organisation's critical infrastructure.

Introduction

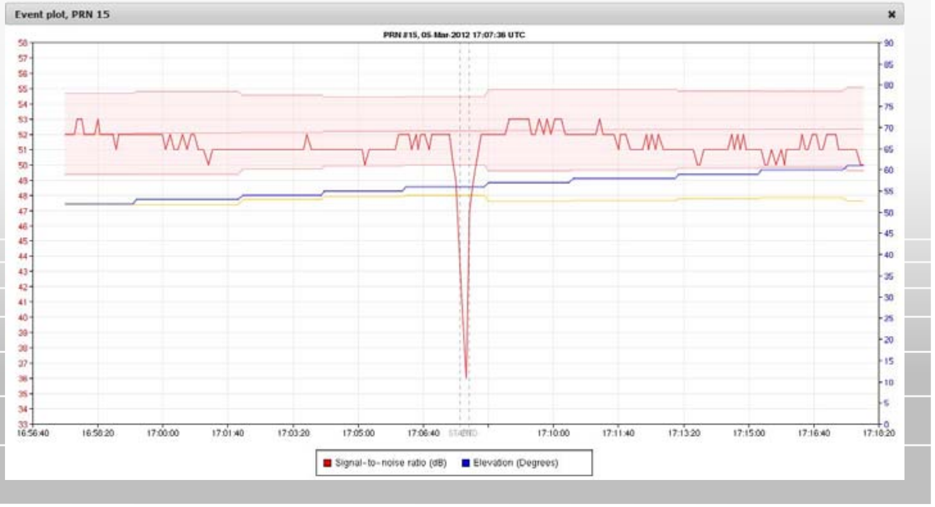
GNSS vulnerability is rightly one of the most talked about topics of 2011. Publicity such as the "accidental" GPS jamming at the Newark Airport in the United States [1-2], the Royal Academy of Engineering report [3] regarding the vulnerability of UK GNSS services, the recent investigations into the LightSquared "problem," [4] numerous conference presentations [5-6], and articles in news media [7] — all address the well-known fact that space-based position, navigation, and timing (PNT) is vulnerable to localised RF interference at or near to the receiver operating frequency.

Some of this publicity relates to the UK's developments in the area of detecting GNSS interference, specifically the GAARDIAN (GNSS Availability, Accuracy, Reliability anD Integrity Assessment for Timing and Navigation) program [6], which was a wide collaboration between government, academia, and industry to develop a robust system for analysing interference phenomena associated with GPS and eLoran systems and the effects on their use in safety- and mission-critical applications.

The GAARDIAN program completed in 2011, this paper gives an overview of the resulting capability to detect GNSS interference and jamming. It also provides details about a specific recent detection event that demonstrated the capability of the system and that, by involving UK Law enforcement agencies, proved the system can be operationally effective. It also gives an overview of the continuing development of this technology under the SENTINEL program.

GAARDIAN

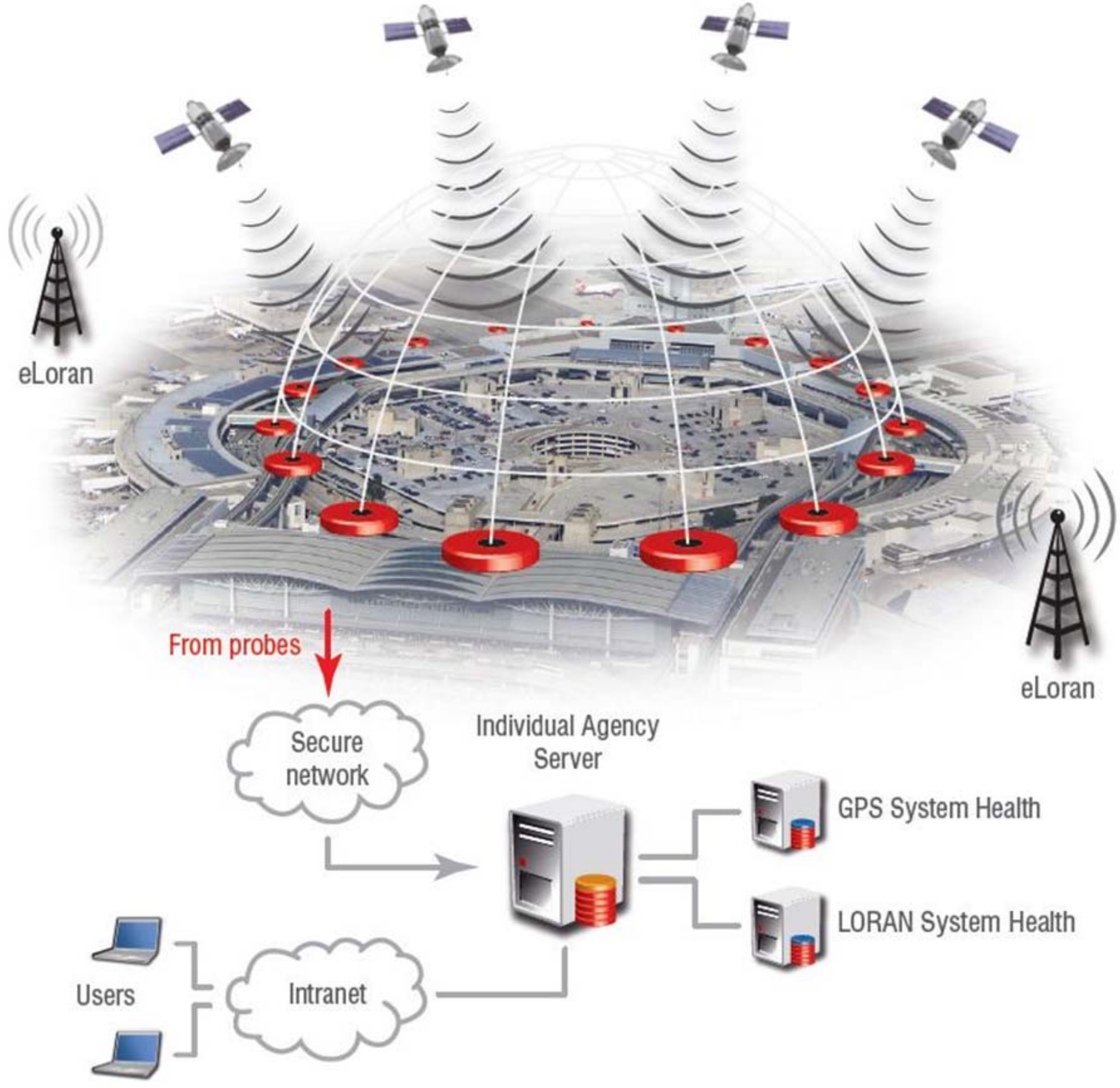
GAARDIAN, a collaboration led by Chronos Technology Ltd., included the University of Bath, General Lighthouse Authorities of UK and Ireland, BT, Ordnance Survey, National Physical Laboratory, and Imperial College London. The project was part-funded by the UK's national



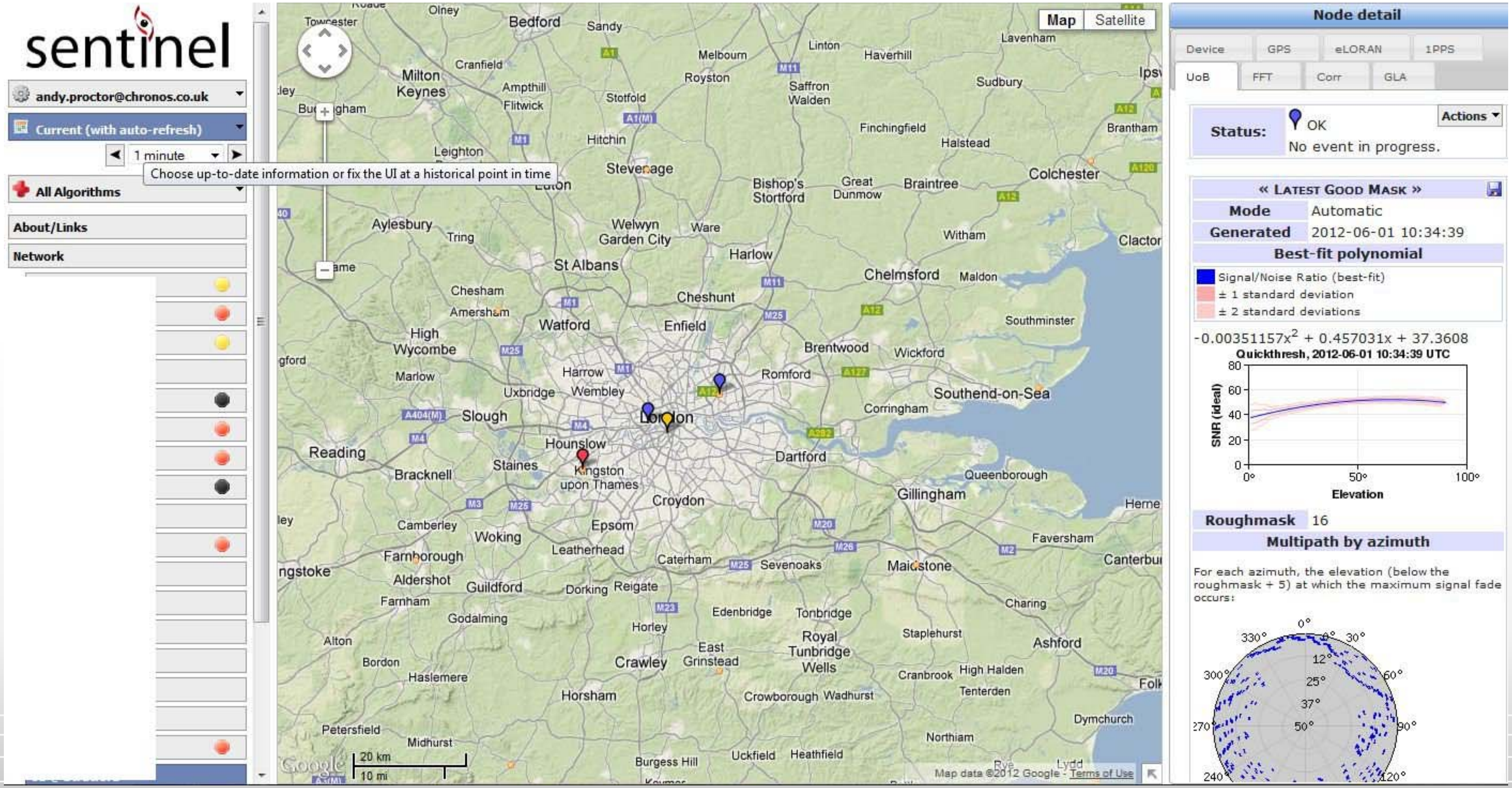
SENTINEL

- GAARDIAN is DETECT the Interference
- SENTINEL is DETECT *and* LOCATE
- 3 key firsts
  - GNSS emitter geo-location research
  - How interference compromises trusted services
  - Enabling trust by understand false alarms
- Mitigation functions for e.g. CNI
  - Use of eLoran etc

SENTINEL


eLoran
eLoran
From probes
Secure network
Individual Agency Server
GPS System Health
LORAN System Health
Users
Intranet

Enhanced monitoring & analysis



sentinel

andy.proctor@chronos.co.uk

Current (with auto-refresh)

◀ 1 minute ▾ ▶

Choose up-to-date information or fix the UI at a historical point in time

All Algorithms

About/Links

Network

Node detail

Device | GPS | eLORAN | 1PPS

UoB | FFT | Corr | GLA

Status: OK
No event in progress.

Actions ▾

« Latest Good Mask »

Mode	Automatic
Generated	2012-06-01 10:34:39

Best-fit polynomial

- 🟦 Signal/Noise Ratio (best-fit)
- 🟥 ± 1 standard deviation
- 🟥 ± 2 standard deviations

$-0.00351157x^2 + 0.457031x + 37.3608$

Roughmask	16

Multipath by azimuth

For each azimuth, the elevation (below the roughmask + 5) at which the maximum signal fade occurs:

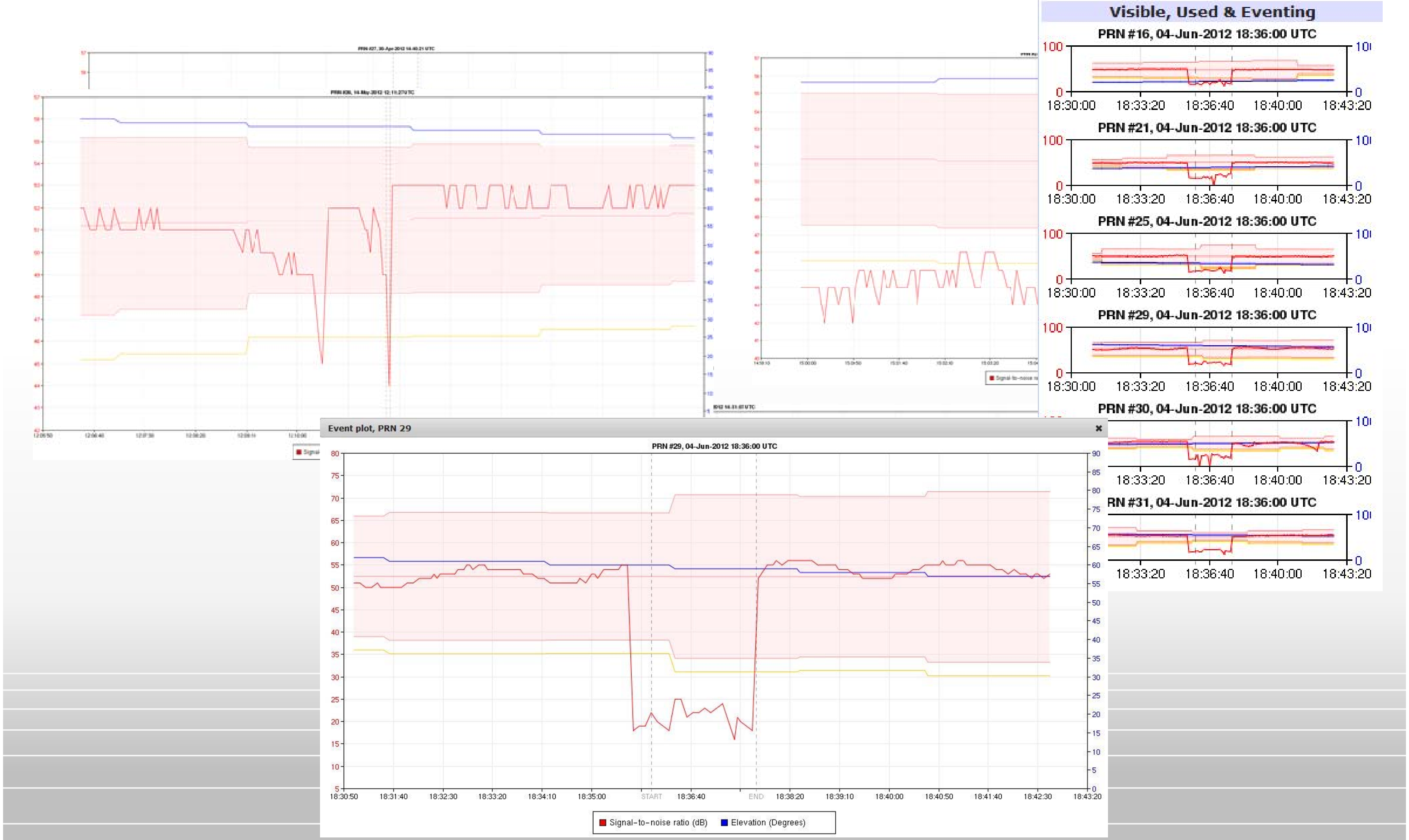
Delivering Outputs

- Key results fed into UK Govt

Location	Road Type	Number of Events	Approx. Months Deployed	Approx. Rate per Month
Location #1	Urban A	41	4	10
Location #2	Town	29	6	5
Location #3	Town	11	8	1
Location #4	Motorway	90	9	10
Location #5	Town	12	10	1
Location #6	Town	10	10	1
Location #7	Motorway	20	5	4

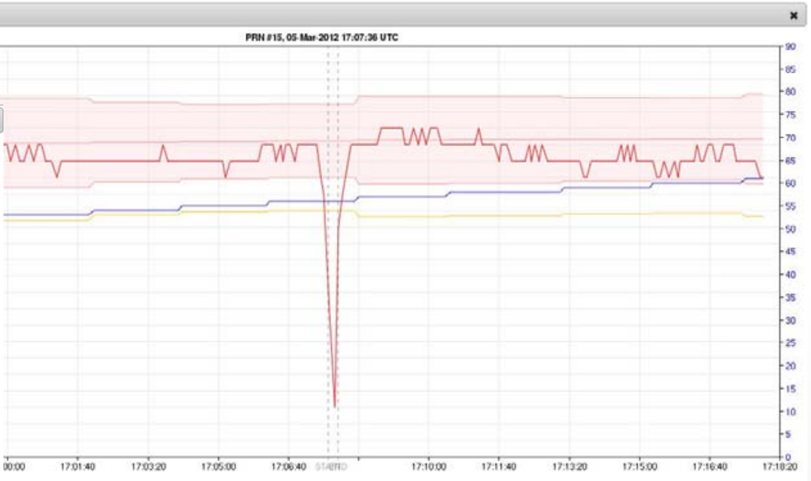
Typical Event

30 Minute Event in London



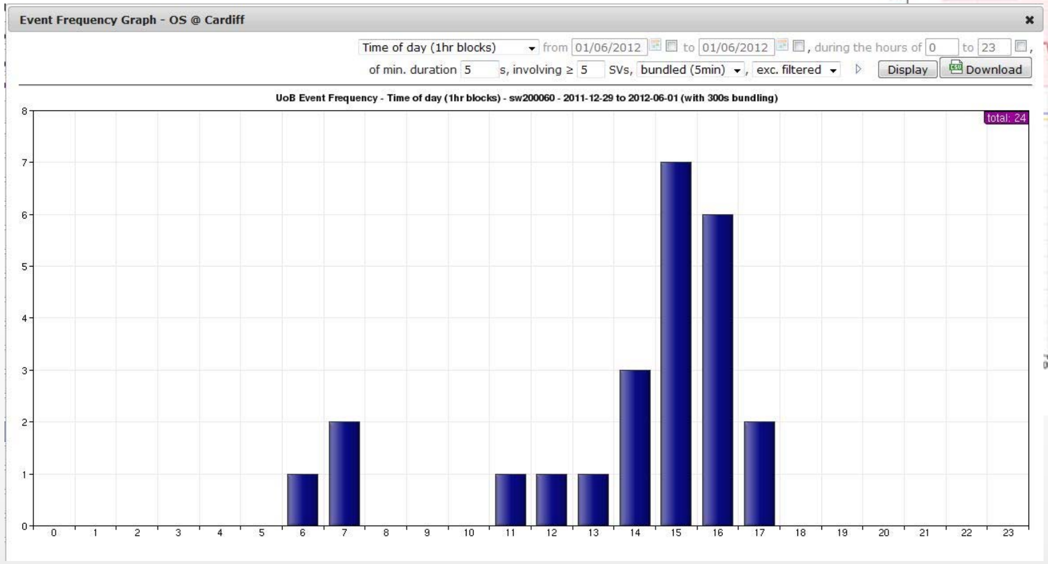
Delivering Analysis

- Analysis of events



Event plot, PRN 15

PRN #15, 05-Mar-2012 17:07:36 UTC

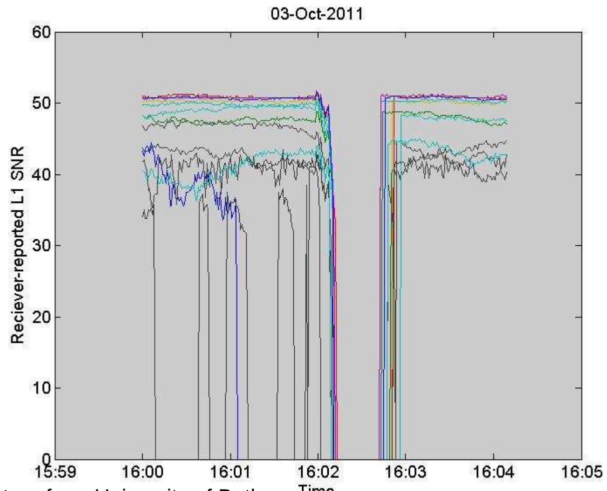


Event Frequency Graph - OS @ Cardiff

Time of day (1hr blocks) from 01/06/2012 to 01/06/2012 , during the hours of 0 to 23 ,

of min. duration 5 s, involving ≥ 5 SVs, bundled (5min) , exc. filtered

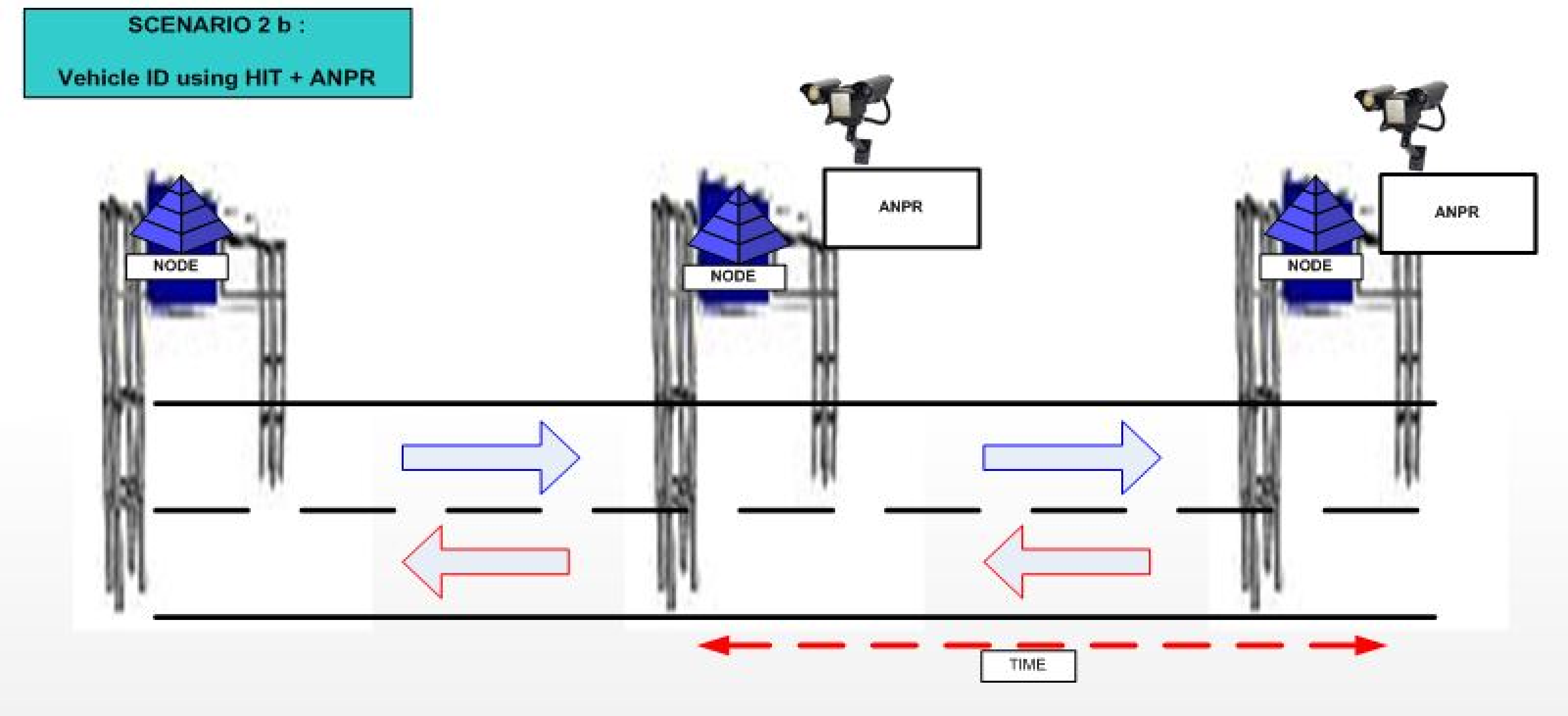
UoB Event Frequency - Time of day (1hr blocks) - sw200060 - 2011-12-29 to 2012-06-01 (with 300s bundling)



Picture from University of Bath

Also testing by scenario

- For Law Enforcement



Picture courtesy of ACPO

Future

- Protection for critical infrastructure/venues
  - Permanent
  - Temporary
  - Mitigation functions (Backup clocks/eLoran)
- Response capability
- Tactical Deployment
- Evidence
- Increased safety
- Actionable Intelligence

Commercial Status

- SENTINEL is a research project
  - Not completed (Dec 2012)
  - Proven operationally (Girvan incident)
- Chronos cooperating with ITT Exelis in USA
  - Demo system in place
  - DHS involved in investigation/output
- Open to work with customers for specific requirements

Summary

- GNSS Interference is growing threat
  - However derived
- Impact can be significant
  - CNI, Energy Finance, Safety, Security, Social
- Lack of detection/monitoring systems
  - SENTINEL builds on UK leadership in this area
- 2012 is a key year

Thank you for listening

Andy Proctor, MA, MRIN, FInstSMM
andy.proctor@chronos.co.uk

Any questions?