Imperial College London

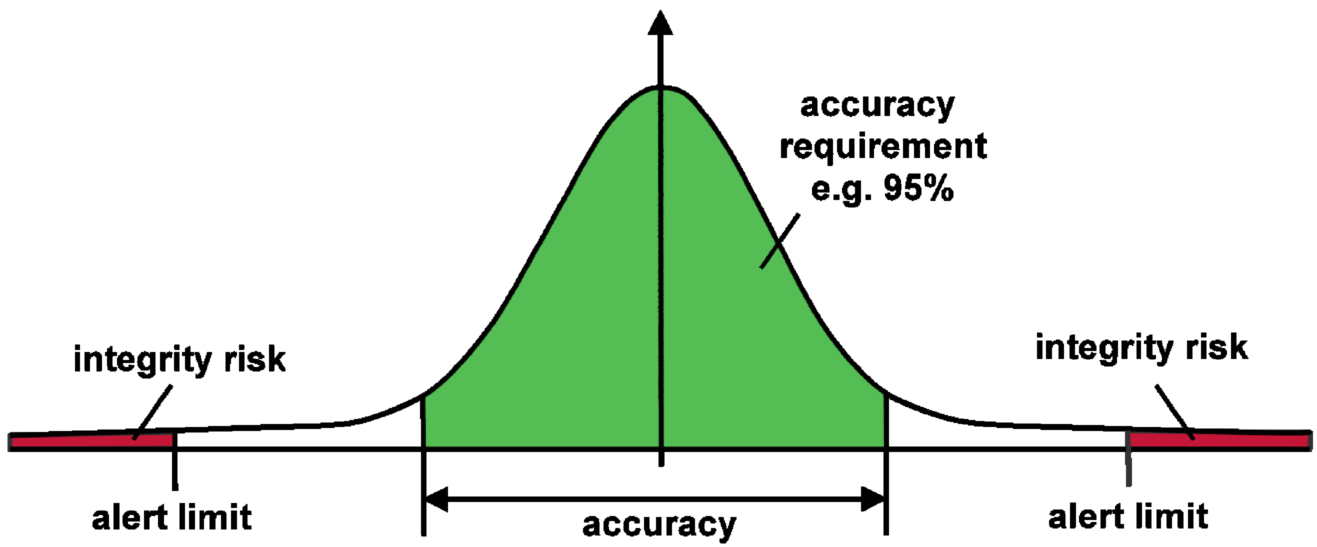
Integrity Monitoring for Detection of Interference

Professor Washington Ochieng
Department of Civil and Environmental Engineering

Imperial College London

Navigation Performance Measures

- Navigation performance measures
  - accuracy, integrity, continuity & availability
- Integrity
  - ability to inform users in the event of a failure
  - most directly related to mission criticality (e.g. Safety)
  - need for consensus on methods for performance spec.
  - need for appropriate test schemes (vital for certification)



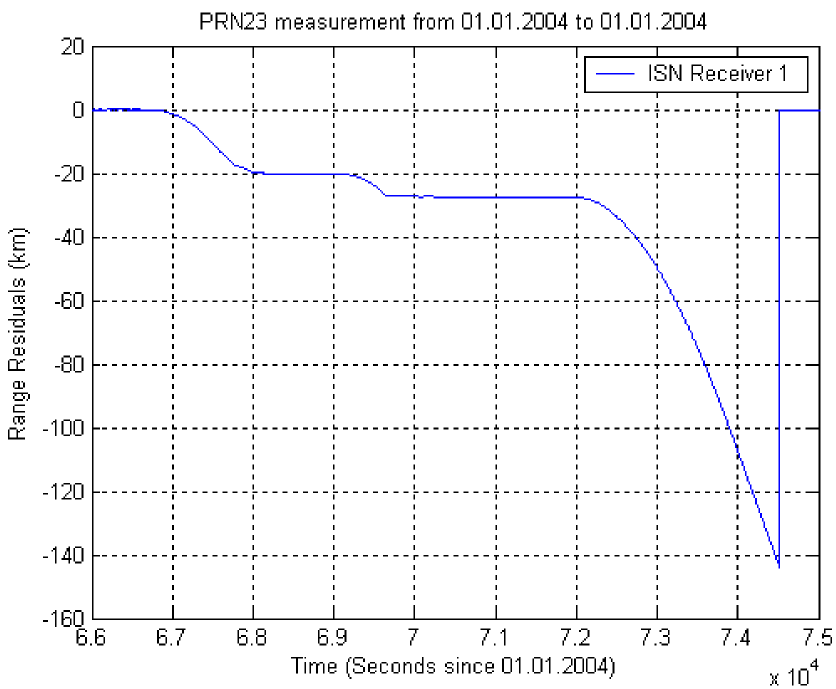
Imperial College
London

Why is GNSS a challenge?

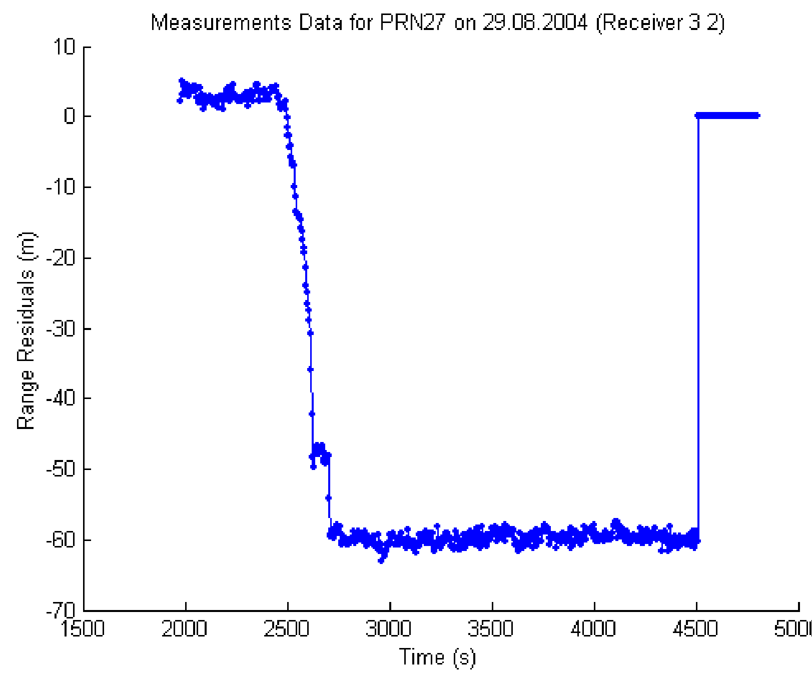
- Complexity
  - control segment, comms, satellites, modelling, signal generation
  - signal path effects, receiver hardware/electronics/algorithms
  - anomalies or failures can occur at any stage
- Positioning/Navigation performance varies with:
  - position of users and satellites in space and time
- Multiple users globally (including mission critical applications)
- Institutional control (some systems)

Failure Modes (1/5)

- System failure examples:
  - SVN23; SVN27 - atomic frequency std failure (01/04; 08/04)
  - SVN54 - orbit modelling error → URE=350m (04/07)
  - SVN49 - inter-freq. phase bias due to integration of L5 (04/09)



SVN23 failure – 1.1.04



SVN27 failure – 29.8.04

Failure Modes (2/5)

- Signal path failure mode examples:
  - solar flares / ionospheric scintillation
  - tropospheric effects
  - multipath
  - interference
    - jamming
    - disturbance
    - spoofing/meaconing

Imperial College London

Failure Modes (3/5)

- Jamming
  - Receiver front-end saturated by unwanted strong signals

    Example : San Diego, CA , on January 22, 2007 [1]

    - US Navy ships on communications jamming tests
    - Navy receivers stopped working
    - jammed the whole San Diego harbour region
    - affected all GPS users within a range of about 15 kilometres

- Disturbance
  - wanted signals distorted by unwanted signals

    Example: Flamborough [2]

    - maritime controlled-Jamming experiments
    - receiver suffered large position errors without warning

1. *Phillip W. Ward, P.E., GNSS Robustness: The interference challenge, ION GNSS proceedings 2010*
2. *National PNT Advisory Board, A National Security Threat: Recent Events and Potential Cures. 2010*

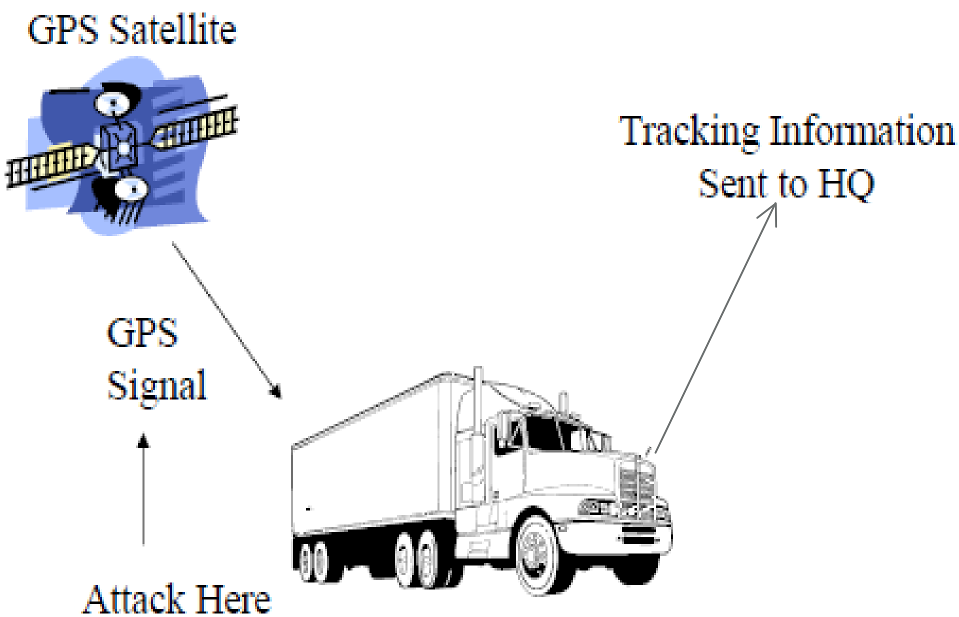
Imperial College London

Failure Modes (4/5)

- Spoofing
  - receiver acquires and tracks fake satellite signals

    Example : GPS simulator attack [1]

    Misleading information sent to HQ



1. Warner, J S. A Simple Demonstration that the Global Positioning System (GPS) is Vulnerable to Spoofing, *The Journal of Security Administration*

Failure Modes (5/5)

- Summary

Type	Effects	Impact
Jamming	Receiver stops working (loss of service)	Continuity/Availability
Disturbance	Degraded performance	Accuracy/Integrity
Spoofing	Degraded performance/MI	Integrity

Imperial College London

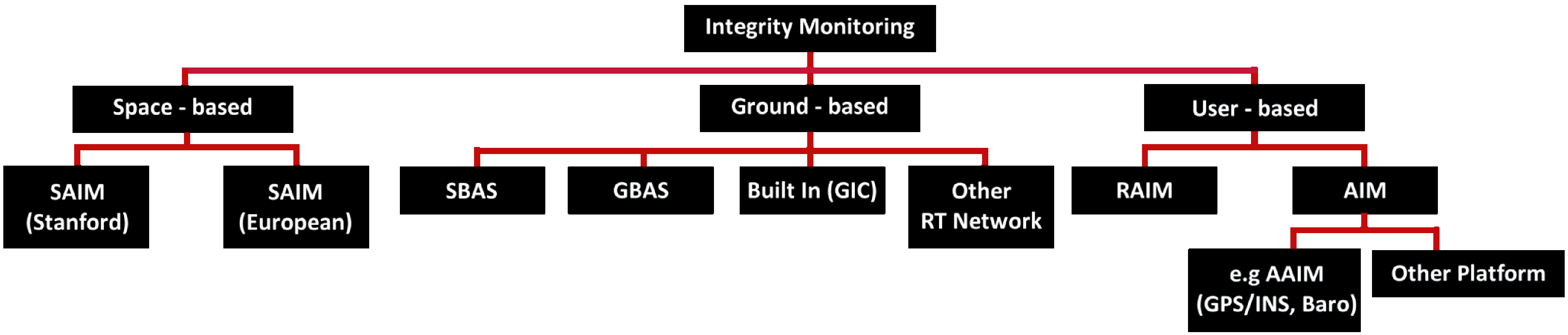
Interference sources and coverage

- Sources (examples)
  - increasing number of wireless systems and users
  - new communication systems (e.g. LightSquared 4G?)
  - new navigation systems
  - new technologies make intentional interference easier
  - terrorists

- **Coverage**
  - wide area (e.g. LightSquared 4G?)
  - local (Radio/TV stations, kilometres)
  - small (car anti tracker jammer, 1-2 meters)

ebay.com

Integrity Monitoring Techniques



- Currently two main approaches
  - system/ground level (GIC/SBAS/GBAS)
  - sensor/user – (R)AIM
- Future
  - SAIM
  - Ground/Space/User level integrity monitoring (apportionment of integrity risk?)

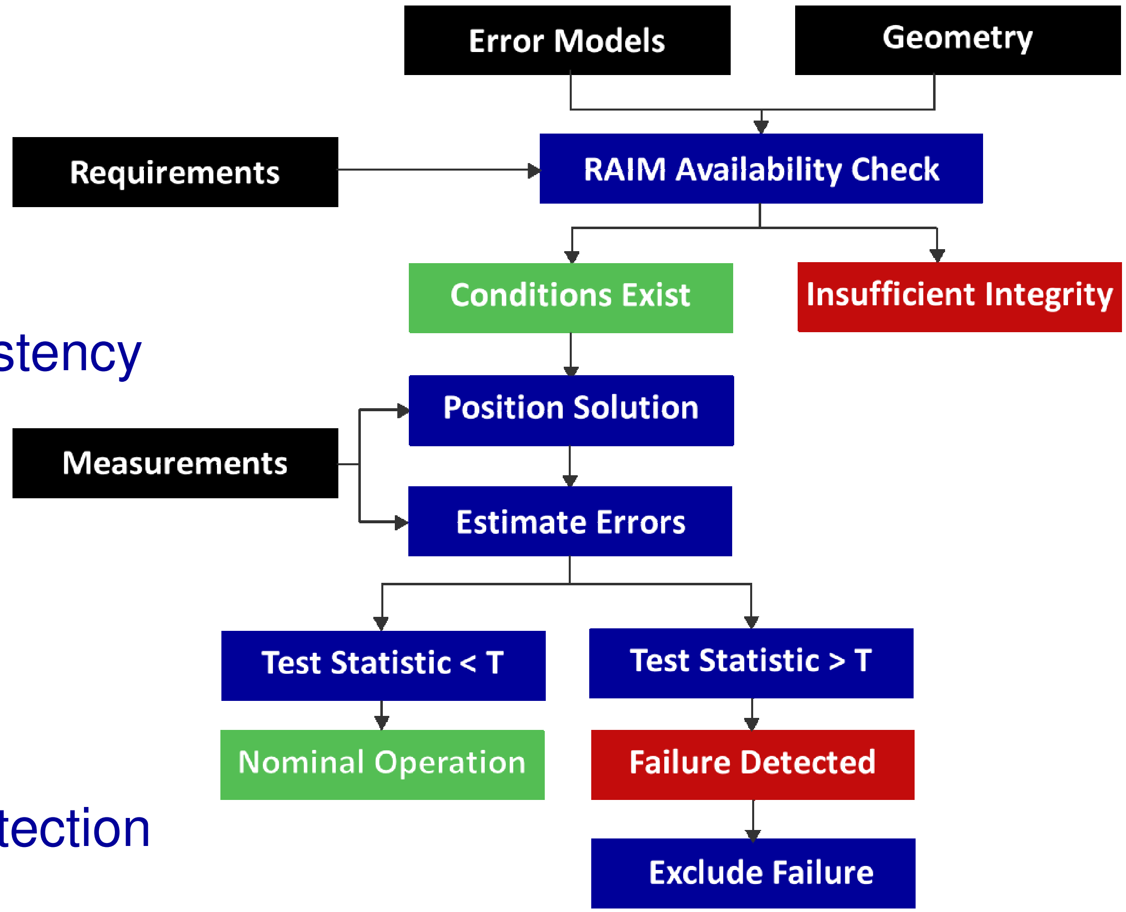
State-of-the-art (Ground Network level): SBAS/GBAS

- SBAS/GBAS designed for:
  - improved accuracy through differential corrections
  - improved integrity (dedicated infrastructure)
  - improved availability by additional ranging (SBAS)

- Integrity
  - failures detected using ref. station location(s) – alerts for ‘major’ failures
  - quality data sent to users for computation of Protection Level (PL)
  - PL is compared to Alert Limit (AL) to determine compliance

State-of-the-art (User Level): RAIM

- Baseline FDE RAIM steps
  - PL computation
  - failure detection
  - failure exclusion
- Detection function
  - measurement consistency
- Exclusion function
  - improves continuity
- Main RAIM strengths
  - autonomy
  - local failure/error detection



RAIM Issues of relevance to detection of interference

Issues	Current attempts at resolution
Critical geometry (max slope)	Integration
RAIM availability	Integration, better PL
Multiple failures	Separation (Group/Solution)
Failure models	FMEA
Residual error characterisation	Dist. drivers, EVT / other models
Failure probability	FMEA
Failure rate (small/brief errors)	FMEA
Exclusion	Separation (Group/Solution)
Time -To-Alert	Early detection techniques (e.g. *difference test* for SGEs)

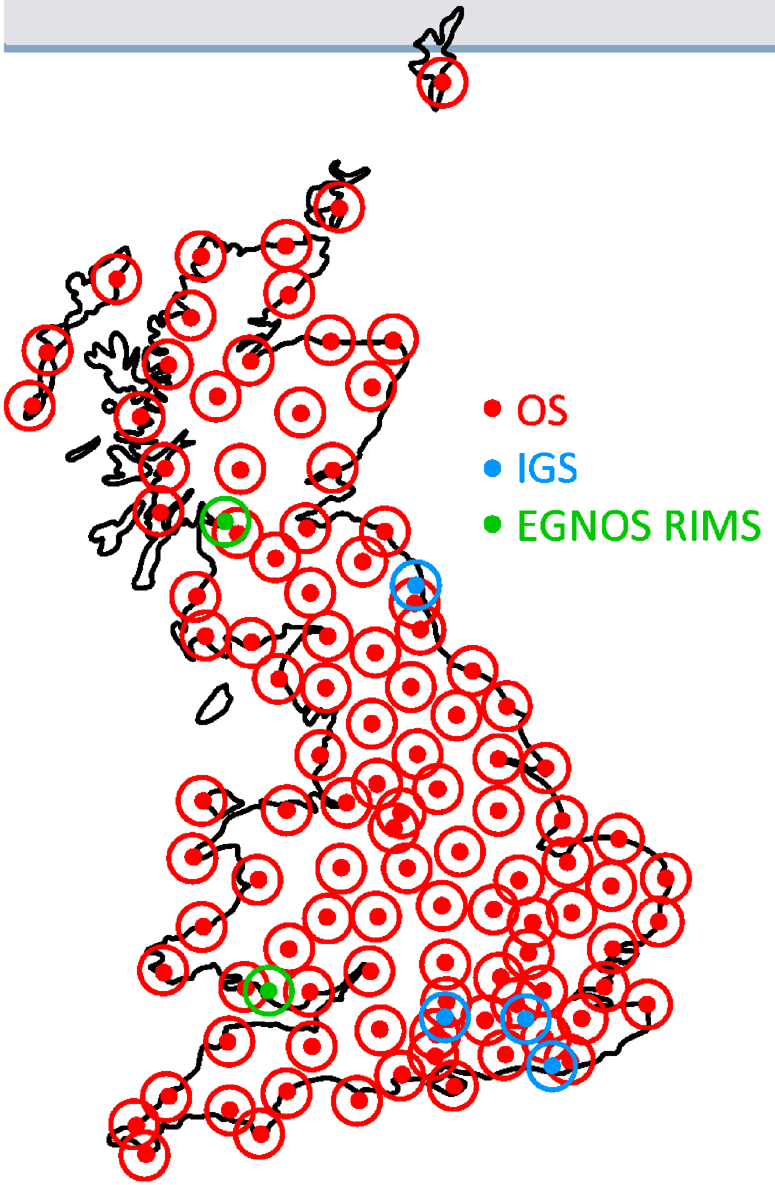
Integrity Monitoring for Detection of Interference (1/4)

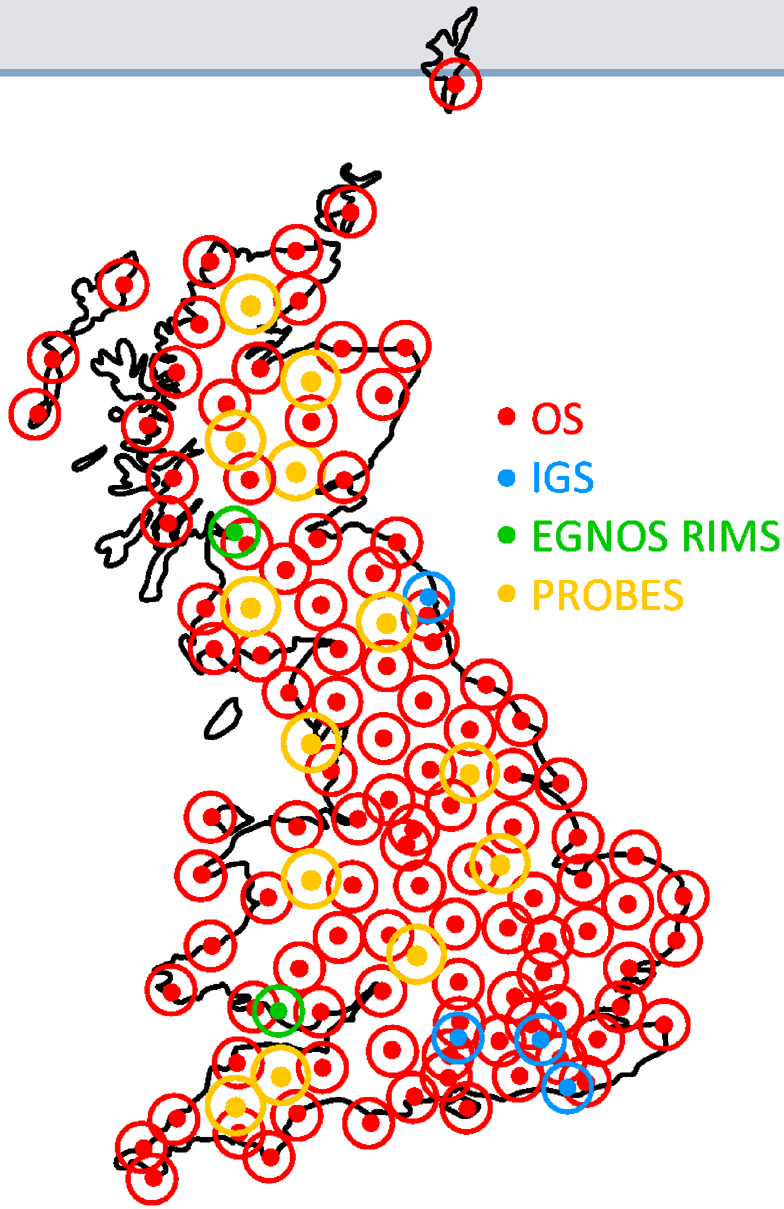
- Potential options

1. Combine data from integrity monitoring stns within GIC, SBAS & GBAS
   - Pro: systems already available
   - Con: low density of the monitoring stations
2. Exploit *networks of opportunity (e.g. OS, Leica, IGS, etc.)*
   - Pro: networks already available
   - Cons: medium density of stations; dedicated processing facility; new investment
3. Deploy *dedicated systems/probes* either at locations of interest or a network
   - Pro: flexible; UK lead in R&D (GAARDIAN)
   - Con: new investment
4. Combination of 1, 2 and 3
   - Pro: better performance
   - Con: complexity and new investment

Imperial College London

Integrity Monitoring for Detection of Interference (2/4)

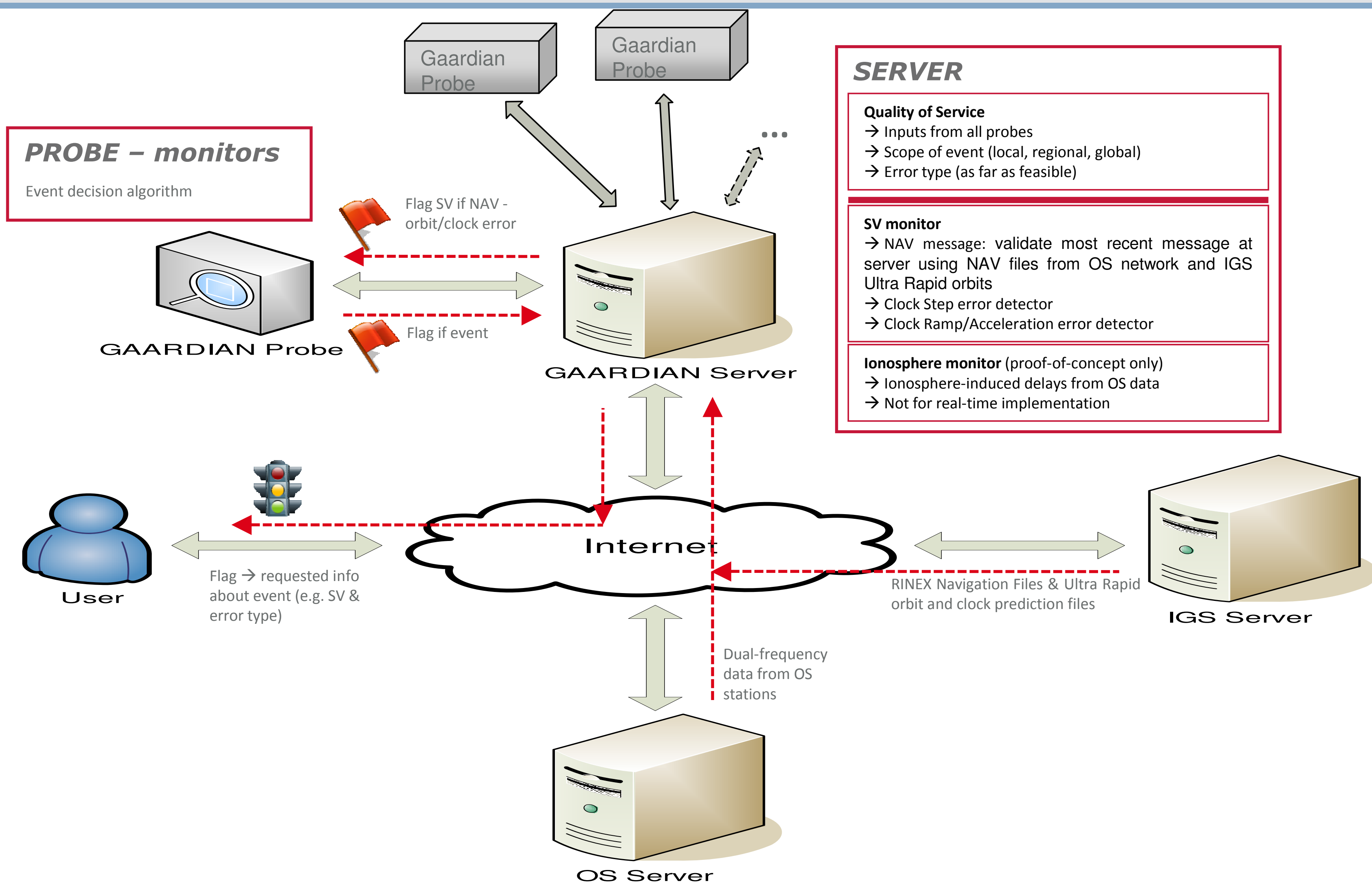




Imperial College London

Integrity Monitoring for Detection of Interference (3/4)

Adaptation of the GAARDIAN System



Imperial College London

Integrity Monitoring for Interference Detection (4/4)

- Potential options (ctd)

5. User receiver level integrity monitoring [e. **(R)AIM**]
   - Pro: Self contained; detection of local interference missed by a network
   - BUT: requires resolution of issues identified earlier (e.g. residual error distribution); characteristics of the effects of interference; need for appropriate test statistics

6. Combination of 1, 2, 3 and 5
   - Pro: Best protection?
   - Con: Complexity

Conclusions

- Network level detection of interference
  - feasible with networks of opportunity & dedicated systems (GAARDIAN)
  - BUT: need for better understanding of characteristics of interference, network density a limitation; responsibility

- User level detection (with AIM)
  - very good performance especially when integrated with other systems/sensors; local to the user
  - BUT need to address issues with (R)AIM and characteristics of interference; local to the user

- Combined network level and user level detection (with AIM)
  - potential to offer maximum protection