GNSS VULNERABILITY AND CRITICAL INFRASTRUCTURE

NNF CONFERENCE
24 MAY 2012

Brynjar Hansen
Senior adviser
Norwegian Space Centre

Lars Giske
Senior adviser
Norwegian Space Centre
MULTI GNSS

- NAVSTAR GPS
- GLONASS
- GALILEO
- BeiDou(COMPASS) Navigation Satellite System
EXTERNAL COOPERATION PARTNERS

- 8 public directorates and authorities
- 3 private entities

- Norwegian Maritime Authority (Sjøfartsdirektoratet)
- Norwegian Coastal Administration (Kystverket)
- Directorate for Civil Protection and Emergency Planning (DSB)
- Norwegian Metrology Service (Justervesenet)
- Norwegian Water Resources and Energy Directorate (NVE)
- Directorate for Emergency Communication (DNK)
- Norwegian Post and Telecommunications Authority (PT)
- Fugro Seastar AS
- Northrop Grumman Park Air Systems AS (Indra Navia AS)
- Norwegian Air Ambulance (Norsk Luftambulanse)
- Joint Rescue Coordination Centres (HRS-Sola)
Main objectives

Background

Criteria for assessment of risk levels

Factors that may cause interference, degradation or loss of signal

Assessment of vulnerability to critical infrastructure and SoL applications:
   Aviation, maritime, DP, SAR, land-based, precise timing

Main conclusions and recommendations
1. Highlight factors that may cause interference or loss of signal (i.e. *Probability and frequency of events*)

2. Assess risk of using current GNSS in support of critical infrastructure, critical societal functions and SoL applications

   **Critical infrastructure defined:**
   *Equipment and systems required for supporting critical functions that satisfy basic societal needs and provide public safety*

3. Assess mitigation effects of future use of multisystem GNSS (GPS, Galileo, GLONASS, COMPASS)

4. Increase awareness among users about GNSS vulnerability as a basis for sector-based risk analyses and mitigation measures
GPS use is already extensive and will increase with future GNSS
- Critical infrastructure, critical societal functions and SoL applications
- Knowledge about continuity requirements, GPS system dependence and risk exposure varies among users

Why and how does GNSS vulnerability represent a challenge?
- Weak signals that can be jammed or spoofed
- Labour intensive and time consuming procedures for detection, localisation and elimination of sources of interference

Extensive use of GPS by authorities has spawned a "disruption industry"
- Increased use of GNSS in payment and tracking systems may reinforce this trend

Need for a GNSS risk assessment taking into account Norway's critical infrastructure, societal functions and user requirements
ASSESSMENT OF RISK LEVEL

- Assessment of risk level is dependent on:
  - Type of application
  - User requirements
  - Degree of dependence on GNSS-based PNT
  - Probability and frequency of degradation or loss of signal
  - Duration of degradation or loss of signal
  - Access to and competence in using redundant equipment

- Risk level may be:
  - **Low** - no mitigation required
  - **Medium** - mitigation recommended when redundancy incomplete
  - **High** - mitigation required in case of no redundancy
A risk is the amount of harm that can be expected to occur during a given time period due to a specific harm event (loss of satellite signal).

The level of risk can be calculated as the product of the probability of the harm event multiplied by the severity of the harm event.

A risk matrix is a tool to make vulnerability more visible and facilitate mitigation planning and implementation.
FACTORS IMPACTING GNSS PERFORMANCE

- Ephemeris, clocks
- Ionosphere: Signal strength and phase variations
- Troposphere
- MP
- Ground segment
- Interference, spoofing
- Signal blocking
- Receiver noise
- Delay
- Signal strength and phase variations
- Receiver noise
SIGNAL INTERFERENCE - SOURCES

- **INTENTIONAL INTERFERENCE**
  - Jamming and Spoofing

- **NON-INTENTIONAL INTERFERENCE**
  - Noise from other radio sources

- **SPACE WEATHER**
  - Flare induced radio noise
    - 0-8 cases per solar cycle

**Scintillation**

- Several times annually
**CIVIL AVIATION**

- Loss of GPS no threat to safety of aviation

- EGNOS improves flight safety whilst reducing operational costs through decommissioning parts of terrestrial infrastructure

- GNSS primary system for navigation and Air Traffic Management (ATM)

- GNSS offers lower risk than GPS for helicopter operations in areas lacking terrestrial infrastructure (Barents Sea and Svalbard)

- GNSS offers lower risk than GPS through improved performance, integrity and availability
In general, a loss of GPS signal implies a low risk to maritime operations, provided redundancy is available.

- GPS only: Increased risk for High Speed Craft (HSC) in restricted waters.
- Multi system GNSS gives lower risk for HSC than GPS only.
- GNSS a pre-condition for e-Navigation and IALA dGNSS service.
- Residual risk for pleasure yachts contingent on competence level.
**DYNAMIC POSITIONING OPERATIONS**

- Galileo/GPS/GLONASS = improved performance and lower risk level
- In case of satellite signal loss operational and environmental safety is maintained by local reference systems (acoustic, laser and short-range radio)
- Broadcast of differential DP signals via Galileo, IOGS or HEO satellites may ensure required performance and low risk DP operations in polar regions
SEARCH AND RESCUE

- Loss of GPS signals increases likelihood of:
  - higher number of distress calls to rescue coordination centres (RCC)
  - reduced operational efficiency during SAR operations
  - less accurate and delayed positioning of EPIRB w/ GPS chip

- GNSS MEOSAR enhances SAR efficiency

- Return message to users in emergency situations (via Galileo only)

- Improved coverage, more accurate and faster positioning of EPIRB than Doppler-based LEOSAR
LAND BASED APPLICATIONS

- GPS signal loss increases vulnerability for fleet management and navigation in emergency services (fire, police, ambulance)

- GNSS offers improved continuity and robustness for navigation and fleet management for rescue and emergency services

- GNSS improves signal availability in urban canyons and difficult terrain

- 2D and 3D positioning of portable alarms and mobile distress calls inside buildings and in tunnels (eCall) still pose a challenge
PRECISE TIMING

- GPS used indirectly for synchronization of base stations in digital public safety network (GPS as stratum 0 source for stratum 1 NTP servers)

- The power grid is dependent on GPS for phase synchronisation, flow control and time stamped commands

- Financial and banking systems are dependent on accurate time stamped transactions (stock trading and ATM)

- Use of GPS as primary (stratum 0) timing source implies increased risk

- Use of GPS-synchronised NTP servers with built-in holdover function reduces vulnerability and is more common
Access to multiple systems will reduce dependency on one system for critical infrastructure, critical societal functions and SoL applications.

Galileo PRS offers encrypted signals for authorised public entities.

More satellites give improved signal availability and performance.

New systems offer new, improved signals and services.

Multi GNSS will have better protection than GPS against some, but not all sources of error or interference.
RECOMMENDATIONS

- Vulnerability must be viewed in a context of accepted risk level and operational cost depending on application (i.e., what risk level can one accept or afford?)

- Focus on increasing GNSS competence in certain sectors

- Need for awareness regarding GNSS dependence and sector-specific continuity requirements

- GNSS risk and vulnerability analyses as a basis for protecting critical infrastructure and safeguarding critical societal functions

- Public and private entities are responsible for analysing sector-related risk and implementing appropriate mitigation measures

- Sources of precise timing to be selected based on individual sector requirements

- Develop a national concept for protection of GNSS signals and infrastructure
GNSS as critical infrastructure

- USA - Critical Infrastructure Protection Program
- EU – European Programme for Critical Infrastructure Protection (EPCIP)
  - Ongoing review of Directive 2008/114/EC on CNI
  - JRC 2010 study on GNSS
  - Dependencies and interdependencies of GNSS in CNI

- National level – Critical National Infrastructure (CNI)
- Norway-CNI
  - New law and regulation on protection of CNI is under implementation
  - Includes satellite navigation infrastructure
  - GNSS signals
GNSS Vulnerabilities and CNI:

 получения требуемого уровня сигнала

T&V assessments:

- Attack
- Sabotage
- Intrusion

- Jamming/interference
- Spoofing
- Spectrum management
GNSS Vulnerabilities and CNI:

GNSS is part of a modern societies CNI:

- Protective measures
  - Active
  - Passive

- National level
- European level

- Multiple GNSS
  - For some users Galileo PRS plus
  - GPS PPS military
  - GPS SPS civil

- GNSS and MEMS

- Other PNT systems?
  - Resilience
  - Cost