The Galileo Commercial Service, status and plans

Ignacio Fernández Hernández
European Commission – DG ENTR
"Reference frames, Positioning and Navigation"
Gothenburg, September 3rd 2014
Table of Contents

• Galileo

• Galileo Commercial Service
  • Introduction
  • Frequency, Signals and Data
  • High Accuracy
  • Authentication

• Results
  • CESAR and GALCS (CS Studies)
  • AALECS (CS Demonstrator)

• Next Steps

• Conclusions
Galileo
Galileo Nominal Constellation

- 24 satellites in Medium Earth Orbit (MEO)
- Altitude: 23 228 km (29600 km axis)
- Period: 14 hours 22 minutes (17 revolutions in 10 days)
- 3 orbital planes inclined at 56° to the Equator
- 2 spare satellites in each plane
- Walker 24/3/1 configuration
- Inclination: 56°
- 15° phasing between planes
Galileo Ground Segments
## Galileo Services

<table>
<thead>
<tr>
<th>Service Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Open Service (OS)</td>
<td>Freely accessible service for positioning, navigation and timing</td>
</tr>
<tr>
<td>Public Regulated Service (PRS)</td>
<td>Encrypted service designed for greater robustness and higher availability</td>
</tr>
<tr>
<td>Search and Rescue Service (SAR)</td>
<td>Assists locating people in distress and confirms that help is on the way</td>
</tr>
<tr>
<td>Commercial Service (CS)</td>
<td>Delivers authentication and high accuracy services for commercial applications</td>
</tr>
</tbody>
</table>

The former "Safety-of-Life" service is being re-profiled:

| Integrity Monitoring Service       | Provides vital integrity information for life-critical applications          |
Galileo Commercial Service: Introduction
Extracts from the Galileo Regulation on CS (1285/2013) and associated Program documentation:

• CS shall enable “...the development of applications for professional or commercial use by means of improved performance and data with greater added value than those obtained through the open service”

• CS based on “commercial ranging and data, whose access shall be controllable in order to allow fees to be levied.”

• "...the CS shall offer a payable added-value service, which can be exploited through a revenue-sharing mechanism with the private sector.”

• “The Commercial Service signals shall be the Open Service signals, plus two encrypted signals in the E6-band.”
CS High Level Objectives

- Maximize satnav **public benefits**
- Creation of **economic value**
- Provide the best **navigation performance** possible with the Galileo infrastructure
- Promote **innovation** by offering new functionalities
- Provide a **revenue source** to offset Galileo costs
Galileo Commercial Service: Frequency, Signals and Data
CS frequency band: E6

Several actions ongoing to insure proper E6 reception:

- Discussions with IARU (International Amateur Radio Union)
- Discussions U.S., Japan and China
- E6 reception characterisation actions and testing plans (JRC & industry support)
- ITU-level actions under consideration.
• **CS signals in Galileo signal baseline:**
  • **E6-B:** data component (448 bps)
  • **E6-C:** pilot tone component
Galileo CS signals

- Modulation

\[ D_{CS}(t) \]
\[ C_{CS}^D(t) \]
\[ C_{CS}^P(t) \]
\[ s_D(t) \]
\[ s_D(t) \]
\[ s_P(t) \]
\[ s_{CS}^{E_6}(t) \]

- Signal characteristics

<table>
<thead>
<tr>
<th></th>
<th>E6-B</th>
<th>E6-C</th>
</tr>
</thead>
<tbody>
<tr>
<td>Component</td>
<td>Data</td>
<td>Pilot</td>
</tr>
<tr>
<td>Carrier Frequency</td>
<td>1278.75 MHz</td>
<td>1278.75 MHz</td>
</tr>
<tr>
<td>Spreading Modulation</td>
<td>BPSK(5)</td>
<td>BPSK(5)</td>
</tr>
<tr>
<td>Chip Rate</td>
<td>5.115 Mcps</td>
<td>5.115 Mcps</td>
</tr>
<tr>
<td>Primary Code Length</td>
<td>5115 chips</td>
<td>5115 chips</td>
</tr>
<tr>
<td>Secondary Code Length/Duration</td>
<td>N/A</td>
<td>100 chips/100ms</td>
</tr>
<tr>
<td>Symbol/Data rate</td>
<td>1000 sps / 500 bps</td>
<td>N/A</td>
</tr>
</tbody>
</table>
• **E6-B data structure (C/NAV): 448 bps effective**

<table>
<thead>
<tr>
<th>Sync</th>
<th>Symbols</th>
</tr>
</thead>
<tbody>
<tr>
<td>16</td>
<td>984</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Word</th>
<th>Page type</th>
<th>Commercial Data / key Management</th>
<th>CRC</th>
<th>Tail</th>
</tr>
</thead>
<tbody>
<tr>
<td>14</td>
<td>448</td>
<td>24</td>
<td>6</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Code Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Coding Rate</td>
<td>½</td>
</tr>
<tr>
<td>Coding Scheme</td>
<td>Convolutional</td>
</tr>
<tr>
<td>Constraint Length</td>
<td>7</td>
</tr>
<tr>
<td>Generator Polynomials</td>
<td>G1=171o</td>
</tr>
<tr>
<td></td>
<td>G2=133o</td>
</tr>
<tr>
<td>Encoding Sequence</td>
<td>G1 then G2</td>
</tr>
</tbody>
</table>

• **Other information:**
  - **Spreading codes can be encrypted**
  - Convolutional encoding and interleaving: same as OS SIS ICD
  - Interleaving block size: 984 symbols (123 x 8)
  - Minimum Power: -155dBW (50% data, 50% pilot)
Data transmission

- Data can come from an external source through the GNSS Service Centre with few sec. Latency.

- Data transmission scheme from several sources under discussion.

- **EXAMPLE** of data transmission scheme (CSP = CS provider): would allow multiple providers vs multiple time slots/satellites.
Galileo Commercial Service: High Accuracy
**High Accuracy:**

- Available data bandwidth (448 bps per satellite at most) is adequate to broadcast High Accuracy data (mainly clocks and orbits) for Precise Point Positioning.

- Data latency achievable: few seconds (exact number TBC).

- Good complement to existing GEO transmission systems, especially at high latitudes and in difficult environments.

- Only satellites connected to ground (ULS) can transmit CS data.

- Performance achievable:
  - Centimeter-level accuracy
  - Availability and coverage (target):
    - 2 satellites at an elevation of 20° or higher, with a 99% availability worldwide
    - 1 satellite at an elevation of 40° or higher, with a 99% availability worldwide
<table>
<thead>
<tr>
<th>Latitude [°]</th>
<th>Best possible GEO elevation [°]</th>
</tr>
</thead>
<tbody>
<tr>
<td>55</td>
<td>27.3</td>
</tr>
<tr>
<td>60</td>
<td>21.9</td>
</tr>
<tr>
<td>65</td>
<td>16.6</td>
</tr>
<tr>
<td>70</td>
<td>11.5</td>
</tr>
<tr>
<td>75</td>
<td>6.4</td>
</tr>
<tr>
<td>80</td>
<td>1.3</td>
</tr>
<tr>
<td>81.3</td>
<td>0.0</td>
</tr>
</tbody>
</table>
• Chalmers U.T., Gotëborg: **Lat 57.69º, Lon 11.97º**

• **Best-case Geostationary satellite elevation:** 22º
Galileo Commercial Service: Authentication
Developing a GNSS Position and Timing Authentication Testbed

**GNSS Vulnerability and Mitigation Techniques**

---

**UAVs Vulnerable to Civil GPS Spoofing**

*Subject of a House subcommittee hearing this week*

In June a research team from the University of Texas at Austin (UT-Austin) demonstrated for the first time that a civilian unmanned aerial vehicle (UAV) can be commandeered in mid-flight by a civil GPS spoofing attack. The result will likely factor into the Federal Aviation Administration’s (FAA’s) plans to draw up rules for integrating
Authentication

- GNSS Authentication purpose is to insure that the processed signals are the ones transmitted from the satellites.
- The CS signal includes GNSS spreading code encryption capability for civil purposes:
  - Access control
  - Authentication
- Exact service performance and provision scheme under analysis. Elements available:
  - CS signal encrypted spreading codes
  - CS data bandwidth of some tens of bps (not all 448 bps may be used for high accuracy)
  - Additional ground infrastructure (GNSS Service Centre) for key management, service exploitation, etc.
  - Spare bandwidth from E1-B I/NAV: 20 bps from "Reserved 1" (ERIS) field.

- Authentication performance: Similar accuracy, availability and TTFF as standard PNT, but authenticated
• Galileo CS + OS Authentication concept (under analysis)

**OS Authentication:**
- Based on asymmetric data origin authentication (eph, clk, iono...) Can support mass market applications: road, handheld location-based services, e-commerce, etc.
- Ideally transmitted in E1B I/NAV spare bits (20bps).

**CS Authentication:**
- Based on symmetric spreading code encryption, but can rely on OS authentication for data.
- A priori higher robustness/receiver/key management complexity.
- Can be adequate for surveying, tracking & tracing, maritime, civil security, etc.
- Based on E1B I/NAV (data) + E6 (code, data).
Results: CS Studies (2013)
• EC launched two parallel studies during 2013.

• Duration: 1 year. Budget: 400k€ aprox. Each.

• CESAR: managed by FDC. Included TAS-F, Fugro, Keynectics, Trimble-Terrasat, BHO.

• GALCS: managed by GMV. Included CGI, Helios.

• The studies analysed service concepts and performance of High Accuracy and Authentication under certain Galileo system assumptions (satellite number, system latency, allocated bandwidth, etc).

• The studies included simulated and real SIS results.

• Today's presentation:
  - Example of achievable PPP performance
  - Real E6B/C tracking performance
Example 1 – PPP performance (GALCS project, GMV, magicPPP):

- 50 worldwide stations
- GPS/GLO real data
- 5-s latency, **5-s clock update rate**
- Realistic BW conditions (<400bps); same data by all satellites
- After convergence.
Example 2 (GALCS project, GMV, magicPPP):

- 50 worldwide stations
- GPS/GLO real data
- 5-s latency, **30-s clock update rate**
- Realistic BW conditions (<400bps); same data by all satellites
- After convergence.
Tracking Performance

Results obtained thanks to TRIMBLE through a prototype firmware installed ad-hoc in the receivers. Galileo codes provided through CESAR project.

- Chennai, India (E6B, E6C, E6B+C)

- Melbourne, Australia (E6B, E6C, E6B+E6C)
Results: CS Demonstrator (2014)
The AALECS (CS Demonstrator) project

- EC launched the CS Demonstrator by Jan 2014.
- AALECS project stands for "Authentic and Accurate Location Experimentation with the Commercial Service".
- Foreseen duration: 2.5 years (1/14-6/16). Total budget: 4m€.
- Objective: develop & test CS with real SIS and support future service providers.
  - The EPOC ("Early Proof-Of-Concept") provided first real SIS results.
  - The project is developing a real-time platform for few second-level latency SIS tests (2015-2016)
EPOC process

- Agree between EC/EPOC/Galileo Ops the weekly test slots of several hours, where 3 sats in view over EU.
- Generate authenticated orbit & clock predictions (1-2 days in advance) for GPS + Gal satellites & provide to Galileo Ops.
- Galileo Ops., to upload predictions during test slot.
- Galileo Satellites E11, E12, E19, to transmit data in E6B signal
- EPOC Rx (L1C/A, L2, E1, E5, E6) to receive results and compute data-authenticated PPP.
EPOC test setup
EPOC transmitted data format (only for testing purposes!):

- High Accuracy (HA) field (SVID for GPS and Galileo)

<table>
<thead>
<tr>
<th>SVID</th>
<th>Epoch</th>
<th>X</th>
<th>Y</th>
<th>Z</th>
<th>Clock Bias</th>
</tr>
</thead>
</table>

- Data message structure (448 bps total)

<table>
<thead>
<tr>
<th>t [s]</th>
<th>HA₁ (160 bits)</th>
<th>HMAC₁ (64 bits)</th>
<th>HA₂ (160 bits)</th>
<th>HMAC₂ (64 bits)</th>
</tr>
</thead>
<tbody>
<tr>
<td>t+1</td>
<td>HA₃ (160 bits)</td>
<td>HMAC₃ (64 bits)</td>
<td>HA₄ (160 bits)</td>
<td>HMAC₄ (64 bits)</td>
</tr>
<tr>
<td>t+2</td>
<td>HA₅ (160 bits)</td>
<td>HMAC₅ (64 bits)</td>
<td>HA₆ (160 bits)</td>
<td>HMAC₆ (64 bits)</td>
</tr>
<tr>
<td>t+3</td>
<td>HA₇ (160 bits)</td>
<td>HMAC₇ (64 bits)</td>
<td>HA₈ (160 bits)</td>
<td>HMAC₈ (64 bits)</td>
</tr>
<tr>
<td>t+4</td>
<td>Bit Pattern (96 bits)</td>
<td>WN+TOW (32 bits)</td>
<td>$K_j$ (256 bits)</td>
<td>HMAC (HAPs, $K_{j+c}$) (64 bits)</td>
</tr>
<tr>
<td>...</td>
<td>HA₉ ...</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- All sats transmitted the same information.
Examples of EPOC results

- Performance computed using Galileo SIS data (E6b) and GPS/Galileo measurements.

- The results show the real-time performance obtainable by a GNSS standalone receiver (no GEO or ground channel).

- Accuracy is very sensitive to age of data. Here 1 to 3-day age of orbit and clock data (!). To be reduced to seconds in the operational system.

- GMV's magicPPP tool used.

- Tests included static/kinematic, open sky/rural/urban tests. All gathered data is currently under thorough study.
Example 1, 22/7: EPOC CS Results – data transmission & tracking

Figure 3–1: Tracking Profile

Figure 3–2: Transmission Performance
Example 1, 22/7: EPOC CS Results – CN0 and Authentication Error Rate
22/7: EPOC CS Results (magicPPP)

Figure 3–22: Difference from Reference Position to the Data-Authenticated Positioning Solution
28/8: EPOC CS Results (magicPPP)
Next Steps
From Demonstrator to Operational service:

- Continue CS Demostrator (AALECS) development and testing.
- GSC development and accreditation to allow E6b external data transmission.
- Agree on exploitation model for HA and Authentication, currently under discussion with EC/GSA/MS.
- Galileo system to implement system changes required to improve service provision.
- Commission Decision formal process with Member States to approve service definition.
- Open the CS Demo platform to potential service providers: 2015/2016.
- 2016/2017: Early CS operational with a subset of satellites.
Commercial Exploitation

• Authentication and High Accuracy are foreseen to be provided and exploited separately.

• Commercial exploitation scheme is under definition by EC & GSA (Market Development Dept. and Exploitation Depts). It will be consolidated once the CS technical & service definition is confirmed.

• Degree of involvement of Public/Private sector is under definition and may be different in each case:
  
  • For High Accuracy, Galileo could be used as a data transmission channel to support existing services.

  • For Authentication, Galileo may have a stronger role in the service provision (security reasons, key management, service definition, combination with OS, etc.).
Conclusions
Conclusions

• The CS is "on track".

• CS studies (2013) showed the way: from "what can we do" to "what do we want to do" with the CS.

• CS Demonstrator (2014): Early results with SIS are encouraging, including first GNSS-only PPP, and Authentication.

• Still work to do on service definition, development and exploitation toward an Early CS by 2016/2017.
CS Response to High Level Objectives

- **Public benefits**: Increased civil security (free NMA, controlled NMA/SCE), robust authentication service for EU Institutional Users

- **Revenue Source & Economic Value**: HA-CS, AUTH-CS commercial exploitation.

- **Navigation Performance**: HA-CS: most accurate (cm-level) **global** service ever (e.g. above 60° latitude GEO signals are not well received)

- **Innovation**: Downstream markets & applications, NMA/SCE + receiver-based authentication, etc.
Thank you for your attention!

Acknowledgements: AALECS (I. Rodríguez, G. Tobías & GMV/IFEN/CGI/QASCOM teams), EPOC (D. Calle, E. Carbonell, E. Göhler), CS EC/GSA team & EC management (J. Simón, R. Blasi, O. Valdés E. Boethius, T. Miquel, L. Dimitrijeva, E. Chatre), ESA (C. Payne, OPS), Spaceopal (P. Fedele & team), CESAR (C. Taillandier & team), GALCS (I. Rodríguez & team), Trimble (H. Landau & team), JRC, V. Rijmen, G. Seco.

http://ec.europa.eu/galileo
http://ec.europa.eu/egnoss
Q & A

http://ec.europa.eu/galileo
http://ec.europa.eu/egnons