GALILEO-BASED TIMING RECEIVER FOR CRITICAL INFRASTRUCTURES:

THE GIANO PROJECT

GSA/GRANT/05/2017
THE GIANO PROJECT

Project Context:
- Space infrastructure are becoming more and more critical and subject to safety and security threats
- Cyberattacks include jamming, spoofing and hacking on communication networks
- Need to protect assets from harmful conditions and events, intentional or not
- Security is being identified by EU Member States as a pillar of space technology developments

Project Drivers:
1. Fulfillment of specific Timing & Synchronization needs for Critical Infrastructures (accuracy, traceability, availability, continuity, security)
2. Provision of robust timing services for critical users belonging to Energy, Telecom, Finance
3. Promotion of Galileo & EGNOS for infrastructures protection, improving GNSS-based timing solutions resilience to RF environmental threats
GIANO CONSORTIUM

Consortium is composed by companies, institutions and experts with background and competence in timing applications:

**Thales Alenia Space** in Italy has plurennial experience in GNSS systems and in the development of GNSS-based products for ground and space applications.

**Business Integration Partners** is involved in the consortium for user groups interface, dissemination activities, providing its experience in strategic analyses and business modelling.

**PIKTime Systems** is experienced in time-based products and services development and is advisor on precise time, scales and design of time & frequency software algorithms.

**Space Research Center** of the Polish Academy of Science has strong heritage in timing systems, has participated to several European scientific and navigation programmes.

**DEIMOS Engenharia** a company largely involved in GNSS projects and with deep knowledge and experience in SW and algorithms development for GNSS-based equipment.
Stakeholders Interviews:
Stakeholders feedback revealed a high interest in **accuracy**, **integrity** and **robustness** features. However, actors still perceive security aspects unrelated to T&S devices.

- **Accuracy**: 91% of the interviewees
- **Integrity**: 64% of the interviewees
- **Robustness**: 60% of the interviewees

### Main Features pointed out by stakeholders

<table>
<thead>
<tr>
<th>Feature</th>
<th>Telco</th>
<th>Energy</th>
<th>Finance</th>
<th>STG</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary</td>
<td>Accuracy</td>
<td>Integrity</td>
<td>Robustness</td>
<td>Continuity</td>
</tr>
<tr>
<td>Secondary</td>
<td>Availability</td>
<td>Continuity</td>
<td>Security</td>
<td>Integrity</td>
</tr>
</tbody>
</table>

**Energy**
- Primary: Accuracy, Integrity
- Secondary: Availability, Continuity

**Telco**
- Primary: Accuracy, Robustness, Continuity
- Secondary: Integrity, Security

**Finance**
- Primary: Accuracy, Security
- Secondary: Robustness, Integrity
## Timeline User Needs: Accuracy Scenario Evolution

### Energy
- **"1 ms to 50 ns"**
- **Scenario Evolution**
- **Specific Function**
  - PMU (Power Measurement Unit)
  - TWL (time and frequency transfer)
- **Accuracy Requirement**
  - 1 ms
  - 1 µs
  - 1 µs
  - 1 ms
  - 100 - 400 µs
  - 100 ns
  - 10 µs
  - 500 ns
  - 1 µs
  - 10 µs
  - 3 µs
  - 260 ns
  - 130 ns
  - 260 ns
- **Future Trend**
  - 50 ns

### Telecom
- **"10 µs to 10 ns"**
- **Scenario Evolution**
- **Specific Function**
  - SCADA (Supervisory Control And Data Acquisition)
  - Optical Networks
- **Accuracy Requirement**
  - 10 µs (for synchronisation)
  - 3 ms
  - 100 ns
  - 100 µs
  - 1 µs
- **Future Trend**
  - Further phases of evolution for 5G technology will foresee an accuracy of 10-50 ns

### Finance
- **"1 ms to 100 ns"**
- **Scenario Evolution**
- **Specific Function**
  - PSTN
  - IS-95 (CDMA)
  - LTE TDD
  - GPRS
- **Accuracy Requirement**
  - 100 µs
  - 100 ms
  - 1 ms
  - 500 µs
  - 1 µs
  - 1.5 µs
- **Future Trend**
  - National standard time generation: 5s-level
  - National standard time generation: 5s-level

### Secondary Target Group
- **Trading**
- **Bank**
- **Rail**
- **Aviation**
- **Research**
- **Timing distribution**

---

**Notes:**
- **Energy** domain to provide more precise fault location
- **Telco** domain to boost 5G applications
- **Finance** domain to enable High-Frequency Trading (HFT) applications
GIANO TIMING PLATFORM: OVERVIEW

GIANO is a TRL7 System Prototype demonstrator in operational environment designed to accommodate L1/E1 & L5/E5 bands.

TIMING RECEIVER composed by GNSS Receiver & Timing Distribution Module

M&C PC control / monitoring SW for platform configuration and evaluation of KPIs

COTS ANTENNA designed to accommodate L1/E1 & L5/E5 bands

* GIANO is a TRL7 System Prototype demonstrator in operational environment

2019 - Design & Development 2020 - Integration & Testing 2021 - Final Product
GIANO TIMING PLATFORM: KEY FEATURES

**GNSS PROCESSING**
- **Multi-GNSS** and **Combined solution** capability (GPS + Galileo + EGNOS)
- **Flexibility** and **Configurability** from single to multi-frequency (L1/E1, L5/E5a)
- **Tunable bands** with innovative **Direct-Sampling** approach and **Digital Down-Conversion**
- Synchronization with **GALILEO SYSTEM TIME** (GST) or **GPS SYSTEM TIME** (GPST)

**IMPROVED TIMING ROBUSTNESS**
- **Jamming & Spoofing** detection / mitigation capability
- Use of **Galileo OS-NMA authentication** service
- Availability of **EGNOS corrections**
- **T-RAIM** algorithm for time solution **integrity** (single or multi-constellation based)
- **Accurate Digital Time-Steering** and **Holdover** with transparent output towards user
- Periodic **Auto-Calibration** capability
TIMING SERVICE ROBUSTNESS: SYNCHRONIZATION

Digital Time Steering Benefits:

1. **Improved timing signal continuity & avail:**
   - No transitory or jumps due to GNSS availability
   - Smooth convergence & synch recovery after holdover
   - Smooth transition between GST and GPST

2. **Higher level of configurability (FW/SW)**

3. **Solution independent from HW clock type**

4. **Early malfunction and anomalies detection:**
   - Easier maintenance (FW/SW approach)
   - On-demand or continuous integrity monitoring & notification

5. **Service-oriented implementation in critical infrastructures:**
   - Timing service performance autonomously monitored against Service Level Agreements
   - Synchronization predictions
   - Stored data for a-posteriori synchronization evaluation
**Interference Detection & Mitigation:**

- **Antenna level:**
  - RHCP Gain Roll-off
  - Front-End (BPF Bandwidth, LNA, …)

- **Pre-correlation level (FPGA):**
  - AGC
  - Digital Pulse Blanking
  - Frequency Excision

**Multipath Detection & Mitigation:**

- **Antenna level:**
  - RHCP-LHCP D/U ratio

- **Post-Correlation level (DSP):**
  - Multi-Correlator based DLL discriminators
  - Observables based (C/N0, CMC, etc.)
**Spoofing Detection & Mitigation:**

@ **Pre-correlation level:**
- AGC Monitoring

@ **Acquisition / Correlation level:**
- Multi-Peak Search
- Centre of Mass & Total Energy

@ **Tracking / Observables level:**
- Doppler / code delay rate consistency check

@ **Navigation level:**
- Anti-Spoofing RAIM

@ **System Based level:**
- GALILEO OSNMA: Navigation Message Authentication

---

**Deception of Service Attacks**

- Spoofing
- Meaconing

---

**Correlators Output Statistics**

- Multi-Peak Search

---

**Trajectory**
- Data
- Real Time Replica
- Record & Replay
TIMING SERVICE ROBUSTNESS: AUTHENTICATION

Open Service Navigation Message Authentication (OS-NMA)

- I/NAV Galileo Message is broadcasted in E1B

- OS-NMA is based on TESLA protocol
  (Time Efficient Stream Loss-tolerant Authentication)

Anti-Replay protection based on **OSNMA unpredictable symbols!**
TIMING SERVICE ROBUSTNESS: INTEGRITY

T-RAIM: Time Solution Integrity Monitoring

For a typical Timing Receiver, the position is known and static.

Reduced number of unknowns has to be estimated with respect to the full PVT solution:

- Clock bias
- Clock drift

Redundancy can be exploited to:

- Increase timing solution reliability
- Detect inconsistencies among GNSS observables
- Identify outliers in measurement set

The availability of several GNSS constellations provides a significant opportunity to further improve T-RAIM performance:

- T-RAIM for Single-Constellation
- T-RAIM for Multi-Constellations

In case of Multi-Constellation T-RAIM, Inter-System Offsets (i.e. GGTO) and Drifts must be carefully handled.
In-factory calibrated equipment is subject to degradation and needs to be **periodically re-calibrated** due to:

- **Aging** of components (i.e. random changes w.r.t. initial operating points)
- **Retrace** (i.e. steadiness of delay measurements after power-cycles)
- **Operating** conditions (typically different from calibration laboratory ones)

Calibration is typically performed in **two ways**:

1. **Absolute Calibration**: delays are measured against a simulated test signal with identifiable RF timing marker:
   a. **@ Antenna level** using a test inject probe antenna
   b. **After Radiating Element** prior to filters and LNA

2. **Relative Calibration**: delays are measured against a reference receiver that has been previously calibrated.

A built-in **Auto-Calibration Technique** will be studied and its feasibility in a commercial product will be investigated for industrialization phase.
Extensive validation test campaign, conducted in four phases, through specific involvement of Team’s experts and support of European laboratories:

1. **TAS-I premises (Italy):** verification of GIANO interfaces, functionalities and platform integration.

2. **SRC PAS (Poland):** calibration and time transfer performance verification in real environment (“Zero”, “Short” or “Long” baseline tests).

3. **TAS-I & EC Joint Research Centre - JRC (Italy):** verification of platform robustness and ability to withstand Jamming or Spoofing threats.

4. **Italian National Metrology Institute - INRIM (Italy):** GIANO performance benchmarking against COTS multi-GNSS calibrated timing receivers and UTC validation at user level.
No unique applicable standard to GNSS timing receivers.

Existing standards are more related to data format and I/F:

- Standards applicable to data format of high-end receivers, such as the CGGTTS format (BIPM).
- Ubiquitous standard used for timing (PPP) i.e. RINEX.
- Receivers used in critical infrastructures generally outputs time coded data in IRIG-B format, with variations for the power grid operators conforming to the IEEE C37.118 Standard (recently superseded by IEEE Std C37.118.1 and IEEE Std C37.118.2).
- Financial transactions conform to recent MIFID-II directive.

Timing services certification is the added-value making service more appealing to users.

An approach to Certification of a GNSS timing receiver could consider as a minimum:

- Receiver overall performances assessment under operating conditions (e.g. jamming, spoofing, etc.).
- Calibration by a certified laboratory (and possibly auto-calibration of the receiver during operation).
- Remote monitoring of overall performance may be required by specific applications.
THANKS FOR YOUR ATTENTION!

Livio Marradi
Navigation Products Manager

THALES ALENIA SPACE
Via E. Mattei 1, 20064 Gorgonzola
Milano (Italy)

livio.marradi@thalesaleniaspace.com

GIANO Project Website
https://gianoproject.eu