GALILEO TIMING APPLICATIONS

Marco Blanchi[1], Renzo Zanello[2], Claudio Cantelmo[3]

Thales Alenia Space Italia, Strada Antica di Collegno 253, 10146 Torino, Italy
[1]Tel: +39.011.7180.928, Fax: +.011.7180636, ***marco.blanchi@thalesaleniaspace.com***
[2]Tel: +39.011.7180.545, Fax: +.011.7180636, ***renzo.zanello@thalesaleniaspace.com***
[3]Tel: +39.011.7180.263, Fax:+.011.7180636, ***claudio.cantelmo@thalesaleniaspace.com***

Stefano Scarda
European GNSS Supervisory Authority (GSA)
Rue de la Loi, 56, B-1049 Bruxelles, Belgium
Tel:+32 2 29 87715, Fax: +32 2 29 21756, ***stefano.scarda@gsa.europa.eu***

Abstract

The Harrison Project is a project dealing with Time and Synchronization Applications started in the framework of the GSA (GNSS Supervisor Authority), a European Union body. The aim of the project is to study the advantages in time and synchronization applications offered by the Galileo System. The project is basically arranged in three major phases: the user community analysis, the development of a solution demonstrator, and the field trials of the demonstrator. The user community consists of partners belonging to several application domains such as: scientific applications on timing and astronomy and quantum cryptography, banking, railways, energy and power, mobile communications, network security, and satellite service providers. The user community is represented by both industrial partners and/or public bodies like university and research institutes. The user community analysis also includes a market analysis performed by a specialized company to identify business opportunities in timing applications for the forthcoming Galileo constellation.

The purpose of the project phase is to analyze the time and synchronization applications for each domain and study the advantages offered by the availability of a common precise time reference recovered by the Galileo SIS (Signal in Space). Moreover, this activity is also a stimulus for the development of new ideas. The proposed demonstrator is called the Authenticated and Certified Time Solution (ACTS) and aims to study the feasibility of using the time distributed by the Galileo System authenticated and certified through the Galileo System and added value services. The legal aspects are also considered and a dedicated analysis is performed considering the European Community laws and the acts in the major EU countries.

The time distributed through the Galileo Satellite System (and GNSS in general) is very attractive for all those applications that need a high level of synchronization over a wide geographical area; the benefit is that a synchronization network with nodes and a subnetwork is no longer necessary, since all the nodes can directly access the main synchronization SIS.

1 INTRODUCTION

The exploitation of telecommunication and information technology and capillarity of power distribution at the end of the last century gave great importance and new meaning to the time and space frame and created the concept of networks distributed over geographical areas.

The initial applications and needs of precise timing distribution over networks came from the telecommunication industries during the seventies of the last century. The available architecture for time and synchronization information distribution was at that time implemented with a single Master Clock. The signal of the Master Clock was distributed to the network node via a dedicated infrastructure, introducing a hierarchical approach with different stratum. At each stratum, specific performance characteristics were associated and performances were degraded, increasing with the stratum layers. Figure 1 depicts the time distribution hierarchical approach. The figure shows the various strata and the various network nodes. Moreover, a dedicated infrastructure is needed to distribute the time and synchronization signals; the intermediate node processes the signal in order to distribute it to the nodes of the next stratum.

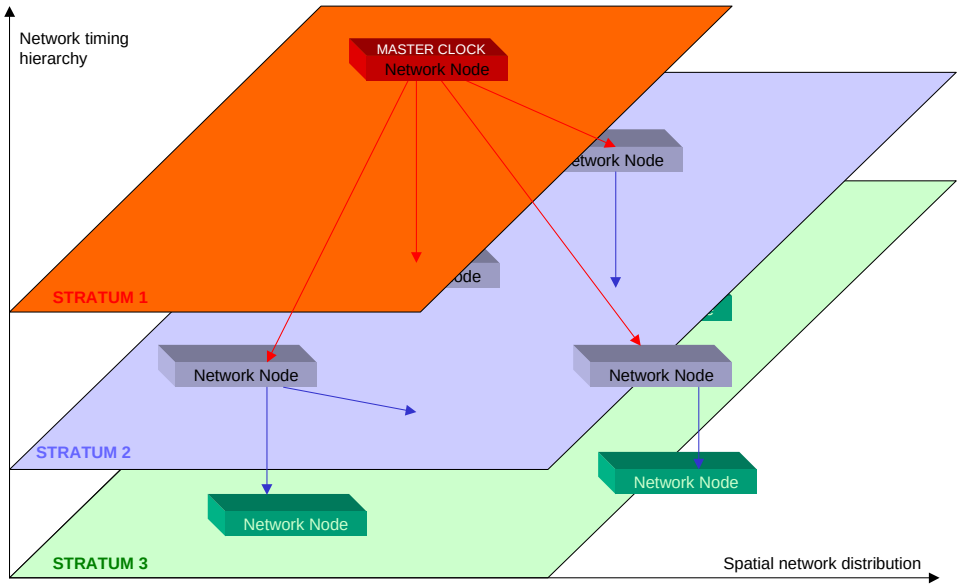

Figure 1. Timing in a telecommunication network based on a hierarchical approach.

Moreover, analyzing this architecture, it is clear that there is signal performance degradation due to the distribution from node to node and the low flexibility with respect to the number and location of nodes. Global Navigation Systems are not only used for localization and navigation purposes, but can solve the problem of high-performance time distribution and synchronization for distributed network applications.

Figure 2 depicts the time distribution architecture implemented via GNSS. The main difference with respect to the previous one is that all the network nodes have access to the same time reference or Master Clock. The access is made through the GNSS on-orbit satellites that are equipped with atomic clocks all synchronized with one another.

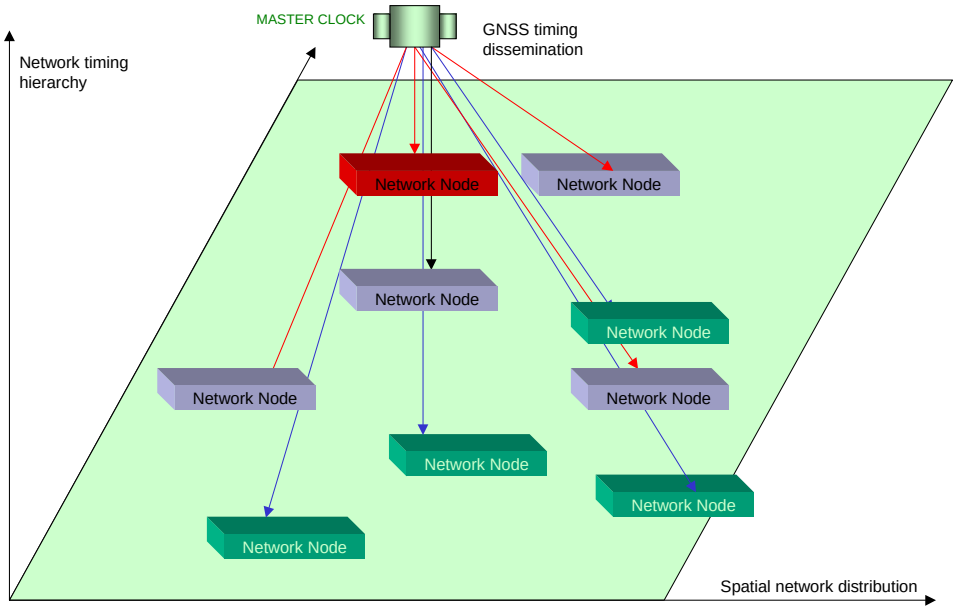

Figure.2. Time distribution and synchronization via GNSS systems.

There are many advantages to the GNSS architecture: (1) the horizontal structure: the picture shows the node colors of the previous picture, but the hierarchical structure implemented by strata has disappeared, (2) all nodes have access to the same SIS (Signal in Space), so all the nodes have the same time distribution performance; there is no degradation from node to node. In addition to the above, there are many advantages on the user side that increase the usage opportunities and make appealing the use of GNSS in many application domains. The considerations are intrinsically linked to the type of architecture proposed, without any modification of the GNSS infrastructure, that allows:

- no limitation on the number of network nodes
- no limitation on the geographical location of the nodes (the GNSS services are available worldwide 24 hours a day)
- the same GNSS infrastructure, used for localization and/or navigation purposes, can also be used by a high number of other users in different application domains.

This last point really makes the difference with respect to the previous architecture (Figure 1), which is a proprietary time distribution infrastructure.

2 HARRISON PROJECT SUMMARY

The Harrison Project is sponsored by the GSA (GNSS Supervisor Authority), a EU (European Community) body in the framework of the research project on the GNSS applications. The project deals explicitly with GNSS time and synchronization applications. The first step of the project was to perform the wider possible analysis of any potential GNSS time and synchronization service users. To cope with this need, the Harrison Consortium involves several companies and public institutions (e.g., universities, research laboratories) that work in several different application domains in order to virtually cover all the possible users.

The project is arranged in the following main phases; Figure 3 shows the project study logic:

- user community analysis and requirement definition (blue and yellow area on the study logic diagram)
- the development of a solution demonstrator (green area on the study logic diagram)
- the field trials of the demonstrator identification of a Service (green area on the study logic diagram).

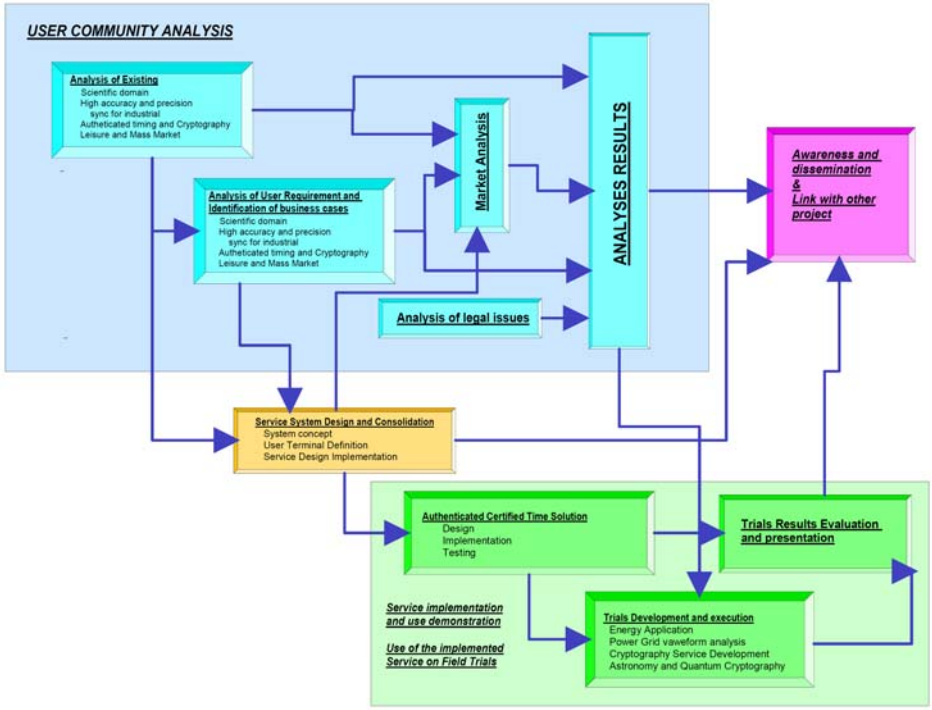

Figure 3. Harrison Project study logic.

In addition to the above three main areas of investigation, the study logic shows two additional analyses that are relevant for the project: the analysis of legal issues related to the use of GNSS distributed time and the market analysis aimed to provide a preliminary evaluation of the potential market for Galileo time services.

Annex 1 lists the Harrison Project contributors, their background experience, their role on the project, their country, and their legal profiles. Many EU countries are represented in order to have a wider contribution.

The Application Domains considered for the Harrison Project User Community Analysis are the following:

- Scientific and time applications
    1) Astronomical and astrophysical applications
    2) Quantum cryptography
- Industrial and transport applications
    1) Application in the electrical and power Industry: real-time and off-line monitoring and transient analysis propagation
    2) Synchronization in communication data transmission networks with a QoS (Quality of Service)

guarantee
3) Mobile and cellular Networks: synchronization of base stations
4) Railway applications
- Economics and financial/banking applications
1) Banking application, anti-money laundering
2) Cryptography, security protocols for timestamping.

In addition to the above-mentioned benefits to the civilian community offered by the Galileo Satellite Navigation System, it was argued, at the time of the proposal preparation, that a great added value is represented by the possibility of the authentication and a certification of the distributed Galileo time. This possibility is at the moment not guaranteed by the basic Galileo Open Services and Safety of Life Services; an additional service layer is necessary.

The Harrison Project investigates also who are the users that need an authenticated and certified time or, even better, a legal time. The legal time definition is obviously not absolute and changes from country to country. Harrison's role is to identify the needs for a legal distributed time and to identify the benefits of Galileo and GNSS in general.

The Harrison Project, in its second part that will start the beginning of next year, will develop a pilot project of an Authenticated and Certified Time Solution. The purpose of the project is to demonstrate the feasibility of this kind of service and to identify the major problems for its implementation. Since Galileo will not be available for the Harrison field trials, the GPS system will be used with EGNOS as necessary.

The needs of the various analyzed application domains are reported in the following sections. They are not to be considered as tutorials on the specific application domains, but a summary description of the identified fields that can use the benefits of time distributed by Galileo and what their requirements are.

3 SCIENTIFIC APPLICATIONS

ASTRONOMY

The expertise in astronomy is represented in the Harrison Project by the University of Padova and by the University of Ljubljana. The needs of optical astronomy, and in particular in quantum astronomy, are to measure the light properties at the second or higher order of magnitude. Coherence in the measurements will open detailed studies of phenomena such as variability close to black holes, surface convection on white dwarfs, nonradial oscillation and surface structures in neutron stars, and photon gas bubbles in accretion flows. These kinds of studies can be performed only by correlating the arrival time of the photons impinging on the telescope. The needs from the time information point of view are ultra-high precision and ultra-stable time references, since the observation time lasts from minutes to hours.

During the study, two different observation configurations were studied: with a single telescope, and with dual or multiple telescopes in a Michelson-type (phase) interferometric configuration.

Figure 4 provides a scheme of waveforms impinging from the direction k on two antennas separated by a baseline B on the Earth's surface. They are followed through the data acquisition system to the point where the correlator determines the delay. The signal waveforms are exaggerated; the actual waveforms are random Gaussian processes.

In extreme synthesis, for all astronomies three different times scenarios must be considered:

- An external UTC (and correction to TAI) available to Earth-based observers and to satellites throughout the solar system, in order to refer events to a common agreed-upon time scale, with a precision of the order of 50-100 nanoseconds. Interruptions and postprocessing are not allowed.
- For particular applications, an internal clock providing a timestamp accurate to the 10-100 picosecond level for the duration of the experiment is needed. Postprocessing is not allowed.
- For multiple telescope operation, a common clock accurate at the 10-100 picosecond level for the duration of the experiment (say, 6 hours). Postprocessing is allowed.

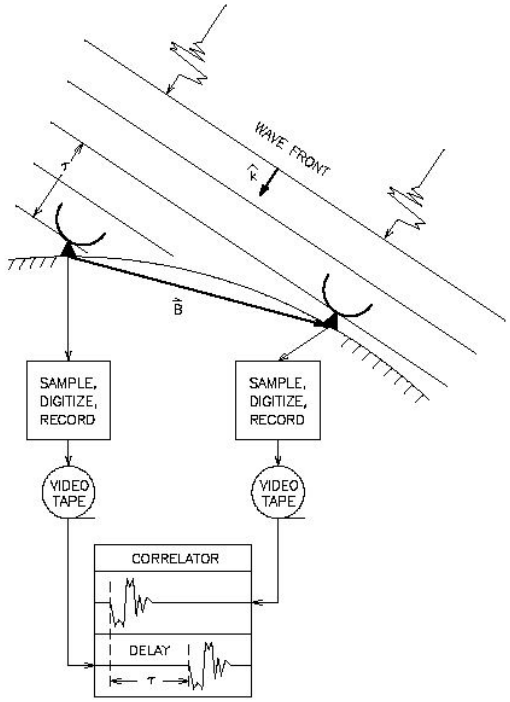

Figure 4. Schematic diagram of a VLBI experiment with multiple observation points.

Most of the current applications require a continuous time running for decades and centuries, keeping its accuracy at the 100 ns level, available to different observatories in different countries, and even in space. At this level, good quality commercial clocks and/or broadcasted times (e.g., the Galileo or GPS signal), meet most of these needs.

In special cases, e.g., for radio astronomy Very Long Baseline Interferometry (VLBI), active H-masers and cesium clocks are employed.

Astronomy does not need legal or authenticated time references, while some dependability requirements can be envisaged in order to allow observation effectiveness.

QUANTUM CRYPTOGRAPHY AND QUANTUM KEY DISTRIBUTION

The expertise in quantum cryptography and quantum key distribution is represented in the Harrison Project by the University of Padova. The quantum cryptography principles from the user point of view will be summarized. Its security is based on the laws of nature. In contrast to existing classical schemes of key distribution, quantum (cryptographic) key distribution does not invoke the transport of the key,

since it is created at the sender and receiver site immediately. Furthermore, the key is created from a completely random sequence, which is in general an extremely difficult task in classical schemes. Finally, eavesdropping is easily detected due to the fragile nature of the qubits invoked for the quantum key distribution. Those features show that quantum cryptography is a superior technology that overcomes the limitations and drawbacks of classical cryptographic schemes by utilizing the fascinating properties of quantum physics.

Cryptography (quantum key distribution) allows two physically separated parties to create a random secret key without resorting to the services of a courier, and to verify that the key has not been intercepted. This is due to the fact that any measurements of incompatible quantities on a quantum system will inevitably modify the state of the system. This means that an eavesdropper (Eve) might get information out of a quantum channel by performing measurements, but the legitimate users will detect her and, hence, not use the key. Quantum physics guarantees that any eavesdropping of the quantum channel will necessarily lead to errors in the key. If the key turns out to be insecure, then Alice and Bob simply discard it, and do not use it for encoding their message.

Quantum cryptography will then not be used to code the plain text, but to generate a secure and secret key to be used for cryptography. An optical channel has to be used for quantum key distribution; a standard communication channel then has to be used for the data transmission.

Figure 5 shows the block diagrams of an experimental QKD application. In that particular case, the optical link was free space. In other cases, the optical link has been implemented using fiber optics; this makes the technology more flexible and appealing.

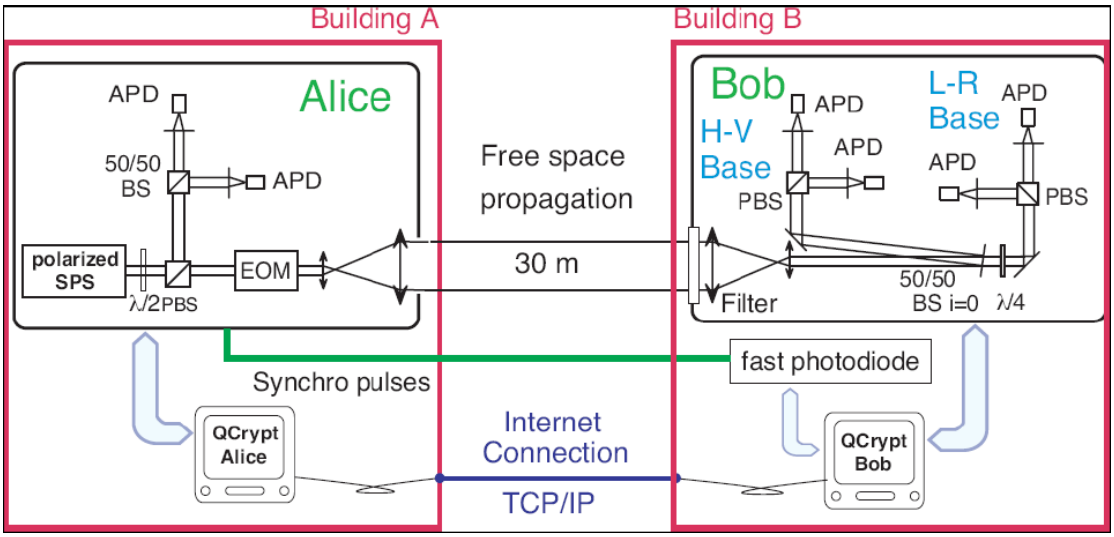

Figure 5. BB84 QKD experiment of the Charles Fabry Laboratory of the Orsay Optical Institute. In this case, the channel is a 30-meter-long free space quantum channel.

For QKD schemes, the strictest requirement is certainly the synchronization of the transmitter and the receiver. It means that it is essential to know that the measure made at a certain instant t1 is the measurement of the qubit sent at the instant t0. This is important for several reasons: first of all, noise reduction, rejecting the signals that arrive outside of our specified time windows, will preserve it from

unwanted detection; second, exploitation of and benefit from the characteristics of the detectors used. The silicon single photon detector, for example, after every detection has a dead time (from 40 to 100 ns) in which it cannot detect anything; this is not a good news in general, but it is clear that any unwanted detection has a double negative effect.

The key features for these applications are:

- relative synchronization between TX and RX < 1 ns
- time accuracy for key timestamping and eventually key authentication <1μs
- time stability when the transmitter and receiver are synchronized 10^{-12} (at 1 s).

To implement the above requirements, the GNSS performance as such are not sufficient and a hybrid setup has to be considered where the Galileo receiver assures the authenticated and initial synchronization between RX and TX, and then the ultra-precise alignment is kept with the internal reference in the optical system.

4 INDUSTRIAL AND TRANSPORT APPLICATIONS

POWER AND ENERGY APPLICATIONS

The expertise in power and energy applications is represented in the Harrison Project by the CESI RICERCA and by the University of Rome "La Sapienza."

Power systems monitoring has been traditionally carried out by means of SCADA (Supervisory Control and Data Acquisition) systems that are characterized by delays on the order of several seconds due to the transmission system. Further, Remote Terminal Units (RTUs) used for measurement may introduce significant inaccuracies and exhibit output sampling rates on the order of seconds (e.g., one measured value every 5 seconds). Measured quantities (rms values of voltages, active and reactive powers) are asynchronously sampled. With the available quantities, the process of power distribution network state estimation is nonlinear and computationally complex.

The increase of complexity of the power distribution network, the increase of distributed power, and the fact that presently the interconnections are over national borders lead to the need for improving the power distribution network monitoring and controls by means of Wide Area Monitoring (WAMS); in particular, time-synchronized measurements of voltage and current phasors performed by Phasor Measurement Units (PMUs). The PMUs are defined by a standard like IEEE Std C37.118-2005.

Figure 6 shows the typical PMU unit architecture, while Figure 7 shows the architecture of a synchronized WAMS controlled in real time by means of PMUs.

The timing requirements for the WAMS application in the power and energy domains are not very stringent; generally speaking, a synchronization of 1 μs is generally necessary and can be easily achieved with a satellite System. In the case of analysis of waveform propagation, the synchronization requirements are higher (1 or 2 orders of magnitude, according to area to be analyzed).

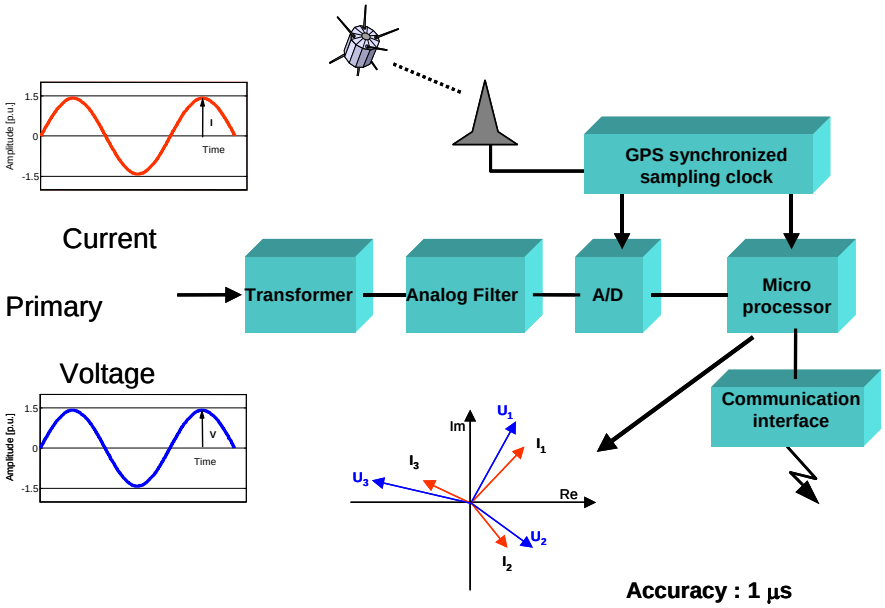

Figure 6. PMU architecture.

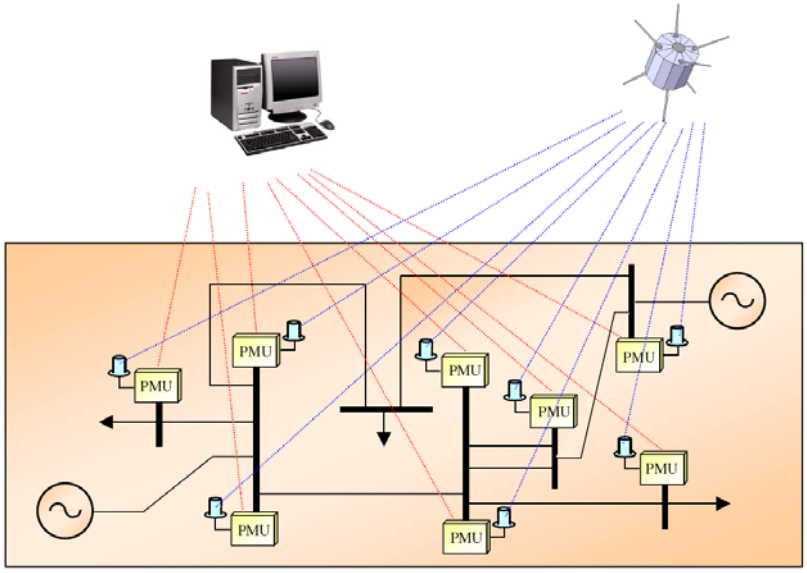

Figure 7. Synchronized WAMS architectures, PMUs directly connected to the Control Center.

In the case of implementation of a WAMS system, the power and energy depend on the GNSS and WAMS network; in fact, a failure in Galileo and/or WAMS may jeopardize power system security. In any case, the GNSS services cannot be the only primary means to get a time reference at PMU levels; a local clock is necessary to cope also with GNSS receiver failure. In the power and energy domain, there are norms that define the Safety Integrity Level for devices used to control the network (e.g., IEC/EN 61508). The dependability of a WAMS system on GNSS is very high; the use of GPS in WAMS creates concerns because of the difficulty to meet any dependability requirement on GPS.

Legal time service might be of interest in case of incident reconstruction, when the responsibilities of disturbances leading to service interruption must be ascertained, especially if legal agreements among system operators are in force. Incidents are reconstructed by identifying the sequence of events and the major phenomena occurred during the disruption process. The activity is done off line by analyzing synchronized information of time evolution of power system quantities, i.e. the PMU data, together with data from other sources (e.g., sequence of events recorders).

SYNCHRONIZATION IN COMMUNICATION DATA TRANSMISSION NETWORK

The expertise of synchronization in communication data transmission networks is represented in the Harrison Project by the Istituto Superiore Mario Boella (ISMB).

QoS is traditionally related to the network capability to differentiate traffic flows and service them in a per-flow basis. The network service depends on end-to-end QoS capabilities–to be more precise, the network capability to provide each flow the service needed from end to end. Applications require different network service in terms of end-to-end delay, jitter, and packet loss. Time-sensitive applications, such as audio or real-time video streaming, require low end-to-end delay and low jitter mainly while enduring low packet loss. On the other hand, for elastic applications, e.g., TCP–based applications such as file transfers, packet loss, not acceptable at the application level, can significantly compromise the performance of the transport layer. Besides traffic and services differentiation, QoS management must control network congestion, which happens when the traffic load is higher than network resources. Today, networks perform poorly at bandwidth mismatch points and data bursts, which typically build up across the packet network, and tend to overload and possibly overflow buffers feeding low-capacity or overloaded links. As a consequence of congestion, the QoS perceived by users decreases as a result of packet drops and large delays and jitter. The congestion control is the key to improve the Quality of Service.

One of the possible solutions is Pipeline Forwarding, which foresees having all packet switches synchronized with a common time reference (CTR), while utilizing a basic time period called the time frame (TF). Pipeline Forwarding is one of the emerging and more promising technologies combining the advantages of circuit switching (i.e., predictable service and guaranteed QoS) and packet switching (statistical multiplexing with full link utilization) that enables a truly integrated services network providing optimal support to both multimedia and elastic applications.

As exemplified in Figure 8, which depicts the journey of an IP packet from node A to node D along three switches, the forwarding delay may have different values for different nodes due to different propagation delays on different links (e.g., Tab, Tbc, and Tcd), and different packet processing times in heterogeneous nodes (e.g., Tbb and Tcc).

The Pipeline Forwarding technique requires a common time reference in all the network switches. The main interest in the time server deployment for this application can be summarized as:

1. **Primary (trusted) time source**: this is especially true for switches that are not equipped with the GNSS satellite receiver
2. Backup secondary time source when the GNSS service is not available or is disrupted
3. Replacement for already existing switches based on clocks disciplined by GPS; in this case, the time server can provide a (secondary) trusted, certified, and legal time reference that can also be used for time congruency verification.

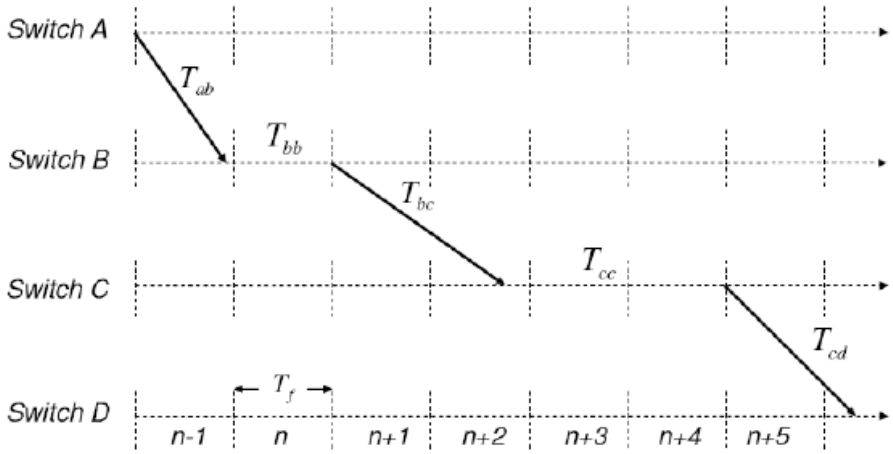

Figure 8. Pipeline Forwarding operations.

The Pipeline Forwarding dependability on GNSS signal can be considered medium, since in case of loss of SIS, the network can continue to operate in synchronous mode using local clocks and in traditional mode (i.e. asynchronous mode) with low QoS.

The accuracy requirements are application-dependent, but 1 μs can be considered a reasonable figure, considering a packet router with buffering and packet processing of 250÷500 μs.

MOBILE AND CELLULAR NETWORK SYNCHRONIZATION OF BASE STATIONS

The expertise in mobile cellular network synchronization of base stations is represented in the Harrison Project by Thales Alenia Space France.

The synchronization needs in mobile phone networks are deeply dependent on the design of the networks and the associated working rules. Some networks require an inherent synchronization, in particular to ensure the handover of a mobile unit from one cell to another one. Other types of networks do not require such synchronization and even present working procedures that are favored by a random synchronization between cells.

- **Synchronous Networks**: examples are IS95, CDMA 2000 (std body 3GPP2). Synchronization is necessary between BTSs (Base Transceiver Stations) and allows great simplification and improvement of many procedures such as handover (seamless handover is easy to implement). In these types of networks, the BTSs are commonly synchronized to GPS. The receiver is incorporated into the base station, but not every station can easily access GPS. An example is provided by the base stations located inside tunnels or in places where there is not a clear view of GPS satellites.
- **Asynchronous Networks**: examples are GSM and UMTS (std body 3GPP). There is no need of synchronization between the BTSs. However, this does not mean that the clocks in the BTSs are not stable. On the contrary, the BTS clocks need to be very accurate, but synchronized with one other. The stability of the clock is 10^{-9} and even in this case BTS could contain a GNSS receiver, provided that the BTS clocks are slaved to the GNSS clocks. The role of synchronization (in time and frequency) is essential for *signal acquisition* and then *improvement of sensitivity at the receiver*.

The accurate time dissemination among BTSs and between BTSs and mobile terminals in a cellular network is important for implementing location-based services (LBS). The basis for LBS is the cellular telephone localization in order to provide the customer with the proper service and information according to his own position.

Various positioning technologies have been developed for GSM/EDGE & UMTS applications. In most of the cases, these technologies have not proven their ability to comply with the requirement of the E911 regulation (regulation for the positioning of users in rescue and alarm calls). This regulation has been the first main driver of the location in the mobile networks. In some cases underlined later, the deployment of such technologies impacts significantly the network infrastructure. It must be noted that the localization performance of the various technologies, and more specifically the accuracy and the availability, vary with the type of use (user environment: masking angle due to buildings, multi-path, indoor …) and for some implementations with the networks characteristics (density of BTS, geometry of BTS).

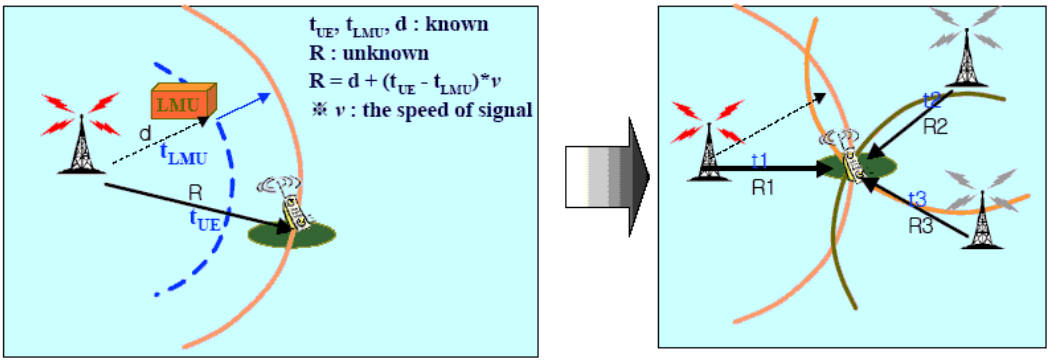

Figure 9. TOA measurement principle made by triangulation. BST synchronization is necessary.

Many of the technologies developed for the LBS services implementation are based on the measurement of the Time of Arrival (TOA). The time-of-arrival measurements are made by the mobile unit itself of signals coming from surrounding base stations, or on the other hand, measurements made by the base stations and coming from the mobile phone (called Uplink TOA). Theses techniques, resting on timing measurements, refer directly to **synchronization aspects of the BTS**. These methodologies have impacts on the network infrastructure only and not on the handset, since basically TOA measurements use standard GSM procedures.

Several techniques have been developed in the mobile telephony application domain in order to distribute the time over the network with different levels of accuracy, leading to different degrees of performances in localization. GNSS is really promising even if in some cases the TS is not directly visible to the satellite (e.g., inside tunnels, commercial centers, in general indoors). Presently the applications are based on GPS service, but the community is considering very promising Assisted GNSS (AGNSS) or Galileo because of the implementation of integrity information that could solve the problems experienced with GPS due to unexpected clocks jumps experienced so far. The main reasons to consider it are:

- it is the less expensive one
- studies reveal that, in the United States, the penetration of the AGNSS market is already sufficient to ensure a good timing collection; thus, this constraint does not seem insurmountable;
- the standards for timing collection are already defined; they only have to be slightly modified

- the integrity of the synchronization may be ensured by the integrity of the AGNSS positioning.

It then comes out that, for the future :

- during the coming years, the standardization of the synchronization methods for all mobile networks will be under discussion
- Galileo deployment will encourage operators to apply this synchronization, mainly for the use of the pilot tone
- the synchronization of the network will open new markets based on cheaper TOA-only technologies, which will ensure positioning with enough precision for rescue recommendation E.911 and for a particular set of services dedicated to terminal positioning around 100 m.

RAILWAY APPLICATIONS

The expertise in railway applications is represented in the Harrison Project by TUEV SUED Rail GmbH.

The use of GNSS systems in railways applications is very often twofold: localization and timing application and both on ground and onboard. Since the railways have to control the trains that travel around, the localization services offered by GNSS are very attractive. Railways do not have stringent requirements on time and synchronization, compared with the GNSS-offered performance, but, therefore, the opportunities offered by GNSS can in principle simplify the railway control and procedures.

Presently, many devices and functions use the GPS system, but they can only be considered and used as an ancillary function, not a primary one, because GPS does not satisfy any Safety Integrity Level (SIL) required by the railway Safety and Certification Standards. In the railway application domains, the safety is very demanding and includes also those aspects related to information integrity and service guarantee.

Figure 10 shows the use of Galileo and EGNOS in the various railway systems.

Railway stations exchange various kinds of information among them and with remote equipment to create itineraries for trains and for signalling purposes; synchronization is a key concept in functional and safety aspects. At the moment, many synchronization methods are used and the result of this situation is an expensive, nonunique approach across the EU. Having a uniform, integrated time reference would represent a cost-effective solution to synchronization problems in an international railway network and stations.

Concerning the most advanced markets, and particularly the European market, a big effort should be addressed toward offering a timing and positioning system with high reliability and safety integrity in a short time. In fact, in these last few years the European countries have initiated a strong modernization activity, aiming to render interoperable trains and relevant driving and control systems. GNSS timing may be used for the following functions:

- Timing for precise and coherent train distancing on the ground
- Timing, speed, and positioning for driving control systems onboard
- Timing, speed, and positioning for train control functions (e.g., doors, pantographs, wheel calibrations, anti-sliding)
- Timing and positioning for infrastructure measuring and gauging
- Timing and positioning for diagnostic systems (both onboard and on the ground, single or distributed)
- Timing, speed, and positioning for juridical recording.

The main challenge, in business terms, is to address the market as soon as possible, before the current design choices are too consolidated. We believe that the target to enter the market with a mature system should be within the next 2 years.

Another important feature that future Galileo-GPS receivers should offer for railway applications is to increase the coverage that is currently offered by the satellite systems, also considering the geographical constraints (e.g., the presence of tunnels) that the railways must address. As such, the future integrated receiver should consider the need of easily interfacing, or even integrating, additional equipment (e.g., a rubidium clock, an odometer) to enhance the overall availability of the user information provided.

The railway industry is waiting for a new generation of GNSS-based equipment capable of providing a time reference or time synchronization with safety-integrity characteristics compatible with the stringent railway requirements to be used as a primary information source.

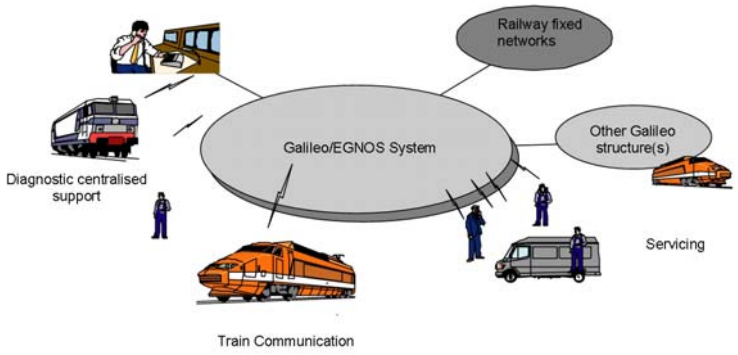

Figure 10. The use of Galileo and EGNOS in the various railway systems.

5 ECONOMICS FINANCIAL AND BANKING APPLICATIONS

BANKING APPLICATIONS

The expertise in the banking and financial community is represented in the Harrison Project by Exodus and by PFI.

Banking and financial institutions tend to be conservative in adopting new technologies when they are not fully proven in the field; this is a known inherent situation and may sometimes be a growth inhibitor. On the other hand, banks and financial institutions are looking all the time for new services and enablers for business growth. Generally, if a technology has a good, even at long-term, ROI (Return of Investments), banks are ready to invest in such a technology to aid in accelerating its market take-up rate.

The banking and financial community does not have strict requirements in the timing and synchronization field; uncertainties range from 10 to 300 ms are presently sufficient to fulfill all its timing requirements.

Nevertheless, a time reference is widely used for event logging, security purposes, and document timestamping. These timing aspects are relevant for many banking services such as: transactions, online banking and e-commerce, time-sensitive conditions (e.g., cancellation of a financial document, a credit

card for instance), and anti-money laundering. All the above services would be greatly improved by the adoption of a worldwide common time reference with legal validity.

Presently, banks will very often use NTP as a time reference, some of them accessing NTP servers on the official list of the BIPM as authorities responsible for TIME DISSEMINATION SERVICES PUBLISHED in the "BIPM Annual Report on Time Activities." This time reference does not have legal validity.

TIME REFERENCE FOR SECURE APPLICATIONS

The use of time for security applications has been studied in the Harrison Project both by the ISMB and by NSL.

The first issue related to security is monitoring and logging activities.

One important application of time for security applications in communication networks is monitoring and logging. A log is a record of the events occurring within an organization's systems and networks. Logs contain log entries; each entry reports the information of the specific event that occurred in a system or in the network. Logs can be generated by many sources, including security software (anti-virus software, firewalls, and intrusion detection and prevention systems), operating systems on servers, workstations, and networking equipment and applications. Log analysis is used for identifying security incidents, policy violations, fraudulent activity, and operational problems. Logs are also useful for auditing and forensic analysis, supporting internal investigations, establishing baselines, and identifying operational trends and long-term problems.

A log record typically contains an indication of the time the event(s) occurred. This time can be expressed in various ways. Nevertheless, time inserted in log files is not an authenticated/trusted time, and very often the correctness of this information relies on the correctness of time provided by the log machine. Thus, each entity generating logs typically references its internal clock when setting a timestamp for each log entry. If the clock of one or more hosts is (are) inaccurate, the timestamps in its logs will also be inaccurate and this can make analysis of logs more difficult, particularly when logs from multiple hosts are being analyzed. An advantage in improving network security is the implementation in the network of a Trusted Third Party implemented with net recorders that monitor the network traffic and record the data traffic. The net recorder would be fed with an authenticated and certified time, since its logs shall be used for forensic disputes.

Timestamping is usually the most popular use of time references in cryptography; nevertheless, other applications are very attractive.

Time synchronous authentication is a form of two-factor authentication. As with forward secure signatures, this deals with the potential compromise of a password. Due to their susceptibility to being lost/forgotten, or discovered by an outside party, passwords alone are insufficient for protecting high-value information.

Time synchronous authentication involves a password only being valid for the point in time at which it is needed, and is based around the use of a token. The advantages of time synchronous authentication are that it is easy to use, more secure, uses token-generation devices that are extremely portable, and is less demanding administratively. It is based on the token's "secret seed" (a symmetric encryption key shared with the server) which is virtually hacker-proof and whose generation is related to the time. Usually, both personal password and one time password are required for authentication. An example of a time synchronous authentication solution is that of RSA SecurID shown in Figure 12.

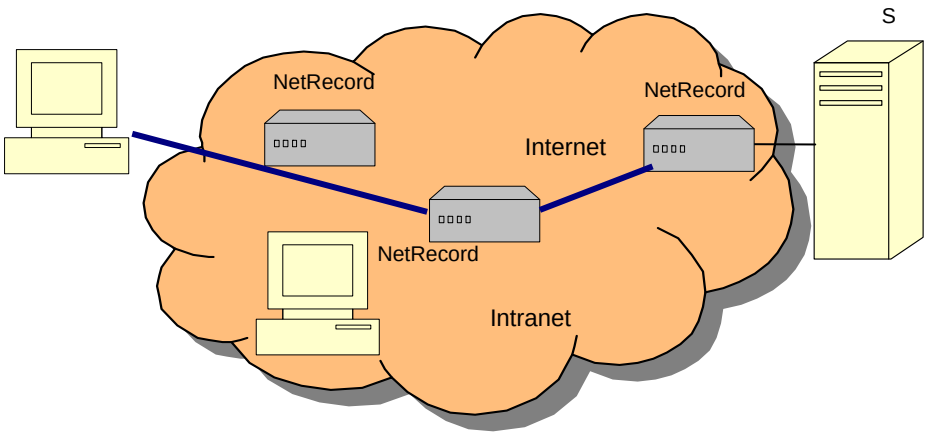

Figure 11. NetRecorder and Trusted Third Party.

Figure 12. Example of a time synchronous cryptography application.

Moreover, high-security cryptography products (e.g., GeoCodex) use a GPS receiver to encrypt messages that can only be decrypted in a certain geographical area; time information is sometimes used as a second layer of protection.

The following table summarizes the possible application domain for cryptography based on time information.

Table 1. Summary of application domains for the use of time in cryptography.

	B2G	B2B	B2C
Applications	Military waypoints, judicial reports, construction plans, civilian data (e.g., NHS)	Digital cinema, business data security, location-based services	Digital TV, online transactions/e-banking, service disablers, online gambling

6 LEGAL ASPECTS

One of the highlights of this study is the need of a definition valid in all Europe of the "legal time." These aspects have been identified in many application domains described above. The use of Galileo and GNSS, and in particular improving the authentication and certification of GNSS time distributed using added value services, depends also on the possibility of using a certain time reference for juridical and forensic disputes. Presently, the situation is not favorable to this approach; the following in fact applies:

- There is no explicit definition of a Legal Pan European (or EU-wide) time or time reference
- UTC is implied as a reference time (with time zone and summer time offsets) in the summer time directive of the EU. However, the same document in different languages uses contradicting terms like "UTC," "GMT," and world time to refer to exactly the same thing
- Individual countries do not have national legislation on the matter, even though they do differ as to which time is considered legal
- Even though there are many legislative acts on timestamping and on electronic signature, the issue of which time is legal for a timestamp depends on single country acts and in many cases remains a gray area.

The need to improve this situation comes also from the political determination to combat cyber crime and activities that may be associated to it, like terrorism, along with the ongoing process of setting a legal framework for event logging, timestamping, and electronic signature.

7 MARKET ANALYSIS

The market analysis has been performed by BAIN.

Galileo timing market is less attractive than the Galileo positioning market, both in professional and mass market areas. Looking at the last players of each value chain (called also the user community), the value of the timing market can be estimated in several hundreds of millions (euros).

The different market domains analyzed involve different players and implies different user needs, so no common strategic guidelines can be sought and they have to be developed independently:

- no synergies can be find and no bundled service can be hypothesized
- time to market can be different
- the entrance and success in one of the markets do not imply the entrance and success in another market
- the Galileo value drivers on which leverage to develop the market are different.

Referring to the analysis performed, the most appealing domains that should be addressed shortly are:

- Power and energy leveraging on availability and integrity Galileo value drivers and on the great benefits for the population in term of reducing the risk of blackouts
- Mobile communication to implement localization-based services
- Astronomy leveraging on the accuracy Galileo value driver and from the great benefits for research activities.

The definition all over Europe of a common acts and rules to define a common time reference to be used for forensic disputes and for juridical event recording or logging will create big opportunities in the security domain. Data network quality of service and railway domains that can be addressed through a marketing strategy will make the user community grow aware of the achievable benefits. Galileo and added value services will be able to create suitable time references, improving the Galileo market penetration.

8 CONCLUSION AND AN AUTHENTICATED AND CERTIFIED TIME SOLUTION

Based on the above results of the user community, it can be argued that the timing performance in terms of stability, resolution, accuracy, and synchronization capability offered by the GNSS is sufficient for all the users identified in the project as a part of the scientific community that needs better performance. The additional need identified is for an Authenticated and Certified Time Reference.

It is also argued that neither GPS nor Galileo in the future will offer directly an Authenticated and Certified Time Reference. In addition, the satellite signal can also be jammed, spoofed, or meaconed; therefore, the need for an added value service. Moreover, the Galileo signal is not available indoors or in tunnels; this could be a problem for railway applications.

In the second part of the Harrison Project, this problem will be studied and a solution prototype will be developed. The basic architecture is depicted in Figure 13. The basic idea is to implement a Service Center that compares the Galileo signal with a National Laboratory, possibly with a Legal Time Source, and validate the Galileo time received. Also, the user terminal receives the Galileo SIS and periodically checks, with the Service Provider, that the received Galileo signal is in line with the time at the Service Center and that no jamming, spoofing, or meaconing has been performed on the Galileo SIS.

In addition, the Service Center and the User Terminal can exchange auxiliary and ancillary data on the Galileo system status; for instance, in the case of a user terminal with a single-frequency receiver, the integrity information can be provided by the Service Center.

The protocol to exchange data between the Service Center and the user terminals can be developed according to user needs.

The ACTS position in the timing system is between the UTC (k) or legal time provider and the user application machine, e.g., PMUs, the Timestamping Authority, a NetRecorder Trusted Third Party, Synchronized Server, or Mobile Communication Base Station. In practice, the ACTS can fit in all the application domains so far analyzed.

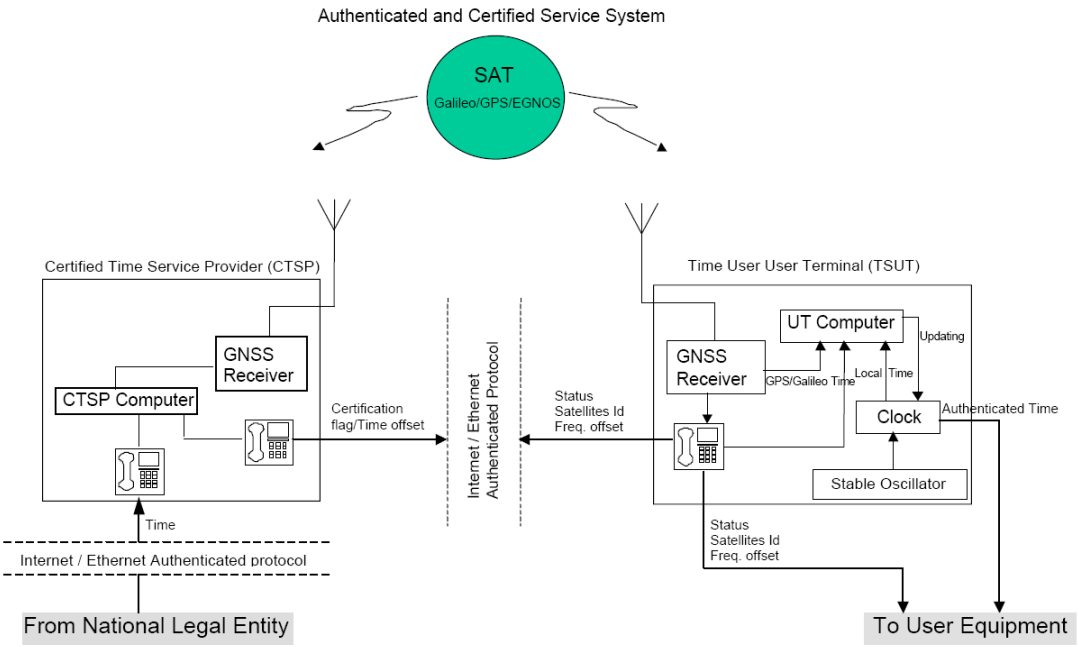

Figure 13. ACTS overall architecture.

ANNEX 1. LIST OF HARRISON PROJECT PARTICIPANTS

Company Experience and Country

Participants	Company Expertise	Contribution to the project	Country	Legal Profile
Consorzio Torino Time	The CTT has a wide range of skills and competences in the scientific, management, and engineering areas. The scientific competences are covered by the shareholders INRIM (previously known as IEN Galileo Ferraris), and by Politecnico di Torino. The industrial competences are covered by the shareholders Alcatel Alenia Space Italia, SEPA, SIA, and ALTEC.	CTT will act as Project Co-ordinator by leveraging the longstanding experience of its scientific and industrial shareholders in both the European GJU projects and ESA tenders. It is worth mentioning that ESA and Galileo Industries selected CTT as supplier of the PTF for the Galileo IOV phase. As Project Coordinator, the CTT will be responsible for both overall organization, planning, and control of the project.	Italy	Nonprofit organization

Participants	Company Expertise	Contribution to the project	Country	Legal Profile
Thales Alenia Space France	Satellite navigation system and applications.	Technical issues related to mobile communication applications.	France	S.A.
Thales Alenia Space Italia	Thales Alenia Space Italia has gained over the last 25 years of space activities a wide and deep experience in real-time system design and HW/SW development, specifically in the area of baseband signal processing in the frame of telecommunications and Earth observation programs. Real-time processing systems were first developed and experienced onboard advanced satellites; this important know-how was built up in the demanding space context and then generated fallout for applications on the ground in various systems.	Technical issues related to mobile communication applications. Will act in the name and behalf of CTT for Harrison Project management, technical coordination. system design, development demonstrators of a Certified Time Provider, supporting demonstrator in power applications, power grid waveform analysis, cryptography service development, and a final workshop.	Italy	S.p.A
AOS	Time and frequency, time transfer receivers, Internet, lan, time scale, calibration of GNSS rec, linux, time-stamping, NTP.	Timing, clocks, time scales, GNSS, GNSS receivers, time stamping, legal issues connected with time. Laser and geodetic applications. Internet, timestamping, time transfer. Time scales, legal issues, description time transfer, geodetic applications. Applications of Galileo timing through Internet, software.	Poland	University / public institute
BAIN	Business planning for GNSS applica-tions in the road domain. Business planning, market analysis, strategy and positioning studies for different industries, i.e.telecommunications, aerospace & defense, automotive, financial institutions, transportation, etc.	Market sizing - Value chain structuring - Business value assessment.	Italy	Ltd.
CESI RICERCA	CESI RICERCA has significant experience on the subject of Wide Area Measurement Systems (WAMS) for electric power system monitoring and control, and specifically in Phasor Measurement Units (PMU).	Analysis on power and energy applications and development of demonstrators.	Italy	S.p.A.
Exodus	Design, development, and implementation of integrated software solutions. Expertise in banking solutions (electronic payments, Internet banking, electronic trade, document management, electronic signatures, anti-money laundering), indoor and outdoor location-based services.	Wp leader in the study on requirements collection and specifications of applications that would benefit by Galileo in the banking /financial sector.	Greece	S.A.

Participants	Company Expertise	Contribution to the project	Country	Legal Profile
Istituto Superiore Mario Boella	**Networking:** Internetworking, Internet architecture and protocols, quality of service over packet networks, migration to IPv6, voice over IP, optical networking, hig-performance switching, programmable software architectures for network processing, network traffic capture and analysis. **Security:** network security (IPsec, intrusion detection, protection of DNS, routing, and ICMP), application security (both channel and message-oriented protection measures, with protocol and formats such as SSL, TLS, and S/MIME), X.509 certificates and related stuff (PKI, OCSP, timestamping, and the secure e-document formats PKCS-7/CMS and XML) **Navigation:** architectures and algorithms for Galileo receivers (professional, timing, mass market, safety of life), multi-path mitigation, interference rejection; software receiver design and implementation; Galileo signal design, Galileo Local Element design, EGNOS signal monitoring, Nav-Com integration.	Analysis of data network security (improvements in cyber investigations, study of time-based security protocols) and improvements of quality of some specific service (e.g., videoconferences) envisaged implementing synchronized data exchange over the network.	Italy	University / public institute
NSL	Nottingham Scientific Ltd. (NSL) is a GNSS applications developer, specializing in positioning and communication technologies, over a wide range of sectors (air, marine, rail and road transportation, and location-based services).	Cryptography applications: analysis and leader of the pilot project on cryptography.	U.K.	Ltd.
PFI	Atomic time scale keeping and dissemination. Digital timestamp technologies.	Implementation digital timestamp technologies.	Lithuania	University / public institute
SEPA	SEPA manufactures timing systems and equipment for specialized military and civilian applications. SEPA is also involved in the Galileo system development (in the Precise Timing Facility) and system start-up and verification.	Development of demonstrator for Certified Time Provider, interface with other demonstrators.	Italy	S.p.A.
Telespazio	Finmeccanica/Alcatel company, is one of the main worldwide players in satellite management and control, and in services for Earth observation, for	Service standardization, service design, and implementation.	Italy	S.p.A.

Participants	Company Expertise	Contribution to the project	Country	Legal Profile
	Navigation and for integrated and added value connectivity, leveraging on its technological competences, its facilities, and the participation in the main European Programs (i.e. Cosmo SkyMed and Galileo).			
TUEV SUED rail	TÜV generally is specialized in RAMS certification, verification, and validation activities according EN61508 and CENELEC Standards. TÜV Rail acts in Europe and in several countries around the world.	Assessment of ATP Wayside engineering process assessment of Radio Block Center EEIG ERTMS Users Group - assessment of the UNISIG Safety Deliverables Infraspeed BV (Siemens/Alcatel equipment for signalling, level 2) Assessment/Notified Body Services for HSL-South Development accompanied assessment of the radio-based warning initialization unit for track warning systems inter system/inter node handover tests UMTS/GPRS protocol conformity, and performance according to 3GPP standardization	Germany	GmbH
University of Ljubliana	Theoretical physics, astronomical observatory pioneering observations of pulsars where accurate timing is absolutely mandatory.	Analysis and implementation of demonstrator in optical astronomy.	Slovenia	University
University of Padova	Leading research center in Italy for astronomy, classical, and quantum optics communication andiInformation, and space activities.	Analysis and implementation of demonstrator in optical astronomy and quantum cryptography.	Italy	University
University of Roma 1 "La Sapienza"	Electrical power systems: power quality; high-speed railway system analysis; telemetering and telecontrolling using low-voltage power network as a communication channel; intelligent systems for electric lines protection; differential protection for power transformers; measurement of power in three-phase circuits with distorted waveforms.	Leader of the pilot project on synchronized measurement of transient propagation in low- and medium-voltage power grid.	Italy	University