Galileo Timing Applications and ACTS Prototyping

Claudio Cantelmo *(Author)*
B.U. Navigation & Integrated Communications, TAS-I
Turin, Italy
Claudio.Cantelmo@thalesaleniaspace.com

Renzo Zanello (Author)
B.U. Navigation & Integrated Communications, TAS-I
Turin, Italy
Renzo.Zanello@thalesaleniaspace.com

Marco Blanchi *(Author)*
B.U. Navigation & Integrated Communications, TAS-I
Turin, Italy
Marco.Blanchi@thalesaleniaspace.com

Paola Capetti *(Author)*
System & SW, SEPA
Turin, Italy
paola.capetti@sepatorino.it

Stefano Scarda *(Author)*
EU GNSS Supervisory Authority, GSA
Bruxelles, Belgique
stefano.scarda@gsa.europa.eu

***Abstract*— 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. Aim of the project is to study the advantages in Time and Synchronization applications offered by Galileo System. The project is basically arranged in 3 major phases: the User Community Analysis, the development of a solution demonstrator, 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, 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 includes also a market analysis performed by a specialized company to identify business opportunity in timing applications for the forthcoming Galileo constellation. Purpose of this 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. Moreover this activity is also stimuli for the development of new ideas. The proposed demonstrator is called Authenticated and Certified Time Solution (ACTS) and is aimed 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 an high level of synchronization over a wide geographical area; the benefit is that a synchronization network with nodes and sub network is no longer necessary since all the nodes can directly access to the main synchronization SIS. A demonstrator system (it obviously uses GPS and EGNOS) has been realized and tested on few domains: Astronomy, Quantum Cryptography, Energy and Power, Satellite Service Providers. The performances and functionalities have fulfilled the demonstrator target and evinced few lacks to fill. Overall the Authenticated and Certified Time Solution (ACTS) Demonstrator has shown its potentials and reliability (although it is just a prototype). It has been a flywheel to introduce few studies on Time and Synchronization improvement.** *(Abstract)*

I. HARRISON PROJECT SUMMARY

The HARRISON project is sponsored by the GSA (GNSS Supervisor Authority) an 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 services users.

To cope with this need the Harrison Consortium involves several companies and Public Institution (e.g. University, Research Laboratories) that works in several different Application Domains in order to virtually cover all the possible users.

The Harrison project deals with Time and Synchronization Applications made available with the use of GNSS (Global Navigation Satellite Systems) and in particular analyzing the benefits of the use of Galileo.

The Harrison Consortium includes companies, organization and authorities that deal in various application interests.

The application domains could be divided by three main domains: Scientific, Industrial and secure services.

The Scientific domains are considered by:

978-1-4244-3510-4/09/$25.00 ©2009 IEEE

- Time and Frequency Department of the Polish Astrogeodynamical Observatory, Space Research Centre P. A. S. (Poland)
- University of Padova - Department of Astronomy (Italy)
- University of Ljubliana (SL)
- University of Torino (Italy)

This community shall evidence of needs coming out from scientific requests. In general time accuracy requests are very pushed. Studies gain information from discrepancies or repeatability of particular phenomena, there are presented astronomical application that implies time and synchronization, an overview of future telescopes are presented.

It is important to highlight the astronomical user community comprises thousands of installations spread overall world and these need high performance instrumentation; therefore it's a valuable market interest.

The industrial domains are considered by:

Power and Energy

- CESI Ricerca (Italy) the research center of the Italian electricity distributor
- Università di Roma 1 «La Sapienza » (Italy) dep. Electrical Engineering

Communication Networks

- Alcatel Alenia Space France (France) with support of France Telecom (France)

Transportation

- Communication Infrastructure railways with TUEV SUED (Germany)

Industrial requirements comes out from technical commercial needs, existing application shall gain from accuracy, system behavior improvement. In the Harrison project three areas are deeply investigated, others are sketched and investigated by consortium as possible expansion field of application starting from the main proposed subject. Telecommunication application GSM, UMTS synchronization aspects are evinced. Transportation presents the Railway applications such as wireless communication dealing with synchronization aspects and signaling systems evidencing areas of improvements.

The industrial domains submit rules to a generic subsystem; therefore these shall be forwarded to a Harrison solution proposal. Characteristic of RAMS (Reliability, Availability, Maintainability and Safety) shall be analyzed and specified also for timing services, it shall be evinced impacts on system definition as well as alternative solution if there are any. Nowadays solution avoid this particular restrictions also in critical subsystem, such as "black boxes data logging", due to this lack. Harrison improvement open this area by implementing a reliable timing, therefore rules shall be implemented and new analysis shall be delivered.

The Secure Services are investigated by:

- Banking /Financial with:
- Exodus (Information Technology SME) (Greece)
- PFI (Time & Frequency Lab. Lithuania) for time stamping analysis

Cryptography applications: NSL (UK)

The interest of timing and synchronization are generally come out from determining schedule of transactions, actions, service furnished by the task provision. The needs aren't often high accuracy or resource demanding, however the economic return or involved interest (imagine a money transaction) could be high or huge. Often law-abiding procedures, reliabilities aren't given up characteristics. Cryptography highlights time-stamping techniques and time dependent encrypt algorithms.

II. LEGAL ASPETCTS

Industrial, financial, scientific application shall gain important improvement if it could be possible to deliver a "Legal Time". The concept is to ensure a reference known and accepted in the country where it is delivered. "Legal Time Delivering" imposes observing of sovereign national and international rules.

The timing receiver shall implement rules by hardware, software, algorithms and procedures in order to be fully law-abiding.

The interfaces, the architecture of timing receiver shall submit the restrictions imposed and it shall demonstrate faithful to all needed rules and it observes all practise in case of fail.

III. TRUSTED TIME STAMP

The Generic Time Machine generates time information, although all restrictions and rules shown are implemented, the value is certified and the user is responsible to establish procedures to bind time to the event.

The binding procedure is trustable how far the user relay on own signal processing. Another fact is to demonstrate that an event is occurred or exist from a certain time.

The concept is similar to the post office, the post stamp is an evidence to everybody the existence of envelop (and its content) at least from the stamp date.

Trusted time stamping is the process of securely keeping track of the creation and modification time of a document. Security here means that no one—not even the owner of the document—should be able to change it once it has been recorded provided that the time stamper's integrity is never compromised. The administrative aspect involves setting up a publicly available, trusted timestamp management infrastructure to collect process and renew timestamps.

A trusted timestamp is a timestamp issued by a trusted third party (TTP) acting as a time stamping authority (TSA). It is used to prove the existence of certain data before a certain point (e.g. contracts, research data, medical records,...) without the possibility that the owner can backdate the timestamps. Multiple TSAs can be used to increase reliability and reduce vulnerability.

IV. Relationship among Certification, Legal and Trusted Time Stamp

Clearly a solution that needs a trusted time stamp, it shall comply to rules stated above, implicitly the Trusted Third Party (TTP) at least shall have a Legal Time reference. The time reference shall delivered from a certified source. It is clear a bind among these properties.

In another hand, the certification follows the needs of the user; a terminal could be certificated in order to deliver a certain frequency, to deliver a time reference, or to be part of Trusted Time Stamp Solution.

The rules to comply depend of the certification level requested to the user; this fact is summarized by the Fig. 1.

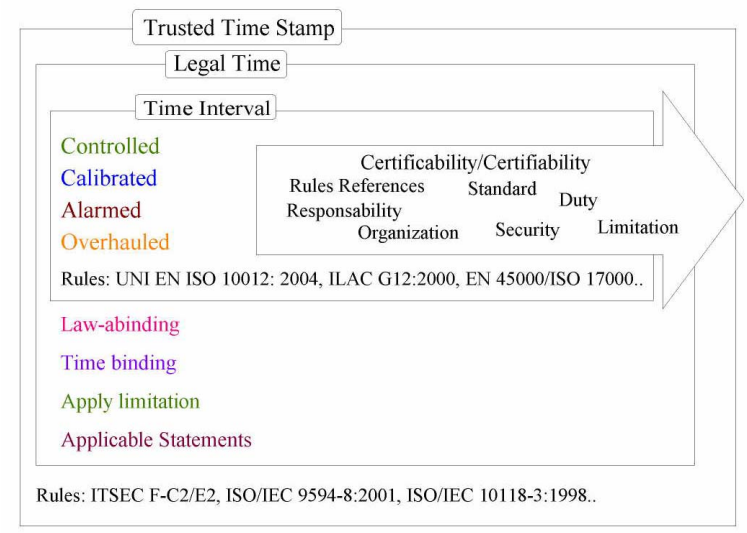

Fig. 1 Rules vs Solution

The main interest in Harrison project was concentrated on Legal Time layer (shown in Fig. 1). A work package was involved to collect rules, law and directive of the European Community, the conclusions of this studies are following:

In the European Union laws, there is a noticeable lack of one single directive that would unify Legal Time for all the EU members. EU rules and definition often wrongly identify UTC as GMT, often there aren't any definitions.

Few member countries haven't organizations in charge of Official Time distribution.

A suggestion made by the work package in Harrison is to unify UE member rules and laws, applying the UTC as official source of time. Any laws, decrees and official documents of the sort dealing in any way with the use of time, should be obliged to adhere to legal official time.

V. Authentication

Authentication implies to receive the time from an authenticated source. An authenticated source means the sender is univocally recognized, it is really what the users understand to be in contact to. Technically this means time data are delivered from an identified sender. Using Galileo SIS, the SOL has data encrypted; the successful verification of signal ensure the provenience of the information. In a hand, the presence of Galileo SIS is satisfactory to deliver "Authenticated Time".

VI. Market Analysis

The different market domains analyzed involve different players and implies different user needs, so no common strategic guidelines can be seek 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 entering and the success in one of the market does not imply the entering and the success in an other market
- the Galileo value drivers on which leverage to develop the market are different

Referring to the performed analysis, 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
- Astronomy leveraging on accuracy Galileo value driver and from the great benefits for the research activities

If a new regulation would set Galileo time reference as the only legally recognized reference, big opportunities will born into the security domain Data network quality of service and railways domains can be addressed through a marketing strategy that make grow the user community awareness of their achievable benefits.

VII. The Authenticated and Certified Time Solution

Within the Harrison project an original idea has been proposed and prototyped: an Authenticated ad Certified Time Solution (ACTS).

The ACTS is a system aimed to provide its user with an Authenticated and Certified time reference. In practice it is one of the possible implementation of a Legal Time distribution system. The ACTS takes advantage of the GNSS technology to distribute Time over wide geographical areas

without need of a deployed infrastructure. Moreover, since all users have access to the SIS, all ACTS network nodes have access to the same time reference with the same accuracy and stability. This implies that there is no node hierarchy, with consequent performance degradation, passing from higher to lower level.

A Generic Time Solution shall state a way to deliver time information to a user. The time information is fetched from a source and is treated in order to deliver it with the smallest modification. The use of broadcasting signal from a Satellite System improved the speed transmission and the number of users reached contemporarily that isn't comparable with other terrestrial method.

This document studies a Satellite Time Solution focusing on providing the time interval and reference by fetching Signal in Space.

A key unit in a GNSS time distribution system is the timing receiver that is the equipment able to extract the time reference present in the SIS. The following chapter deals with the key parameters used to characterize a time reference and time source that will be used also for the characterization of the timing receiver considered as a time reference source.

VIII. Design of the ACTS Demonstrator

Since the ACTS terminal have access to the SIS distributed, time performances (accuracy and stability) depend only on user needs and, consequently, on the implementation of the terminal itself; they are independent from the Service architecture. Consequently it is possible to improve performances of one ACTS node or terminal by improving the HW of the terminal.

ACTS consists of a Provider and of several User Terminals. The provider is not the time reference distributor but the entity that authenticates and certifies the time reference received through the SIS by the User Terminal.

The timing receiver is one of the key units both for the Service Provider and User Terminal since it is able to extract the time from the GNSS SIS.

An Authenticated and Certified Time Solution (ACTS) shall provide all subsystems to provide the data to impose the sovereign nation rules and therefore permits to deliver a law-abiding "Local Time". A basic idea of ACTS is shown in Fig. 2.

The ACTS demonstrator shall use the infrastructure available, therefore it will be retrieved timing signals from a GPS receiver, since GPS hasn't integrity nor authentication of the SIS, an EGNOS receiver is used to check integrity.

The Authenticated and Certificated Time Provider

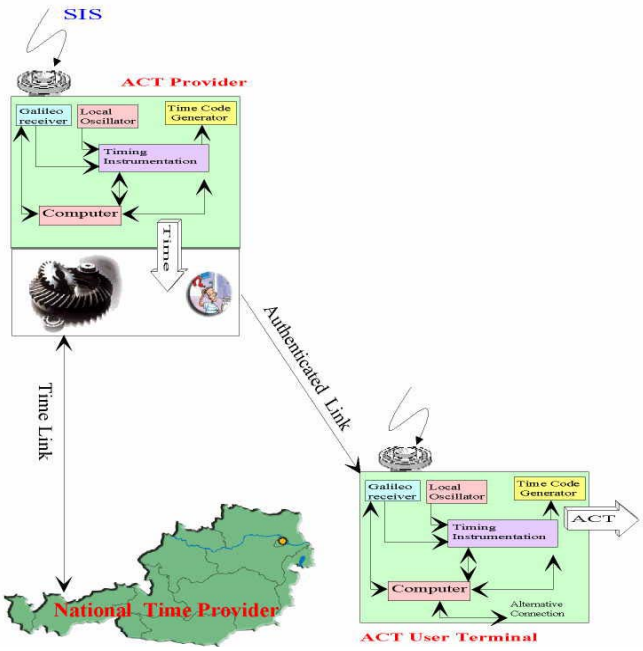

Fig. 2 ACTS principle

(ACTP) is equipped with a Galileo Time receiver similar to a User Terminal and it is connected with the National Time Provider. The provider sends elaborated information to the ACT User Terminal via an Authenticated Link.

The User Terminal has a Galileo Time Receiver and it receives by another link certification data from the ACTP; therefore it is able to deliver time information and acts all rules needed to certificate a legal and authenticated signal (Authenticated and Certificated Time –ACT).

IX. ACTS Demonstrator Test Run

The demonstrator system has been tested on few domains: Astronomy, Quantum Cryptography, Energy and Power, Satellite Service Providers. It follows description of the test set up, case and environment.

A. Power Grid waveform

The Power Grid waveform test analyzes the Voltage Transient Propagation Timing (VTPT) can be achieved by the

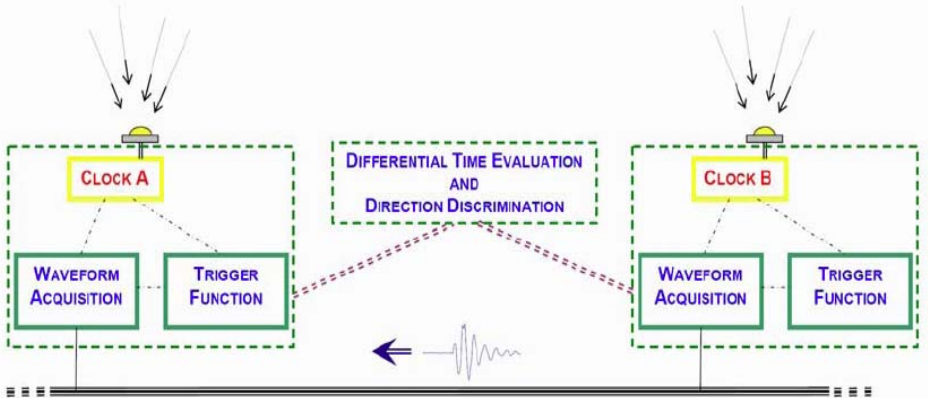

Fig. 3 Demonstrator simplified Lay-out

development of a common basic tool of Waveform Analysis.

By this tool it is possible to evaluate Power Quality (PQ) event causes (e.g., capacitor switching upstream or downstream from monitor position) and/or the correlation of events with ordinary switching operations.

For the system protection it is possible to extend TWFL (traveling wave fault locators) technique to distribution systems.

The demonstrator has been studied for a Low Voltage (LV) or Medium Voltage (MV) power system behavior analysis. The voltage transient considered will be normal switching operation generated or artificially generated (if in the considered grid no heavy switching is present).

The demonstrator simplified lay-out (see Fig. 3) comprises:

− "Clock" blocks that are common with others WP demonstrators as ACT-UT;

− Specialized Blocks that can be physical or virtual.

The aim of the demonstrator is to determine the origin of a voltage transient by the knowledge of the grid geometry and the difference of transient time stamps.

B. Quantum Cryptography

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 this 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.

At the beginning of September, the Quantum Cryptography Experiment was transported from Padova to Asiago installed in the control room of Cima Ekar Observatory. A flat mirror was mounted in the porch of the guest house some 50 m away (see Fig. 4).

Fig. 4 The QKD document installed in the control room at Asiago Observatory. See the thick fog on the right.

C. Quantum Astronomy

The Padova Group have built and put in operation a prototype (AquEYE, the Asiago Quantum Eye) for the Asiago 182 cm telescope, with special regards to its photon counting capabilities in a real astronomical environment. Such a photometer, even if mounted on a small telescope which falls short of providing the high photon rates necessary to reach the astronomical quantum domain, can produce data with an exceptionally high dynamic range, limited only by photon statistics.

The overall acquisition and control scheme is shown in Fig. 5.

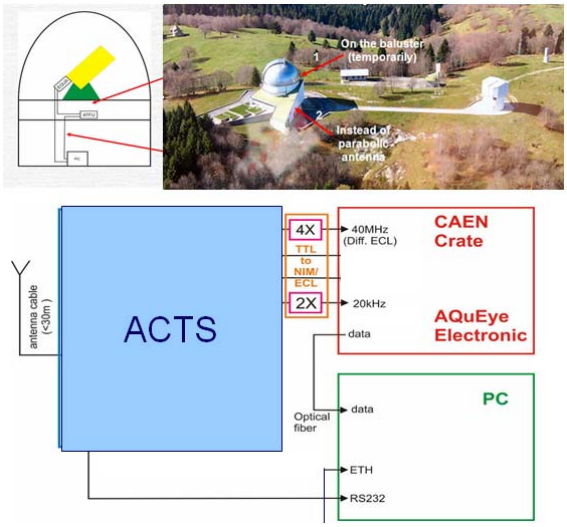

Fig. 5 Quantum Astronomy AQuEye with ACTS

The optical instrument of the Ljubljana group is a one fiber optic channel connected to a low noise SPAD (Single Photon Avalanche Photodiodes) that is mounted on a 70cm alt-az telescope. The fiber is aligned in the optical plane of the telescope, together with a CCD camera to allow pointing and tracking information.

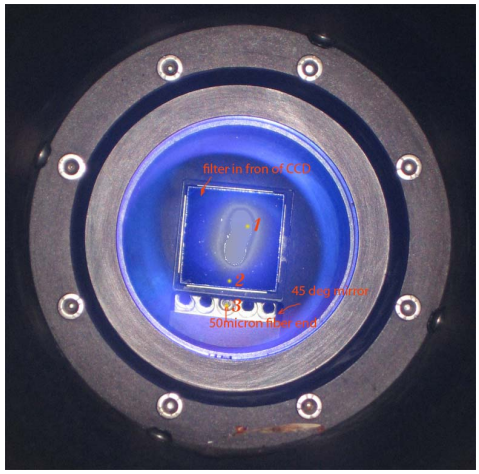

Fig. 6 Telescope image plane with the CCD and fiber(s)

The electronic part consists of a TDC (Time-to-Digital) board and a bridge build by CAEN (board of "CAEN S.p.A. Costruzioni Apparecchiature Elettroniche Nucleari" used in CERN research).

D. Cryptography Service

Time And Position Assisted Security (TAPAS) is an NSL invention. The system adds an additional level of security to data transmitted over a satellite communications link, through only allowing decryption to occur at certain locations. It is planned to be applicable to both business content and media content data delivered over services such as broadband via satellite that is aimed at the remote worker and the traveling businessman.

With the TAPAS components tested and validated, it was possible to proceed with the official TAPAS/Harrison ACT-UT Demonstrator Test. Such a test was made possible by the ACT User Terminal being installed within NSL along with the antennae being fitted to the roof. The test's purpose was to tell if the two separated systems can work together.

E. Monitoring and Control of energy transmission corridors

The data centre of Wide Area Monitor Systems (WAMS) application is extended to include protection and control algorithms and the possibility to send action signals: a wide area protection system is thus designed. Such a system can be supplied by a few PMUs up to tens of PMUs, depending on the size of the power system and the complexity of the protection functions.

Among the application of PMU technology the supervision and control of energy transmission corridors is one of the most interesting. Energy transmission corridors between European Countries are critical bottlenecks that limit network performance and, in recent past, a fault involving one of them has been the triggering event for a large black out in Italy, the main weakness being the lack or late information exchanged between different country's grid operators.

The basic set up for corridor monitoring that will be used as an application demonstrator of enhancements provided by Harrison technology.

Limitations to power transmission through a line or corridor come from three main causes:

- Thermal overload,
- Voltage instability,
- . Rotor angle instability

X. TEST ANALYSIS RESULTS SYNTHESIS

The Harrison project deals with Time and Synchronization Applications made available with the use of GNSS (Global Navigation Satellite Systems) and in particular analyzing the benefits of the use of Galileo.

The application domains could be divided by three main domains: Scientific, Industrial and secure services. Tests were performed on following domains:

The Scientific evidences needs coming out from scientific requests. In general time accuracy requests are very pushed. Studies gain information from discrepancies or repeatability of particular phenomena.

University of Padova was involved in Quantum Key Distribution (QKD) demonstration. The two ACTS terminals were successfully installed at the beginning in Asiago for QKD; the terminals were connected via LAN to the ACTS Server at TAS-I premises in Torino

The ACTS worked correctly they are satisfied.

The ACTS system satisfies all necessity of QKD application, so in this case it's not necessary to have any further upgrade of ACTS. However they had some problems due to bad weather conditions leading to have just a minimum set of measurements to satisfy their experiments.

University of Padova and University of Ljubljana was involved in Quantum Astronomy demonstration together. Test set up has been fully satisfactory and during experiments they had a high SNR.

The ACTS terminal was installed successfully and the terminal has worked properly.

The industrial domains are considered by:

- Power and Energy
  - CESI Ricerca (Italy) the research center of the Italian electricity distributor
  - Università di Roma 1 «La Sapienza » (Italy) dep. Electrical Engineering

Industrial requirements comes out from technical commercial needs, existing application shall gain from accuracy, system behavior improvement.

ACTS installation and system is enough to fulfill their needs during the tests.

The Secure Services are investigated by:

- Banking /Financial with:
  - Cryptography applications: NSL (UK)

The interest of timing and synchronization are generally come out from determining schedule of transactions, actions, service furnished by the task provision. The needs aren't often high accuracy or resource demanding, however the economic return or involved interest (imagine a money transaction) could be high or huge. Often law-abiding procedures, reliabilities aren't given up characteristics. Cryptography highlights time-stamping techniques and time dependent encrypt algorithms.

The added value of the ACTP is apparent through the validity flag. It is possible to be within the correct time slot but to get a "time invalid" flag thus denying decryption and this is a differentiator from other NTP sources.

The integrity offered by the ACTS is relevant for the cryptography using GNSS.