Say 'Hello' to Galileo's PRS

Making the Case to Security-Minded User Communities

ALAN KENDALL, ALEXIS VIDAL, FRANÇOIS BOULLETE
EADS ASTRIUM SERVICES

PASCAL CAMPAGNE
FDC

BERNARD PANEFIEU
THALES AVIONICS

USAF photo/Tech. Sgt. Jeremy T. Lock

One feature that distinguishes Galileo from other GNSS systems is the Public Regulated Service or PRS, an encrypted signal that will be used by European governmental agencies, including police, emergency services, and, potentially, military services. Drawing on on information from the on-going PACIFIC (PRS Application Concept Involving Future Interested Customers) project this article discusses the need for and applications of the service.

GPS's widespread success has increased the use of and reliance on positioning, navigation, and timing (PNT) technologies to support all kinds of civil applications. Among others, these include emergency operations, critical transport guidance, tracking of hazardous goods, and synchronization of radio communications and energy supply networks.

With Europe's Galileo system under development, it's time to consider how that system's planned Public Regulated Service (PRS) will add value to Europe's overall GNSS program. PRS is designed to provide position and timing to specific users requiring a high continuity of service, with controlled access ensured by encryption of the ranging codes and data. The sidebar, "Galileo Menu of Signals," describes the full suite of Galileo's services.

This article will outline the potential benefits that a secure GNSS signal will have for agencies and organizations involved in public safety and security and describe work under way to identify and inform prospective users of PRS.

Demonstrated Need

On one hand, PRS will provide continuity of PNT service for GNSS-dependent, critical applications in day-to-day operations; on the other hand, it will potentially enable access restriction of GNSS capabilities to authorized users only.

Why is this necessary?

Open GNSS services still have major weaknesses, including very low signal power. (Picture a 40-watt light bulb seen from 20,000 kilometers — or 12,427 miles — away.) This makes them vulnerable to unintentional interference and malicious jamming. Many examples of critical signal loss or jamming have been noted in the last decade, and these are likely to increase proportionately to GNSS popularity.

In December 30, 1997, for example, a Continental trans-Atlantic flight lost all GPS signals as it descended for landing in New Jersey. Officials at Continental Airlines originally believed that the flight had been subject to intentional military jamming exercises, but later investigation revealed that the interference was actually due to a U.S. Air Force test gone awry. The source of the 200-kilometer "interference zone" was a GPS antenna with a 5-watt signal, stepping through frequencies.

In other cases, the causes are less benign. Hostile or malicious GNSS jammers are indeed proliferating, boosted by low prices and do-it-yourself information on GNSS.

As a critical infrastructure, GNSS is a likely target for hostile organizations. The capabilities offered by GNSS to hostile users should also not be ignored.

In addition to the terrorist threat, hackers may experiment with degradation of GNSS for personal entertainment in the same way that they have attacked many websites on the Internet. This results in a risk of loss of PNT capabilities for any user of open GNSS services lacking appropriate mitigation capabilities.

Moreover, publicly available signal structures and interface control documentation make open GNSS services easy to replicate spuriously. Existing GNSS infrastructures do not allow users to authenticate signals readily and in real-time, rendering them vulnerable to spoofing, the broadcast of fake GNSS-like signals, and meaconing, the rebroadcast of same GNSS signals to create confusion.

In this context, the need to have an enhanced, asymmetric, global PNT capability arises for a variety of users who do not have access to the secured, military GPS signal.

Introducing PACIFIC

The PACIFIC project involves 20 companies from more than 14 European countries (see **Figure 1**) and was established in the context of the Galileo research and development activities funded under the European Union's 6th Research Framework Program (FP6). PACIFIC's acronym stands for "PRS Application Concept Involving Future Interested Customers" and addresses a clear need to foster the development of the PRS user segment.

The project gathers a unique set of expertise across the PRS value chain, including equipment manufacturers, system integrators, secure system operators, and secure service providers.

Since September 2006 this consortium, led by the European GNSS Supervisory Authority (GSA) and EADS Astrium Services, has been working on developing an understanding of the needs of PRS users including technological and organizational aspects within an appropriate security framework.

The main objective of the project is to pave the way towards the introduction of the added value of the PRS capabilities into the user community. (See **Figure 2**.)

After honing the explanation of PRS benefits as part of its initial review, the PACIFIC team held its first workshop for potential users in Brussels last March. More than 130 potential users, and institutional and industrial representatives from 21 countries attended the session. Now the project team is interacting with representatives of user communities in order to provide input to the elaboration of the PRS technology development plan and the analysis of interface and market aspects.

Illustrating PRS Benefits

Wideband signals will be permanently broadcast on frequencies (the so-called

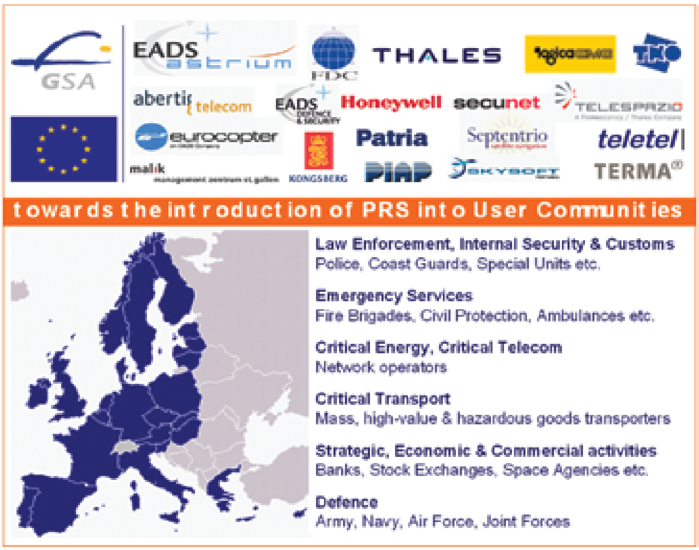
GSA
EADS Astrium
THALES
logicaCMG
TNO
FDC
abertis telecom
EADS Defence & Security
Honeywell
secunet
Telespazio
eurocopter
Patria
Septentrio
teletel
malik
Kongsberg
PIAP
Skysoft
TERMA
towards the introduction of PRS into User Communities
Law Enforcement, Internal Security & Customs
Police, Coast Guards, Special Units etc.
Emergency Services
Fire Brigades, Civil Protection, Ambulances etc.
Critical Energy, Critical Telecom
Network operators
Critical Transport
Mass, high-value & hazardous goods transporters
Strategic, Economic & Commercial activities
Banks, Stock Exchanges, Space Agencies etc.
Defence
Army, Navy, Air Force, Joint Forces

FIGURE 1 PACIFIC Team

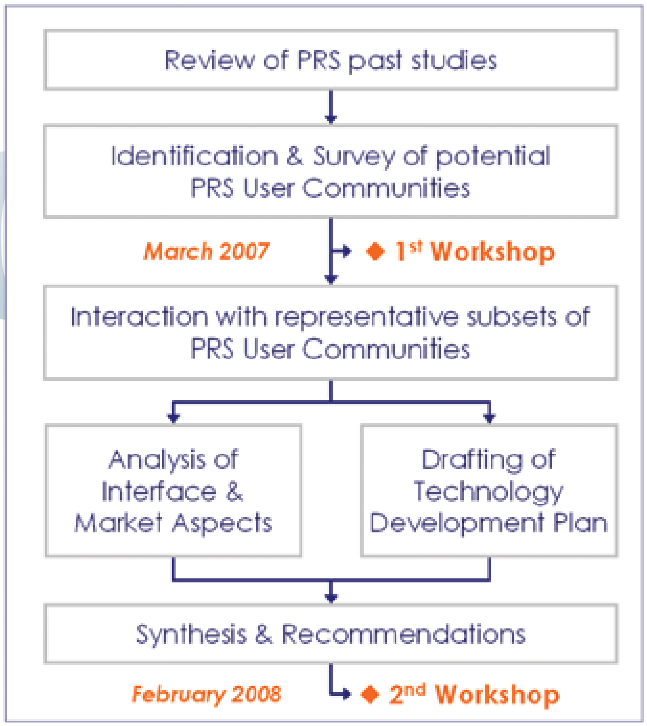
Review of PRS past studies
Identification & Survey of potential PRS User Communities
March 2007
1st Workshop
Interaction with representative subsets of PRS User Communities
Analysis of Interface & Market Aspects
Drafting of Technology Development Plan
Synthesis & Recommendations
February 2008
2nd Workshop

FIGURE 2 PACIFIC study logic

E2-L1-E1 and E6) separate from Galileo open services. Thus, they will be resistant to interference or malicious jamming of OS signals and will preserve PRS service when open services are denied locally.

Although PRS is independent from other GNSS signals, it will be interoperable with other Galileo services (OS, CS, SoL), with GPS open and military services, GLONASS, and their augmentations. Such combined use is already planned by receiver manufacturers to offer enhanced performance in terms of accuracy, integrity, continuity, and availability of PNT services, including a better robustness against interference and jamming.

The following likely scenarios clearly show the added value of PRS.

Take, for example, a threat to everyday GNSS services — one that might affect the police, fire fighters, or emergency medical transport, and weaken their ability to navigate or synchronize operations.

The potential threat could involve several low-power jammers, or a single high power jammer placed in strategic locations, or intense interference environment.

In this context, those users relying on open GNSS services would very likely experience reduced capability to operate in that jammed area. Coordination at the control center would be strongly affected, particularly when the mission involves other emergency services. Moreover, GNSS-dependent infrastructures such as the telecom network could fail, creating multiplied effects outside the jammed area.

In this scenario, a robust PRS signal could maintain PNT capability in an area affected by low-power jammers. It would require high-power jamming to affect PRS in any way — but such equipment is more expensive to procure and easier to detect, which reduces the likelihood of its use.

A second scenario refers to a hostile use of open GNSS services. Terrorist capabilities are enhanced by open signal availability and, as a result, it is probably inevitable that hostile forces, such as terrorists and criminals, will take advantage of this vulnerability.

In fact, similar scenarios using communication networks capabilities have already been demonstrated through the use of GSM-triggered bomb systems (fuel depot bomb attack in Israel in 2002, Madrid train attacks in 2004).

Local voluntary denial of GSM is now being investigated or implemented for use in such critical circumstances. Similarly, authorities could voluntarily interrupt open GNSS services to prevent forms of hostile use in situations where intelligence sources report a high threat of attack.

Galileo's Menu of Signals

Galileo, Europe's initiative for a state-of-the-art Global Navigation Satellite System (GNSS), will provide a highly accurate, guaranteed global positioning, navigation, and timing service. The following Galileo satellite-only services will be provided worldwide and independently of other systems by combining Galileo's signals in space:

- The *Open Service (OS)* results from a combination of open signals, free of user charges, and provides position and timing performances competitive with other GNSS systems.
- The *Safety of Life Service (SoL)* improves the open service performances, providing timely warnings to the user when it fails to meet certain margins of accuracy (integrity). It is envisaged that a service guarantee will be provided for this service.
- The *Commercial Service (CS)* provides access to two additional signals to allow for a higher data rate throughput and to enable users to improve accuracy. It is envisaged that a service guarantee will be provided for this service. This service also provides a limited broadcasting capacity for messages from service centers to users (on the order of 500 bits per second).
- The *Public Regulated Service (PRS)* provides position and timing to specific users requiring a high continuity of service, with controlled access. Two PRS navigation signals with encrypted ranging codes and data will be available.
- The *Search and Rescue Service (SAR)* globally broadcasts the alert messages received from distress-emitting beacons. It will help enhance the performance of the international COSPAS-SARSAT Search and Rescue system.

In this scenario, PRS users will benefit from a full GNSS capability in the denied area, because they are registered as authorized users by their own government.

In summary, users equipped with PRS will benefit from the robustness of a PNT service anywhere and at any time, especially when the open signal experiences interference, hostile jamming or spoofing. They will enjoy service availability in emergency situations that require denial of open GNSS signals.

Galileo PRS will benefit users of open GNSS services, in replacement or in combination, as well as users of military GPS signals when employed in combination with a secured service.

PRS Users & Applications

PACIFIC identified and surveyed sampled 200 user communities across the European Union and Norway in nine application areas. They gathered feedback on market, operational, and technical aspects of 600 systems that employ positioning, navigation, or timing technologies or services in nine defined application domains. The amount of information per application domain and per platform is considered sufficient to establish the survey as being representative of most of the potential PRS user communities and relevant for specific user categories and associated applications.

While it is premature to give final conclusions, the following general trends can be highlighted in terms of perceived interest in PRS by customers and applications as well as the potential for its introduction in each.

Defense. A high interest in PRS manifested itself in the defense domain, particularly for applications that need to operate in times of crisis worldwide in which the need for high robustness and continuity of PNT capabilities is critical. This need is evident from users of military GPS signals, as well as users of civil GPS signals. Users of military and civil GPS signals show great interest in PRS, particularly in its ability to pro-

NATO photo

vide robustness and continuity during worldwide crises. Further investigation is required to address specific applications and operational scenarios with all type of platforms because of stringent performance requirements, integration constraints, and potential operations in unfriendly environments.

Law Enforcement, Internal Security, and Customs. These groups are also interested in PNT continuity in times of crisis, although with moderate performance requirements. PACIFIC must address applications and operational scenarios, especially for civil protection, health services, and police forces that use handheld terminals and land vehicles in urban or indoor environments The needs of border police and coast guards who operate helicopters or ships in rural or marine environments must also be investigated further.

Emergency Services. The needs in this area are similar to law enforcement requirements. Further operational scenarios must be developed for civil protection and health services units who use handheld terminals and land vehicles and for fire brigades and search and rescue units who operate in rural environments with land vehicles, helicopters, and aircraft.

Critical Transport. Civil aviation uses PNT capabilities extensively; however, interest in PRS is subject to regulatory requirements for operational procedures, equipment certification, and so forth. Adoption of PRS by civil aviation also depends on a cost/benefit assessment. Further investigation is required, especially for state aircraft or airport assets.

Transport of Hazardous Goods. A lower interest in PRS is perceived for high-value items and hazardous goods transportation. This is likely due to lack of awareness of the vulnerabilities of open PNT services for tracking and tracing applications. The increasing concern about traceability of dangerous goods will probably trigger a need for more robust and secure capabilities.

Users equipped with PRS will benefit from the robustness of a PNT service anywhere and at any time, especially when the open signal experiences interference, hostile jamming or spoofing.

Energy, Telecom, and other Strategic Economic and Commercial Activities. In these domains, interest in PRS revolves around the timing and synchronization of networks and fixed ground systems or around space applications (Here, the adequacy of satellite technology in general needs to be investigated.) More information is needed from a few expert user communities in each domain.

The information from the user communities compares with a 2006 top-down survey of European Union member states regarding use of PRS that was conducted by the European Commission and presented at the first PACIFIC workshop. EU Member States were asked to indicate, for the nine application domains described earlier, whether use of PRS would be "most likely," "potential," or "not planned."

As of end of 2006, the highest rankings for "most likely" use of PRS appear in critical transport, emergency services, critical energy, and law enforcement, with between 35 and 47 percent posi-

tive answers. Use of PRS was deemed as "potential" for strategic economic & commercial activities, customs, defense, and internal security with between 60 and 69 percent positive answers. The total of both categories of answers show a global interest of more than 90 percent among EU member states for the identified applications.

The survey also provided information on the potential market for PRS, indicating that more than 80 percent of the total volume of PRS receivers would lie within agencies and organizations involved with defense, internal security, law enforcement, and critical transport. The survey indicated that, following the roll out of PRS receivers to users. there would be in the region of one million PRS receivers in operation.

Conclusion & Next Steps

PACIFIC's ongoing work highlights the necessary activities to be conducted in order to advance the introduction of PRS capabilities into user communities. Within the framework of the PACIFIC project, three activities are currently being carried out to support this objective:

- the refinement of the user requirements from the various application domains investigated, in particular, the expected performance requirements, the associated operational environment, and the integration constraints, as well as the market analysis
- the elaboration of the PRS technology development plan, including the identification, planning, and costing of the mandatory research and development activities to secure the availability of PRS core techniques and technologies
- the elaboration of an initial architecture for the provision of PRS, including the identification of associated organizations and interfaces to the end users.

PACIFIC will also provide the initial elements for the certification of PRS and the standardization of the related equipment. We expect that such activities will be completed in early 2008 by the PACIFIC project, which will eventually provide the basis for further work on the introduction of PRS into user communities. In the meantime, other elements of PRS development will be confirmed or undertaken, in particular the PRS access policy currently being finalized by the European Commission.

More information on the PACIFIC project and preliminary results on PRS can be found on the project's website: <www.prs-pacific.eu>.

Authors

Alan Kendall is head of Secure Navigation Services with EADS Astrium Services. He is currently the project manager for an EU project (PACIFIC) examining the user aspects of PRS. As he is British, living in Paris with a German boss, Kendall can claim some insight into complexities of life in Europe. Since graduating from Portsmouth Polytechnic with a degree in electrical & electronic engineering he has worked on a number of major UK defense projects (including the Skynet 5 PPP) before moving to the field of satellite navigation.

François Boullete has a diploma in engineering, with specialization in aerodynamics, from the French engineering school École Centrale. He also holds a master's degree in large projects management from the business school HEC, Paris (France). He is currently project manager in satellite navigation business development within EADS Astrium Services.

Alexis Vidal holds a specialized masters degree in project management from HEC School of Management, Paris (France) and originally graduated as an aerospace engineer from École Centrale, Lyon (France) and Imperial College, London (UK). He has been working on satellite navigation since he joined EADS Astrium Services in 2004, focusing on governmental applications and on the Galileo Public Regulated Service.

Pascal Campagne holds the position of CEO of FDC. He started his professional career in Dassault Electronique, followed by IBM, and has been responsible at the French Ministry of Defense for studies, development., and procurement of navigational systems and airborne computers. In the field of satellite navigation for 20 years and supporting PRS for the last 10 years, he is currently involved personally in several projects of the European GNSS Supervisory Authority dealing in particular with security, R&D, and international relations.

Since 2001 **Bernard Panefieu** has been responsible for the navigation strategy of Thales Avionics AME and the navigation product line manager for the Thales Aerospace division in France. From 1996 to 2001, he was the French representative in the GPS Joint Program Office hosted by the Los Angeles Air Force Base, California. Between 1990 and 1996, Panefieu was the head of the GPS and Navigation department in LRBA (Laboratoire de Recherches Balistiques et Aérodynamique) French technical centre of expertise for radionavigation. From 1985 to 1990 he and his team created the LRBA expertise on GPS and hybridization with inertial systems.He holds an engineering degree in mechanics and aerodynamics from ENSSEIHT of Toulouse. Panefieu obtained his master in mechanics at the Marseille Institute France. IG