Active Road Management Assisted by Satellite - ARMAS Phase II

PAULO GOMES,
ARMAS PHASE II TECHNICAL COORDINATOR, SKYSOFT PORTUGAL
JOÃO CANÁRIO,
ARMAS PHASE II PROJECT MANAGER, SKYSOFT PORTUGAL
PAULO ANDRÉ,
IT DIRECTOR, AUTO-ESTRADAS DO ATLÂNTICO
FIRMINO SÁ,
OPERATIONS AND MAINTENANCE DIRECTOR, LUSOPONTE

The ARMAS Phase II project is being developed under a European Space Agency (ESA) contract, and intends to prove the feasibility of an Intelligent Car Navigation System, based in Global Navigation Satellite Systems (GNSS) and Cellular Network (CN) technologies, that improve the safety of car navigation by an order of magnitude, make dynamic traffic management an attractive and realistic proposition and provide a competitive solution for Tolling based in Satellite Positioning.

This paper presents the overall objectives of the project, plus some conclusions from performed activities.

1.   INTRODUCTION

European Space Agency's (ESA) project "Active Road Management Assisted by Satellite" (ARMAS) aims at transforming the transport infrastructure (roads, bridges, tunnels and urban roads) into safer and more customer-friendly environments, by:

- Improving Safety;
- Increasing Dynamic Traffic Management capabilities;
- Providing Electronic Fee Collection mechanisms;

The project is divided in phases. The ultimate objective of the ARMAS Phase I project was to assess the feasibility of such a system, based in Global Navigation Satellite Systems (GNSS)

– especially EGNOS - and Cellular network (CN) technologies – GSM and GPRS, including issues like legal and regulatory aspects. The ARMAS Phase II project main goals are then:

- Implement an ARMAS Test-bed for advanced Intelligent Transport Systems (ITS) applications;
- To investigate the critical issues related to a successful introduction of Virtual Tolling using the above Test-bed, focusing on topics like reliability, integrity and fraud robustness.

The above mentioned goals will be translated in the implementation and demonstration of the following functionalities:

- *Electronic Fee Collection* based on Satellite Positioning (also known as "Virtual Tolling"), contemplating various road pricing models:
  o *Gatekeeper*: single tolling point (e.g. a bridge or tunnel);
  o *Corridor Pricing/Passage Tolling*: charges a fee for the use of a given section or road, bridge or turnpike.
  o *Congestion Zones/Cordon Pricing*: a fee is charged when entering into a specific area or cordon usually congested urban areas.
  o *Distance Based Pricing*: charges a fee related to the distance travelled along one or more roads.
  o Combination; various combinations of distance travelled, within a cordon, at a certain time, using a particular class of vehicle.
- *Warnings Provision*: provision of information about hazards ahead in the road to the driver of a vehicle, in order to increase the time-to-act;
- *SOS Request*: ability to request (and receive acknowledge) assistance upon an emergency;

The Project Logic and the associated activities covered, in line with the ESA requirements are:

- Investigation of user needs and related service and system requirements;
- Investigation of major system constraints through qualitative and quantitative analysis;
- System definition and design;
- Development of key new technologies;
- System implementation;
- Field demonstrations and dissemination activities;
- Analysis of results and future evolutions.

The ARMAS Phase II project consortium, lead by Skysoft Portugal, is also composed by two other software engineering companies (LogicaCMG from the Netherlands, and Mapflow from Ireland), Road Infrastructure Operators (Auto-Estradas do Atlântico, Brisa, Lusoponte), hardware manufacturers (SetCom and Delphi-Grundig), telecom companies (TMN and PT Inovação) and research institutes (IDMEC – IST and Fraunhofer Gesellschaft AIS from Germany).

2. THE ARMAS SYSTEM

At this stage of the project the system architecture and allocation of functions is still an open issue and subject to the outcome of various activities of the project. However, the basic definition and structure of ARMAS, with respect to the Electronic Fee Collection (EFC)

service, is illustrated in the following figure, which describes the organisational framework, roles and entities of a generic interoperable EFC[1]:
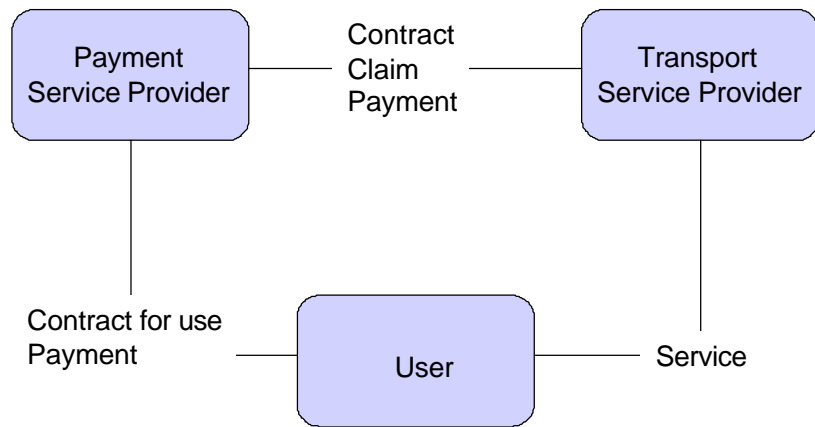
Figure 1: Basic definition and structure of the interoperable EFC service

The basic roles (actors) in this interoperable EFC service are:

- The User: uses the transport service and pays for it by means of a payment service offered.
- The Payment Service Provider (PSP, often called Issuer): is the entity responsible for the payment means.
- The Transport Service Provider (TSP, often called EFC Operator): is the entity offering a transport service to the User (e.g. toll road access).

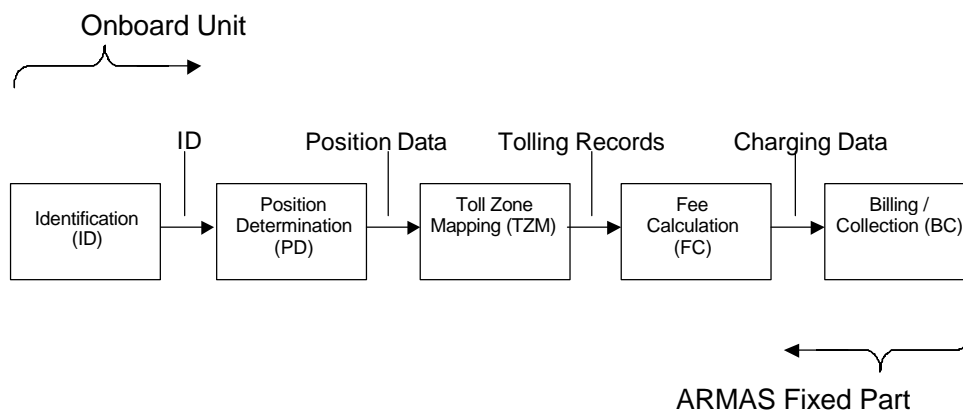The following figure below identifies the primary functions that are required for Virtual Tolling.

Figure 2: Primary process of virtual tolling

The description of the functions depicted above is provided bellow:

- _Identification (ID)_: Unique identification of the user. For example a DSRC tag contains in principle only user specific information.

---

[1] According to the CARDME architecture;

- *Position Determination (PD)*: Determination of the position of the vehicle. This may include input from GPS/EGNOS and functionalities like map matching. With, for instance, GSM it would be possible to determine the position of a vehicle from the road-side.
- *Toll Zone Mapping (TZM)*: Correlation of position data with toll zones and spots. Output of this function is for instance kilometres driven in a toll zone, passage of a toll spot, entrance of a toll area, etc. This may require a map that indicates the tolled zones and a time clock to be able to determine the time of the day, time in zone, etc.
- *Fee Calculation (FC)*: Calculation of due toll fees based on the stored toll related information. This may require input like the toll regime (generic toll scheme applicable to all users) and personal charging information (user specific information, vehicle class, exempt user, discount, etc). This may also deal with the exchange rates.
- *Billing Collection (BC)*: Payment of the due toll fee. This includes invoicing and payment via debit from a pre-paid account, post paid, or paid directly.

3. ASSESSMENT OF GNSS POSITIONING ISSUES

One of the key issues of the project is the use of GNSS Positioning. To better understand the actual behaviour of GNSS, field trials were performed in London using test vehicles equipped with a representative variety of device and sensor configurations. Trials were performed in a broad variety of environmental conditions, typical to this application (highway and urban areas).

Test vehicles were set-up to enable benchmarking of a range of commercial devices, thus enabling the leading combinations of the mitigation methods to be tested. Rather than testing a prototype device, the logic behind these field trials was to learn from the success or failure that other leading 'state-of-the-art' GNSS technology companies have been able to achieve.

This bench marking set out to satisfy two objectives:

1. Identify weaknesses in the concept of using GNSS devices for road tolling and take account of such weaknesses in the design process for the ARMAS prototype development;
2. Provide benchmark results for qualification of the test results from the ARMAS prototype once it has been developed.

Based on millions of observations collected in the field trials, a detailed analysis of the properties of the available "onboard unit" (combination of GNSS device and onboard sensors) was performed. This analysis focuses on various aspects that are considered to be important for the setup of a fault tolerant virtual tolling system.

The analysis approach leverages a standard RNP methodology, and set out to focus on a number of topics including:

- Limits and requirements for precision of:
  - Position and trajectories collected by the onboard unit;
  - Precision-to-road-map algorithms used in the onboard unit;
- Availability, for these optimal mixes of receiver technologies, as a function of geography and terrain properties (country side, towns, highways);
- Integrity of the information provided by these commercial device technologies;
- Ability for the leading technologies to provide adequate continuity of service, for a given level of accuracy and availability.

Following the analysis work outlined above a more detailed analysis was performed for the "urban area", where performance is thought to be most critical. Using this methodology, the following Accuracy findings where identified taking into account all the devices used in the field trials:

Average Error	Min Error	Max Error
10.40	0.00	603.82

Table 1: Field trials Accuracy findings

We found that while the average accuracy (10.40m) is not huge, five of the six devices exceed this average error. One particular telematics product, with an average error of 8.79m, counterbalanced poorer performance of the other devices. The average accuracy for most of these devices does not follow a normal curve. Many observations exceeded 150m error. The fabled telematics product did not suffer to the same extent from these outliers.

We also found that there were significant variations in average accuracy across the geographies within London City. The points in the North West of the study area (Nottinghill) provided an average accuracy of 8.61m. The 'City' of London, to the East of the study area provided an average accuracy of 12.44m, with a modest variance. While in the Victoria area of London provided an average accuracy of 28.03m with a large variance.
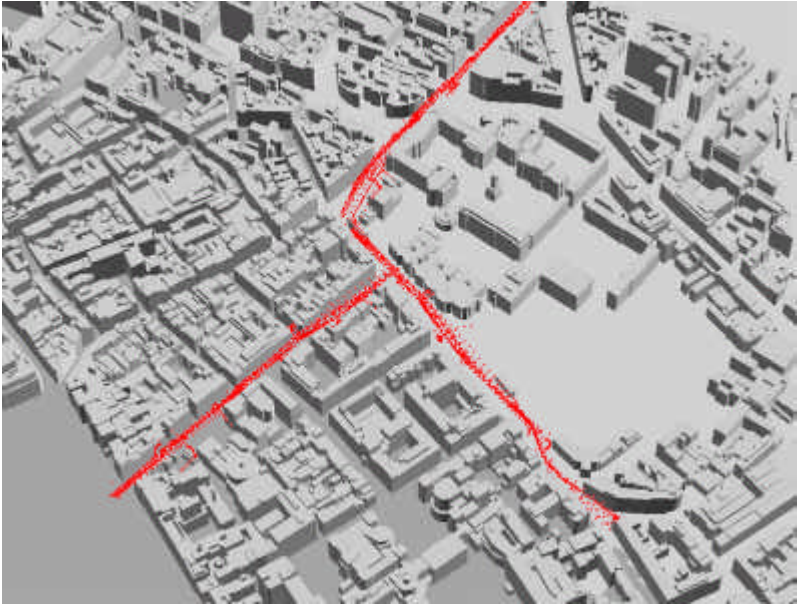

Figure 3: Analysis of error with respect to environmental conditions.

In summary, while the overall accuracy may be encouraging, the nature of the London City environment appeared to cause significant variations in Accuracy, from one device to the next.

Based on the multitude of observations of device accuracy, we were also able to build up an empirical understanding of device performance. Taking all observations made during this analysis, we identified that that 75% of the readings fell within 8m of the vehicle's actual location, 95% fell within 20m and 99% fell within 40m. From this empirical model we can determine the number of readings required in an area to provide a given level of confidence that a vehicle is present.

Analysing the road layout (in a rudimentary fashion) we found that many areas within London City have similar roads within the 20m and 40m radius required to be 95% and 99% confident respectively.

By taking the time duration (seconds) between each acceptable location report (position report with acceptable accuracy), for each device independently, we have been able to understand the Continuity of typical GNSS devices. This measure provides an indication of the typical time periods where interruption may occur.

Accuracy Required (metres)	Average Duration (seconds)	Min Duration	Max Duration
8	1.69	1.00	301.00
20	1.50	1.00	423.00
40	1.47	1.00	417.00

Table 2: Typical duration of interruption for Accuracy requirements

The most profound effect of loosening the accuracy requirements is in frequency distribution of these readings. With an accuracy requirement of 8m, these devices require 1 second, 3.5 seconds and 23 seconds to be 75%, 95% and 99% confident that an accurate reading will occur within the duration. Loosening this accuracy requirement to 20m or 40m means that only 4 seconds are required to be 99% confident that an acceptable reading will occur.

It became also apparent, by mapping these results geographically, that continuity varies across the geography of London City. Some Run Segments provide an average continuity of around 1 second to achieve 8m accuracy, while others typically require 5-10 seconds to achieve 8m accuracy.

4. INTEROPERABILITY, STANDARDISATION AND SECURITY

When multiple instances of items have to cooperate interoperability becomes an issue. This is especially true when these items are in the scope of different organisations. In those circumstances it would be beneficial if the agreements that enable interoperability could be formalised, thus become standards. There are two reasons for interoperability:

- Business reasons: interoperability might result in more income and/ or less costs for the parties involved;
- Legislation, Authorities require parties to become interoperable.

Experience in the toll collection field has shown that interoperability is hard to achieve. If standardisation is proposed without taking in account the existing situation, both technical and organisational, this will result in a major hurdle towards interoperability. Without a clear prospect on return on investment most organisations will be very reluctant to change their technical and/or organisational situation.

On the other hand new developments do exist. These new developments should be standardised in such a way that at least coexistence with the existing situation is enabled. And ideally a gradual migration from the existing towards to new should be enabled.

Having in mind what is stated above, the review performed resulted in the identification of around 40 plus recommendations/system constraints for ARMAS. Some examples of these recommendations are:

- *Recommendation 2*: It is recommended to follow the FRAME recommendations with respect to standardisation and interoperability where possible and practical;
- *Recommendation 3*: It is recommended to be compliant and interoperable with the CESARE project;
- *Recommendation 4*: In general it is recommended to be compliant, at least to follow the progress, of the projects related to the "Emergency Request" functionality namely E-merge, eSafety and LOCUS.
- *Recommendation 5*: The Onboard Unit shall be interoperable and thus the interface between the Onboard Unit and the roadside shall be standardised. This should result in an Onboard Unit that can be provided by multiple suppliers and used by road users when travelling through the different concession areas.
- *Recommendation 10*: For representing information to the driver it is recommended to take into account the standards EN-ISO 15008 and the EN-ISO/CD 15006-1.

5.   FRAUD ROBUSTNESS AND PREVENTION ASSESSMENT

Fortunately many humans are law obedient and follow regulations. Unfortunately there are also people that have different principles. These people will use any system's weaknesses to their benefit. The most obvious example in the case of ARMAS is to avoid paying tolls.

For this reason, virtual tolling is the most important and obvious subject in reviewing the ARMAS robustness. The money that is involved with this will seduce many to attempt to fraud the system.

The fraud risks can be grouped into internal and external risks. The external fraud risks are related to the people that will attempt manipulate the system to pay no or less tolls than they ought to. The internal risks are related to the people who operate the system.

Also various forms of vandalism should be taken into account. Undoubtedly some people will attempt to disturb or manipulate the functioning of the system. This does not necessarily have to be related to an attempt to fraud. Every one knows the examples of hackers and the virus makers on the internet.

The attempts to fraud or vandalism can also have consequences for the road safety. By interfering with the virtual tolling functionality, the warnings provision and the emergency service functions can also be disturbed or otherwise negatively influenced.

Besides interference through fraud or vandalism related to virtual tolling, some people could influence the warnings provision or emergency service functionality directly for reasons of vandalism. An example is to create unsubstantiated warnings or SOS requests causing chaos.

No matter what the reason is, whether fraud or vandalism, it brings high costs and a possible negative effect on the road safety. Knowing that the potential market for road charging in Europe is many billions of Euros, every percent of loss of revenue represents a serious amount of money. One may not forget that not only fraud but vandalism also causes a loss of income to the operator.

There are also legal reasons to prevent fraud. The equality of citizen may not be compromised by the vulnerability of the system. For that reason fraud robustness shall be a leading aspect in the system design of ARMAS.

A system that is totally fraud proof is either practically impossible or really expensive to commit fraud. The system is allowed to have some weak spots as long as attempts of fraud or vandalism can be detected and the violators can be enforced. Most road charging schemes in Europe operate a combination of fixed enforcement equipment and mobile teams that randomly verify the correct functioning of the in-car devices.

Fraud robustness is inextricably connected with enforcement mechanisms. As attempts to fraud the system can never be completely ruled out, enforcement schemes have been set up to discourage potential frauds and to discover fraud attempts.

Enforcement is realised through a combination of fixed road-side based enforcement equipment, portable enforcement equipment that can be positioned at varying locations, mobile enforcement teams that flow with the traffic and a range of ICT measures related to network and system security.

In the end we found that, the inherent functionality and architecture of the ARMAS system introduces a number of risk factors. The impact and likely hood of the risk factors have a strong relation with the design choices. Particular attention shall be paid to the system aspects in the list below during the design of the system.

- Interfaces;
- (Security) Key management procedures;
- Software and data integrity;
- Integrated platform;
- Flexibility to (functional) changes;

The "fraud robustness and prevention assessment" that was performed resulted in the identification of several recommendations/system constraints for ARMAS. Some examples of these recommendations are:

- _SR.0001_: The ARMAS system shall not rely on the satellite system as a sole source of position location or precision timing;
- _SR.0002_: The ARMAS system shall have backups for positioning and precision timing for all GNSS applications involving the potential for life-threatening situations or major economical or environmental impacts;
- _SR.0003_: The Onboard Unit should have a DSRC interface that enables local interrogation by road-side equipment for the purpose of:
  o Verifying the correct functioning of the Onboard Unit (to be used by e.g. enforcement agency);
  o Verifying the Identification (ID) stored on the Onboard Unit (to be used by e.g. TSP);
- _SR.0005_: The Onboard Unit shall be physically sealed to ensure that physical tampering with the Onboard Unit can be discovered by visual inspection.
- _SR.0006_: The ARMAS system shall have a secure interface for data communication between the ARMAS Fixed-Part to the Onboard Unit;
- _SR.0007_: The ARMAS system shall require for reading _User Public data_, altering all data or updating software in the Onboard Unit:
  o Authentication;

- o Authorization; and
- o Encryption;
- _SR.0009_: The Onboard Unit shall not solely rely on the vehicles power supply and be able to function on its own battery back-up for a minimum of t.b.d. number of days.
- _SR.0010_: The Onboard Unit shall not loose any data when there is no external power supply (from vehicle) for a period of t.b.d. number of years.
- _SR.0011_: The enforcement concept shall encompass mobile enforcement units that can interrogate the Onboard Unit on its correct functioning by means of DSRC. The Onboard Unit is not functioning correctly when the Onboard Unit log as defined below indicates an attempt of fraud.
- _SR.0012_: The Onboard Unit shall log possible attempts of fraud, including:
  - o No receipt of GNSS signal for more than t.b.d. number of minutes;
  - o No receipt of data of other vehicle's sensors for more than t.b.d number of minutes;
  - o Discrepancy between GNSS data and other sources (Gyroscope, tachograph, etc);
  - o Attempt of accessing the system where the authentication or authorisation failed;
  - o Failed attempts of connecting to the back-office;
  - o Failure of the vehicles battery for longer than t.b.d. number of days;
  - o Occurrences of altering of the data in the Onboard Unit;
- _SR.0013_: The Onboard Unit shall report a mal-functioning to the driver.

6. IMPORTANCE OF THE USE OF EGNOS

The following service differentiators of EGNOS have been identified and are important in the scope of the ARMAS Phase II project:

- Accuracy: EGNOS provides wide area differential corrections that improve significantly the positioning and timing accuracy provided by GPS. The accuracy level generally obtained by GPS is in the 5-10m range but not guaranteed. Results from the EGNOS System Test Bed are already in the 2-3m range, which promises direct benefits to all users. Though the accuracy and alarm limits required for the various ARMAS functionalities have to be defined as part of the investigation of system and service needs, it is clear that the accuracy provided by EGNOS is a key issue and a major requirement for providing those functionalities;
- Availability and Integrity: In the specific case of Virtual Tolling (but also for the other functionalities), system availability and integrity is a key issue since service breakdowns or malfunctions have severe implications on the charging and revenue collection mechanisms. EGNOS ensures that the most stringent accuracy and integrity performances are available for most of the time;
- Certification: EGNOS will meet international standards against which they will be certified. This on the other hand, will allow systems like the one proposed for the ARMAS Phase II project, to "build" their safety case on top of this certification;
- Area Coverage: EGNOS will provide a single, seamless service over Europe. This characteristic will allow that a system be developed targeting the whole of Europe and not only a specific country or region.

REFERENCES AND BIBLIOGRAPHY

[1]: European Space Agency – "Intelligent Car Navigation System Using Advanced Global Navigation Satellite Services (GNSS) Statement of Work". Reference "TOS-ETT/2001.34/AG" – Date: 15 March 2002.

[2]: ESA Navigation Satellite Applications Web Site (http://www.esa.int/esaNA/index.html).

[3]: European Satellite Services Provider (ESSP) Web Site (http://www.essp.be).

[4]: ARMAS Phase I Consortium – "D1.12 – Initial Feasibility Report on ARMAS". January 2004.

[5]: Mapflow – "Feasibility Study into linking Vehicle Positioning Systems to Virtual Toll Areas". December 2003.

[6]: ARMAS Phase II Consortium – "D2.1.1 – User Requirements". July 2004.

[7]: ARMAS Phase II Consortium – "D2.1.2 – System and Service Requirements". August 2004.

[8]: ARMAS Phase II Consortium – "D2.2.1 – Assessment of GNSS Positioning & GI Issue". September 2004.

[9]: ARMAS Phase II Consortium – "D2.2.2 – Assessment of CN Communications Issues". September 2004.

[10]: ARMAS Phase II Consortium – "D2.2.3 – Standardization, Security, Interoperability Review". September 2004.

[11]: ARMAS Phase II Consortium – "D2.2.4 – Fraud Robustness & Prevention Assessment". September 2004.

[12]: ARMAS Phase II Consortium – "D2.2.5 – System Scalability Mechanisms Assessment". September 2004.