VIENNA 2018 TRA
TRANSPORT RESEARCH ARENA
A digital era for transport
solutions for society, economy and environment

Proceedings of 7th Transport Research Arena TRA 2018, April 16-19, 2018, Vienna, Austria

Towards Intelligent Mobility: The Mobility Intelligent Cooperative Systems (MOBICS) Platform

A. Luis Osório[a], Lara Moura[b *], Rui Costa[b], Paulo Borges[a]

[a]*ISEL - Instituto Superior de Engenharia de Lisboa, Instituto Politécnico de Lisboa, and POLITEC&ID, 1959-007 Lisboa, Portugal*
[b]*A-to-Be, Lagoas Park, Edifício 15, Piso 4,*
2740-267 Porto Salvo, Portugal

Abstract

Intelligent Mobility (IM) is a growing development area challenging an integrated management and operations of diversity (heterogeneous) of both cyber-physical and informatics (systems) infrastructures. The approach that has been taken by A-to-Be, powered by Brisa in the SCOOP@F Part 2 project on developing cooperative systems assuring the interoperability among different road operators and across borders, based on vehicle to vehicle/infrastructure (V2X) communications, is presented and discussed. The project is challenging making transparent the specificities of the involved stakeholders for drivers from Portugal, Spain, France, and Austria to freely travel multi-concessions and multi-country road infrastructures under a continuous offering of a suite of mobility services. This requires, beyond a proper operation of the On-Board Units (OBU), an efficient coordination among the participating road operators' infrastructure (stakeholders). Collaborative models where stakeholders with different technologies, processes, and organizational culture are invited to participate is also discussed.

Keywords: Cooperative Systems, Cyber-physical and Informatics Systems Integration, Collaborative Networks, Informatics Systems Security.

* Corresponding author. Tel.: +351-214-233-418
E-mail address: lara.moura@a-to-be.com

1. Introduction

With the increased demand for safety, vehicles tend to be always connected as cooperative autonomous mobile systems. In this way, in the very near future, vehicles will be ready from the factory (and enhanced with onboard units for legacy vehicles) to interact directly with each other and with the road infrastructure. This is crucial to improve road safety, traffic efficiency and comfort, helping the driver to take the right decisions. Such endeavor has been pushed by the EU Directive 40-2010 "*on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport*" (Directive 2010/40/EU, 2010) while a suite of European level strategy policies. Nevertheless, the endeavor is challenging considering that the required intelligence need cooperative systems and further well-coordinated informatics systems managing the needed business collaborations among stakeholders with their own technology and processes culture. One main challenge begins inside each stakeholder with their own difficulties to establish an integrated informatics systems landscape (informatics system means a system which elements are mainly computational components involving data management, processes enactment, from other computational responsibilities, usually mentioned as a software system, enterprise application and so forth). Another no less easy challenge is to make such heterogeneous stakeholders to coordinate common business processes, known as collaborative business processes, itself a complex endeavor (Osório & Camarinha-Matos, 2008). The Mobility Intelligent Cooperative Systems (MOBICS), centrally explored in the paper is being designed and prototyped under the Informatics System of Systems framework proposed as a strategy for the integration of the computational responsibilities, the Informatics systems (I-systems) of an organization (Osório, Belloum, Afsarmanesh & Camarinha-Matos, 2017).

Beyond the specific computational responsibility to manage and coordinate the V2X network, the role of a Cooperative Central System is the communication management between vehicles and road infrastructures as crucial for a successful information sharing and traffic events management. In fact, more data exploiting channels are envisaged considering vehicles are becoming intelligent, and nomadic systems prepared to interact with infrastructure, e.g., automatically entering in a parking lot based on its identification (already deployed by Brisa/Via Verde Portugal since 2005). Being vehicles so autonomous and always connected the question is if car manufacturers will take the leadership of the vehicle data interactions. It is a fact that some manufacturers already track (and remotely monitor) their vehicles under an assistance contract making them sources for rich data from their mobile vehicles potentially used as probe data mobile elements. However, like the mobile manufacturers are not the exclusive users and managers of the rich probe data from mobiles neither do are telecoms, the same is expected for the always-connected vehicles. Many service providers in different contexts and under different regulation agencies (mobility, customer quality assurance, communications quality, payments security, and liability, etc.) will be responsible for regulating and certify service providers, in some cases the same entity offering a suite of services under a unique brand (integrated services), e.g., Via Verde payment services. In any case, when a vehicle enters an area of the responsibility of a highway or bridge concessionaire, it is the responsibility of the traffic management center to coordinate the traffic and the communication with vehicles, what is of paramount importance to improve driving safety and comfort. When in (ACEA, 2016) is written that, "Vehicle manufacturers are prepared to make vehicle-generated data available for third-party services" it must happen on the decision of the owner and according public policies regulating how the data is accessed for added value services the owner subscribe, like stated in the same position paper from ACEA[2] "*Except where a legal requirement or a contract exists, personal data will be made available to service providers only with the consent of the vehicle user. Service providers shall use this data only for the purpose(s) for which the vehicle user gave his or her consent*". This paper, while centered on traffic management and road safety through the well-discussed cooperative systems, is also a contribution for the normalization of the onboard computational responsibility, as a node of a more complex network. Such network, depending on user decision and an open competitive market for the growing integrated services, is expected to involve a chain of stakeholders with complementary responsibilities in what is being researched as collaborative networks. One important contribution from the collaborative networks research area is the study of a symbiosis of cyber-physical systems and the Internet of Things towards a generalized digitalization (Camarinha-Matos, Fornasiero & Afsarmanesh, 2017). Such digitalization needs further research able to establish a web of stakeholders (a collaborative network) coordinated on managing the business processes underlying the new offered integrated services.

Therefore, the innovative A-to-Be traffic management solution implemented in Brisa (ATLAS) is responsible for managing traffic events and process incidents. This I-system cooperates with the MOBICS that has the

[2] ACEA, European Automotive Industry Association

responsibility for the management of data exchanges between road infrastructures' equipment, Road Side Units (RSUs) and vehicles' On-Board Units (OBUs). A huge number of messages originated from OBUs and crossing RSUs, as well as the mechanisms to broadcast or multicast traffic information messages to selected targeted OBUs is managed by the MOBICS platform. One main concern has been to establish a standard modular computational responsibility able to reorganize the current monolithic and closed approaches into an open technology landscape. The endeavor is difficult considering the panoply of middleware technologies from CORBA/DCOM to the more recent SOAP/REST web services and distributed frameworks, however without a known convergence for a generalized interoperability among heterogeneous products. Such heterogeneity generates technology dependencies (vendor-lock-in) and is an obstacle for the required generalized interoperability between systems from different technology cultures. This concern is not common for cyber-physical and informatics systems developers but is considered as strategic for A-to-Be as a proactive investment in an open system of systems. Beyond this more strategic endeavor, each I-system is developed putting on the edge quality and adaptability concerns. One example is the adoption of a differentiating dynamic configuration based on a rules engine based on the standard Decision Model and Notation (DMN) (OMG-DMN, 2016). The adoption of rules engine has the following advantages:

- Provide real-time decision-making;
- Offer robustness and effectiveness;
- It is less dependent on mistakes;
- Present dynamic adaptability capabilities based on its configurable feature.

In addition, human intervention in operation actions is less prone to mistakes considering there is no need to know where the RSUs are located or which RSU sent an alert message. The traffic management center operator only triggers the alert for the specific location (kilometer) and the rules engine automatically identifies the RSU that should disseminate the message. In this sense, critical messages that come from OBUs through the RSUs or warning messages from the traffic management center can be analyzed and processed by the intelligent decision engine. It makes possible informed immediate decisions about which RSU will disseminate the warning message, in order to advise drivers about potentially dangerous situations. In addition, dissemination via smart gateways occurs, as these devices can receive the information from the traffic management center and send it to the proper RSU, as well as it can receive information from the RSU and redirect it to the traffic management center.

The adoption of an open architecture makes possible for the central system to cooperate with other central systems or with an access point for sharing the information about the events that are close to specific locations. The coordination between different concessionaires is crucial for the improvement of traffic management and assure a transparent dissemination of the messages when vehicles cross concessions and country borders. The central system is then able to exchange information with other platforms, in a direct way or through a common access point, allowing a more efficient operation. Common access points are commonly implemented at national level, in order to guarantee the flow of information between different road operators.

The MOBICS platform is being tested under the European project, SCOOP@F Part 2, being able to assure the interoperability between the different road operators and also across borders, assuring V2X communications in Portugal, Spain, France, and Austria.

In chapter 2 a discussion on requirements for the cooperative systems and the more ambitious collaborative business processes management on offering to European drivers' transparency in relation the infrastructure they are crossing is presented and founded. In chapter 3, the Mobility Intelligent Cooperative Systems (MOBICS) is presented and discussed. Some preliminary results from the running prototype are shown and discussed. In the last chapter 4, conclusions and further challenges and research needs are presented and discussed.

2. Intelligent Mobility and Systems Requirements

The concept of intelligent mobility has been discussed associated with the growing potential of communication and computing, from many other facilitators (North, Worsley, Bradley, Neffenforf & Fletcher, 2015). However, such facilitators brought new integration challenges (as a challenge ahead of interoperability) for both processes and organizational modeling and technology infrastructure and systems. The intra-organization processes and more recently the fast scaling collaborative business or "*of inter-enterprise collaborative processes*" (IBM, 2008) establish a complex web of heterogeneous technical systems difficult to support under a sustainable lifecycle management setup. In fact, technical systems from collaborating stakeholders need to interoperate and to coordinate events and actions under different technology cultures. This means that the current "adapter" approach needs to be reconsidered by developing more semantic level normalization efforts. This means that the upcoming cyber-physical (onboard systems, sensors), infrastructure (switch, routers, roadside units) and informatics systems (enterprise back-office systems, financing applications) need to cooperate following a dynamic adaptability (plug-ability) strategy. This is a complex challenge for both business and technology requiring the contribution from complementary knowledge bodies for the design of new business, and technology strategies (architectures). The Informatics System of Informatics Systems (ISoS) framework (Osorio, Belloum, Afsarmanesh & Camarinha-Matos, 2017) is a scientifically founded proposal in this direction. Such multidisciplinary (or multiple knowledge bodies) for the development of integrated system of systems (SoS) is an ambitious endeavor guided by the proposed substitutability principle that states that any Informatics System (I-system), while a computational responsibility has one or more equivalent I-system from a competing supplier able to replace an operating informatics system with equivalent features and quality. Even if not a standard so far, the ISoS framework under previous partial approaches proved to be grounded on validated results. The Portuguese national speed enforcement network (SINCRO project) is being developed under such multi-supplier (and substitutability) principles. The cabinet and the cinemometer (radar) system, both of cyber-physical systems and the back office I-system were designed to be independent of a specific supplier.

Nevertheless, the problem is not only at cyber-physical neither at infrastructure levels. If we imagine a Portuguese driver to park his/her car in a parking lot, e.g., in Paris with the same payment service he/she already has for long in Portugal, the payment with Via Verde initially exclusively a multi concession toll payment and later (from 2005) an integrated payment services company (tolling, parking lot, gas stations, McDonald drive-in, from other services under a single brand). This has been establishing novel challenges on how to promote a convergence of technical infrastructures of the responsibility of different stakeholders with different technical systems (from suppliers adopting their specific models and implementations). The A-to-Be company was one of the first tolling technology and cyber-physic/informatics systems to adopt a service-oriented Electronic Toll Collection (ETC) system under the condition the Road Side Unit, the Dedicated Short Range Communication (DSRC) antenna to operationalize vehicle identification, through an On-Board Unit based on CEN/TC-278 standards suite (Gomes, Jacquet, Machado, Osório, Gonçalves & Barata, 2003).

In the first decade of the current millennium, many standardization efforts were under development targeting a technology unification, e.g., from the CORBA normalization efforts, the adoption of a common model for informatics systems from the cyber to the enterprise levels can't be exclusively conditioned by market dynamics. The industry and scientific community have to recognize that the validation of some formal models didn't consider all the variables of the real world. The example of the relative unsuccessful experience with CORBA, as argued by many technical and scientific publications, was on the adopted strategy to unify general and complete models for the development of informatics systems without a clear leadership from end-organizations. Instead, the CORBA dynamics has been led quasi in exclusion by informatics-organizations, what unbalance the business interests in favor of a common technology landscape. It is quite interesting to read from (Campbell, Coulson & Konavis, 1999) on the one hand that middleware is the key to avoid the distribution systems nightmare and at the same time recognize that DCOM "*Being a closed specification maintained by only one company has one major advantage: DCOM has the potential to evolve at a much faster rate than CORBA because there are no time-consuming politics involved in generating the next version of the specification*.". In fact, beyond a steep learning curve, a failure to CORBA Component Model (CCM) get industry adoption and at the end of 90's the fast growing of Web/XML are some of the justification for the failure of this tentative for a unified distributed systems infrastructure (Henning, 2016). More than fifteen years later we have to recognize that no formal model was robust enough to succeed so far to promote a truly open informatics system (I-system) and open informatics system of informatics systems (ISoS).

This means that, in spite of the many industries and scientific community efforts, there is a need to "rethink" the upcoming truly cooperative systems, not only at the roadside but also at the different levels of the involved organizations. It is why the research on Collaborative Networks (CN) that has been undertaken by the scientific and practice communities is of paramount importance to achieve a common understanding of such fast emerging complex business and technical web arrangements (Camarinha-Matos, Fornasiero & Afsarmanesh, 2017). When we challenge Smart Cities, more than advanced traffic management, we expect a sustainable city digitalization where citizen access services from mobility to entertainment in an integrated and consistent way. Furthermore, citizen expects from regulating agencies that business competition at all levels exists making such integrated and high-quality services moderated by equivalent market offerings. This is, however, a key challenge for the future since the cyber-physic system (CPS), and the informatics systems (I-systems) are lacking standards coping with a generalized need for systems to interoperate. The state of the practice has been happening based on adaptation efforts in many cases with additional costs and additional operational risks. The existing governance models are not prepared to cope with independent responsibilities of technology landscapes based on multiple suppliers. In most of the cases, a unique integrator establishes the technology landscape that copes with the established requirements leading to closed (specific) integrated technology setups with the well-discussed technology dependence, or vendor lock-in problem. A-to-Be, formally known as Brisa Innovation and Technology, has been from its inception concerned to this problem, which is why its technology systems have been designed for open, collaborative scenarios, where dynamic adaptability is of paramount value.

Furthermore, the more recent C-ROADS Platform[3] as an open initiative co-founded by the European Commission, beyond C-ITS, towards Connected, Cooperative and Automated Mobility (CCAM) (C-ITS Platform, 2017), establishes challenging requirements for the governance, for the enforcement of public policies, and for the complex networked technology systems lifecycle management. More than interoperability, there is a need to establish a collaborative platform where business stakeholders can openly join (dynamic plug-ability) without the need to adopt a specific adapting technology system. Such dynamic plug-ability shall make possible for a stakeholder to more easily integrate the intra-organization informatics systems making this way agile and reliable the management of events or transactions in such a complex business network. When a Portuguese driver enters to a parking lot in some neighborhood in Paris, the payment service should work seamlessly even if some cooperating subsystem fails for some unexpected reason.

In the next chapter, the Mobility Intelligent Cooperative Systems (MOBICS) that is being developed under the European project SCOOP@F Part 2 is discussed under this dynamic "*integrability*" concerns. The discussion while centered on both cyber-physical and informatics technology approach, it also discusses the need for road and traffic operators (concessionaires) from different countries to collaborate. This means that the business models need to evolve accordingly. The vision of a Portuguese citizen driving to Paris and get a public parking lot somewhere in a mobility hub where she/he leaves (parks) the car and travel around the city using public transports or a rented electric vehicle, paying every service with a unified business contract (using her/his mobile), e.g., the Via Verde payment service, is a great technical and business challenge.

3. The MOBICS Architecture

The Mobility Intelligent Cooperative Systems (MOBICS) is a computational responsivity (an I-system) targeted for the management of event messages coming from OBUs through one or more RSUs or directly through the 3G/4G network; if an RSU did not coordinate possible message repetitions, based on multiple OBU reachability, from the same OBU. It is also responsible for generating C-ITS messages based on a suite of business rules implementing selected message standards. The decision about selected messages answering to specific events is based on a rule engine interpreting rules defined based on the Decision Modeling and Notation (DMN) standard (OMG-DMN, 2016). The received, and delivered messages are formatted as Constrained Application Protocol (CoAP) standard and can be or Cooperative Awareness Message (CAM) or Decentralized Environmental Notification Message (DENM). However, as CoAP is not an ETSI ITS standard, the adoption of DATEX2 is being considered. The adopted message formats follow the ETSI European Standards for Intelligent Transport Systems (ITS) EN 302 637-2 (specification of Cooperative Awareness Basic Service), and EN 302 637-3 (specification of Decentralized Environmental Notification Basic Service). The MOBICS is an informatics system (I-system) responsible for presenting to the Traffic Management Centre (TMC) a suite of services making possible for operations room users to manage traffic events, as depicted in Fig.1. This interface is an open specification considering that different TMC products shall be able to cooperate with MOBICS.

[3] www.c-roads.eu

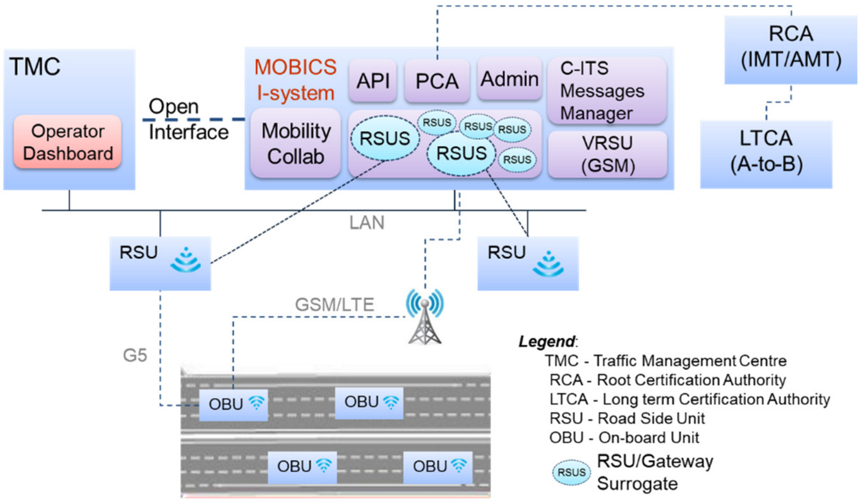

Fig. 1 The general architecture of the MOBICS system framed related to the TMC I-system and road elements

While complying with the standard, MOBICS adopts a service-oriented approach where a specialized message dispatcher, based on a flexible and adaptive rule-based mechanism, and on protocol processors (at different layers), establish the basis for an agile business cases management and operation.

A huge number of CAM messages will arrive at MOBICS platform, pointing the position of a certain vehicle. This information is very important to warn only the right vehicles on incidents that are occurring in a specific location, either through the RSUs with ITS-G5 (802.11P) or directly the OBUs, through the 3G/4G network. Every time the OBUs enter a covered area by the ITS-G5, its 3G/4G interface is disconnected, being the communications only held via ITS-G5 to the RSUs and from these to the platform. Advertising services will be used in the RSUs to alert the OBUs that they are in an area covered by ITS-G5. The central platform then monitors in real time all the OBUs that are in the non-covered area by ITS-G5, through the reception of its CAM messages.
While the cooperative systems concept has been centred in the context of vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) context, the proposed challenge for the development of a central system, suggests the span of the discussion to the (enterprise) distributed systems and the more recent system of systems discussion associated with the flowing complexity of technology landscapes. It is complex to manage a network of distributed roadside equipment (while playing a gateway role with a number of potential added value and fundamental services for a motorway operation).

Therefore, MOBICS has been designed and validated under the technology dependency constraints considering they are an obstacle to sustainable innovation processes. By sustainable innovation processes, we mean the promotion of innovation processes without constraints on adopting the most valuable market competitive solutions. This brings us to the need to develop an open system of systems where any subsystem of such an (informatics, usually identified as Information Technology - IT) system of systems shall be supplied by at least two competing suppliers. The FIWARE initiative is one example addressing this complex research question by introducing the substitutability principle that is operationalized by the Generic Enabler (GE) concept (Fernandez, Santana, Ortega, Trujillo, Suarez, Dominguez, Santana & Sanchez, 2016). This, in turn, throws the modularity of informatics systems into a priority discussion.

As a contribution from A-to-Be to such an open technology landscape, it was decided the development of an Open Cooperative Intelligent Transport Systems (OCITS) as a reference concept for the Mobile Intelligent Cooperative System (MOBICS) I-system. It is proposed on the assumption that the MOBICS product will be not a unique implementation but rather a conforming implementation of the reference standard OCITS specification. In Fig. 2 a subset of the Stakeholder's informatics systems is depicted adopting the ISoS framework (A. Luis Osorio, Adam Belloum, Hamideh Afsarmanesh, and Camarinha-Matos, 2017). In such a framework a kind of meta-informatics system is responsible for managing the other systems. Systems integration is based on an adaptive coupling infrastructure, making the mentioned TMC and OCITS and the head referenced ECoM I-systems dynamically plug-able.

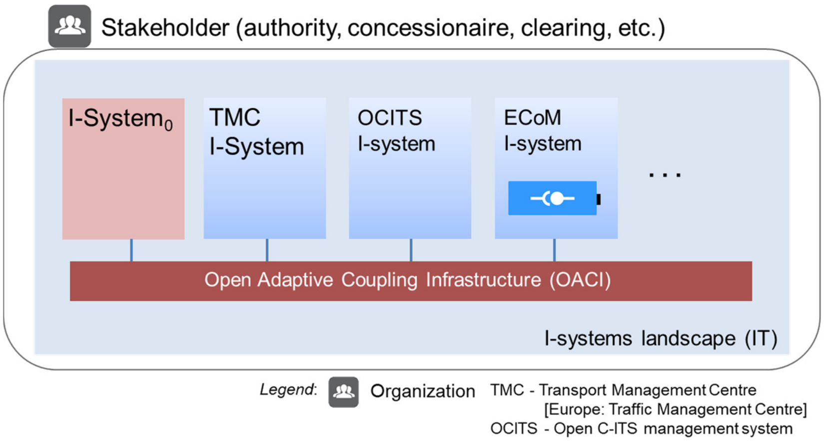

Fig. 2 The ISoS framework structuring the Informatics Systems Landscape of a network Stakeholder

The MOBICS implementation is being used to validate the approach and from it to derive the generic concepts (implementation independent) that will integrate the reference OCITS. This means that if a standards definition consortium is founded to develop the OCITS open specification and conforming procedures, the Stakeholders will be free to adopt the most compliant product for this specific computational responsibility. An orthogonal initiative is being developed motivated by the diversity of development cultures and tools named Enterprise Collaborative Development Environment (CEDE) (Osório, 2016). It aims at making possible a streamlined collaborative among heterogeneous and distributed teams and companies cooperating for common designs and developments. An initial prototype of the CEDE platform is hosted at ISEL (a research partner of A-to-Be company) and is being used (accessed) by A-to-Be development teams to assess research achievements and for research contributions.

In answering requirements discussed in chap.2 an additional challenge for Intelligent Mobility is the need for a network of stakeholders to make their informatics systems to cooperate, i.e., exchange or share data and coordination information considering the communication channels and insecure, that are prone to failure. Existing approaches establish complex adaptation systems difficult to maintain and evolve. Beyond the already discussed ISoS framework, the answer to such complex web of relationships established by the Intelligent Mobility services, the Enterprise Network Collaboration Network (ECoNet) framework is being evaluated (Osório, Camarinha-Matos & Afsarmanesh, 2015). In a simplified definition, the Enterprise Collaboration manager (ECoM), initially depicted in Fig. 2, is, in fact, the formalization of the diversity of adapters for specific semantic exchanges, in the proposed model operationalized by the Collaboration Context (CoC) concept. For example, imagine a scenario that considers Brisa (Portuguese concessionaire), a Mobility authority, and other concessionaires represented by others. In this scenario, all the stakeholders have installed an implementation (a compliant product) of the ECoM I-system configured with an instance of the collaborative context CoC_{OCITS}. With the proposed approach, each stakeholder, private or public is expected to be free to adopt a compliant implementation (product from competing suppliers) of a standardized I-system.

Therefore, the MOBICS I-system cooperates with the TMC under a specific computational responsibility of managing message exchanges and sharing in the context of the cooperative systems, as shown in Fig. 2. In Fig. 1, is depicted one important feature related to the security of the overall approach. It is of paramount importance for Intelligent Mobility users to trust on the distributed technology elements when accessing the platform through a mobile, a vehicle OBU, a laptop or from any other user interaction to access (use) the offered services, more recently based on web interfaces. The next subchapter addresses security issues by presenting and discussing the proposed security model for the SCOOP project.

3.1. The Intelligent Mobility Security Challenges: The SCOOP@F Part 2 project's adopted strategy

In order to assure security in the communication between vehicles and vehicle-to-infrastructure, it is being implemented a Public Key Infrastructure (PKI) that is able to establish and ensure a reliable communications networks, providing certified management services and keys that use encryption and digital signatures in all the communications between the different platforms and equipment. The PKI implementation is crucial to avoid the insertion of fake messages on the network and to authenticate entities (RSUs/OBUs/MOBICS) to access the network.

In this subchapter, the impact on MOBICS architecture of the Certificate Policy (CP) for the European Cooperative Intelligent Transportation System (EC-ITS) proposed by SCOOP@F Part 2, is presented and discussed. The certificate policies framework proposed is based on the following main entities (based on the standard PKI):

- Root Certification Authority (RCA);
- Long-Term Certification Authority (LTCA);
- Pseudonym Certification Authority (PCA);
- Long-Term Certificate (LTC); and
- Pseudonym Certificate (PC).

While not mentioned in the project documents, the CP of SCOOP@F Part 2 shall adopt a trend for a global federation of trusted entities responsible for managing the PKI hierarchy of the participating entities (those that generate certificates: RA, LTC, and PC). One example of a global entity that emerges with such a global role is the Transglobal Secure Collaboration Participation, Inc. (TSCP), a private association involving governments and companies on a collaborative association to establish a worldwide PKI trust infrastructure for TSCP[4]:

- Interpersonal Communications — email, instant messaging, and conferencing
- Group Collaborative Working — document sharing and access to applications
- Automated Data Exchange — product life-cycle and supply chain management

Furthermore, while a SCOOP@F Certificate Policy was proposed to be used by SCOOP implementers, a strategy shall be defined for a country level PKI management. It seems an entity from the Trusted List from other participating countries shall be selected to be the responsible for the root of each country. In Portugal, it is the responsibility of *Gabinete Nacional de Segurança* (National Security Authority) the management of the trusted list of Portugal where all the national accredited entities (Trust Service Provider) are listed. The current Trust Service Providers are:

- ECCE - State Common Certification Service Provider (national PKI – SCEE);
- Cartão de Cidadão - ECCC - National Identification Card Certification Service Provider (part of national PKI - SCEE);
- Justiça - ECM Justiça - Ministry of Justice Certification Service Provider (national PKI - SCEE);
- ECAR - ECAR - Assembly of the Republic Certification Service Provider (national PKI - SCEE);
- MULTICERT - Serviços de Certificação Electrónica S.A.;
- British Telecommunications plc;
- digital sign - Certificadora Digital - DigitalSign, S.A.

Before a detailed analysis of the strategy to follow by the MOBICS informatics system and the management of the adopted SP for the C-ITS at a global level, let's analyze the security requirements as established by SCOOP (and prior) projects.

The MOBICS I-system is responsible for the exchange of CAM from vehicles to a Traffic Control Centre (TCC) and DENM from TCC to vehicles (in target zones). According to the SP model, as proposed by the SCOOP project, one main objective is to guarantee that an OBU and RSU are valid networked connections in a C-ITS systems landscape. However, this guarantee is necessary to be made effective without accessing the identity of the OBU's owner; i.e., anonymity mechanism needs to be implemented in order to avoid any access to the real identity of the vehicle's owner. This means that at the infrastructure level, the connection of an OBU is authenticated based on pseudo certificates generated by a pseudonym certification authority (PCA). Summarizing, the SCOOP SP is based on the following main entities and roles, see Fig. 1:

- The root certification authority as trust common anchor: the RCA certificate generation and management by France (and other participating countries) according to the certification policy (CP);
- The long-term certification authority (LTCA) certificated by the RCA according to the CP;
- The long-term certificate (LTC) generated and managed by the LTCA according to its CP;
- The pseudonym certificate authority PCA certificated by the RCA according to the CP.
- The pseudonym certificate (PC) certificate generated and managed by the PCA according to CP.

[4] www.tscp.org

Considering that the adoption of the PKI has aimed to guarantee the authenticity of the connected OBUs and RSUs, it is the responsibility of the MOBICS to validate RSU entities. The OBU can be authenticated by the authenticated RSU's. However, when the mobile network (GSM/LTE) is used for OBUs to connect directly to the MOBICS I-system, it is up to this MOBICS to process authentication procedures. In both cases, the authentication process involves the verification of the respective certificate against its signature, the PCS for a PC certificate and an LTCA for an LTC certificate. As an example, if a CAM message is received from an OBU for which the verification of the signature fails, the message shall be discarded. It can be a fake OBU sending a message with an accident only to disturb the network.

3.2. The MOBICS Implementation Issues

The MOBICS implementation (prototype) manages a set of user interfaces making possible to browse relevant data to access configurable system behaviors. Nevertheless, the most valuable interfaces are available or integrated into the TMC I-system. The MOBICS subsystem plays a mediation role by managing message exchanges with OBU/RSU infrastructures answering safety related traffic events. In fact, the value of MOBICS is demonstrated as enhanced features available for traffic operators and made available to them through the TMC I-system user interfaces. However, at least for administration and maintenance, the MOBICS implements an administration interface which access login window is depicted in Fig. 3. It manages authentication and role-based control based on user roles and access capabilities.

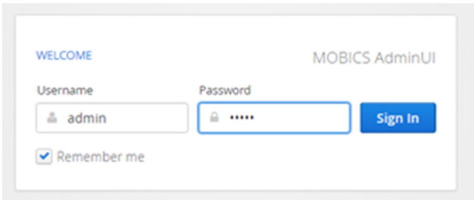

Fig. 3 Access to the MOBICS I-system's Administration Interface

A demonstrator dashboard is shown in the next picture, aggregating the most relevant operations/functions through which is possible to observe RSUs location in the highway, from where messages are defined and further sent to RSUs/OBUs and end users.

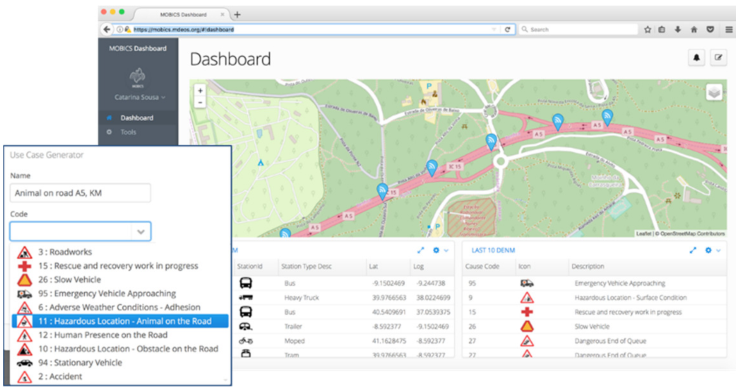

Fig. 4 An interface of the MOBICS platform showing the map representation of different incidents

The dashboard interface makes further possible to send standard messages, by selecting a given RSU. It is possible this way to validate the planned use cases. The relevance direction of the traffic is defined according to the standard EN302637-2.

In addition, incident schema images are inserted into the MOBICS dashboard map based on the reported GPS coordinates. The RSUs location is also represented on the map, based on their GPS coordinates (blue balloons in the picture above).

4. Conclusions and Further Research and Developments

The paper presents and discusses contributions to Intelligent Mobility based on the work that has been developed in the context of the SCOOP@F Part 2 project. The project also incorporates other research contributions, namely the ECoNet collaborative networks platform that was initially proposed in the European MIELE project. The ECoNet platform was motivated by the fast trend for collaborative logistics and transports where groups of stakeholders need agile mechanisms to exchange data and coordination information. The Intelligent Mobility share common requirements considering groups os stakeholders need to join on complex data and coordination exchanges. Beyond the architectural dimension, the unification of the development culture and common language and tools are also discussed. The MOBICS project is being collaboratively developed by (A-to-Be, ISEL, and University of Aveiro).

The MOBICS itself is evolving for an implementation of a standard computational responsibility named OCITS. Following the ISoS framework, the main objective is to achieve a really open MOBICS with the advantage it can be replaced by a competing product. This way, A-to-Be is aligned to the technology dependency problems, that large and small organizations will face over the next decades. As discussed in (Osório, Belloum, Afsarmanesh & Camarinha-Matos, 2017), such vendor lock-in is an obstacle of innovation processes while they are dependent on current suppliers capabilities and in most of the cases, the costs factor are not moderated by a competitive market.

Acknowledgements

The research leading to these results has been co-financed by the European Union's Connecting Europe Facility under grant agreement INEA/CEF/TRAN/A2014/1042281, namely Project SCOOP@F Part 2 - Système Coopératif Pilote. This research is also co-sponsored by the BP Portugal and Galp petroleum companies through the Horus project. The ECoNet framework has been partially supported by Administration of the Port of Lisbon and Leixões through the European project MIELE. The University of Aveiro (UA) through Instituto de Telecomunicações is contributing to the development of a reference model for OBU and RSU elements. Infraestruturas de Portugal is contributing to the definition of the MOBICS requirements.

5. References

ACEA. Access to vehicle data for third-party services position paper. ACEA web site, December 2016.

Luis M. Camarinha-Matos, Rosanna Fornasiero, and Hamideh Afsarmanesh. *Collaborative Networks as a Core Enabler of Industry 4.0*, pages 3–17. Springer International Publishing, Cham, 2017.

A.T. Campbell, G. Coulson, and M. E. Kounavis. Managing complexity: middleware explained. *IT Professional*, 1(5):22–28, Sep 1999.

EU_CITS. C-its platform phase ii, final report; cooperative intelligent transport systems; towards cooperative, connected, and automated mobility. Web, September 2017.

EUDIR40_. Directive on the framework for the deployment of intelligent transport systems in the field of road transport and for interfaces with other modes of transport. web, June 2010.

Fernandez, Pablo and Santana, Jose Miguel and Ortega, Sebastian and Trujillo, Agustin and Suarez, Jose Pablo and Dominguez, Conrado and Santana, Jaisiel and Santana, J.Sanchez, Alejandro. Smartport: A platform for sensor data monitoring in a seaport based on fiware. *Sensors*, 16(3):417, 2016.

J. Sales Gomes, Gastao Jacquet, Miguel Machado, A. Luis Osorio, Carlos Goncalves, and Manuel Barata. An open integration bus for efc: The ITS-IBUS. In *ASECAP conference*. ASECAP-2003, 18 - 21 May 2003 in Portoroz, Slovenia, May 2003.

R North T Worsley R Bradley H Neffendorf, G Fletcher. Modelling for intelligent mobility. *Transport Systems Catapult*, Catapult issue, 2015.

Michi Henning. The rise and fall of CORBA. *Queue*, 4(5):28–34, June 2006.

IBM. Collaborative business process management. Web: Business process management White paper, January 2008.

OMG-DMN. Decision model and notation (DMN), June 2016.

A. Luis Osorio. *Towards Vendor-Agnostic IT-System of IT-Systems with the CEDE Platform*, pages 494–505. Springer International Publishing, Cham, 2016.

A. Luis Osorio, Adam Belloum, Hamideh Afsarmanesh, and Camarinha-Matos. *Agnostic Informatics System of Systems: The Open ISoS Services Framework*. Springer International Publishing, 2017.

A. Luis Osorio and Luis M. Camarinha-Matos. Distributed process execution in collaborative networks. *Robot. Comput.-Integr. Manuf.*, 24:647–655, October 2008.

A. Luis Osorio, Luis M. Camarinha-Matos, and Hamideh Afsarmanesh. Econet platform for collaborative logistics and transport. In Luis M. Camarinha-Matos, Frederick Benaben, F., and Willy Picard, editors, *Risks and Resilience of Collaborative Networks*, volume 463 of *IFIP Advances in Information and Communication Technology*, pages 265–276. Springer International Publishing, 2015.