

An implementation of EURORADIO protocol for ERTMS systems

Gabriele Cecchetti*, Anna Lina Ruscelli*, Filippo Cugini[†], Piero Castoldi*

Abstract—European Rail Traffic Management System (ERTMS) is the European reference for interoperable and safer signaling systems to efficiently manage trains running. If implemented, it allows trains cross seamlessly intra-European national borders.

ERTMS has defined a secure communication protocol, *EURORADIO*, based on open communication networks. Its *RadioInfill* function can improve the reaction of the signaling system to changes in line conditions, avoiding unnecessary braking: its advantages in terms of power saving and travel time has been analyzed.

In this paper a software implementation of the *EURORADIO* protocol with *RadioInfill* for ERTMS Level 1 using GSM-R is illustrated as part of the *SR-Secure* Italian project. In this building-blocks architecture the *EURORADIO* layers communicates together through modular *Application Programm Interfaces*. Security coding rules and railway industry requirements specified by EN 50128 standard have been respected. The proposed implementation has successfully passed conformity tests and has been tested on a computer-based simulator.

Index Terms—ERTMS, ETCS signaling, *EURORADIO* protocol, *RadioInfill* function.

I. INTRODUCTION

SECURITY and optimization of trains circulation are key issues for traffic railways management systems. Complex technology architectures, *Automatic Train Protection* (ATP) systems, are set to automatically control trains running, to recover and avoid human errors and to prevent trains collisions in normal situation and when circulation or routes status are changed. ATP are based on trackside equipments, installed along the railway, that monitor routes conditions and trains circulations, collect and send the related information to the trainborne system using different technologies. At its turn the onboard train equipment elaborates these data and makes those available to the driver (cab signaling). ATP integrates the pre-existent signaling systems with *information points*, distributed along the route in positions important for train circulation management, that have the function of protection on the circulation. They can be distinguished in *fixed* information points sending constant data such as speed limits, acceleration line slope, and *variable* information points, transmitting dynamic signaling data associated with the preexistent light signals. Thus, when the train is transiting in proximity of these beacons, see Fig. 1, its trainborne subsystem picks up the information on train circulation sent as telegrams from

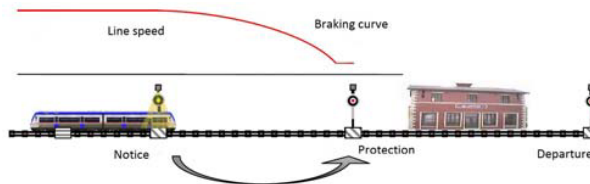


Figure 1. Example of ATP system.

the trackside system and displays that to the train driver. In general, in order to alert the driver to modify the train speed and to avoid abrupt speed changes, a further "notice" beacon is located around 1200 m before the protection information point, see Figure 1. Thus, when the driver sees the notice beacons as *yellow*, which corresponds to a *red* protection beacon, it adopts a deceleration curve suitable to brake and stop the train when crossing the related protection beacon. If this profile and the allowed maximum speed are not respected, the automatic braking system is activated. However, if the speed change is no more needed, due to a sudden modification of route condition, and the protection point becomes *green* again, these ATP systems are not so reactive to enable the driver to modify the speed curve and to come back to the previous one. Indeed, the trainborne subsystem cannot exchange its configuration until the next information beacon is reached. This means that, even when it is no more necessary, the process of deceleration has to be extended until the next information point, otherwise automatic braking system stops the train, and only after this beacon the train can accelerate again and recover the original speed. Accordingly the train running can be discontinuous, with a stop-and-go behavior that makes traffic circulation irregular and not optimized. This impacts also on power saving, increasing power consumption, on wear of the brakes, on the noise, and on passenger comfort, travel time, and delays. Thus an improved signaling system, more reactive to the variability of the railway network conditions, is necessary. Moreover, as far as international trains are concerned, it is required that the signaling system is interoperable with different national

European Rail Traffic Management System (ERTMS) [1]–[10] is an advanced version of ATP about signalling, control and train protection, set by European Union as the reference for European interoperable railways signaling. ERTMS is regulated by Directive 96/48/EC [11] that has specified standards, procedures and technologies, and Directive 2001/16/EC [12] about the interoperability of the trans-European conventional

*Gabriele Cecchetti, Anna Lina Ruscelli and Piero Castoldi are with Scuola Superiore S. Anna, Pisa, Italy (phone +39 050882009 e-mail: {g.cecchetti|a.ruscelli|p.castoldi}@sss.up.it).

[†]Filippo Cugini is with Consorzio Nazionale Interuniversitario per le Telecomunicazioni, Pisa, Italy (e-mail: f.cugini@cnit.it).

railway system. ERTMS aims at providing a signaling system common to all European nations in order to make the rail traffic circulation seamless and safer when crossing different national boundaries. Indeed, each European country has its national ATP, almost twenty in Europe [2]: for instance, INDUSI system, based on inductive beacons, is adopted in Germany, ASFA/LZB in Spain, AWS in UK. In Italy the national railway company, RFI, has developed two different ATP systems [7], both of them based on discontinuous communication: SCMT [13], the most compatible with ERTMS, distributed along the most important routes, and SSC [14], distributed along the remaining routes, with speed limitations.

Thus, in absence of an interoperable European signaling system like ERTMS, when a train is transiting over international boundaries, it is necessary to replace locomotives equipped with different national signaling instrumentations, and/or the cabin crew, trained to use its national signaling system. Otherwise, different equipments have to be installed on board, increasing the construction costs (consider, for instance, the TGV Thalys, linking Paris-Brussels-Cologne-Amsterdam, equipped with seven different signaling systems) and requiring drivers able to work with all of them.

Taking into account the technology used for the trackside-onboard communication system three levels of implementation are provided for ERTMS. ERTMS *Level 1* deals with the pre-existent communication infrastructure and on a discontinuous communication between trackside and trainborne systems, based on inductive beacons, the *EuroBalises*, whereas ERTMS *Level 2* *Level 3* are based on continuous radio communication. Furthermore ERTMS has defined a secure communication protocol, EURORADIO [15], that allows secure subsystems communication based on an open communication network, like GSM-R [16], [17], in order to support the continuous communication of ERTMS level 2 and 3. Moreover, in order to overcome the lack a responsive and flexible train speed management of ERTMS level 1, due to its discontinuous communications, EURORADIO integrates this system by expecting the implementation of a further function, named *RadioInfill*. RadioInfill introduces the opportunity of an *early release* of the running restriction *before* the crossing of the information point associated with this command, when routes conditions are further exchanged and a train deceleration is no more necessary. Indeed, as previously explained, in the presence of beacons, this early release is not enabled and the changes on speed profile are possible only after the next information point. As the best of our knowledge, at the time of beginning of the project none implementation of RadioInfill was available for commercial trackside communication subsystems.

In this paper a software implementation of the EURORADIO protocol with the RadioInfill function for trainborne and trackside subsystems based on ERTMS Level 1 systems is illustrated. This contribution is innovative since a not commercial implementation of EURORADIO is not available and RadioInfill has not been yet implemented. The choice of using GSM-R as communication network allows to reduce the impact of the support of this function on costs, risk of intrusion, temporal railway availability with respect to other more invasive technological solutions. Moreover, since GSM-R

is the European standard for trackside-onboard communications, this makes our implementation compliant with any future evolution of ATP systems. Finally a further key issue of the presented implementation is the deployment of the Key Management System, described in Section II, that has made possible the support of cryptographic functionalities.

The presented software framework is based on a building-blocks architecture where the different EURORADIO layers communicates together by means of *Application Programm* (API) that maintain a common structure along the stack. This allows a clear and modular implementation. Furthermore the architecture has been implemented taking into account security requirements as set by coding software rules and railway industry requirements specified by CENELEC, the European Committee for Electrotechnical Standardization, through the EN 50128 standard about *Software for railway control and protection systems* [18]. EN 50128 standard describes software safety integrity levels, deeply illustrates coding rules about objectives, input documents, output documents and software requirements specification, architecture, design and implementation, verification and testing as well as software/hardware integration, software validation, quality assurance, and maintenance [19]. In particular the SIL4 level of security has been adopted.

The rest of the paper is organized as follows: in Section II the ERTMS systems are deeply described, whereas in Section III the EURORADIO protocol and the RadioInfill function are illustrated. Section IV presents and analyzes the architecture developed for EURORADIO protocol with RadioInfill within the SR-Secure. Moreover some numerical results derived from the testing phase, and a theoretical analysis of the advantages from the use of RadioInfill in terms of power saving and travel time are illustrated. Finally, in Section VI some conclusions are drawn.

II. ERTMS SYSTEMS

ERTMS is an advanced ATP system introduced both to enable an interoperable European signaling system and to overcome the limits of the discontinuous trackside-onboard communications in order to make the trains circulation safer and more efficient. It integrates the pre-existent discontinuous communication infrastructure by adding some equipments based on the information points with the goal to make possible a "continuous" communication, and it is suitable to provide more data useful for the running train management. Moreover ERTMS is designed as reference European signaling system to offers the required level of interoperability to enable a seamless international traffic circulation across European national boundaries.

The ERTMS technical platform encompasses on two main components:

- *European Train Control System* (ETCS), a signaling, control and protection system for in-cabin train control, where a train-based computer, the Eurocab, elaborates the information sent by the trackside system, compares the speed curve with the current speed and position and slows down the train when needed, and

- *Global System for Mobile communication - Railway* (GSM-R) [16], [17], the European standard for trackside-to-train communication. GSM-R functional specifications was set by *European Integrated Radio Enhanced Network* (EIRENE) project [20] and, then, validated by *Mobile Radio for Railway for Networks in Europe* (MORANE) [21]. GSM-R relies on GSM networks and can manage data, voice, messages about reliable trains circulations, and it is set as wide range radio bearer for ETCS.

A third layer, *European Traffic Management Layer* (ETML), related to traffic management, is on demonstration phase under the Europtirails pilot project, on the North-South corridor of the trans-European network (Rotterdam-Milan route). It aims at optimizing train movements at operation management level by means of data about train running, and at improving real-time train management and route planning, [4].

Main components of the onboard ERTMS command/control equipment are [22]:

- *European Vital Computer* (EVC), the onboard computer-based system that elaborates the information about the train circulation.
- GSM-R mobile unit for the bidirectional radio communications between ERTMS trainborne system and *Radio Block Center* (RBC) trackside communication.
- Odometry that provides information about train position, speed and driving direction to the EVC.
- *Driver Machine Interface* that interfaces the driver with the EVC, displaying vital information for the train circulation.
- *Balise Transmission Module* and *Train transmission Module* that pick up the information from Eurobalises and Euroloop (whose function will be explained below).

Main components of the trackside ERTMS command/control equipment are:

- Eurobalise, the distributed beacons.
- Euroloop, used for unidirectional semi-continuous transmission from trackside to onboard.
- *Lineside Electronic Unit* (LEU), the encoders, that connect Eurobalises and Euroloop to the signaling system.
- *RadioInfill Unit* (RIU) that is used in ERTMS Level 1 to transfer the information about train direction to the GSM-R network.
- Trackside radio communication equipments distributed along the railway line.
- *Radio Block Center* (RBC) that is a computer-based system that sends information to the onboard system taking into account the data received by the interlocking and ERTMS itself.
- *Key Management Center* (KMC) that configures and distributes the key for the GSM-R communications.

ERTMS specifies three implementation levels:

- *ERTMS Level 1*, see Figure 2, deals with the pre-existent communication system (*ERTMS Level 0*) to provide information to the driver using light signals in order to modify the train running and/or to brake the train, when needed. Moreover, inductive beacons (Eurobalise), that work as information points, are placed in crucial positions along the route of the train. The trainborne subsystem, the

EVC, keeps and elaborates the cab signaling information; it can modify the train running only in correspondence of these points, thus discontinuously. This makes the speed curve not optimized and the trains circulation not efficient. The first railway line with ERTMS Level 1 was the Zaragoza-Huesca Spanish high-speed railway line in 2004.

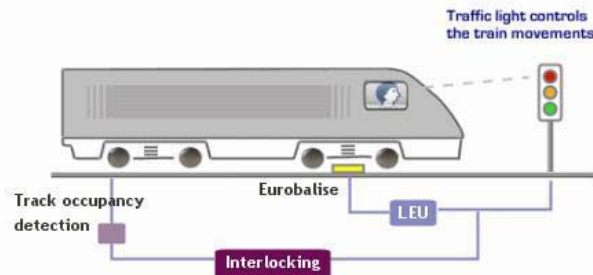


Figure 2. ERTMS Level 1.

- *ERTMS Level 2* and *ERTMS Level 3* [10], are digital radio-based signaling systems based on a RBC that collects the information sent by the trackside systems, monitors train movements and continuously sends to the train, through a GSM-R connection, information about train positions and directions, permission to proceed or to stop. These data are displayed in the cab. In this architecture passive beacons can be used as position train sensors to correct distance measurements errors. Furthermore *Base Transceiver Stations* (BTS) are needed to guarantee a continuous information exchange as well as some temperature sensors for axles, bushings and brakes. In particular, ERTMS Level 3 is based only on radio communication, and sends its rear end position making the optimization of circulation easier and reducing the trackside equipment.

The first railway line with ERTMS Level 2 was the Rome-Naples high-speed railway line in 2005.

Currently ERTMS Level 2 is diffusing in Europe and several ERTMS commercial projects are in progress worldwide like in South Korea, Taiwan, Australia, in Algeria, Saudi Arabia, Turkey and Libya. Moreover it is considered for the long-term integration between Central and Eastern Europe and for the corridors to Asia and Middle Europe [22].

ERTMS has defined a secure communication protocol, *EURORADIO* [15], that allows a secure subsystems communication based on an open communication network, like GSM-R. EURORADIO will be deeply analyzed on Section III along with the RadioInfill function and in Section IV, where the implementation of this protocol, subject of the paper, is

III. EURORADIO PROTOCOL

In this section a general description of EURORADIO protocol is provided. It is limited to architectural aspects since a

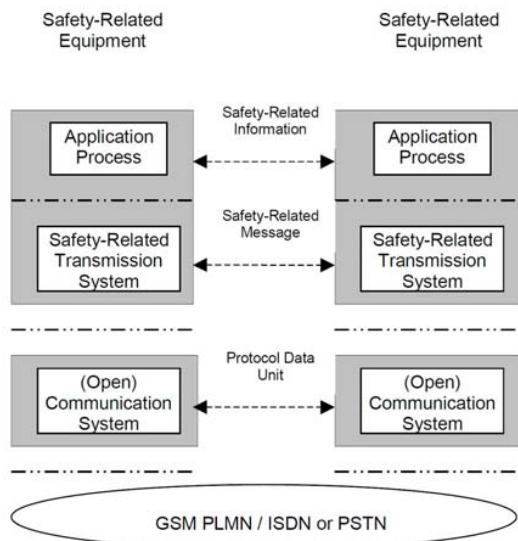


Figure 3. Structure of the radio communication system of EURORADIO.

deeper explanation of its structure and its messages handshake will be illustrated in Section IV, where our implementation of this protocol is presented.

A. EURORADIO general architecture

The general architecture of ERTMS/ETCS system is derived from the model illustrated in the Directive EN 50159-2 [23] about “Railway applications - Communication, signalling and processing systems - Safety related electronic systems for signalling” that defines the reference architecture for safety-related systems based on open transmissions. A safety system designed in conformity to this model can be used by application processes to exchange safety-related and non-safety related information with remote application processes using the services of the *Radio Communication System (RCS)*.

RCS is part of the *Open Transmission System* along with the Open Network (public or railway owned), as established by EN 50129 and depicted in Figure 3. At its turn RCS encompasses on two components:

- *Safety Functional Module (SFM)*, that encompasses the functionalities of the safety-related transmission system.
- *Communication Functional Module (CFM)* that provides the functions of the communication system based on circuit switched bearer services of GSM-R PLMN.

EURORADIO, as safety communication protocol, is compliant with this RCS architecture [15] and in Figure 3 it covers only the service features requested at the interface to the network.

B. EURORADIO level and interfaces

The EURORADIO protocol level communicates with its neighboring levels through interfaces.

Referring Figure 4, the lowest level interface, the interface *I*, is interposed between RCS and the chosen transmission medium; it is composed by a user plane, that deals with

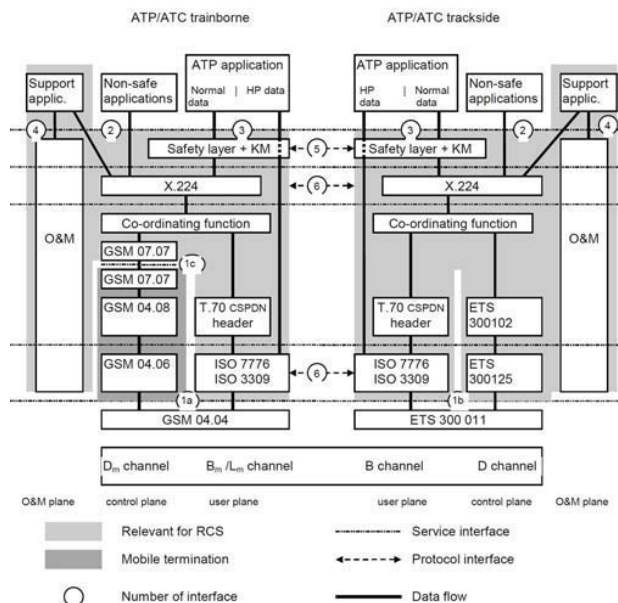


Figure 4. Reference architecture of EURORADIO system.

the transferring of user data, and a control plane, that take care of connection management. This interface is divided into three different submodules: the on-board GSM PLMN-Interface *Ia*, the on-board interface *Ic* between RCS and the mobile termination (MT), and the interface *Ib* toward fixed networks (trackside).

The service interface 2, optional and not required for ERTMS level 1 RadioInfill unit, interfaces non-safe applications or support applications and the Communication Functional Module. Interface 3 is a service interface between safe applications (e.g. ATP/ATC) and SFM (safety layer). Both these service interfaces 2 and 3 are not mandatory for interoperability and only a functional definition is provided. The coordinating function of the CFM covers the OSI layer 4 (Transport layer), layer 3 (Network layer) where performs routing, and layer 2 (Data Link layer) where can handle GSM-R modems and fixed network.

At the Transport layer the X.224 protocol for connection-mode transport service [24] is used; it also ensures the interoperability with remote entities.

The safety services of SFM provide safe connection set-up, and safe data transfer during the connection lifetime. In particular, the Safe Service (SaS) user exchanges data with the SaS provider and the safe data transfer takes care of data integrity and data authenticity. These safe services are accessed by means of safe service primitives with their corresponding parameters at the *Safe Service Access Point (SaSAP)*. These service primitives are similar to the service primitives defined in X.224 for connection-mode service. As far as interfaces are concerned, the service interface between safety layer user and safety layer, which gives the data flows to/from SFM, is not mandatory for interoperability.

Finally, SFM reports the errors that occur in the safety layer and transfers error indications from the lower layers.

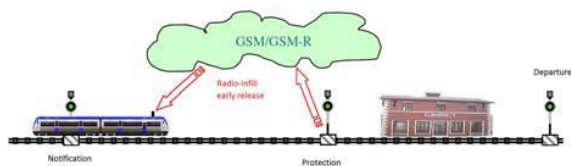


Figure 5. EURORADIO RadioInfill function.



Figure 6. Euroloop.

C. RadioInfill function

As explained in Section I, EURORADIO expects the implementation of a function, the *RadioInfill*, in order to improve the inadequate responsiveness of ERTMS level 1 to changes in routes and trains circulation conditions. RadioInfill enables the *early release* of the braking command when routes conditions are further exchanged and a train deceleration is no more necessary, see Figure 5.

Current implementations of RadioInfill function are based on pre-existent signaling systems or on dedicated components of trackside system, but no solutions use wireless communication. For instance, Italian SCMT sends the RadioInfill signal as coded electric signal along the railway through the track circuit, used by the anti-collision system like the Italian BACC braking system. This solution needs an interlocking system interface and an interference management between neighboring trains in order to avoid the reception of the message by not interested trains; furthermore, it is affected by the risk of intrusion. As far as ERTMS Level 1 is concerned, as the best or our knowledge, at the present time and without considering the contribution presented in this paper, RadioInfill is implemented by means of an electric coil along the railway, the *Euroloop*. It is used for a dedicated unidirectional semi-continuous transmission from trackside to onboard of the same telegram, that, otherwise, is sent when the train crosses the next information point, see Figure 6. This makes the cab signaling almost continuous, but requires the tooling of dedicated and specific instrumentation, the modification of the information point structure and the adding of suitable sensors in the trainborne subsystem. Furthermore it has the same interference problems than SCMT-based solution.

IV. SR-SECURE PROJECT: THE EURORADIO IMPLEMENTATION WITH THE RADIOINFILL FUNCTION

In this section the implementation of the EURORADIO protocol and of the RadioInfill function as part of the SR-Secure project is illustrated.

The aim of this regional project was to provide a software implementation of EURORADIO for ERTMS level 1 suitable to

use the GSM-R network with the goal to improve the railways infrastructure performance in terms of speed, travel time and, consequently, infrastructure capacity and efficiency. This was due to the fact that, at the beginning of the project, an open and not commercial implementation of this communication protocol was not available. Moreover the further contribution of our participation to the project innovativeness was the support of the RadioInfill function. This contribution is particularly relevant since it was not yet previously implemented by means of a wireless communication network. As previously mentioned in Section II, the implementation of RadioInfill allows the introduction of a continuous communication between the Information Point and the on-board equipment, avoiding architectural and technological solutions invasive for the pre-existent signaling system, see Euroloop. In particular, the choice of GSM-R was forced by the fact that it is set as European standard for the trackside-onboard communication suitable for voice, data and information about signaling and train circulation management. It allows to reduce the impact of the RadioInfill implementation on costs, temporal availability of the railway, and risk of intrusion with respect to the solutions based on SCMT and Euroloop described in Section II. Moreover its diffusion in Europe is a guarantee for the support of the signaling communications in general, and for RadioInfill in particular. Finally, this choice is expected to be compliant with any further evolution of ATP systems.

Furthermore, the deployment of the Key Management System of EURORADIO, described in Section II, that has made possible the support of cryptographic functionalities suitable to protect the system from external intrusions, was another key point of the project.

In the following the description of the structure of the proposed framework and of its interfaces is presented, as well as the explanation of the coding rules and of the adopted Safety Integrity Level in order to fulfill the requirements of the railway vital system. Furthermore the testing strategies used to validate the proposed EURORADIO implementation will be illustrated. Finally, a theoretical study suitable to highlight the positive impact of the RadioInfill function implementation on the trains power consumption and on the travel time, due to the avoiding of unnecessary braking, will be deeply explained.

A. Analysis of the impact of RadioInfill on energy consumption and travel time

The integration of the RadioInfill function in ERTMS level 1, as well as on SSC and SCMT systems, increases the security and efficiency of the train control systems. Indeed, as explained in Section III, the "early release" of the braking command, enabled by RadioInfill avoids unnecessary modifications of the speed curve, and improves the reactivity of the systems. It is intuitive to deduce that this optimization on trains circulations positively impacts on the comfort of the passengers, that are no more stressed by stop-and-go running of the train. But further results suitable to highlight the advantages of RadioInfill about power consumption and travel time can be derived mathematically.

a) *Assumptions*: The analysis is based on a simplified model of the motion of the train. It is assumed that energy necessary to move the train along the selected route has essentially two components:

- the energy E_v required to increase the speed, essentially due to the mass of the train, and
- the energy E_a required to compensate the air friction, that is dependent primarily on the speed of the train.

b) *Scenario*: The chosen scenario suitable to compare the behavior of the system with and without the RadioInfill function is based on the following acceleration-deceleration profile :

- the trains starts accelerating from 0 Km/h to a speed line of 150 km/h.
- the line speed is maintained until a certain distance;
- as a consequence of a *yellow* advise signal the train decelerates to 30 Km/h;
- after the protection signal the train accelerates again until 150 km/h;
- the train maintains the speed line and then decelerates until 0 km/h at a distance of 100 Km.

In particular, the study considers also the situation without intermediate deceleration and deceleration, i.e. when the the protection signal commutes to the *green* light immediately after the train crossed the *advise* beacon and the RadioInfill allows the early release of the breaking command. In this case the line speed of 150 Km/h is maintained along the route. Moreover, in order to investigate how the acceleration-deceleration affect the power consumption in dependency of the mass of the train, two types of trains are considered, a passenger train with a mass of 200 tons, and a freight train with a mass of 1500 tons.

c) *Hypotheses*: Some hypotheses are assumed in order to simplify the analysis, without any impact on the study:

- the motion of the train is along a straight track; consequently only the kinetic energy varies, whereas the potential energy is unchanged.
- The acceleration (equal to 0.3 m/s^2 , value derived from experience) is constant in absolute value, both during the acceleration and the deceleration.
- The motor efficiency and various energy losses such as mechanical and rolling frictions, that affects both the considered energy components but not their ratio, are not included.
- Even if a speed line of 150 Km/h is high for a freight train, the choice of an unique value for both the type of trains is due to homogeneity motivations and does not invalidate the meaning of the results.

d) *Results*: The energy E_v required to speed up the train is obtained by the difference between the final and the initial kinetic energy, and it is equal to:

$$E_v = \frac{1}{2}m(v_2^2 - v_1^2) \quad (1)$$

where v_2 and v_1 are the final and initial speed during the acceleration phase.

The energy E_a required to compensate the air friction is obtained by the product of the resisting force F

distance along which it is applied. F_a is expressed by the following equation:

$$F_a = \frac{1}{2}C_x \cdot \rho \cdot S \cdot v^2 \quad (2)$$

where C_x is the dimensionless coefficient of resistance; a value of 1.8 for the passenger train and roughly twice for the freight train are derived from the literature; ρ is the air density, equal to 1.2 Kg/m^3 at sea level and at a temperature of 20° Celsius degrees; finally S is the front section of the train set to 10 m^2 for both the considered types of trains. The numerical results are summarized in Table I.

It is possible to infer from the results that the main energy component is E_a , due to the air friction. This elements is yet more prominent when RadioInfill is not used, since in this case the effective distance traveled at the maximum speed is greater. However the absence of deceleration-acceleration can compensate this effect since in this case there is not energy consumption due to the acceleration. Thus it is possible to conclude that, by the use of RadioInfill, also saving only *one* braking, along a route of 100 Km it is possible to obtain a power saving equal to 4% and 18% respectively with a passenger train and a freight train. As far as the travel time is concerned, it is possible derive a reduction from 43.8' to 42.3' for both the trains due to the constant acceleration. Since these results are obtained in *ideal* traffic conditions, it is possible to deduce from the experience that, in situation with high density traffic and complex routes instrumentation, and where the number of unnecessary braking can arise to 5 along 100 Km, the advantages about power saving and travel time can be still higher.

B. Software architecture

EURORADIO is composed of different layers that can be implemented through a stack of different software layers communicating with each other, as specified by its *Functional Interface Specification* (FIS) [15].

The EURORADIO software stack is illustrated in Fig. 7.

The layers form a hierarchy of functionalities starting with the physical hardware components (Modem GSM-R) to the user interfaces at the software application level (RadioInfill Application). In particular, the RadioInfill has been implemented at the Application Layer.

Following a modular approach, each layer receives information from the layer above, and processes and transfers that to the layer below. Each layer adds its own encapsulation information (*header*) to the incoming information before it is passed to the lower layer.

C. The Safety Layer

When the application level want to send a RadioInfill message to another remote entity it prepares a *Safe Protocol Data Unit* (SaPDU) and sends that inside a *Safe Software Data Unit* (SaSDU) to the contiguous lower level. The Safety Layer process this message and then sends that to the Transport Layer. At the same time the Safety Layer process the messages incoming from the lower level and forward the results back to the connected application.

Table I
ENERGY SAVING WHEN USING RADIO INFILL FUNCTION.

Train	C_x	Mass (Kg)	wo RadInf			with RadInf			Power saving	
			E_v	E_a	E_{TOT}	E_v	E_a	E_{TOT}	Kwh	(%)
Pas.	1.8	$2 * 10^5$	95	478	572	48	499	548	25	(4%)
Fr.	3.6	$1.5 * 10^6$	710	956	1665	362	999	1361	305	(18%)

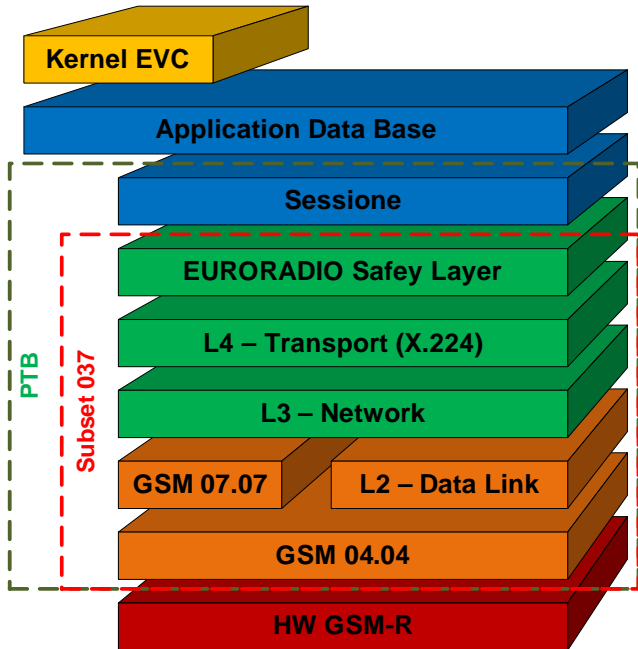


Figure 7. EURORADIO developed layers.

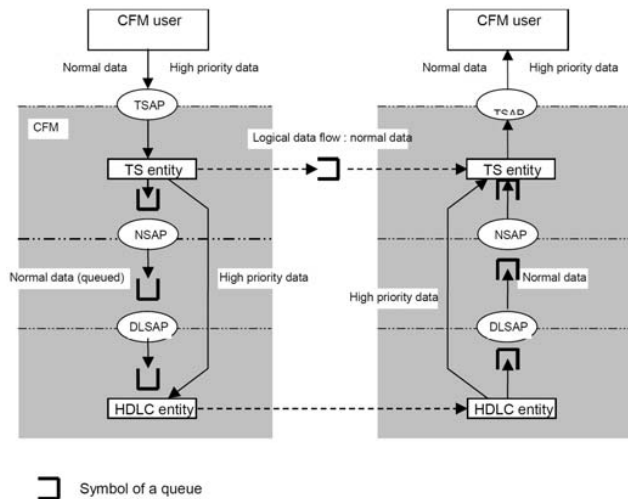


Figure 8. EURORADIO model of communication service.

This process is illustrated in Fig. 8.

The Safety Layer API is composed by the following interfaces:

- void **SaApiInit**(const SaInit_t* init);
it must be called before requesting the scheduler to initialize data structures;
- void **SaApiRun**(void);
it has to be called every task cycle to run: it moves messages from the Safety to Transport layer and back;
- bool_t **SaApiPutMsg**(uint8_t msg);
it lets the application to enqueue a SDU to be processed by the Safe layer; it returns false if the queue is full;
- uint32_t **SaApiGetNumMsg**(void);
it returns the number of messages queued at the Safety layer available for the application;
- bool_t **SaApiGetMsg**(uint8_t msg);
it lets to read the next message available in the queue; it returns false if there no messages.

The *SaApiRun*(void) behaviour is well illustrated by the following pseudo-code:

```

1 void SaApiRun (void) {
2   SaTrMsgs = SaTrGetNumMsgs ();
3   while ( SaTrMsgs > 0 ) {
4     SaTrGetMsg (msg)
5     TrApiPutMsg (msg)
6     SaTrMsgs--;
7   }
8   TrApiRun ();
9   TrSaMsgs = TrApiGetNumMsgs ();
10  while ( TrSaMsgs > 0 ) {
11    TrApiGetMsg (msg)
12    SaPutTrMsg (msg)
13    TrSaMsgs--;
14  }
15 }

```

Listing 1. Example of Safety Layer API: SaApiRun

The format of message varies depending on the primitive sent to the layer. The Safety Layer can accept the following primitives:

- Sa-CONNECT.request,
- Sa-CONNECT.indication,
- Sa-CONNECT.response,
- Sa-CONNECT.confirmation,
- Sa-DATA.request,
- Sa-DATA.indication,
- Sa-DATA.confirmation,
- Sa-HP-DATA.request,
- Sa-HP-DATA.confirmation,

- *Sa-DISCONNECT.request*,
- *Sa-DISCONNECT.indication* and
- *Sa-REPORT.indication*.

Each primitive is composed by different fields of information.

For instance *SA-CONNECT.request* and *Sa-DATA.request* are defined as follows:

```

1 typedef struct _Sa_CONN_req_MSG {
2     uint8_t MsgID;           // message type Id.
3     uint8_t AddressType;    // Network address or
4                             // Mobile phone.
5     uint8_t Address[ADDRESS_SIZE];
6     uint8_t CalledETCSIDType;
7     uint8_t CalledETCSID[ETCSID_SIZE];
8     uint8_t CallingETCSIDType;
9     uint8_t CallingETCSID[ETCSID_SIZE]
10    uint8_t ApplicationType;
11    uint8_t QoS;             //!< QoS level
12 } Sa_CONN_req_MSG_t;
13
14 typedef struct _Sa_DATA_req_MSG {
15     uint8_t MsgID;         // message type Id.
16     uint8_t SaCEPID;      // Safety layer Connection
17                             // Identifier.
18     uint8_t UserDataSize[2];
19     uint8_t UserData[MAX_AppPDU_SIZE];
20 } Sa_DATA_req_MSG_t;

```

Listing 2. Example of Safety Messages

1) *The Key Management System*: As mentioned in Section II, one of the components of the trackside ERTMS subsystem is the Key Management Center (KMC) that configures and distributes the key for the GSM-R communications. Indeed, since the exchange of the signaling telegrams is subject to strict security constraints, in order to prevent dangerous external intrusions and to avoid that a not interested train receives a message with a different destination, the adoption of some cryptographic functionalities is required when a GSM-R connection is established. In EURORADIO protocol stack, inside the Safety Layer, it is expected the implementation of Key Management System that deals with the correct exchange of symmetric cryptographic keys required during the creation and authentication phases of the radio sessions. The creation of these keys and their exchange are based on the well-known *Data Encryption Standard* (DES) encryption standard, proposed by IBM and standardized by the *Federal Information Processing Standard* (FIPS), now named National Bureau of Standards, in 1977 as FIPS PUB 46 [25]. In this block cypher, a block of fixed length equal to 64 bits is modified into a ciphertext bitstring of the same length by the use of a key of 64 bits. However, since only 56 bits of the key are effectively used, whereas the 8 bits are used for parity check, the effective length of the key is 56 bits.

D. The Transport Layer

The Transport layer setups a transport connection, if it is not yet established, sending a Connection-Request *Transport Protocol Data Unit* (TDPU) to the Network layer. When the connection is up it can propagate the SaPDU encapsulated in *Data-TPDU* (DT-TPDU). Each TPDU is sent using a *Transport Service Data Unit* (TSDU) to the Network layer. Moreover

the Transport layer receives the TSDU incoming from the underlying Network layer.

The Transport Layer API is composed by the following functions:

- **TrApiInit**,
- **TrApiRun**,
- **TrApiPutMsg**,
- **TrApiGetNumMsg**, and
- **TrApiGetMsg**.

Their functions is similar to the function provided by the Safety layer API.

E. The Network Layer

The Network layer usually has just two functions:

- it opens/closes the modem using the modem API interface for GSM-07.07 layer;
- it sends/receives *Network PDU* (NPDU) to/from the Data Link Layer.

The Network layer API is composed by the following interfaces:

- **NwApiInit**,
- **NwApiRun**,
- **NwApiPutMsg**,
- **NwApiGetNumMsg**, and
- **NwApiGetMsg**.

Thanks to the adopted modularity, their functions is similar to the function provided by the Safety layer API.

F. The Data Link Layer

The Data Link layer API exports the following interfaces:

- **DLApiInit**,
- **DLApiRun**,
- **DLApiPutMsg**,
- **DLApiGetNumMsg**, and
- **DLApiGetMsg**.

As with the previous layer, their functions is similar to the function provided by the Safety layer API.

G. The Physical Layer

The GSM modem API exports the following interfaces:

- **GSMApiInit**,
- **GSMApiPutMsg**,
- **GSMApiGetNumMsg**,
- **GSMApiGetMsg**,
- **GSMModemApiRun**,
- **GSMModemApiPutMsg**,
- **GSMModemApiGetNumMsg**, and
- **GSMModemApiGetMsg**.

While the GSMApi functions are used to transfer data to/from the GSM layer, the GSMModemApi functions interact directly with the attached GSM-R modem.

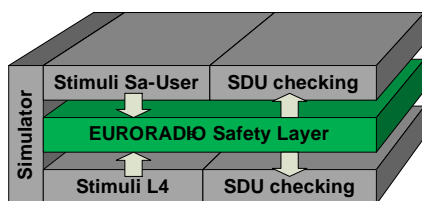


Figure 9. Test of a single layer.

H. Implementation notes

The EURORADIO software has been developed using opensource tools, and has been compiled under different Operating Systems such as Windows, Linux and FreeBSD to ensure portability between different platforms.

Furthermore the initial implementation of the EURORADIO protocol on an host machine has taken into account the subsequent code migration on the targets of the onboard and trackside communications equipments. Indeed, they have limited computation capacity and memory, in particular the trackside equipment. Hence, in order to maintain the same performance, the software has been developed by subdividing the code into small functions (NB mettere la lunghezza massima): this limits the expansion of the stack.

Moreover, since the railways signaling system is a vital system, the software development has to follow strict design and programming rules set by the Safety Policy as stated by the CEI EN 50128. In particular, the Safety Policy adopted is based on the Safety Integrity Level 4 (SIL4), the higher, that has to be fulfilled by all the functions in order to ensure the needed level of security and a safe and robust behavior of the system. The SIL4 enforces the adoption of clear and precise coding techniques to avoid unpredictable system behavior due to the use of different hardware platforms. Indeed, special instruction like cycles, conditional instructions (*case*, *switch*, etc.), or an ambiguous use of global, private and local variables (definitions, names, etc.), structures, pointers, preprocessor directives, macros, the definitions of functions etc., depending on the hardware where the software is running, can produce different system behaviors and performances. This can negatively impact on the system predictability and security, that are crucial features of a vital system. Thus the use of the standard C and the respect of the strict coding rules of CEI EN 50128 allow to ensure both portability and a predicable and safe behavior of the software architecture. Furthermore, the use of the basic data type of C have been avoided since different hardware platforms can assign diverse lengths. In order to have unambiguous data types, fixed length data types have been expressly defined.

V. SR-SECURE SOFTWARE TESTING AND PERFORMANCE EVALUATION

Each software layer has been tested by using a computer-based simulator. Each software layer has been tested isolated, see Figure 9, and together with the other layers, see Figure 10. In this way find programming and logical errors has been easier.

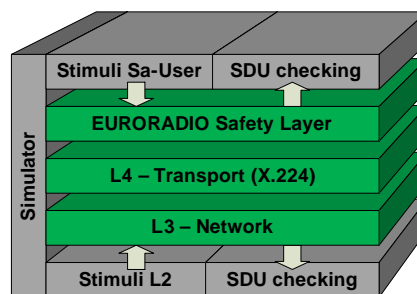


Figure 10. Test of multiple layers.

Moreover the overall EURORADIO stack has been validated using the tests illustrated in Subset092 suitable to check the conformity of the whole software.

Then the RadioInfill application and the EURORADIO protocol stack have been uploaded on a real embedded system adopted in production, where these tests have been replicated.

Finally the software has been validated by an external agency (Italcertifier) specialized on Train Systems.

A. Performance evaluation in emulated environment

A stress test had been set to check how many Safety primitives can be issued per seconds, after a connection has been established. This test is composed by the following phases:

- 1) Safe connection, composed by modem dialing, network and transport connection;
- 2) Safe data transmission of a payload of a variable length;
- 3) Safe disconnection.

The payload length varies from 1 to 1023 byte (that is the longest EURORADIO user data message).

We check that each transmitted *Sa-DATA.request* is correctly received. If any error happens, due to dropped packets at any layer, the *Sa-DATA* packet loss count is incremented.

It is assumed to operate in ideal conditions, with no errors due to the medium. The presented results have been obtained by simulating independent replications until the 95% confidence interval is reached for each measure.

Fig. 11 shows that the packet loss is decreasing when *Sa-DATA.request* Interarrival time increases, as expected in a real system.

Then a *Sa-DATA.request* Interarrival time equal to 500 ms is set in order to check if the packets loss is affected by the Scheduler Tic Time. The Scheduler Tic Time is the time elapsing between two calls of the EURORADIO protocol stack. A lower Scheduler Tic Time means that *SaApiRun()* will be called more often by the EURORADIO application. It is possible to tune this parameter, whose lower limit is depending by the hardware and the kernel used. If the value of this parameter is too low the EURORADIO stack will consume more CPU time, whereas if it is too high the EURORADIO stack could miss more packets coming from the network.

Fig. 12 highlights that the packets loss is decreasing when the Scheduler Tic Time increases.

Both these results, obtained by means of the presented software implementation of EURORADIO in an emulated

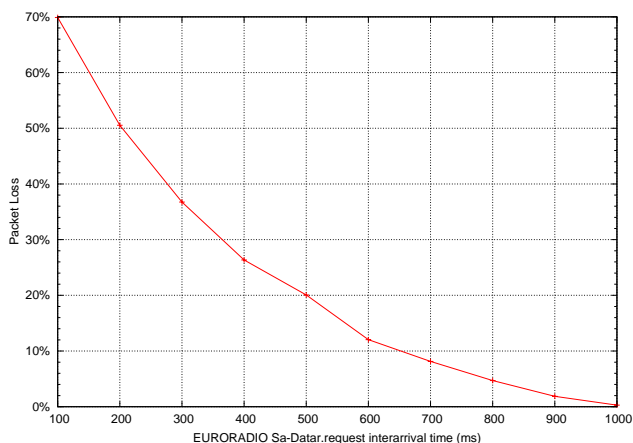


Figure 11. Packet loss vs Sa-DATA.request Interarrival time.

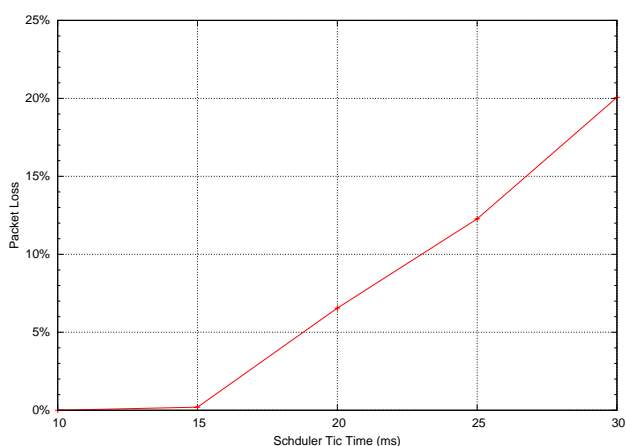


Figure 12. Packet loss vs Scheduler Tic Time, when Sa-DATA.request Interarrival time is 500ms.

environment, confirms the good behavior of the system suitable to reproduce real communication network phenomena.

VI. CONCLUSIONS

European Rail Traffic Management System (ERTMS) is set by European Union as the reference for interoperable signaling systems and a safe and optimized railway traffic management. It aims to allow European trains cross national borders without replace locomotives equipped with national cab signaling systems and/or drivers. It defines a safe communication protocol, Euroradio, based on an open communication network like GSM-R. Euroradio is used to safely exchange data about trains circulation between trackside and trainborne equipments. Its RadioInfill function is suitable to avoid unnecessary braking, whose advantages in terms of power saving and travel time have been analyzed.

In this paper a software implementation of the Euroradio protocol for ERTMS Level 1 systems designed for the *SR-Secure* Italian project is illustrated. The implementation is based on a building-blocks architecture where the Euroradio layers communicates together through *Application Programm*

Interfaces. Security coding rules and railway industry requirements specified by EN 50128 standard have been respected.

The proposed implementation has successfully passed conformity tests and has been tested on a computer-based simulator. Finally the results obtained in an emulated environment confirms the good behavior of the system suitable to reproduce real communication network phenomena.

ACKNOWLEDGMENT

This work has been partially supported by the *SR-Secure* national project, developed within the "POR FESR 2007 - 2013, Activity 1.1, lines of action A E B, 2008 Tuscany regional call for joint projects between companies groups and research bodies about Environment, Transport, Logistics, Infomobility and Energy".

REFERENCES

- [1] "Euroradio European Union." http://europa.eu/legislation_summaries/transport/rail_transport/l24458_en.htm.
- [2] "European Railway Agency." <http://www.era.europa.eu/Pages/Home.aspx>.
- [3] "European Union ERTMS 10 questions." http://ec.europa.eu/transport/rail/interoperability/ertms/doc/ertms_10_questions_en.pdf.
- [4] "ERTMS UIC." <http://uic.org/spip.php?article381>.
- [5] "ERTMS economic group." <http://www.ertms.be/new/>.
- [6] A. Jarasuniene, "General description of european railway traffic management (ertms) system and strategy of ertms implementation in various railway managements," *Transport Telecomm.*, vol. 6, no. 5, pp. 21-127, 2005.
- [7] F. Senesi and E. Marzilli, *European Train Control System - Development and Implementation in Italy*, vol. First Ed. CIFI - College of Italian Railway Engineers, Jul 2007.
- [8] F. Flammini, "Sistemi di controllo per l'alta velocita' ferroviaria," *Mondo Digitale*, no. 4, pp. 18-32, 2010.
- [9] I. Korpanec, "Major projects of european railway research," *Japan Railway and Transport Review*, pp. 16-21, Mar 1996.
- [10] E. Marzilli, F. Senesi, D. Caronti, N. Filippini, R. Malangone, U. Foschi, M. Ciaffi, and M. Frandi, "ERTMS/ETCS level 2 high speed / high capacity line feedback on RAMS and performance parameters: Experience after two years of commercial service in italy and features of the new HS/HC italian lines," in *WCRR* (UIC, ed.), (Seoul, Korea), May 2008.
- [11] "Directive DC 96/48/ec." <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31996L0048:it:HTML>.
- [12] "Directive DC 2001/16/ec." http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexplus!prod!DocNumber&lg=en&type_doc=Directive&an_doc=2001&nu_doc=16.
- [13] "SCMT RFI." <http://www.rfi.it/cms/v/index.jsp?vgnextoid=7c908c3e13e0a110VgnVCM10000080a3e90aRCRD>.
- [14] "SCC RFI." <http://www.rfi.it/cms/v/index.jsp?vgnextoid=e3908c3e13e0a110VgnVCM10000080a3e90aRCRD>.
- [15] S.-. ERTMS/ETCS, "Subset-037 ERTMS/ETCS - class 1 euroradio functional interface specifications." www.era.europa.eu, jul 2005.
- [16] "GSM-R RFI." <http://www.rfi.it/cms/v/index.jsp?vgnextoid=07b08c3e13e0a110VgnVCM10000080a3e90aRCRD>.
- [17] C. Decision 2006/679/EC, "Technical specifications for interoperability relating to control-command and signaling subsystem of the tran-european conventional rail system," mar 2006.
- [18] "EN 50128." http://www.cenelec.eu/dyn/www/f?p=104:110:2912039195125329:::FSP_PROJECT,FSP_LANG_ID:20508,25.
- [19] "EN 50128 industrial." <http://www.vectorcast.com/industries/railway-embedded-software-testing-cenelec.php>.
- [20] "GSM EIRENE UIC." <http://www.uic.org/spip.php?article676>.
- [21] "GSM-R Industry Group." <http://www.gsm-rail.com/technology>.
- [22] S. Abed, "European railway traffic management - an overview," *Iraq J. Electric Electronic Enginnering*, vol. 6, no. 2, pp. 172-179, 2010.
- [23] "EN 50129-2." http://www.cenelec.eu/dyn/www/f?p=104:110:1199452564785258:::FSP_PROJECT,FSP_LANG_ID:13550,25.
- [24] I. T. Union, "X.224 : Information technology - open systems interconnection - protocol for providing the connection-mode transport service," nov 1995.
- [25] N. B. of Standards, "Data encryption standard," 1977.