THE GRIDES (GSM-R INTEGRITY DETECTION SYSTEM) FOR THE ITALIAN ERTMS HIGH SPEED LINE

Authors: Raffaele Malangone, Enzo Marzilli, Cristina Malta, Stefano Marcoccio (Rete Ferroviaria Italiana)

Fabio Senesi (National Safety Railway Authority for Italy, ANSF)

Marco Luise, Vincenzo Pellegrini
Università di Pisa Dipartimento di Ingegneria dell’Informazione

Enzo Bagagli, Giuseppe Rubino,
INTECS informatica e tecnologia del software S.p.A.

Introduction

In the last years the evolution of the railway has also concerned the telecommunication systems. In fact in the ERTMS, the connection between the EVC (the On-board train sub-system) and the Radio Block Center (The Trackside Sub-system responsible for Train Spacing) of the High Speed lines is based on a GSM-R connection, an enhanced version of the normal GSM communication standard. This technical solution has involved problems for the safety as the open space communication can be easily disturbed by an external source. Actually RFI has GSM-R installed along 9.000 km of its network but the most important part is of course the one supporting the ERTMS HS lines, where GSM-R is necessary for the regularity of the service and where there aren’t other back-up signaling system.

In the following paper we want to give a brief description of the GSM-R in Italy and an overview to the GRIDES, a research project funded by the EPCIP Programme of the European Commission - Directorate General Freedom, Security and Justice to demonstrate the feasibility of a network of low-cost, trackside and trainborne sensors based on a technology called Software-Defined Radio (SDR). These sensors analyze in real-time the entire GSM-R spectrum in order to detect and classify interferences and to provide early-warning alarms to the railway signalling system in case of (malicious) network-disruptive radio attacks.

THE GSM-R

In the ‘80s, the telecommunication system chosen for the ERTMS was the GSM, but, in order to improve it, some additional characteristics have been added so that the correct definition for the system is GSM-Railway.

The most important distinctiveness, with respect to the normal GSM-R, is the possibility to maintain a continuous connection for speed up to 500 km/h, of course this is a performance requirement necessary for high speed trains (see fig.1).
Challenge H: For an even safer and more secure railway

The GSM-R specification was developed and validated by the MORANE and EIRENE projects. So, since the putting in service of the first Italian ERTMS HS/HC line (Roma-Napoli) in 2004, RFI has continuously worked on its network in order to reach practically full GSM-R coverage. Currently, the GSM-R infrastructure status is as follows:

- Planned: 10600km (HS+HL)
- Built: 9200km
- Operating: 8600km

The band frequencies adopted are 876-880 and 921-925 MHz (see fig. 2) with 19 carriers for uplink and the same number for downlink.

![FIG.2 Frequency bands for GSM-R, E-GSM, P-GSM](image)

The system must support the data transmission for the safety train movement and the regularity of service, so that the principal goals required concern the following problems:

- Coverage
- Network selection
- Handover and Selection of BTS
- Connection Time
- Transmission delay and bit error rate
- Frequency band and channels arrangement

The network architecture of GSM-R (see fig. 3) is quite similar to the basic GSM architecture and it includes components like Base Transceiver Stations (BTS), Base Stations Controllers (BSC) and Mobile Services switching Centers (MSC).
FIG. 3 Logical Scheme of the communication between train and Radio Block Center

GSM-R also provides a set of communication services:

- voice broadcast service
- voice group call service
- enhanced multi-level precedence and pre-emption
- General Packet Radio Service (GPRS)
- Emergency calls

The system must also ensure the level of coverage for at least 95% of the time on 95% of the area, with a radio terminal installed in a vehicle with an external antenna, assumed to be isotropic, with a nominal height at the level of 4 m from the track.

For the coverage probability the following values must be applied:

- coverage probability of 95% with a coverage level of 38.5 dB μV/m (-98 dBm) for voice and non-critical data security;
- coverage probability of 95% with a coverage level of 41.5 dB μV/m (-95 dBm) on lines with speeds less than or equal to 220 km / h.

These values are instead the minimum recommended:

- coverage probability of 95% with a coverage level of 44.5 dB μV/m (-92 dBm) on lines with speeds in excess of 280 km / h;
- coverage probability of 95% with a coverage level of 41.5 dB μV/m and 44.5 dB μV/m (-95 dBm and -92 dBm) on lines with speeds in excess of 220 km/h and less than or equal to 280 km/h.

These values must be respected even in the event of a BTS transmission failure, as the coverage redundancy, by the adjacent BTS to the one out of service, must ensure an adequate level of field (see fig. 4).

The actual values of coverage (tested with train rides) are always well above this margin.

FIG. 4 Coverage Redundancy by adjacent BTS

In any case, it is required that in the eventual passage of the train from one network to another (roaming) less than 0.5% of calls being lost.

With regards to the handover and cell selection, the probability of success in case of handover must be 99.5%.

A handover is successful if all the specifications on the burst of errors during the handover are satisfied and if you get an error-free transmission for at least the following 10 seconds after the handover.

Regarding the call connection establishment time, a value is required being smaller than two seconds for train emergency calls, and smaller than ten seconds for all other lower priority calls. These values must
be observed in 95% of cases, and in 99% of the time calls for the establishment should not exceed 1.5 times the time specification.

Concerning the error probability of the link, we must consider two different types of error in the radio interface:

- systematic error due to the train speed and the number of cells running on the connection. This depends on the handover, causing a loss of data and so can be predicted;
- error due to radio propagation, noise and interference with a BER (Bit Error Rate) not depending on the handover.

However, the possibility of system failure, specifically in the case of the ERTMS GSM-R is minimized because all the LRUs are redundant.

**Monitoring and prevention on the GSM-R System**

Even if the system has been redounded in all its components, a possible source of problems is represented by external interference (intentional or not) that may affect the communication between the on board CAB Radio of the train and the BTS.

Interferences may be very different and random, can be directed to the same frequency band or out of band emissions, come from adjacent channels or mix product of other signals, can be induced or radiated by RF instruments near the railway, etc.

Obviously the problems also depend on the value of the signal/noise ratio.

A preliminary analysis of potential interference sources, such as other GSM operators and broadcasting systems, can certainly provide an initial hypothetical result, keeping in mind that random problems of temporary or permanent nature may still occur.

In particular, the main risk comes from possible attacks from outside the GSM-R network from hackers with simple equipment. Noise generators (*jammers*), which cost a few thousands euro or even some hundreds in certain cases, can cover the GSM-R useful signal and block radio communication. Data confidentiality is not however compromised as Euroradio guarantees it by means of the protocol and its encryption algorithm.

This raises the need by the Manager of the railway infrastructure, in order to ensure an adequate and available service on the HS/AC, to detect any possible interference and to classify its type (see table 1).
**Challenge H: For an even safer and more secure railway**

Identified hazardous event | Related hazardous event (from 50159-2 Erreur ! Source du renvoi introuvable.) | Effects over railway systems | How the network monitoring identifies the hazardous event
---|---|---|---
Extra-system (RADAR, TV, EGSM...) transmitter with high level of power emissions within the GSM-R band | • Transmission of not authorised messages  
• Human Mistakes | • The train will be stopped | • Spectral analysis of channels within the GSM-R band  
• Post-processing of data received by the monitoring station from two or more consecutive software receivers.

Fault of one or more GSM-R BTS | • HW random failure  
• HW ageing  
• Wires breaking  
• HW damage or breaking | • The train will be stopped | • Spectral analysis of channels within the GSM-R band  
• Analysis of received signal level  
• Post-processing of data received by the monitoring station from two or more consecutive software receivers.

Intentional radio transmissions (jammers or fraudulent / terrorist transmitters) | • Transmission of not authorised messages | • The train will be stopped | • Spectral analysis of channels within the GSM-R band  
• Post-processing of data received by the monitoring station from two or more consecutive software receivers.

Multipath effects | • Fading Effects | • The train will be stopped | • Spectral analysis of channels within the GSM-R band  
• Post-processing of data received by the monitoring station from two or more consecutive software receivers.

Strong noise level in empty channels | • Thermal Noise  
• Magnetic Storm | • The train will be stopped | • Spectral analysis of channels within the GSM-R band  
• Analysis of received signal level

Reduced level of useful GSM-R signals | • Antenna misalignment  
• Thermal Noise  
• Magnetic Storm  
• Human Mistakes | • The train will be stopped | • Spectral analysis of channels within the GSM-R band  
• Analysis of received signal level  
• Post-processing of data received by the monitoring station from two or more consecutive software receivers.

Weak C/I (carrier over interference) ratio in a particular point of the track | • Human Mistakes | • The train will be stopped | • Spectral analysis of channels within the GSM-R band  
• Analysis of received signal level  
• Post-processing of data received by the monitoring station from two or more consecutive software receivers.

**Tab. 1 GSM-R system Hazards**

**GRIDES (GSM-R INTEGRITY DETECTION SYSTEM)**
The goal of GRIDES project has been to implement a prototype of a low-cost, re-configurable Software Defined Radio (SDR) based GSM-R receiver, the so-called GSMR_REC, to be used in order to monitor and enhance the availability and security of a GSM-R radio network typically employed for ground/board wireless communications and signalling in High Speed/High Capacity (HS/HC) railway applications, according to the ERTMS/ETCS Level 2 system specifications.

The main aim of the GRIDES system is basically to perform acquisition, processing and analysis of the radio signals in the GSM-R frequency bands and in proximity of one HS railway line. Both in uplink and downlink directions, the GRIDES surveillance network performs the functions of:

- acquiring signals within the GSM-R frequency bands;
- performing spectral analysis of the signals within the 200 KHz-spaced 19 channels of the GSM-R system;
- detecting via digital signal processing (DSP) techniques the presence of GSM-R signal by scanning each occupied GSM-R channel;
- detecting via DSP techniques incidental radio interference sources transmitting within the GSM-R channels;
- for each channel, measuring via DSP techniques the SNIR (Signal to Noise+Interference) ratio.

More in depth, GSMR_REC has been developed in two different configurations. The first, from now on referred to as GSMR_REC_OB, could be installed “on board” (OB) an HS/HC train, in order to scan both the uplink (UL) and downlink (DL) GSM-R radio carriers, and to detect possible radio interferences within the useful GSM-R signal bandwidth.

The second configuration, named GSMR_REC_TS, where TS just means “trackside”, performs the same processing of the GSMR_REC_OB but will be specifically designed to be installed in proximity of the HS/HC railway tracks. In fact, in addition to GSMR_REC_OB and GSMR_REC_TS receivers, GRIDES system is composed of one other element, the so-called GSMR_MOC where MOC refers to “monitoring center”, which will be basically in charge of gathering and processing the information about the quality of the GSM-R connection. To be more specific, the status of the GSM-R radio link (for instance in the sense of measured field, interference and noise levels over the carriers) will be monitored by the GSMR_MOC thanks to messages periodically received from the different GSMR_REC_TS’s placed close to the railway track and sent through an intranet connection.

Therefore, by implementing an “ad-hoc” network of low-cost GSMR_REC_TS receivers which are reconfigurable by SW because they are SDR-based, a smart and cost-efficient monitoring of the useful GSM-R signal and, at the same time, of potential radio interference sources over the overall GSM-R bandwidth is possible.

Since the GSM-R radio link is in charge of transporting information concerning the current (and, of course, future) speed limit to be respected by the train, it is important to perform, for each HS/HC railway track, an (almost) time-continuous monitoring of the radio link “status”, especially against external radio interference sources.

The adhesion to the SDR (Software Defined Radio) paradigm is of course one of the key ideas of the GRIDES project. In fact, an SDR-based system is a radio communication system which uses software routines for demodulation and digital signal processing (DSP) of radio signals. An SDR-receiver performs significant amounts of signal processing in a general purpose computer or a reconfigurable piece of digital electronics, combined with an RF front-end. The goal is to produce a radio that can receive, if needed, a new form of radio protocol just by running new software and using COTS hardware, getting the software as much as possible close to the antenna section, as shown in the following picture.

The advantages of choosing an SDR system are the full reconfigurability with no HW changes as the upgrades and add-ons are very easily implemented. Moreover it can implement very complicated and advanced signal processing algorithms (only limited by one’s fantasy). It’s ideal for “special” functions and it takes a short development time. On the other hand it presents a limited computational processing power given the general purpose nature of its computing backend (General Purpose Processor – GPP).

By resorting to the above paradigm, each SDR-based GSMR-REC receiver (see fig. 5) will be composed of:

- a COTS analogue/digital front-end (with analogue RF/IF filters and A/D converters);
- a processing unit (standard PC or GPP/DSP board with “ad-hoc” SW routines);

therefore it can be considered a low-cost, low-complexity system, being easily re-configurable / upgradeable by using of new SW routines/HW components.
A GRIDES Trackside Sentinel (GSMR_REC_TS) can:

- Monitor the entire spectral band assigned to GSM-R communications
- Provide 2 fully independent analysis chains for UPLINK and DOWNLINK spectra
- Process the acquired signal fully in real time. Which means: avoiding any “snapshot + post-process” approach: GRIDES never stops watching the spectrum it is meant to oversee.
- Detect the presence of ANY UNAUTHORIZED SIGNAL within the GSM-R bands as well as identify good authorized GSM-R signals
- Extract a complete report about the status and the relevant parameters of all the 38 GSM-R channels in less than one second.
- Instantly deliver Alarms to a remote monitoring centre via a TCP connection over IP network.

When the GSMR_MOC has processed data coming from the network of GSMR_REC_TS receivers (see picture below), it can identify an hazardous event and send an alarm to the railway operator so that a maintenance intervention / countermeasure (to be planned) can remove or mitigate possible threats to the GSM-R radio network.

The architecture of the overall GRIDES monitoring network is sketched in fig.6, where it is possible to see a GSMR_MOC that receives data from each GSMR_REC_TS via a TCP/IP channel established through a GPRS/UMTS connection. A GSMR_REC_OB operates instead on board the train.
Challenge H: For an even safer and more secure railway

Fig. 6 GRIDES system: GSM_REC_OB, GSM_REC_TS and GSMR_MOC.

The GRIDES system is conceived as a SIL 0 (Safety Integrated Level) system, because it is a measurement and monitoring system that does not interfere with the onboard/ground safety sub-systems.

GRIDES PROTOTYPE TEST CAMPAIGN

To verify the equipment correct functionality a test campaign was carried out both in the laboratory and on the HS/HCTrain with GSMR_REC_OB, HS/HCTrain with GSMR_REC_OB, HS/HCTrain with GSMR_REC_OB, HS/HCTrain with GSMR_REC_OB, HS/HCTrain with GSMR_REC_OB, HS/HCTrain with GSMR_REC_OB, HS/HCTrain with GSMR_REC_OB, HS/HCTrain with GSMR_REC_OB, HS/HCTrain with GSMR_REC_OB, HS/HCTrain with GSMR_REC_OB, HS/HCTrain with GSMR_REC_OB, HS/HCTrain with GSMR_REC_OB, HS/HCTrain with GSMR_REC_OB, HS/HCTrain with GSMR_REC_OB, HS/HCTrain with GSMR_REC_OB, HS/HCTrain with GSMR_REC_OB, HS/HCTrain with GSMR_REC_OB, HS/HCTrain with GSMR_REC_OB, HS/HCTrain with GSMR_REC_OB, HS/HCTrain with GSMR_REC_OB, HS/HCTrain with GSMR_REC_OB, HS/HCTrain with GSMR_REC_OB, HS/HCTrain with GSMR_REC_OB, HS/HCTrain with GSMR_REC_OB, HS/HCTrain with GSMR_REC_OB, HS/HCTrain with GSMR_REC_OB, HS/HCTrain with GSMR_REC_OB, HS/HCTrain with GSMR_REC_OB, HS/HCTrain with GSMR_REC_OB, HS/HCTrain with GSMR_REC_OB, HS/HCTrain with GSMR_REC_OB, HS/HCTrain with GSMR_REC_OB, HS/HCTrain with GSMR_REC_OB, HS/HCTrain with GSMR_REC_OB, HS/HCTrain with GSMR_REC_OB, HS/HCTrain with GSMR_REC_OB, HS/HCTrain with GSMR_REC_OB, HS/HCTrain with GSMR_REC_OB, HS/HCTrain with GSMR_REC_OB, HS/HCTrain with GSMR_REC_OB, HS/HCTrain with GSMR_REC_OB, HS/HCTrain with GSMR_REC_OB, HS/HCTrain with GSMR_REC_OB, HS/HCTrain with GSMR_REC_OB, HS/HCTrain with GSMR_REC_OB, HS/HCTrain with GSMR_REC_OB, HS/HCTrain with GSMR_REC_OB, HS/HCTrain with GSMR_REC_OB, HS/HCTrain with GSMR_REC_OB, HS/HCTrain with GSMR_REC_OB, HS/HCTrain with GSMR_REC_OB, HS/HCTrain with GSMR_REC_OB, HS/HCTrain with GSMR_REC_OB, HS/HCTrain with GSMR_REC_OB, HS/HCTrain with GSMR_REC_OB, HS/HCTrain with GSMR_REC_OB, HS/HCTrain with GSMR_REC_OB, HS/HCTrain with GSMR_REC_OB, HS/HCTrain with GSMR_REC_OB, HS/HCTrain with GSMR_REC_OB, HS/HCTrain with GSMR_REC_OB, HS/HCTrain with GSMR_REC_OB, HS/HCTrain with GSMR_REC_OB, HS/HCTrain with GSMR_REC_OB, HS/HCTrain with GSMR_REC_OB, HS/HCTrain with GSMR_REC_OB, HS/HCTrain with GSMR_REC_OB, HS/HCTrain with GSMR_REC_OB, HS/HCTrain with GSMR_REC_OB, HS/HCTrain with GSMR_REC_OB, HS/HCTrain with GSMR_REC_OB, HS/HCTrain with GSMR_REC_OB, HS/HCTrain with GSMR_REC_OB, HS/HCTrain with GSMR_REC_OB, HS/HCTrain with GSMR_REC_OB, HS/HCTrain with GSMR_REC_OB, HS/HCTrain with GSMR_REC_OB, HS/HCTrain with GSMR_REC_OB, HS/HCTrain with GSMR_REC_OB, HS/HCTrain with GSMR_REC_OB, HS/HCTrain with GSMR_REC_OB, HS/HCTrain with GSMR_REC_OB, HS/HCTrain with GSMR_REC_OB, HS/HCTrain with GSMR_REC_OB, HS/HCTrain with GSMR_REC_OB, HS/HCTrain with GSMR_REC_OB, HS/HCTrain with GSMR_REC_OB, HS/HCTrain with GSMR_REC_OB, HS/HCTrain with GSMR_REC_OB, HS/HCTrain with GSMR_REC_OB, HS/HCTrain with GSMR_REC_OB, HS/HCTrain with GSMR_REC_OB, HS/HCTrain with GSMR_REC_OB, HS/HCTrain with GSMR_REC_OB, HS/HCTrain with GSMR_REC_OB, HS/HCTrain with GSMR_REC_OB, HS/HCTrain with GSMR_REC_OB, HS/HCTrain with GSMR_REC_OB, HS/HCTrain with GSMR_REC_OB, HS/HCTrain with GSMR_REC_OB, HS/HCTrain with GSMR_REC_OB, HS/HCTrain with GSMR_REC_OB, HS/HCTrain with GSMR REC OF MILANO-BOLOGNA.

Fig. 7 Example of GSM-R receiver installed on Milano-Bologna
Challenge H: For an even safer and more secure railway

Fig. 8 DEMO SET-UP for laboratory tests

For the on-board GRIDES analyzer, using the test train runs during the pre-exercise period, it has been possible to evaluate (see fig.9) and validate the functionality at the 300km/h train speed. An Engineer Group has followed the tests on trains.

In the same period two fixed GRIDES detectors were installed along the route of the Milano-Bologna High Speed Line (see fig. 10) among three BTS; as previously mentioned these detectors were connected via TCP / IP network and supervised by the checkpoint installed at the PCS of Bologna.

The collected data was analyzed and found consistent with the known network status at the time of the test.

Fig. 9 On board Grides Test campaign Example: A valid GSM-R Base Station Signal is visible at f0 + 1000 kHz
and it is detected by the system as “ACTIVE GSM-R” on channel 5 DOWNLINK. Train Speed during this test was above 250 Km/h
CONCLUSIONS AND FUTURE ACTIVITIES

The increasing use of wireless telecommunication systems provides major advantages for the safety and the management ease of the railroad infrastructure. On the other hand, it introduces the problem of vulnerability of safety-critical and operation-critical telecommunication networks. The development and implementation of an instrument to prevent interference or attacks to the GSM-R system comes from the observation of this potential weakness of the railroad infrastructure.

The GRIDES system has demonstrated its capability to:

- capture the entire spectral band assigned to GSM-R communications;
- process the signal resulting from such acquisition by using two separated processing chains;
- process the acquired signal fully in real time;
- determine whether any of the GSM-R channels is correctly active, empty, acceptably interfered, or critically interfered;
- detect the presence of discontinuous, impulsive interferers;
- accurately estimate the SNIR of the signal that, from any of the receivable base stations, reaches the train;
- raise an early alarm for the local user in case potential dangers for communication on GSM-R channels are detected;
- instantly deliver Alarms to a remote monitoring center via a TCP/IP network;
- recognize even very weak and/or doppler/multipath-degraded GSM-R signals (e.g. from far away terminals or base stations);
- bear a low implementation cost.

The funding received through the program EPCIP 2007 of the European Commission (Directorate General Justice, Freedom and Security) and the interest shown by ERA, UIC, and several European railway administrations within the final GRIDES Workshop (see fig. 11) emphasize once again the importance of the issue.

RFI, after successfully testing the first prototype of the GRIDES (GSM-R System Integrity Detection) system is foreseeing the monitoring of its entire HS network through such system which, it’s important to say, has been developed with COTS elements, thus enabling the full-scale HS network coverage on a very low investment budget.
Challenge H: For an even safer and more secure railway

Fig. 11 Grides Workshop, in RFI ERTMS Laboratories

GLOSSARY

EVC, European Vital Computer
RBC, Radio Block Center
GSM-R, GSM Railway
HL, Historical lines
HS/HC, High Speed/High Capacity

REFERENCES