Management and communication of data on board of the vehicles of the Italian railway

G. Cau & E. Mingozzi
FS - TRENITALIA - Unità Tecnologie Materiale Rotabile
Firenze, Italy.

Abstract

In this paper are described the techniques and the exploitation results of a new system, which the Italian Railways install in their vehicles and in many ground location of the network, finalised to extend and to increment the survey of operational conditions and driving events on board of their trains. The Driver Information System (DIS), this is the name of the system, collects in real time, transmits to ground and elaborates all data corresponding to the status of the train and to the actions performed on the driver’s desk. This allows a higher potentiality, in comparison to similar systems currently available, for quality, nature and amount of acquired information and it opens the way to substitute the traditional and limited paper recording with an electronic storage according to the most recent technologies. The architecture of the DIS, intrinsically distributed, is constituted by the on-board system, which automatically transmits data to ground, and by the radio base station infrastructure present on the whole Italian country, responsible to implement a sophisticated database suitable to analyse and to classify the journeys according different criteria. Data are stored on board too, both in a "black box" capable to support strong accelerations and very high temperatures and in the Communication Computer, which transfers data to ground, piloting a spread spectrum radio based on IEEE 802.11 standard.

An essential characteristic of DIS, in which a very high number of computer exists, is the acceptance of legal validity of the treated information, for whose achievement the Directives issued by the Italian Authority for Computer Technology and Applications have been implemented. At the moment (JAN 2002) 18 ground data collecting locations and 100 locomotives have been equipped, with the program to complete the first 500 vehicles by June 2002; afterwards the scheduling forecast the application of the DIS on some 100 vehicles/month on the remaining part of the fleet of TRENITALIA.
Generality

An accurate measure and display of the train speed - on which drivers base the control of the journey - is a fundamental prerequisite for safety and for this reason this quantity has been recorded on paper, with legal value, since a long time. Nevertheless, the DIS (Driver Information System) has been introduced by the Italian Railways not only to supply an intrinsically safe tachymetry, but also to improve and extend the set of stored signal (traditionally only speed, time and signalling equipment codes) and the knowledge of the operative and exploitation conditions, to finally allow the automatic analysis of the Tachymetric Electronic Zones (TEZs) of FS-TRENITALIA fleet.

The DIS collects, memorises, transfers and elaborates a great amount of data: in the worst case, some 1700 bits are sampled each 100 ms in the active vehicles (4 o 5 thousand), equipped with a driver's desk, for an average duration of 10 hours each day. It follows that to get a practical exploitation of the system, the DIS uses strategies which contemporarily offers on one side a high degree of inherent, formal and legal validity, on the other the massive implementation of coding, compression and rationalisation of the managed data.

DIS architecture and functionality

The on board part consists of equipment which samples, transfers to ground and stores into the black box the driving events. The radio link takes place among a set of peripheral radio, installed in each vehicle of the fleet, and peripheral radio base stations located in the most important railway sites. Each peripheral site is connected to a central site through a WAN to concentrate the collected information, perform the analysis of the TEZs and transmit them back again on demand (see figure number 1). Due to the optical propagation of the chosen radio link - according WLAN standard IEEE 802.11 - the channel between peripheral radio and peripheral base stations is not always available: for this reason a fully automatic procedure of activation of the radio transmission, based on a measure of the radio coverage, is implemented.

![Figure 1: DIS architecture.](image-url)
This requires that the vehicles keep data until they arrive in any of equipped location where they can download them; referring to figure 1, this happens for vehicles $V_{a2}$, $V_{a3}$ e $V_{b1}$ on base station $a$ that covers the site $a$. It results that data transmission may be spatially and temporarily divided and takes place in minimal units equal to a TEZ.

The ground system works offline and organises the received data to decide if:
1. to label them for a further and deeper analysis by the competent bodies;
2. to send them to the central site for the final filing;
3. to perform query to specified vehicles to look for anomalies.

The DIS is completed by a service equipment that reproduces the basic functions of the ground system used as maintenance tool and for emergency situations.

The subsystems which compose the DIS are the tachymeter $T$ (see figure number 2), the event recorder $ER$ with the black box $BB$, the remote terminal $RT$, the communication computer $CC$, the radio $R$ and the service tool $ST$ (see figure number 3).

The $ER$ stores the information coming from the tachymetry, the signalling system, the GPS and the devices on the driver's desk. However, as the DIS is installed on different kind of rolling stock, it is possible configure the number and the function of the sampled signal to match the real internal structure.

Data, stored into the vehicle - both in the $BB$ and in the $CC$ - with proper strategies, are transmitted to ground when it is reachable by a radio base station; functions of correct routing and transferring are managed by the $CC$.

The $ER$ stores the information coming from the tachymetry, the signalling system, the GPS and the devices on the driver's desk. However, as the DIS is in-
stalled on different kind of rolling stock, it is possible configure the number and
the function of the sampled signal to match the real internal structure. Data,
stored into the vehicle - both in the BB and in the CC - with proper strategies,
are transmitted to ground when it is reachable by a radio base station; functions
of correct routing and transferring are managed by the CC. The on board system
is never switched off and a low power mode is introduced to limit the battery
consumption: in this state the radio link is continuously monitored to allow re-
 mote operations; each exclusion of the DIS is detected and recorded.
Data downloading takes place sending to ground one or more files, organised in
sequential records, containing the chronological memorisation of the events
composing the TEZs; each one of them is addressable using a suitable header
comprising the relevant elements which characterises it. Depending on the stor-
age status, the TEZs into the CC will be in one of the following conditions:
opened if the record storage is in progress, available if the TEZ file has been
closed, transmitted if the data transfer has been completed successfully - even if
without application ACK and finally marked if the CC has received the applica-
tion ACK from the WAN.
Data can be attained from the DIS via radio connection, local serial link or with
the reading of the black box: of these, the first one is obviously the most sophis-
ticated since it requires a more complex protocol and some mechanisms to opti-
mise vehicles multiple access. This way of information collecting can be totally
configured from the railway operator, which can decide how to activate the
downloading to meet his real necessities (for instance the transmission may take
place below a defined speed threshold ).

Figure 4: The DIS main unit.
Marked TEZs are not re-sent to ground, but it is also possible to make selective queries according criteria based on the items contained into the header (time, number of train, driver, etc.).

The sampled data flux is organised in a strictly sequential manner, without any bifurcation, in order to guarantee in any case the consistency and the absence of unwanted duplications and variations in comparison with the previous instances. If this were not the case, one might find, for example, data sampled in two different instants mixed in the same record, loosing in this way the main target of the system, or the capability to reconstruct the monitored train driving events.

In figure number 4 we can see the photograph of the DIS main unit which contains the T central unit, the ER, the CC, the R and the vehicle interfaces.

Data recording and safety

Monitored data are sampled with a period of 100ms and gathered into a unified record, but only a part of them is memorised into the ER: this happens when a variation, at least in one of the observed signals, takes place; in any case the entire record is stored to generate a consistent piece of information. To avoid loss of records, the maximum delay of memorisation is limited to 500 ms. If no variation is present in the signals, a record is stored the same every 60 s to maintain a sufficient degree of continuity in the TEZ. The minimum amount of data the black box is required to retain correspond to 10 hours, while for the CC is 20 days of normal service; it is quite sure that within this period the vehicle passes under the covered area of a ground radio station and so downloads all its data and frees its memory. The black box is a monobloc structure capable to withstand to very hostile environmental conditions: it can supports 700°C for 5 minutes obtained with a flux of 150 KW/m², half-sinusoidal acceleration of 100g and shocks of 20 kN on the 3 principal and diagonal axes.

The aim for which the information is collected, elaborated and stored by the DIS hold a vital importance: black box data have, in fact, legal value, while the other into the CC or in the distributed WAN data base have disciplinary, fiscal and administrative effects. For this reasons the project has taken advantage of the newest data protection techniques, whose principles are enounced in the standard of AIPA, which is the Italian Authority for Computer Application in the Public Administration. In the ground-board connection the end is to guarantee the identity of the received TEZ with the transmitted one: this is obtained by generating a digital imprint of the data, which is transferred together the informative part, applying a Hash function. Later on the imprint is calculated again on the ground side to verify if the received and transmitted files are equal. Beyond this, the user's identification bases itself on a double key algorithm applied only to the digital imprint, in order not to intolerably degrade the real time performances of the system (these algorithm are in fact very time consuming). The double key is composed by a private on board key and by the corresponding public one in each ground station: in this way the electronic signature of the driver is obtained. From the association of
the electronic signature to the TEZ, the Zone file results: this is compressed and sent to ground (see figure number 5).

![Diagram](image)

**Figure 5: Electronic signature generation and TEZ authentication.**

Thanks to all these feature, the TEZ is capable to fully substitute the old paper recording because, not only integrity, singleness and chronological order of data is assured, but also the acceptance of its validity by the driver through his signature; the interaction with the system is done on the basis of a personal smart card and a secret PIN. The DIS records data the same even without the insertion of the personal smart card, although in this case the association of the service to a driver requires other considerations. The man-machine interface is shown in figure number 6.

The visualisation of the speed on the driver's desk is done using an intrinsic safe speed indicator, too. A microprocessor in the tachometers sends the speed value on a dedicated serial line; then it is displayed commanding a stepper motor; this is coaxial with a resolver which decodes the position reached by the needle and transmits it back again to a second microprocessor, which operates a comparison between what it is sent and what it is received. In case an error is detected, a safety piloted LCD fault display is commuted to warn the driver.

![Image](image)

**Figure 6: DIS man-machine interface.**
Communication processes and radio infrastructure

The communication computer CC manages all full-duplex data transmission functionality with the ground sites; the radio interface is based on the WLAN standard IEEE 802.3 on a PCMCIA card. The whole transfer operations are protected against deadlock and livelock situations without loss of data. In addition, at application level many strategies have been introduced to avoid multi-access conflicts. The radio link is done on a client-server model where the CCs are the clients and the base stations are the servers, which offer connection and downloading services. All software modules have been developed following the rules of the document "Guidelines for the Applications of ISO9001 to the development, supply and maintenance of software", with reference to the general definition of the architecture, to the writing rules and to the failsafe behaviour of the microprocessor. These aspects have been particularly considered because they are strictly connected to software reliability and with data integrity along all the data path. The general software design is drawn in figure number 7.

![Figure 7: CC software architecture.](image)

Software is structured into layers; on the CC hardware there is the QNX® operating system: it sustains the HRIL (Hardware Resources Interface Library) that provides basic services to the upper application software. The HRIL is composed by some functional blocks SVS, MVB CL3, DOM/DOC, DSSS and SL; of these MVB CL3 allows upper layers to access to the MVB (Multifunction Vehicle Bus), DOM/DOC is the DiskOnModule and DiskOnChip driver; DSSS is the Network Interface Controller driver which controls the WLAN radio IEEE 802.11, while SL is the serial lines RS485 and RS232 driver. Process SVS supervises HIRL layer, makes the starting autotest and initialises the system together with the Exception Handler. Data downloading communication protocol is assured by functional blocks IP (Internet Protocol), TCP/UDP and DHCP (Dynamic Host Configuration Protocol) which realises the functions of a DHCP client on board: this links itself to the ground server to receive the IP address that is attributed to the radio card. T&S1 and T&S2 realise test, diagnostic and maintenance of the system and can be accessed both locally, by a PC connected...
Computers in Railways VIII

Communication infrastructure bases on IEEE 802.11 standard chosen for the high level immunity and data rate (11 Mbit/s). This is the WLAN, standard developed by IEEE (Institute of Electrical and Electronic Engineers), that makes a pair with the 802.3 for conventional wired Ethernet LAN. The radio carrier is centred on 2.4 GHz, which is in the ISM (Industrial Scientific Medical) band, and the propagation occurs by direct beam and moderate scattering. This standard allows the implementation of integrated ground architectures using more base radios, even operating in parallel without any physical and protocol conflict.

Medium Access Control uses CSMA/CA (Carrier Sense Multiple Access - collision avoidance) allowing an asynchronous and deterministic data transmission: a user may begin to send data only if the communication channel is available, otherwise it waits for a random time before making a new attempt. This procedure is repeated in case of necessity and a proper strategy is introduced to have a good throughput by reducing and optimising the random time.

Operating the system on the territory: the DIS protocol

On the Italian territory a certain number of ground peripheral sites are installed on the main locomotives workshops and depots where the vehicles normally are maintained, passes or stops with a high frequency. In these locations a ground radio base station, characterised by a proprietary address and able to receive the TEZs, has been activated and it constitutes an access point HFS (Host FS) to the geographical FS network. High level data transfer between on board equipment and HFS occurs by a TCP/IP connection with a dynamic IP assignment to the CC. We may have unmarked TEZs transmission either by spontaneous CC decision, or by HFS initiated selective request. Safety against unauthorised accesses is guaranteed by a 32 bit WLAN identification sequence at radio layer and by user ID and key word at FTP (File Transfer Protocol) layer. The CC interfaces to HFS through an application software which uses the following services: TCP/IP with DHCP (Dynamic Host Configuration Protocol) client-side and FTP plus UDP (User Datagram Protocol). As we said, CC and HFS are items of a client and server structure, which is valid also for the DHCP function.

Here are reported some elements of the main affiliation (figure number 8) and normal operation (figure number 9) procedures to give a feeling about DIS application layer way of working and the kind of adopted solutions: actually these are many more and more sophisticated in order to assure the correct and efficient ground-board managing of TEZs. In these pictures time out, retry and exceptions are not reported and simplified versions only using DHCPDISCOVER, DHCPOFFER, DHCPREQUEST e DHCPACK UDP datagrams are shown. When a train enters an access point influence area, IEEE802.11 connection activates and DHCP discover procedure starts: at the end, the CC gets a temporary
IP address, that automatically falls off after a time out, unless the CC, in normal operation, asks the HFS for a renewal. If a vehicle knows that it is going to leave the radio base station, it can release the received IP address and inform of that the HFS by a DHCPRELEASE message.

Figure 8: Vehicle affiliation procedure.

Once an IP address has been assigned, the vehicle CC sends the CDC_PRESENT datagram containing the following information: source IP address, destination IP address, train number, number of TEZs into the CC, state of each TEZ, date and time of last UDP message reception; then it waits command from ground. On the other side, the HFS receives the CDC_PRESENT, updates its covered vehicles status table and decides or not to request the remote CC for the availability to send ZTEs, by using FILE_ZONE_REQ message. Thus the CC updates the HFS IP address, verifies the availability of TEZs and transfers them using FTP; at the end, in case of positive transmission, it changes the attribute of each transmitted TEZ to "sent", otherwise leaves it unchanged and informs HFS with a CDC_PRESENT.

Figure 9: TEZs transmission and acknowledge.
In case of failure, the HFS requires a new transfer using the same procedure, otherwise it analyses the TEZs and in case of success it sends the MARK message; when this is received by the CC, the attribute of the pertinent TEZs are updated to "mark", a CDC_PRESENT with the new status is sent and finally the HFS sets the "mark" on ground side too, to assess that the "mark" attribute has been received on board and that the CC may even overwrite those TEZ. This is a double ACK procedure that contemporarily assures the correct receiving of the relevant information and of the basic ACK; at the same time the correct storage of the TEZs into the FS WAN is set. In figure number 10 the locomotive E 652 159, on which the first DIS prototype was applied in November 2000 to perform the protocol tests, is shown.

![Figure 10: The E652 159 loco that hosted the DIS prototype.](image)

**Conclusions**

The application of the DIS system on a first lot of 500 vehicles with driver's desk is in progress. This system is destined to became a new standard in driving events sampling, collection, storage and analysis for a long time. This is why it has been conceived to offer the user the maximum flexibility: the DIS is suitable for the new and the existing vehicles and it can also host the future accessory functions which will be requested. Then the presence of the black box gives a true recording of all driving parameters that is a fundamental contribution to railway safety. The results of this first period of running demonstrate the fully compliance to the project specifications, with great advantages on the way of a more and more reliable and effective railway transport.