THE APPLICATION OF THE CE REGULATION 402/13 AND THE QUANTITATIVE EVALUATION OF RISK TO THE ITALIAN RAILWAY ‘SSC’ (SUPPORTING SYSTEM FOR THE DRIVER) CONTROL COMMAND SYSTEM

F. SENESI, G. RIDOLFI & S. BUONINCONTRI
Control Command Office, Italian Railways Network (RFI).

ABSTRACT

Proper hazard analysis and risk evaluation management are the main steps to define the safety requirements of a railway control command system aiming to protect trains from their physical constraints, the limits of the infrastructure they have to run on and the traffic constraints as they share the same infrastructure with other vehicles.

After a short overview of the Italian national railway control command systems, the goal of this paper is to describe the approach adopted for providing the hazard analysis to the protection system named SSC (Supporting System for the Driver – *Sistema di Supporto alla Condotta*) with a special focus on the risk assessment phase where the quantitative evaluation of risk at system level was performed including human factor (particularly driver error).

The applied methodology adheres to the European Commission Regulation 402/13 on the common safety method for risk evaluation and assessment, and it is in line with the CENELEC standards EN50126 and EN50129 valid for safety-related electronic systems for railway signalling and communication applications.

Keywords: European Commission Regulation 402/13, quantitative risk evaluation, railway control command and signalling systems, risk acceptance,.

1 INTRODUCTION: EVOLUTION OF NATIONAL TRAIN CONTROL COMMAND SYSTEMS ON ITALIAN NETWORK

At the end of the 1900s and in the first years of the 2000s, RFI (the main Italian Railway Infrastructure Manager – *Rete Ferroviaria Italiana*) developed and put into operation two control command systems: SCMT (Train Control System - *Sistema Controllo Marcia Treno*) and SSC (Supporting System for the Driver - *Sistema di Supporto alla Condotta*).

Both are Automatic Train Protection (ATP) discontinuous systems controlling the maximum allowed speed in a transparent and independent way from the driver; the former based on Eurobalise air-gap and the latter on microwave air-gap.

SCMT was created for the main lines; it is able to provide full protection, within the limit of a reasonable feasibility, to all railways functionalities and the constituents implementing its functionalities were developed according to the highest Safety Integrity Level (SIL4) defined by CENELEC Standards [1–3]; a quantitative evaluation of the residual risk was not provided. Also SSC equipment was developed according to SIL4 however, the system itself was conceived in a simpler way (not covering all railways functionalities) to be deployed on 3,600 km of secondary non-electrified lines (see Fig. 1).

This paper is part of the Proceedings of the 10th International Conference on Risk Analysis (RISK 2016)
www.witconferences.com

ISSN: 2041-9031 (paper format), ISSN: 2041-904X (online), http://www.witpress.com/journals
DOI: 10.2495/SAFE-V6-N2-394-405

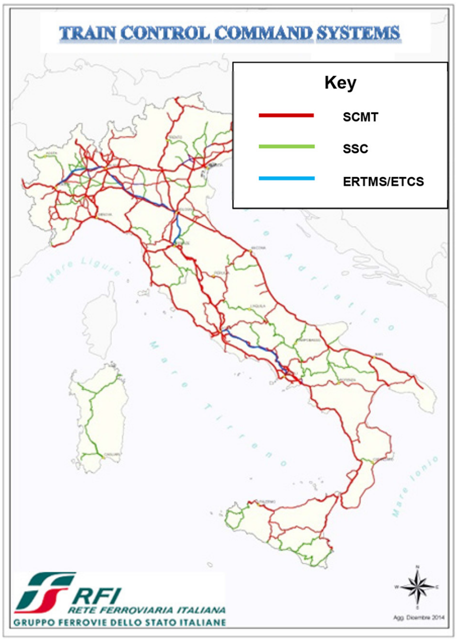
TRAIN CONTROL COMMAND SYSTEMS
Key
SCMT
SSC
ERTMS/ETCS
Mare Ligure
Mare Adriatico
Mare Tirreno
Mare Ionio
RFI
RETE FERROVIARIA ITALIANA
GRUPPO FERROVIE DELLO STATO ITALIANE
Agg. Dicembre 2014

Figure 1: Protection systems on RFI network.

1.1 Overview on the SSC control command system

SSC is an ATP system which performs the following functions:

- control according to speed limits imposed by lineside signals
- control of line static speed profile
- control of temporary speed restrictions
- control of maximum speed of the vehicle

SSC uses a microwave technology to transfer information from trackside subsystem to on-board subsystem; some fixed information (e.g. temporary speed restrictions) is transferred to on-board by means of Eurobalise technology (removable balise groups made by two balises).

SSC system is applicable on the low traffic non-electrified lines (maximum speed of 150 Km/h) of the conventional Italian network (both single track and double track lines).

SSC is composed of the Trackside and On-Board subsystem (see Fig. 2).

The Trackside subsystem is made of Information Points (PI): there are two kinds of PIs.

- convertible PIs used to transfer information related to lineside signals
- fixed PIs used to transfer information related to static speed profile and linking between PIs

A convertible PI is driven by a Lineside Electronic Unit (LEUs) interfaced with the trackside signal to detect signal aspects (see Fig. 3); the information from the trackside signal is

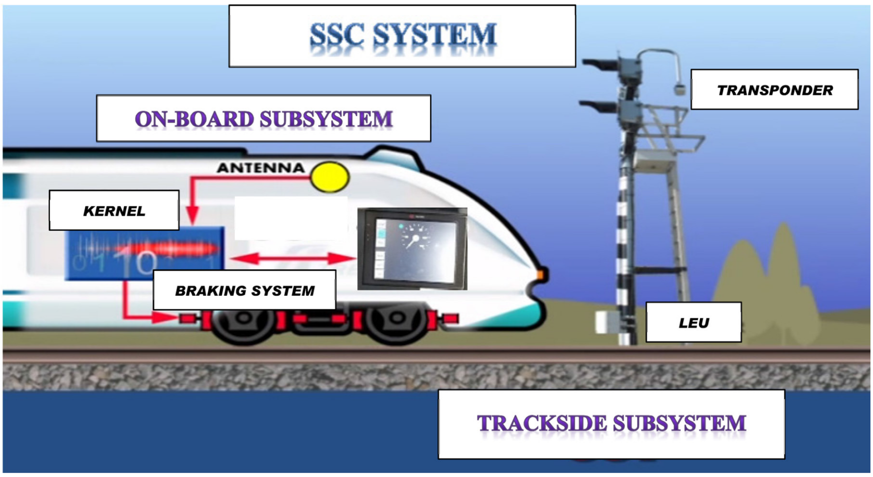

Figure 2: SSC system architecture

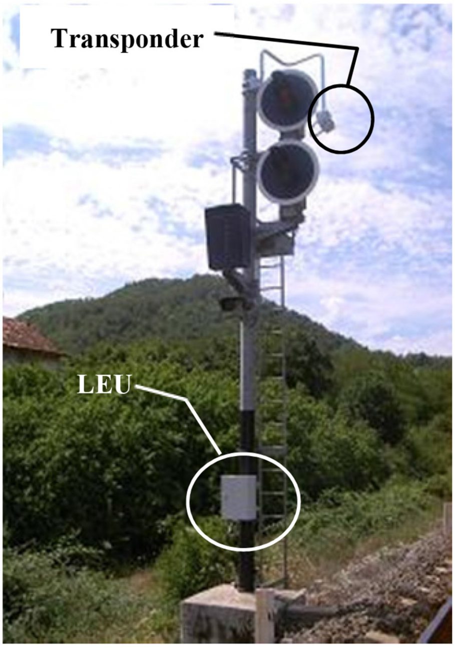

Figure 3: Lineside signal with LEU and Transponder.

transferred to the On-board subsystem by means of a Transponder connected to the LEU via serial line (RS485 technology).

The LEU and the Transponder connected to the LEU are powered by the trackside signal so no cables from the station are needed to feed the PIs.

Fixed PIs are made by a Transponder (see Fig. 3) powered by a battery charged by means of a solar panel; the Transponder is installed on its own structure (see Fig. 4).

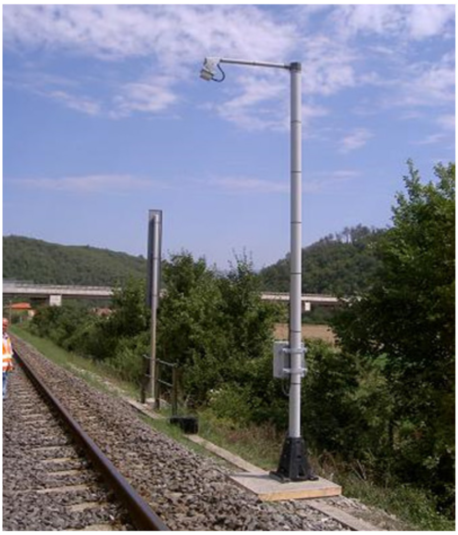

Figure 4: Fixed PI.

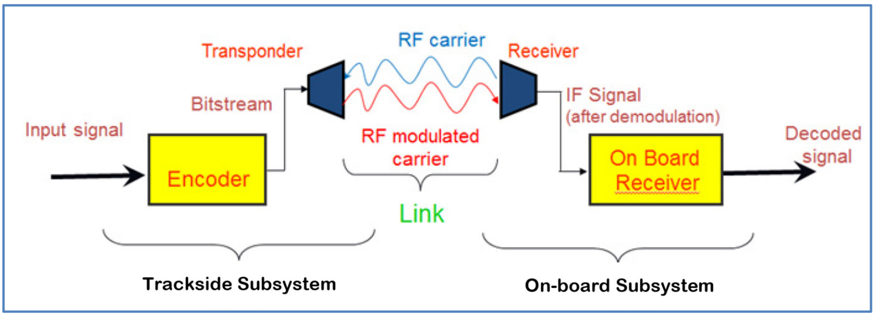

Figure 5: Air-gap architecture.

The air-gap interface (see Fig. 5) makes use of microwave technology (a Radio Frequency carrier around 5 GHz modulated by means an IF carrier); the Intermediate Frequency carrier is specialized to distinguish the PI installed on the left side (10,7 MHz) of the track and the PI installed (13 MHz) on the right side of the track.

Both these types of PIs are not redounded.

In addition, the information related to temporary speed restrictions and to specific variations of the static speed profile are transferred to the on-board system by means of redundant fixed balise groups using Eurobalise technology (the same technology used by the interoperable European Train Control System ETCS).

On-board subsystem is made of:

- Microwave receivers used to get information from fixed PIs and convertible PIs (Fig. 6)
- Eurobalise receiver used to get information from balise groups
- Wheel sensors used to determine speed, distance and acceleration of the train
- A kernel that elaborates the information coming from Trackside subsystem and from

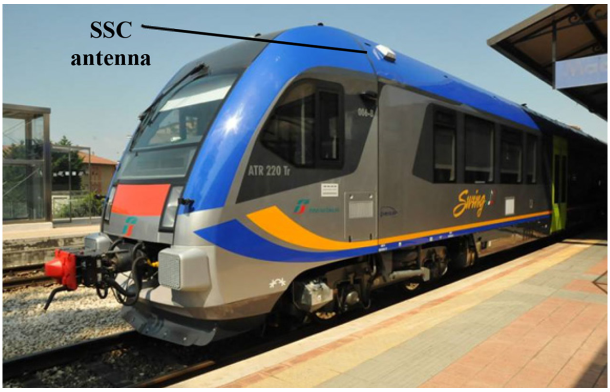

Figure 6: Vehicle ATR220Tr equipped with SSC On-Board subsystem.

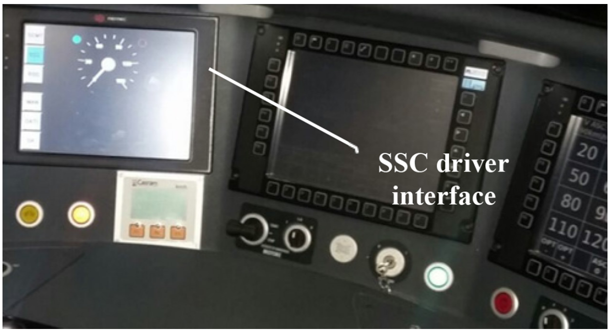

Figure 7: Vehicle ATR220Tr SSC driver interface.

wheel sensors and, on the basis of train data, determines the dynamic speed profile of the train to be controlled

- Driver Machine Interface (DMI) used to input train data and other orders from the driver and to display speed and auxiliary information to the driver (Fig. 7)
- Braking system interface module used to apply emergency brake ordered by the kernel when the current speed of the train is major than the permitted speed plus a specific margin (Fig. 8).

2 THE HAZARD ANALYSIS PROCESS APPLIED TO THE SSC CONTROL COMMAND SYSTEM

Although SSC was conceived as a simplified system to be deployed on secondary non-electrified lines, while the development of SSC still underway, a change in the legal framework occurred (Transport Minister Directive), imposing that also SSC system had to be assessed according to the same certification criteria used for the SCMT.

Due to this, an incremental path was conceived to avoid stopping the deployment of the already developed SSC control system and in parallel to provide a system hazard analysis according to European standards in law [1, 4] adopting, as first risk assessment criteria, the comparison to the reference system SCMT (Fig. 8).

When the level of protection ensured by the SSC system was lower than the relevant level provided by SCMT, an additional technological mitigation or the 'accurate risk evaluation' criteria were adopted according to a cost/benefit assessment.

Technological mitigations are considered sufficient by definition because they are implemented by constituents developed according to the maximum SIL4, which guarantees the highest possible level of confidence against random and systematic unsafe failures.

For the application of the 'accurate risk evaluation' criteria, the quantitative calculation of the hazard rate (HR) was chosen according to the following equation:

HR = frequency of risk exposure [event/hours of SSC operation] * probability of occurrence [from 0 to 1] of events contributing to induce an accident.

The frequency of risk exposure is the number of times, per SSC train operation hours, a hazardous event occurs (e.g. the number of line speed reductions in one hour ride). The calculation of the frequency risk exposure is based on the definition of a reference operational scenario (see section 2.1).

The probability of occurrence of an event contributing to induce an accident is the rate of cases out of the totality, where a scenario leads to a hazardous situation (e.g. unavailability of technological mitigation due to a hardware failure or driver error to respect the maximum permitted speed).

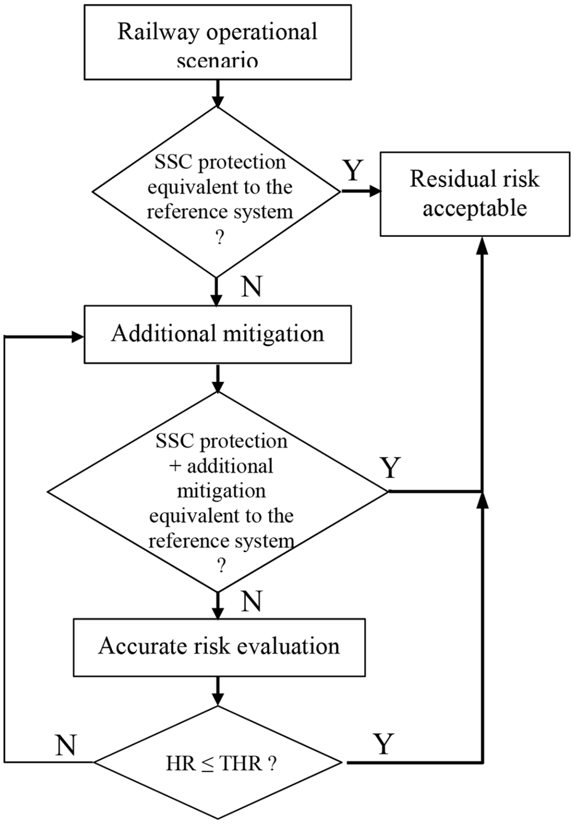
Railway operational scenario
SSC protection equivalent to the reference system ?
Y
Residual risk acceptable
N
Additional mitigation
SSC protection + additional mitigation equivalent to the reference system ?
Y
N
Accurate risk evaluation
N
HR ≤ THR ?
Y

Figure 8: SSC system Hazard Analysis and risk assessment process.

Therefore, the method used for the quantification of the hazard considers:

- the operational context and the characteristics of the SSC lines (such as for instance traffic, average operating speed, frequency of line speed variations, frequency of level crossing) through the definition of a reference operational scenario
- the maintenance organization of the signalling system on lines equipped with SSC, through the defectiveness of trackside and/or on-board protection system constituents and the latency of failures (Mean Time between Failure MTBF and Mean Time to Repair MTTR recorded from the field)

The risk will be considered acceptable if the relevant HR is lower than the tolerable hazard rate (THR) legally recognized as reference target (see section 2.2).

In addition, the SSC being a protection system not influencing driver operation (it does not provide the maximum permitted speed to the driver), driver error (behavior not compliant with operational rules) has to be considered among the events contributing to induce an accident.

2.1 The reference SSC operational scenario

The reference SSC operational scenario considered for the quantitative evaluation of each HR was defined studying the traffic and the characteristics of the 3.600 km of lines equipped with SSC system. The results of this survey gave the following figures:

- the average distance between stations is 5 km
- average speed train 50 km/h (see section 2.2 for more details on the way this value was established)
- a line speed reduction every 15 km
- average time of a mission 1 hour
- trains crossing every 30 min
- one or a group of line level crossing protected by the same signal every 5 km
- trains headway between 1 and 4 hours

2.2 The Tolerable Hazard Rate (THR) reference target from the national reference value defined by CE Decision 2012/226/UE

Since no reference THR is explicitly defined by the Italian legislation, the first criticality to apply the quantitative approach was the need to define such a THR to compare each calculated HR against.

Italian law [5] indicates, as a general commitment for the Railway Authority, to fulfill at least the reference safety targets (named National Reference Value – NRV) allocated to Italy by the CE Decision 2012/226/UE which provides a NRV for every European country.

NRV is however expressed in terms of 'fatalities and weighted serious injuries' (FWSI); to translate the FWSI into a THR a value has to be given to the following additional factors:

a. the amount of the FWSI (referring to the entire railways system) to be allocated to the failure/absence of a control command system.

b. the average value of FWSI associated to an accident due to the failure/absence of the control command system.
c. the commercial average speed of a mission of a train on a SSC line.

The values for the first two factors were deduced from the RFI safety data base (containing data related to safety relevant events) referring to the years from 2001 to 2003 preceding the introduction of the control command systems on the RFI networks (after the introduction of the control command systems no FWSI can be allocated to a failure of the control command system).

For factor A, the rate between the total FWSI and the FWSI allocated to the failure/absence of the control command system was found to be equal to 2.8 10^{-2}.

For factor B, the rate between the FWSI due to the failure/absence of the control command system, and the number of relevant accidents has been found equal to 5.7 10^{-1}.

The value of the third factor was deduced from the average speed recorded in the On-board juridical recorder of the SSC fleet, considering an observation window of 1 month equal to more than 21.000 hours and almost 1.100.000 km of operation; the average speed is found to be 50 km/h.

CE Decision 2012/226/UE provides the NRV targets according to the following categories:

- passengers
- employees
- level crossing users
- others
- unauthorized persons on railway premises

Dealing with a control command system, the most significant category to be considered is 'passengers'. For this category and for Italy, CE Decision 2012/226/UE provides the following target:

$$\frac{\text{no of passengers FWSI per year}}{\text{no of passengers train} - \text{km per year}} = 38.1\ 10^{-9} \tag{1}$$

Using factors A, B, and C:

$$\frac{\text{no of pass. FWSI per year attributed to protection systems}}{\text{no of passengers train} - \text{km per year}} = 38.110^{-9} * 2.810^{-2} = 1.0710^{-9} \tag{2}$$

$$\frac{\text{no of accident per year attributed to protection systems}}{\text{no of passengers train} - \text{km per year}} = \frac{1.0710^{-9}}{5,710^{-1}} = 1.8710^{-9} \tag{3}$$

$$\frac{\text{no of unwanted events}}{\text{h}} = 1.8710^{-9} * 50 \approx 10^{-7} \tag{4}$$

which becomes the reference THR target used for the quantitative evaluation of risks.

2.3 The contribution of human factor

The probability the driver makes a mistake, overcoming the permitted speed, is considered equal to 10^{-3} which means the driver can fail once over 1,000 events requiring him to comply with operational rules imposing him to reduce the speed. This value was derived from the literature on the matter [6, 7] considering that:

- a driver is purposely trained and completely aware of the consequences of his mistakes
- driver skills are periodically checked and measured
- stress and fatigue conditions are kept under control by rules which define the maximum shift length and the rest intervals

When necessary also the contribution of the error of the trackside traffic manager is considered following the same criteria.

3 THE APPLICATION OF THE QUANTITATIVE EVALUATION OF RISK TO THE FUNCTION ‘CEILING SPEED (MAXIMUM CONSTANT SPEED) LIMIT AFTER OVERRIDE OF A RUNNING TRACK STARTING SIGNAL AT DANGER’

This chapter describes the application of the quantitative evaluation of risk to the function ‘ceiling speed (maximum constant speed) limit after override of a running track starting signal at danger’.

The control of a ceiling speed after the override procedure operated by the driver to overcome a running track starting signal at danger due to a failure (see Fig. 9), is not provided by the SSC system unlike the SCMT system which controls a ceiling speed of 30 km/h up to the last switch of the station according to operational norms.

Below the consequences of the missing function are analyzed with regard to the reasons that prevent a starting signal to be set at green:

a. if the route after the signal is set and locked and the signal is at danger due to a failure of the lamp, the control of the ceiling speed of 30 km/h does not mitigate any risk as the route is free, and it can be taken up by the train.
b. if the signal is at danger because a track circuit or the train detection system between two stations is occupied due to a failure, provided the route is free from vehicles, the traffic manager can authorize the departure of the train (through the override procedure) and also in this case the ceiling speed of 30 km/h does not mitigate any risk.

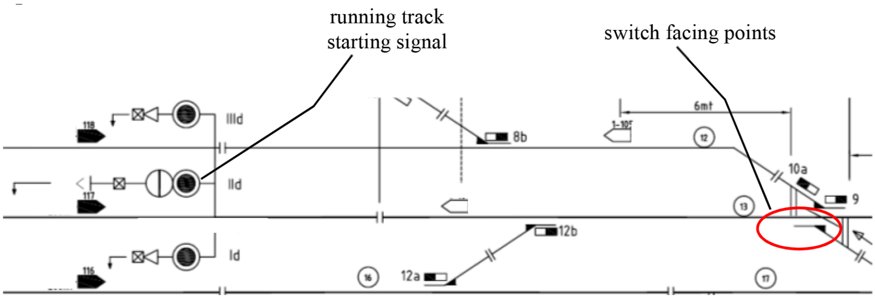

Figure 9: Detail from Borgo San Lorenzo (Florence) SSC station.

c. if the signal is at danger due to the presence of a switch out of control, operational norms allow the train to pass through the switch facing points at the maximum speed of 30 km/h; in this case the ‘ceiling speed (maximum constant speed) limit after override of a running track starting signal at danger’ function provides the mitigation against the risk of derailment.

With regard to the considerations above, the quantification of the risk was applied to scenario 3), and it is summarized in Table 1.

The hazard rate given by the quantification is lower than the reference tolerable rate (see section 2.2) hence the relevant risk is considered acceptable.

3.1 Switch failures statistic and survey

To estimate the unavailability of a switch due to a failure, RFI maintenance network data base was checked.
The survey was done according to the following conditions:

- geographical area of observation were limited to non-electrified lines (normally equipped by SSC system) where 1,357 switches electrically controlled are present.
- years 2011 and 2013 for a total of 17,520 hours represent the observation time.

Within the conditions above, 44 failures causing a switch out of control were recorded with an average time to repair equal to 2 hours and a maximus time to repair (in one case) equal to 16 hours.

Hence the MTBF can be calculate as:

$$1.357\ (\text{no of switches}) * 17.520\ (\text{hours}) / 44\ (\text{no of failures}) = 5,410^{5}\,\text{h} \qquad (5)$$

Table 1: Application of the quantitative evaluation of risk to the function ‘ceiling speed limit after override of a running track starting signal at danger’.

Risk exposure/events contributing to induce an accident		**Quantification**	**Source of data**
Risk exposure	No of starting signal met during the mission	10 / train hours	Reference scenario (see section 2.1)
Contributing event	Probability to cross a switch facing points after the starting signal	$4\ 10^{-2}$	SSC lines survey
Contributing event	Probability of switch out of control causing a starting signal to be at danger	$7.4\ 10^{-6}$	RFI Network maintenance database (see section 3.1)
Contributing event	Probability of exceeding speed limit due to driver error to comply with operational rules	10^{-3}	See section 2.3
HR total		$2.96\ 10^{-9}$ hazard / train hours	

and considering a MTTR of 4 hours, the unavailability of switches due to lack of control results to be:

$$\text{unavailability} = 1 - \frac{\text{MTBF}}{\text{MTBF} + \text{MTTR}} = 7.410^{-6} \tag{6}$$

4 CONCLUSION

The hazard analysis and the risk assessment process applied to the SSC train protection system has permitted the identification of the hazards, the related risks both on nominal and degraded conditions and the relevant technical or operational mitigations; all information have been recorded in the system Hazard Log.

RFI expertise on norms and on control command systems attended the hazard analysis sessions with the support of two Designated Body (DeBo) recognized by the Italian Railways National Safety Authority having, respectively, the role of validator according to CENELEC standards [1, 2] and of independent common safety method assessor.

For every hazardous scenario, the protection offered by the SSC system has been compared with the one provided by the SCMT system taken as 'equivalent reference system' in accordance with section 2.4 of Annex 1 of CE Regulation [4].

Where, after the introduction of new mitigations, the level of protection of the SSC system was still lower than the level of protection of the reference system, the quantification of residual risk was carried out considering physical and operational characteristics of SSC lines and the data from the network maintenance database.

In conclusion it is possible to state that:

- the hazard analysis and risk assessment process was carried out in accordance with CE Regulation [4] and with the provisions required by CENELEC standards [1, 2] for the highest SIL4.
- the systematic application of the totality of the mitigations identified during the hazard analysis guarantees an increase of the level of protection of the SSC system, ensuring a protection equivalent to the reference system SCMT for the totality of hazards and anyway the full observance of the target tolerable hazard rate of reference.

The declaration above is valid in the operational and maintenance framework of the present lines equipped by SSC. To continue to keep it valid, the availability of devices safety related (such as switches) must not decrease as operating conditions in terms of train headway must not deviate significantly from those assumed and used for the risk evaluation.

REFERENCES

[1] CENELEC European Standard EN50126, Railway applications – the specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS).

[2] CENELEC European Standard EN50129, Railway applications – communication, signalling and processing systems – safety related electronic system for signalling.

[3] CENELEC European Standard EN50128, Railway applications – communication, signalling and processing systems – software for railway control and protection systems.

[4] European Commission Implementing Regulation (EU), No 402/2013 of 30 April 2013.

[5] Italian Legislative Decree n° 162/2007 - art. 10 e 12.

[6] Hammerl, M. & Vanderhaegen, F., *Human Factors in the Railway System Safety Analysis Process*, 3rd International Rail Human Factors Conference.

[7] Kim, J., Jung, W., Jang, S.C. & Wang, J.B., Case study for the selection of a railway human reliability analysis method (issued by Korea Atomic research institute and Korea Railroad research institute).