TECHNICAL TRANSACTIONS | **CZASOPISMO TECHNICZNE**
ELECTRICAL ENGINEERING | ELEKTROTECHNIKA
1-E/2016

DOI: 10.4467/2353737XCT.16.034.5296

MAREK PAWLIK*

CONTROL COMMAND SYSTEMS IMPACT ON THE RAILWAY OPERATIONAL SAFETY

WPŁYW BEZPIECZNYCH SYSTEMÓW KONTROLI JAZDY NA BEZPIECZEŃSTWO RUCHU KOLEJOWEGO

Abstract

Since the very beginning, safety in railway transport has been perceived as an absolute necessity for market success of the rail. However, it is not at all obvious what safety is really about, as it means different things to different experts. The article analyses the impact of a safe travel control system on the operational safety, taking into consideration: safety of the safe travel control system, interfaces connected at one end with rail traffic control systems, and at the other with the vehicle control systems. It also indicates the importance of the transmission system, and maintenance as well as operating procedures, particularly those used in emergency situations. The analysis is recapitulated by conclusions concerning the commissioning of track-side and on-board safe train control devices.

Keywords: travel control system, safety in railway transport

Streszczenie

Bezpieczeństwo w transporcie kolejowym od samego początku jest postrzegane jako bezwzględna konieczność dla rynkowego sukcesu kolei. Jednakże to wcale nieoczywiste, co tak naprawdę składa się na bezpieczeństwo, jako że oznacza ono różne rzeczy dla różnych ekspertów. Artykuł analizuje wpływ bezpiecznego systemu kontroli jazdy na bezpieczeństwo ruchowe, biorąc pod uwagę: bezpieczeństwo systemu bezpiecznej kontroli jazdy, interfejsy z jednej strony z systemami sterowania ruchem kolejowym i z drugiej strony z systemami sterowania pojazdem. Wskazuje także na wagę systemu transmisji oraz procedur utrzymania, a także procedur ruchowych, szczególnie tych stosowanych w sytuacjach awaryjnych. Analizę podsumowano wnioskami dotyczącymi przekazywania do eksploatacji urządzeń przytorowych i pokładowych bezpiecznej kontroli jazdy pociągu.

Słowa kluczowe: system kontroli jazdy, bezpieczeństwo w transporcie kolejowym

* Ph.D. Eng. Marek Pawlik, Railway Institute, Warsaw.

1. Introduction

Railway vehicles and trains are very heavy – hundreds and thousands of tones – and therefore, railway tracks must be stable and supportive. Heavy trains are also resulting in very long braking distances, which are much longer then braking distances for vehicles in other transport modes. Upshot train drivers can't see all the way, which is necessary to stop the train in normal operational conditions. As a result, railway engineers, since the very early beginnings of railway, assumed that safety is a must for railway transport. All safety aspects were seen as very important. Solving the related challenges was based, among others, on the existence of single national railway companies with unified rules for permanent way construction and train characteristics as well as operational rules. Since 2004, when Poland jointed the European Committee, the Polish National Railway was split into many companies also splitting the responsibility for safety. Keeping high railway safety requires much deeper analyses of the risk subdivision between actors of the railway market. This article is intended to show safety ensured by control command systems as a component of the railway operational safety and challenges for them associated with the subdivision of the national railway.

2. What safety means

To answer the key question what safety means, one can point that all the safety-critical components have to be designed, constructed, assembled and maintained in a way ensuring operational safety. This is the key statement; however, it is not so easy to point to what it really means.

The wheel/rail contact must meet the stability requirements to ensure protection against derailments up to maximum authorised speed. Not only vertical, but also horizontal forces along the tracks and horizontal forces perpendicular to tracks, which are caused by vehicles, can't excide the related track limits. The parameters of brake equipment must guarantee that it is possible to stop within a given brake distance from the maximum authorised speed.

All components of the infrastructure as well as all components of the vehicles, including all kind of interfaces inside the infrastructure and inside the trains, must withstand normal and possible exceptional stresses during the entire life cycle. The consequences of possible failures must be mitigated. All used materials must be chosen taking in to account limiting the generation, propagation and effects of fire and smoke in the event of a fire. Materials can't cause any health hazard in normal and degraded situations.

All devices intended to be operated by railway personnel and passengers must be designed so that they do not impair the safe operation of the devices or the health and safety of users, if used in a foreseeable manner, albeit not in accordance with the posted instructions. Additionally, prevention against access of intrusions into installations is also important for safety. Moreover, traction supply systems must not impair the safety either of trains or of persons.

The electrical equipment must not impair the safety and functioning of the control-command and signalling installations. The control-command and signalling systems and devices as well as related procedures have to ensure active protection in normal operation

and in a degraded one. Rolling stock – traction and non-traction vehicles for passengers and cargo as well as specialised vehicles like track maintenance machines or bi-road vehicles for running on tracks and on roads, and all the links between vehicles, must be designed in such a way as to protect all the people involved, even in the event of collision or derailment, including passive safety by structures taking over the energy during collisions.

In passenger trains, appropriate devices must enable passengers to inform the driver and accompanying staff about an emergency and/or to impose emergency braking. However, passenger imposed braking should not lead the train to a stop in some locations, e.g. in tunnels where panic may be extremely dangerous and fire may propagate faster. Access doors must incorporate an opening and closing system, which guarantees passenger safety. Emergency exits must be provided and indicated.

Finally, last but not least, operating rules and the qualifications of drivers and on-board staff as well as of all kinds of the trackside staff must ensure safe operation. Maintenance of the infrastructure in vehicles has to be carried in appropriate intervals by competent staff using appropriate equipment.

So, for one person, safety is related to the parameters of rails and appropriate geometry of tracks; for another, safety is related to the competence and health of the drivers. For us, in this article, safety is related to the control command systems based on classic signalling systems, ensuring the so-called active protection.

A completely different thing is security; although, in many languages including Polish, both are expressed in many situations by the same word.

3. Control Command and Signalling

Signalling systems are seen by the drivers as colour light signals (semaphores in old solutions) giving them permission to run with a given speed and over a defined, restricted distance. For dispatchers, signalling systems are monitors (cubic based pulpits in old solutions) ensuring safe setting and locking of train running paths and setting signals in appropriate positions, meaning displaying appropriate colour light signal aspects (semaphores positions in old solutions). For signalling engineers, signalling systems are interlockings, block systems, level crossing protection systems, and other technical systems, all ensuring vital verification of the permissions given by dispatchers, and automatic safety related technical systems to the drivers by colour light signal aspects.

The control command systems are seen by the drivers as detail information about the running limits on the cab signalling. For dispatchers, control command systems are nearly invisible, except situations where control command systems provide means for larger areas serviced from a single location. For signalling engineers, control command systems have to be subdivided into trackside components and on-board components. The trackside components are taking vital information in a vital way form vital technical signalling systems and transmitting it in defined languages using vital transmission channels. The on-board components are receiving and verifying vital information from transmission channels; then, proceeding vital computing of received information and displaying running permissions (only receiving, verifying and displaying limited information in old solutions) to the drivers.

Implementing contemporary the European control command solution – the European Train Control System (ETCS) [2, 3] and using the European Global System for Mobile Railway Communication (GSM-R) [4, 5] for voice digital communication and as a digital channel for ETCS, ensures higher safety, but sets new kinds of challenges in front of the engineers. As a result of implementing ETCS and GSM-R, the railway lines' capacity is growing, border disruptions between railway systems of the neighbouring countries is lowering – additional traction units and additional tracks for shunting in many locations disappear, necessity of the different drives and different equipment in traction units is strongly minimised, and as a result, the time needed to pass borders is limited significantly. Border disruptions start to be comparable with other transport media. For better understanding of the different types of documents related to ETCS and GSM-R, it is important to know that they are jointly called the European Railway Transport Management System (ERTMS) [1, 6, 8].

To emphasise safety aspects related to signalling and control command systems, it is necessary to point that signalling systems are verifying work of the dispatchers, but not verifying work of the train drivers. Introducing control command systems ensures the possibility to verifying whether train drivers drive the trains in accordance with the limits given by dispatchers. Together, they provide active safety for train movements. This is extremely important because trains, due to extremely big masses (up to over 3 000 tones and even more) and relatively high speeds (up to over 160 km/h and even more), gain high kinetic energy, while at the same time having an adhesive coefficient about eight times lower than road vehicles. As a result, the braking distances for trains are long and each accident appearing inconsiderable may cause catastrophic consequences [7, 9, 11]. This is why railway movements are regulated by signalling and control command systems, ensuring meeting the following safety related functionalities:

- keeping safe distances between trains running on the tracks between stations – train spacing management,
- preventing setting conflicting train routs for the trains running into and out from the stations – train routing management,
- locking of the mobile elements of the switches for the entire train in correct positions – preventing derailments caused by switch movements under trains,
- protection of the level crossings constituting by the roads and railway lines one level – ensuring automatic level crossing protection as well as putting appropriate signs on the rail and road side,
- enabling safe incorporation of additional trains from the branches, sidings, industrial tracks etc., without creating disturbances – train movement start-up procedures.

4. Safety of the Control Command systems

The safety related functions of the control command systems do not ensure safety of the control command system. As it was already pointed out, safety must be ensured not only in normal operational conditions, but also in degraded ones. It is therefore important what will happen when control command system is malfunctioning or even damaged.

Malfunctioning and damage must not cause the so-called wrong side failures, which means that the authorised speed can't be higher than the safe one and the authorised

running distance can't be longer than the safe ones. The safe ones meaning authorised by dispatcher, given by signalling system, reflecting current operational circumstances. They can cause failures, as all technical systems are not failure free forever. However, acceptable malfunctioning and damage are those, which certainly mean that the authorised speed is lower than the safe one and the authorised running distance is shorter than the safe ones [11–14].

The question is how to ensure that wrong side failures do not appear in the entire life cycle of the control command system. The old method, which is still applied on a functional level, is simulating failures by switching off single modules, verifying results of short-circuits in different places, switching off the control command system power supply. This is mainly done during construction and known as the fail-safe principle. For electronic systems, which are based on vital interfaces, vital transmission and vital data computing are certainly not enough. It is necessary to verify the consequences of failures in electronic hardware and software. This is also done during the construction phase, but in that respect, the safety integrity level (SIL) principle is applied. The SIL levels are defined in the European Standard EN 50 129. The levels are from zero to four. SIL 4 is the only one acceptable for control command systems. Usually, SIL 4 is seen as an acceptable level of failures for one hour of working of the electronic system lower then 10E-9. This is true, but only in relation to hazard failures. Additionally, the EN 50 129 for each safety integrity level defines principles, which are intended to minimise the so-called systematic failures, which means failures caused during design, construction, assembly, maintenance – generally, failures caused by people. Confirmation of safety of the electronic systems – vitality of the control command – is done by a 'safety evidence report'. This is a document, which is verified by an independent safety assessor. It is seen as a company commercial secret and kept only for limited staff of the companies. It requires to be kept secret by all of the people involved, including the assessor.

Is it enough to apply to control command system fail-safe principle and SIL 4 supported by safety evidence report. It is not. The fail-safe principle and SIL 4 are applied to the product itself, while the control command system is connected to a number of other systems by interfaces. The interfaces related failures may cause wrong side failures for the entire active safety system between the dispatcher and the train driver (dispatcher ➔ vital signalling system e.g. interlocking ➔ vital trackside control command e.g. ETCS ➔ vital transmission system e.g. GSM-R ➔ vital on-board systems e.g. braking system e.g. ETCS ➔ train driver).

5. Impact of the Control Command systems on operational safety

An active safety system, based on control command, can support railway operational safety. However, it will not always support operational safety.

First of all, trackside control command system is based on the signalling system. It will not work if the signalling system is malfunctioning or damaged, and if interfaces between signalling systems and control command are malfunctioning. Of course, a wrong side failure in the signalling system must not cause an authorised speed higher than the safe one or an authorised running distance longer than the safe ones.

Secondly, the trackside control command system is connected to a vital transmission system by vital interfaces. The control command system will not work if the transmission itself or interfaces are malfunctioning or damaged. Of course, a wrong side failure in interfaces to the transmission system and the transmission system itself must not cause an authorised speed higher than the safe one or an authorised running distance longer than the safe ones.

The same applies to all vital systems and interfaces constituting the entire active safety system between the dispatcher and the train driver. Moreover, all systems and interfaces must ensure safety integrity level SIL 4. Any system with lower safety integrity level in a chain system structure will cause lowering safety integrity level of the whole active safety system between the dispatcher and the train driver to the level of such system. SIL 4 must therefore be ensured for all components.

Additionally, it is important to understand and to take into account that operational safety will not be supported in all situations when the control command and/or transmission trackside and on-board systems will not be compatible. This constitutes a challenge, as all lines and all traction vehicles can't be equipped at the same time. The first certification process has to be based on new trackside and new on-board control command equipment and assume that both are working correctly if all the tests are passed without problems. Then, additional trackside equipment has to be tested using the already accepted on-board equipment and additional on-board equipment has to be tested using the already accepted trackside equipment. More and more trackside and on-board installations will require defining strategy, as it is impossible to test new vehicles against all existing trackside installations and vice versa.

Control command implementations will certainly improve operational safety if all the components, including interfaces, are properly designed, constructed, assembled and maintained; however, operational safety depends on many other solutions and procedures.

References

[1] European Economic Interest Group-European Rail Traffic Management System 04E117 ETCS/GSM-R Quality of Service – Operational Analysis, 14/10/05.

[2] ERTMS/ETCS Functional requirement specification, version 5.0, signature ERA/ERTMS/003204.

[3] ETCS System Requirements Specification, version 3.2.0, reference UNISIG Subset 0-26.

[4] GSM-R Functional Requirements Specification, version 7.3.0, reference EIRINE FRS.

[5] GSM-R System Requirements Specification, version 15.3.0, reference EIRENE SRS.

[6] UIC ERTMS Users Group, 30/09/98, *ERTMS/ETCS RAMS Requirements Specification*.

[7] Pawlik M., *Polski Narodowy Plan Wdrażania Europejskiego Systemu Zarządzania Ruchem Kolejowym ERTMS*, „Technika Transportu Szynowego", 1/2007.

[8] Pushparatnam L., Taylor T., *GSM-R Implementation and Procurement Guide*, V 1.0 15.03.2009, UIC ISBN 978-2-7461-1631-3.

[9] Pawlik M., Żurkowski A., *Ruch i przewozy kolejowe. Sterowanie ruchem*, KOW, Warszawa 2010.

[10] Sameni M.K., *Railway Track Capacity: Measuring and Managing*, University of Southampton Faculty of Engineering and the Environment Transportation Research Group; Thesis for the degree of Doctor of Philosophy, October 2012.
[11] Pawlik M., *Zarządzanie ryzykiem w transporcie kolejowym*, „Technika Transportu Szynowego", 9/2013.
[12] Pawlik M., *Bezpieczeństwo ruchu kolejowego w legislacji unijnej*, „Technika Sterowania Ruchem", 4/2007.
[13] Siergiejczyk M., Gago S., *Zagadnienia bezpieczeństwa systemu GSM-R w aspekcie wspomagania transportu kolejowego*, „Logistyka", 6/2012, Wyd. ILiM, Poznań.
[14] Siergiejczyk M., Gago S., *Problemy zapewnienia bezpieczeństwa informacyjnego w sieci GSM-R*, Konferencja Transport XXI w., Ryn 2013.