ISSN 2307–3489 (Print), ISSN 2307–6666 (Online)

Наука та прогрес транспорту. Вісник Дніпропетровського національного університету залізничного транспорту, 2015, № 2 (56)

УДК 656.25.08

MAREK PAWLIK[1]*

[1]*Vice Director of the Warsaw Railway Institute, Chłopickiego Józefa Street, 50, Warsaw, Poland, PL 04-275, tel. +48 22 47 31 070, e–mail mpawlik@ikolej.pl. ORCID 0000-0003-3357-7706

CONTROL COMMAND SYSTEMS IMPACT ON THE RAILWAY OPERATIONAL SAFETY

Purpose. Safety is seen as a must, for railway transport market. However it is not so obvious what does safety exactly mean as it means different things for different experts. Showing safety ensured by control command systems as a component of the railway operational safety and pointing associated challenges especially those arising from subdivision of the national railway system into different entities. **Methodology.** To achieve this purpose control command and signalling systems keeping safe distances between trains, preventing setting conflicting train routs, locking of the mobile elements of the switches, protecting the level crossings, enabling safe incorporation of additional trains were analyzed. **Findings.** Article analyses how control command system influence operational safety taking into account safety of the control-command system itself, interfaces on one side between signalling systems and control command system and on the other side between control command system and vehicle control systems, transmission, maintenance, and operation in degraded modes of running. **Originality.** New and high-effective scope of tests which are necessary for putting new control command installation into service both track-side and on-board are proposed. **Practical value.** Control command implementations will significantly improve operational safety, however it is possible only when recommendations defined in this article are taken into account. This means that all the components including interfaces have to meet acceptable hazard rate 10E-9 and have to be properly design, constructed, assembled and maintained, all taking into account whole chain of functions performed and supervised by different railway entities.

Keywords: railway; safety; control command system; electrical equipment; signalling systems

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 railway very early beginnings assumed that safety is a must, for railway transport. All safety aspects were seen as very important. Solving related challenges was based, between others, by existence of single national railway companies with unified rules for permanent way construction and train characteristics as well as operational rules. In accordance with EU regulations Polish National Railway was split into many companies splitting also responsibility for safety. Keeping high railway safety requires much deeper analyses of 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 point associated challenges especially those arising from subdivision of the national railway system into different entities.

Purpose

Showing safety ensured by control command systems as a component of the railway operational safety and pointing associated challenges especially those arising from subdivision of the national railway system into different entities.

Methodology

To answer the key question what the 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 what does it really means.

The wheel/rail contact must meet the stability

doi 10.15802/stp2015/42160

ISSN 2307–3489 (Print), ISSN 2307–6666 (Online)

Наука та прогрес транспорту. Вісник Дніпропетровського національного університету залізничного транспорту, 2015, № 2 (56)

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 related track limits. The parameters of brake equipment must guarantee that it is possible to stop within a given braking 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 infrastructure and inside trains must withstand normal and possible exceptional stresses during whole life cycle. The consequences of possible failures must be mitigated. All used materials must be chosen taking into account limiting the generation, propagation and effects of fire and smoke in the event of a fire. Materials can't cause in normal and degraded situations any health hazard.

All devices intended to be operated by railway personnel and passengers must be so designed as not to 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 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 kind of involved people even in the event of collision or derailment including passive safety by constructions taking over energy during collisions.

In passenger trains appropriate devices must enable passengers to inform the driver and accompanying staff about emergency and/or to impose emergency braking. However, passenger imposed braking should not lead to stop the train 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 and of the all kinds of the trackside staff must ensure safe operation. Maintenance of infrastructure and 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 competence and health of the drivers. For us in this article safety is related to control command systems based on classic signalling systems ensuring so called active protection.

Totally other thing is security although in many languages including Polish both are expressed in many situations by the same word.

Signalling systems are seen by the drivers as colour light signals (semaphores in old solutions) giving them permission to run with given speed and on 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 position 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 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

doi 10.15802/stp2015/42160

ISSN 2307–3489 (Print), ISSN 2307–6666 (Online)

Наука та прогрес транспорту. Вісник Дніпропетровського національного університету залізничного транспорту, 2015, № 2 (56)

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 European control command solution – the European Train Control System (ETCS) [1, 3, 4, 8, 9] and using European Global System for Mobile Railway Communication (GSM-R) [9, 11, 14, 15] for voice digital communication and as a digital channel for ETCS ensures higher safety but sets in front of the engineers new kind of challenges. As a result of implementing ETCS and GSM-R 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 time needed to pass borders is limited significantly. Border disruptions starts 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 together called European Railway Transport Management System (ERTMS) [1, 5, 6, 8, 9].

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 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 as 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 having at the same time adhesive coefficient about eight times lower than road vehicles. As a result braking distance for trains is long and each accident appearing inconsiderable may cause catastrophic consequences [2, 5, 7, 9, 10]. That is why railway movements are regulated by signalling and control command systems ensuring meeting 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 in to and out from the stations – train routing management,

− locking of the mobile elements of the switches for entire train runs in correct positions – preventing derailments caused by switch movements under trains,

− protection of the level crossings constituting by the roads and railway lines crossing at one level – ensuring automatic level crossing protection as well as putting appropriate signs on the rail and on the road side,

− enabling safe incorporation of additional trains from the branches, sidings, industrial tracks etc. without creating disturbances – train movement start-up procedures.

Findings

The safety related functions of the control command systems do not ensure safety of the control command system itself. As already pointed 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 when it is damaged.

Malfunctioning and damage must not cause so called wrong side failures which means that authorised speed can't be higher than the safe one and authorised running distance can't be longer than the safe one. The safe one meaning authorised by dispatcher, given by signalling system, reflecting current operational circumstances. It has to be accepted that all technical systems are not failure free, especially for ever. However, acceptable malfunctioning and damage are those which mean that certainly authorised speed is lower than the safe one and authorised running distance is shorter than the safe one [2, 7, 10, 12, 13].

The question is how to ensure that wrong side failures do not appear in a whole 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,

doi 10.15802/stp2015/42160

ISSN 2307–3489 (Print), ISSN 2307–6666 (Online)

Наука та прогрес транспорту. Вісник Дніпропетровського національного університету залізничного транспорту, 2015, № 2 (56)

switching off control command system power supply. This is mainly done during construction and known as fail-safe principle. For electronic systems which are based on vital interfaces, vital transmission and vital data computing this is certainly not enough. It is necessary to verity consequences of failures in electronic hardware and software. This is also done during construction phase, but in that respect a safety integrity level (SIL) principle is applied. The SIL levels are defined in a 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 half true as it applies only in relation to hazard failures. Additionally the EN 50 129 for each safety integrity level defines principles which are intended to minimise 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 «safety evidence report». This is a document which is verified by independent safety assessor and seen as company commercial secret and kept only for limited staff of the companies and requiring keeping it secret by all involved people including 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 it-self, while control command system is connected to

a number of other systems by interfaces. The interfaces related failures may cause wrong side failures for a whole active safety system between dispatcher and 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).

Originality and practical value

New and high-effective scope of tests which are necessary for putting new control command installation into service both track-side and on-board are proposed

Control command implementations will significantly improve operational safety, however it is possible only when recommendations defined in this article are taken into account. This means that all the components including interfaces have to meet acceptable hazard rate 10E-9 and have to be properly design, constructed, assembled and maintained, all taking into account whole chain of functions performed and supervised by different railway entities.

Conclusions

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 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 wrong side failure in signalling system must not cause authorised speed higher than the safe one or authorised running distance longer than the safe one.

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

The same applies to all vital systems and interfaces constituting whole active safety system between dispatcher and 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 dispatcher and train driver to the level of such system. SIL 4 must be

doi 10.15802/stp2015/42160

therefore ensured for all components and all interfaces.

Additionally it is important to understand and to take into account that operational safety will not be supported in all situations when control command and/or transmission systems trackside and on-board will not be compatible. This constitutes
a challenge as all lines and all traction vehicles can't be equipped at the same time. First certification process have 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 have to be tested using already accepted on-board equipment and additional on-board equipment have to be tested using 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 design, constructed, assembled and maintained, however operational safety depends on many other solutions and procedures.

LIST OF REFERENCE LINKS

1. Białoń, A. Polish national european railway traffic management system plan / A. Białoń, A. Toruń // Computer systems aided science and engineering work in transport, mechanics and electrical engineering. – Radom : Technical University of Radom, 2008. – P. 37–44.
2. Białoń, A. Problematyka analizy ryzyka w urządzeniach SRK / A. Białoń // Telekomun, Sterow, Ruchem, 2008. – № 2. – P. 17–21.
3. ERA/ERTMS/003204. Functional requirement specification, wersja 5.0, sygnatura. – Poland : ERTMS, 2010. – 98 p.
4. ETCS System Requirements Specification, version 3.2.0, reference UNISIG Subset 0-26.
5. ERTMS 04E117 ETCS/GSM-R Quality of Service – Operational Analysis, 2005.
6. ERTMS/ ETCS RAMS Requirements Specification / UIC ERTMS Users Group, 1998.
7. Pawlik, M. Bezpieczeństwo ruchu kolejowego w legislacji unijnej / M.Pawlik // Technika Sterowania Ruchem. – Warszawa, 2007 – № 4.
8. Pawlik, M. Polski Narodowy Plan Wdrażania Europejskiego Systemu Zarządzania Ruchem Kolejowym ERTMS / M. Pawlik // Technika Transportu Szynowego, 2007. – № 1–2.
9. Pawlik, M. Ruch i przewozy kolejowe. Sterowanie ruchem / M. Pawlik, A. Żurkowski // KOW, Warszawa. – 2010
10. Pawlik, M. Zarządzanie ryzykiem w transporcie kolejowym / M.Pawlik // Technika Transportu Szynowego. – 2013 – № 9. – P. 56–69.
11. Pushparatnam, L. GSM-R Implementation and Procurement Guide V 1.0 / L. Pushparatnam, T. Taylor. – 2009. UIC ISBN 978-2-7461-1631-3.
12. Siergiejczyk, M. Problemy zapewnienia bezpieczeństwa informacyjnego w sieci GSM-R / M. Siergiejczyk, S. Gago // Konferencja Transport XXIw. – 2014.
13. Siergiejczyk, M. Zagadnienia bezpieczeństwa systemu GSM-R w aspekcie wspomagania transportu kolejowego / M. Siergiejczyk, S. Gago // Logistyka. – Poznań : IliM, 2012. – № 6.
14. UIC CODE 950. GSM-R Functional Requirements Specification, version 7.3.0. – France : Intern. Union of Railways, 2012. – 111 p.
15. UIC CODE 951. GSM-R System Requirements Specification, version 15.3.0. – France : Intern. Union of Railways, 2012. – 170 p.

doi 10.15802/stp2015/42160

ISSN 2307–3489 (Print), ISSN 2307–6666 (Online)

Наука та прогрес транспорту. Вісник Дніпропетровського національного університету залізничного транспорту, 2015, № 2 (56)

М. ПАУЛІК[1*]

[1*]Заст. директора Варшавського інституту залізничного транспорту, вул. Chłopickiego Józefa, 50, Варшава, Польща, PL 04-275, тел. +48 22 47 31 070, ел.пошта mpawlik@ikolej.pl, ORCID 0000-0003-3357-7706

УПРАВЛІННЯ КОМАНДНИМИ СИСТЕМАМИ, ЩО ВПЛИВАЮТЬ НА ЕКСПЛУАТАЦІЙНУ БЕЗПЕКУ ЗАЛІЗНИЦІ

Мета. Безпека на залізничному транспорті – нагальна необхідність. Проте складно точно сказати, що означає поняття «безпека», оскільки для різних фахівців це можуть бути різні фактори. В роботі передбачається розкриття аспектів безпеки національної залізниці, що забезпечуються командними системами управління в якості компонента експлуатації залізниць, та описання проблем, пов'язаних із ними. **Методика**. Для досягнення поставленої мети проаналізовані системи сигналізації та управління залізничним рухом. Розглянуто такі аспекти: безпечні відстані між поїздами в міжпідстанційних зонах; запобігання установці суперечливих маршрутів для поїздів, що прибувають та відправляються зі станцій; блокування рухомих елементів перемикачів поїзда в правильному положенні; забезпечення безпеки на залізничних переїздах, що знаходяться на одному рівні з залізницею. Проаналізовано також забезпечення безпечного руху та запобігання перешкодам для поїздів, які курсують по під'їзним та промисловим шляхам. **Результати**. В статті зроблений аналіз системи командного контролю за управлінням безпекою з урахуванням наступних чинників: безпеки самої системи командного контролю; взаємодії між системами сигналізації й управління, з однієї сторони, та адміністративно-командної системи управління і системи управління поїздом,–з іншої. Розглянуті також питання передачі, технічного обслуговування, режимів експлуатації. **Наукова новизна**. Запропоновано нові високоефективні випробування, необхідні для здачі в експлуатацію нової системи контролю. **Практична значимість.** Реалізація командного управління підвищить експлуатаційну безпеку, якщо рекомендації, визначені у цій статті, будуть враховані. Це означає, що всі компоненти, включаючи з'єднання, повинні відповідати допустимому ступеню ризику 10E-9, бути правильно сконструйованими, виготовленими, зібраними, збереженими (з урахуванням всього ланцюжка виконаних функцій) та контролюватися різними залізничними організаціями.

Ключові слова: залізниця; безпека; система контролю команд; електрообладнання; система сигналізації

М. ПАУЛИК[1*]

[1*]Зам. директора Варшавского института железнодорожного транспорта, ул. Chłopickiego Józefa, 50, Варшава, Польша, PL 04-275, тел. +48 22 47 31 070, эл.почта mpawlik@ikolej.pl, ORCID 0000-0003-3357-7706

УПРАВЛЕНИЕ КОМАНДНЫМИ СИСТЕМАМИ, ВОЗДЕЙСТВУЮЩИМИ НА ЭКСПЛУАТАЦИОННУЮ БЕЗОПАСНОСТЬ ЖЕЛЕЗНОЙ ДОРОГИ

Цель. Безопасность на железнодорожном транспорте – насущная необходимость. Однако сложно точно сказать, что означает понятие «безопасность», поскольку для разных специалистов это могут быть различные факторы. В работе предполагается раскрыть аспекты безопасности национальной железной дороги, которые обеспечиваются командными системами управления в качестве компонента эксплуатации железных дорог, и описать проблемы, связанные с ними. **Методика.** Для достижения поставленной цели проанализированы системы сигнализации и управления железнодорожным движением. Рассмотрены следующие аспекты: безопасные расстояния между поездами в межподстанционных зонах; предотвращение установки противоречивых маршрутов для поездов, прибывающих и отправляющихся со станций; блокировка подвижных элементов переключателей поезда в правильном положении. Проанализировано также обеспечение безопасности на железнодорожных переездах, находящихся на одном уровне с железной дорогой; обеспечение безопасного движения и предотвращение препятствий для поездов, которые курсируют по подъездным и промышленным путям. **Результаты.** В работе сделан анализ системы командного контроля управлением безопасностью с учетом следующих факторов: безопасности самой системы командного контроля; взаимодействия между системами сигнализации и управления,

doi 10.15802/stp2015/42160

с одной стороны, и административно-командной системой управления и системой управления поездом, – с другой. Рассмотрены также вопросы передачи, технического обслуживания, режимов эксплуатации. **Научная новизна**. Предложены новые высокоэффективные испытания, необходимые для сдачи в эксплуатацию новой системы контроля. **Практическая значимость**. Реализация командного управления повысит эксплуатационную безопасность, если рекомендации, определенные в этой статье, будут учтены. Это означает, что все компоненты, включая соединения, должны соответствовать допустимой степени риска 10E-9, быть правильно сконструиро-ванными, изготовленными, собранными, сохраненными (с учетом всей цепочки выполненных функций) и контролироваться различными железнодорожными организациями.

Ключевые слова: железная дорога; безопасность; система контроля команд; электрооборудование; система сигнализации

REFERENCES

1. Białoń A. Torun A. Polish national european railway traffic management system plan. Computer systems aided science and engineering work in transport, mechanics and electrical engineering. Radom, Technical University of Radom Publ., 2008, pp. 37-44.
2. Białoń A. Problematyka analizy ryzyka w urządzeniach SRK. *Telekomun, Sterow, Ruchem*, 2008, no. 2, pp. 17-21.
3. ERA/ERTMS/003204. Functional requirement specification, wersja 5.0, sygnatura. Poland, ERTMS, 2010. 98 p.
4. ETCS System Requirements Specification, version 3.2.0, reference UNISIG Subset 0-26.
5. ERTMS 04E117 ETCS/GSM-R Quality of Service – Operational Analysis, 2005.
6. ERTMS/ ETCS RAMS Requirements Specification / UIC ERTMS Users Group, 1998.
7. Pawlik M. Bezpieczeństwo ruchu kolejowego w legislacji unijnej. *Technika Sterowania Ruchem*. Warszawa, 2007, no. 4.
8. Pawlik M. Polski Narodowy Plan Wdrażania Europejskiego Systemu Zarządzania Ruchem Kolejowym ERTMS. *Technika Transportu Szynowego*, 2007, no. 1-2.
9. Pawlik M., Żurkowski A. Ruch i przewozy kolejowe. Sterowanie ruchem. KOW, Warszawa, 2010.
10. Pawlik M. Zarządzanie ryzykiem w transporcie kolejowym. *Technika Transportu Szynowego*. Warszawa, 2013, no. 9, pp. 56-69.
11. Pushparatnam L., Taylor T. GSM-R Implementation and Procurement Guide V 1.0. 2009. UIC ISBN 978-2-7461-1631-3.
12. Siergiejczyk M., Gago S. Problemy zapewnienia bezpieczeństwa informacyjnego w sieci GSM-R. Konferencja Transport XXIw. 2014.
13. Siergiejczyk M., Gago S. Zagadnienia bezpieczeństwa systemu GSM-R w aspekcie wspomagania transportu kolejowego. Logistyka. Poznań, IliM. 2012, no. 6.
14. UIC CODE 950. GSM-R Functional Requirements Specification, version 7.3.0. France, International Union of Railways Publ., 2012. 111 p.
15. UIC CODE 951. GSM-R System Requirements Specification, version 15.3.0. France, International Union of Railways Publ., 2012. 170 p.

Dr. hab., Prof. V. G. Kuznetsov (Ukraine) recommended this article to be published

Received: Feb. 03, 2015.
Accepted: Apr. 15, 2015.

doi 10.15802/stp2015/42160