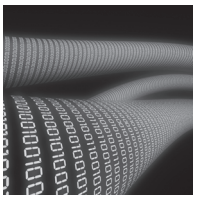

Archives of
Transport System
Telematics

Volume 2

Issue 1

February 2009

Execution of contradictory commands in automatic line block system

W. OLPIŃSKI
Railway Scientific and Technical Centre, Chłopickiego 50, 04-275 Warszawa, Poland,
EMAIL: wolpinski@cntk.pl

ABSTRACT
The automatic line block system may be constructed as a chain of autonomous distributed set of functional blocks located along a railway line section, interlocked by the data transmission subsystem and controlled from two ends of the section. Thus, a certain possibility of simultaneously issued contradictory commands creating conflicts during their execution to be settled by a functional block controlled by them particularly while the data transmission subsystem failure occurs have to be considered. Testing of automatic line block system proper functioning in a range of reaction to contradictory commands and examples of typical conflicts and general rules of solving them are discussed in the paper.

KEYWORDS: railways, signalling, line block

1. Introduction

The main purpose of this paper is to put forward the problem of possible conflicts in signalling systems during execution of commands which may be issued by more than one operator's board with the same entitlement to control the executive equipment.

In some functional states of complex signalling systems, it is possible to encounter situations when a certain command, which may be legally issued from one of the operator's boards, is not allowed to be executed by a functional block due to its current, local functional state. Possible conflicts will be explained on the example of an automatic line block system, where this type of problem was several times identified by the author of the paper, particularly during certification tests of signalling equipment and his involvement, to a certain extent, in different phases of a system development, from requirement specification to exploitation tests, of all electronic automatic line block systems approved until today for their application on railway lines in Poland. [3] ÷ [7].

2. General three-level model of signalling system

Taking into consideration a wide range of railway signalling systems we may find systems developed to control certain, sometimes quite large areas with a number of signalling equipment of a different kind. Such system is usually composed of several separate functional blocks of equipment distinguished by their localisation and purpose. In a large signalling system, it is usually possible to find several identical blocks of particular types. If the complexity level of the signalling system architecture allows isolation of functional blocks which will have features described below, they will be called "control points" further in this paper.

2.1. Control point definition and types

Control point (CP) is a functionally isolated set of equipment which combines an interlocking part and usually an executive part and which communicates with a larger signalling system by the appropriate data transmission subsystem (in the simplest case, by direct galvanic

connections). For the purpose of describing the problem considered in this paper, a three level model of control points' structure is proposed.

On the lowest level, we may define a Slave Control Point which performs the activity only on the base of its executive equipment status and information received by the data transmission subsystem. Received data may include information of the other control points' status with which it is interlocked and commands are sent by a Master Control Point. Master CP may perform all Slave CP activities and it is also able to issue commands to be executed by the other control points of the system. Master CP is usually interfaced with the system operator's board and may be interlocked with the other signalling systems. The system operator's level may be called a Supervisory Control Point and regarded as the third, highest hierarchy control points' level of this model of a signalling system. On that level, we may usually find system operator boards. In the specific type of signalling systems the same role may be played by interfaces with the other signalling systems, as for example station interlocking systems.

Each control point in several strictly defined functional states is allowed to send a command which should be executed by the appropriate executive equipment or functional blocks of the system. In case of Slave, Master or Supervisory CP respectively, their orders are executed by a set of controlled executive signalling equipment, by relevant Master and Slave CPs or by all involved CPs in the system.

2.2. Contradictory commands in static situation

In the first step of the possible contradictory commands consideration, we will take into account static circumstances without detailed analysis of timing relations between these commands. The signalling system operator's board regardless of the signalling system technology, even in relay based systems and obviously in computerised ones is equipped to a certain extent with command filtering functions. The basic purpose of a command filtering function is to avoid the possibility of issuing orders which are forbidden in a certain functional state of controlled system or at least impossible to be executed in a particular situation. This function is also called the command pre-selection.

There is a group of signalling systems which are originally planned to be simultaneously controlled by more than a single operator. In this group, we may find all different types of line block equipment. This first phase of the following considerations will be illustrated on the example of a generic line block system. The line block is a signalling system developed to secure the train movement between two traffic control posts (usually two stations). The simple situation with tracks dedicated only for single direction traffic and thus, the single direction line block equipment is not related to the main subject of this paper. The following considerations will be focused on a situation when a certain, single, open section track is prepared for the train movement in both directions. The basic requirement for a line block system developed for such a case is the determination, in a safety manner, which traffic control post is entitled to use an open section track between these neighbouring posts. Thus, it is necessary to ensure the appropriate procedure of mutual taking over the entitlement to send a train to the open section track. The line block system operation is relatively simple because the considered train traffic runs in a station distance, when due to the traffic rules only single train is allowed to use the open section track. Traffic control by the line block system in such a case has almost only one purpose: the safety exchange of information about entitlement for using the track controlled from these two posts. The appropriate procedure of taking over the entitlement needs the relevant information exchange between two train control posts involved in the train traffic movement on this single, open section track. However, already in this simple case, it is possible to notice that both traffic control posts are generally independent except of the necessity to use common resources (as open section track which connects them). It can be said in other words that both traffic control posts are acting fully asynchronously and only the usage of the connecting them open section track requires a certain synchronisation between these both posts.

2.3. Dynamic relations in execution of contradictory commands

The next step will move us to a consideration of the time relations between commands possible to be sent from Supervisory CPs located on both traffic control posts. As it has been noticed, these posts are fully asynchronous. Thus, it is possible with a very low, however greater than zero probability, that if the current traffic situation and the functional state of a system allows for certain activity, train operators on both posts will start to execute a command in exactly the same moment. It is still not a very complicated problem in case of typical line block system. A more complicated situation occurs when the control point access to common resources has to be performed through a set of slave control points. An automatic line block is a good example of a signalling system constructed that way.

One of the basic requirements for an automatic line block system which are until today always demanded by the Polish State Railways [9], is the real independence of the particular control points comprising the whole

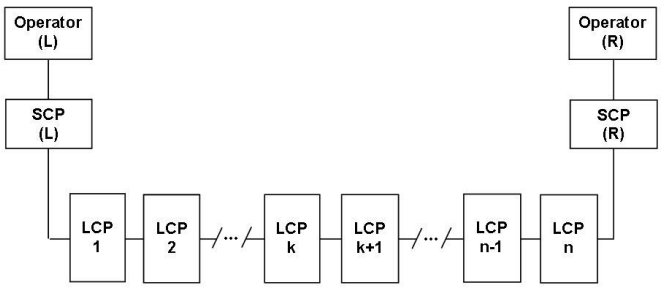

Fig.1.Three-level model of an automatic line block system

system. The main reason for such an approach is the scale of the negative results for the possible train traffic, i.e. for the line capacity, while a failure of a single control point located somewhere in the middle of a line occurs. The second, less justified reason is probably originated in the safety philosophy of previous, relay based systems. The idea, sometimes also implemented somehow in new electronic systems is based on the solution that the train detection subsystem is connected with the automatic line block in such a way that the track occupation by the train results in physical cut of the interlocking data transmission to the preceding line block post, which makes the red light on the controlled line block signal. The similar safety philosophy may be also found in later, more sophisticated, fully electronic systems [2]. Regardless a physical level of an interlocking data transmission subsystem, a logical structure of this subsystem allows to take into account received data, even physically available, only when an appropriate, intermediate control point is functioning properly and permits these data to pass through, i.e. it is confirming appropriateness of this data usage. So, each control point in its certain functional state may block the interlocking information to pass through, at least logically. Abandoning of this functionality is not reasonable, because a proper operation of all subsequent CPs is needed to provide the expected performances of a complete automatic line block system.

3. Three-level hierarchic model of automatic line block system

A typical structure of a generic automatic line block system is shown on Figure 1. There may be found three levels of functional blocks, as mentioned above. On the lowest hierarchical level (Slave CPs) there are Line Control Points (LCPs) connected to train detection equipment and an automatic line block distant signals located along an open section of a railway line. On the higher level (Master CPs), intermediate in our three-level model, we may find Station Control Points (SCPs), typically interfaced with a station interlocking equipment and with a system operator's board, which may be recognised as the highest level of control points i.e. Supervisory CPs.

The generic line block system model is appropriate also for the case when the system is not equipped with LCPs. Such a system may be treated identically as a line block operating on a single open section connecting two traffic control posts. In one step more complicated case, a single LCP (i.e. for n=k=1) on a double direction line controls two signals oriented in the opposite direction and performs a warning signal function for station entrance signals. Both these cases are not good examples for the further considerations of the main subject of this paper. For the purpose of contradictory commands execution problem analyses, we should take into consideration the situation when $n \geq k \geq 2$.

Firstly, we can take into account the line block equipment or any other system in which both asynchronous Supervisory CPs exchange information directly and in which the final functional state of a system depends only on their mutual agreement based on that data exchange. The possible conflict situation in such systems will not cause any big problem. Moreover, it is usually well thought-out during a system requirement definition and development. It is also appropriately checked in the test and operation phases. The situation is not so comfortable in systems that are more complex. Then the contradictory commands execution will create substantially greater problem than in a simple line block system or any other system in which both control posts exchange information directly with each other. It is a practical result of the situation that commands introduced on both ends of line will have to be appropriately recognised, judged and executed by particular local control post situated on the line between two station control posts.

3.1. Natural solution in simple cases

As it was mentioned above, it is possible to imagine several different functional states of an automatic line block system when certain commands are allowed to be issued by a system operator on each end of a line section, thus they are not blocked by a filtering function.

For example, we may take into account the situation when any specific traffic direction is set on the track. In such a case, the track (being more accurate, the line block control equipment) is in a state so called "neutral". In the neutral state, each of two operators has the same possibility to introduce the procedure to take over the control of train traffic on the open section track to prepare a train departure to the neighbouring station. Thus, it is possible to analyse the situation, when both operators are introducing

their commands simultaneously, what is allowed for each of them in a certain moment and a current local traffic situation. However, these commands are in mutual contradiction taking into account available resources (single open section track in this case). It is important to assume, that we are not considering the problem of simultaneous events with the time resolution of the intermediate states of the particular switching parts, either relay or electronic, but in the time range of particular system functional states and exchange of information between co-operating systems, also without consideration of the data propagation time in the physical communication channel. It is possible to conclude, that the first approach should be analysed on a generic equipment and data transmission safety evaluation level [2], while the signalling equipment functioning on the application level is considered.

In the simple case, when both operators are introducing an appropriate and allowed command, but contradictory from the point of view of the resources usage, in all real systems and situations always one of line block ends will "win" the competition – it is a practical result of an obvious phenomenon that any relay or electronic latch circuit may be only in one of two stable states except of a certain intermediate, temporary, not defined state during switching. An appropriate equipment development and tests ensures, that the equipment will always finish the physical level intermediate state and reach the certain functional state, even if we may call it "temporary" or "intermediate" on the application level.

The Supervisory CP, particularly the system operator's board, receives information about the functional state of all necessary signalling equipment. This information may be called the functional state of this CP (or generally, the functional state of a line block system). In the defined functional state of a whole automatic line block system, each of two operator's boards may be locally in a different functional state. It means that in a certain moment, a different set of legal commands may be available on each of the line ends. For the consideration purpose of a contradictory command execution, all possible command pairs in all system functional states shall be analysed.

3.2. Limited command execution time

The basic set of requirements for an automatic line block system, similarly to any other signalling system, includes restrictions regarding particular command execution time. It means that in most cases any intermediate state between two subsequent stable functional states should be strictly limited due to its occurrence time. If during a certain assumed time, the final stable state is not achieved, the equipment shall perform one of two possible actions. Either it shall return to the previous stable state, in which it was before beginning of the command execution, or it shall go to the defined stable "safety" state [1], [9]. The specific system activity, which may be described as storing of commands or putting them on the stack of orders to be subsequently executed, is also strictly forbidden. In most of typical signalling system solutions, it is not possible by the system to accept any next subsequent command until the previous one is finally executed and the system has achieved expected stable functional state [8]. For some defined commands, a certain cancelling commands are available. They may be legally issued during the execution of previous command which is supposed to be cancelled.

The purpose of command execution time limits is to avoid the possibility of blocking the operator's board and make it impossible to issue any other command before the final execution of previously issued command (for which the cancellation command is not used). Such a situation may occur due to many different causes, particularly on possible system failures. One of obvious reasons of such a problem in the automatic line block system may be the data transmission subsystem failure. The combination of contradictory commands execution with the possible data transmission failures creates a lot of problems which shall be well thought-out and solved during the system development. It is also a big challenge for the system testing process to simulate appropriately such possible situations and prove that the system always reaches either an appropriate stable state or the safety state.

3.3. Transmission subsystem failures

The automatic line block system, if constructed as a chain of autonomous Line CPs is to a certain extent tolerant to data transmission subsystem failures. It is important particularly on long open sections with a relatively big number of distant signals. If a break of the data transmission occurs when the appropriate direction of automatic line block is set, it will be still possible to use the system in such a degraded mode. Than, each subsequent train speed reduction is limited only on a single part of an open section between two subsequent distant signals. It is not important which real reason of the data transmission break happened. Either it may be a subsystem failure or only a "logical" break caused, for example, by true or in a worse case, wrong information received from train detection equipment. Unfortunately, the unexpected occurrence of a data transmission subsystem failure during the execution of commands sent from Supervisory CPs can create several problems. The purpose of these commands is usually to change the whole automatic line block functional state. Depending on the given system architecture and functions, the examples of the system functional state change may include a line block direction change, turning

off the system to the neutral state or setting the direction by turning it on from the neutral state. All such possible cases should be well thought-out during system development. Some possible results of the data transmission failures combined with the execution of system control commands may be accepted, although, even if it is not the case of contradictory command execution, some cases of such superposition of operational events and failures may be dangerous and should be certainly avoided.

We may try to define here a set of possible wrong behaviours of the automatic line block occurred as a result of transmission subsystem failures. First of all, it should be absolutely excluded that after any combination of subsequent events including commands and transmission subsystem failures, a line block will be split up into parts in a way that it would be possible to send trains from both stations with line-clear signals on exit semaphores. It means exactly the same that along the whole open section equipped with several distant signals, there will never appear the situation that any two signals:

- one controlled from the Line CP with a number from 0 to k (see fig. 1) for the train running in left-to-right (R) direction to Station CP (R),
- the other controlled from the Line CP with a number from k to n (see figure 1) for the train running in right-to-left (L) direction to Station CP (L),

will be able to show simultaneously a line-clear signal (or even red lights).

It should be also avoided that due to possible events, limited command execution time will be exceeded, i.e. that an intermediate system state caused by such a command execution will last longer than certain restricted time. The effect of commands storage also should not occur. On the contrary, it may be accepted as a result of some events that automatic line block is split up allowing trains to run from a line to stations. It means that it may be allowed to have some signals from k to 0, for the train running to Station CP (L) turned on simultaneously with some signals from k+1 to n which face the train running to Station CP (R). The condition mentioned above to exclude the opposite situation shall be also concurrently fulfilled.

4. Conclusions for future research

Possible results of system control commands execution disturbed by the transmission subsystem failures are usually well-thought and solved, thus all conceivable wrong side effects are excluded by the system hardware and software construction. However, the author's practice allows stating that more often than expected, the automatic line block systems treated by their developers as "almost ready" version, i.e. prepared to first functional and safety tests, still are not resistant to the combination of transmission subsystem failures combined with the execution of contradictory commands legally issued on both operator's boards at the same time. Moreover, these kinds of possible conflicts during execution of commands as well as rules to solve implicated problems are usually not defined in typical signalling system functional requirements. The lack of comprehensive description defining the expected system behaviour if similar commands execution problem occurs simultaneously with relevant system failures is even more frequent.

It seems advantageous to develop general principles of solving conflicts which may occur during the execution of commands which are contradictory on the executive functional block level in complex signalling systems, similar to the ones mentioned in the paper. Necessary rules of settling that type of competency problems should be thoroughly defined in the system requirement specifications.

From similar reasons, typical test procedures usually cover the checking of all commands in all possible system functional states. However, very often the situation of simultaneous execution of commands which may be legally issued by both operators, particularly with consideration of disturbances caused by the transmission subsystem failures, is not appropriately solved. Thus, a research unit authorised to carry out signalling equipment and systems certification assessment shall prepare and perform functional and safety tests. These tests shall be complete and particularly able to check possible effects of contradictory commands legally issued at the same time on both system Supervisory Control Points in all conceivable cases including failures of the data transmission subsystem.

It also seems reasonable to invent general principles of creating test procedures to ensure their ability to check all possible conflict situations during the execution of contradictory commands both in an undisturbed system operation and in case of various failures, particularly in interlocking data transmission subsystem. The important condition to achieve expected safety level of newly developed complex signalling systems is to provide system evaluators with well-defined test procedures to be followed instead of relying on the evaluator's experience as the basic safety determinant.

Bibliography

[1] EN 50129:2007, Railway applications: Safety related electronic systems.

[2] EN50159-1:2001, Railway Applications: Communication, Signalling, and Processing Systems - Part 1: Safety-related Communication In Closed Transmission Systems.

[3] OLPIŃSKI W.: Opinion on automatic line block SHL-12 type in single section version., CNTK, task 4171/10, Warsaw, December 2006.
[4] OLPIŃSKI W., TORUŃ A.: Automatic line block SHL-1 computer system adapted to co-operation with Ebilock 950 type interlocking system. Technical opinion., CNTK, task 4250/10, Warsaw, June 2007.
[5] OLPIŃSKI W., TORUŃ A.: Rapport from exploitation test of the automatic line block system SHL-1 version 01 type., task 4283.04/10, Warsaw, May 2008.
[6] OLPIŃSKI W.: Automatic line block SHL-1 version 01 type. Technical opinion., CNTK, task 4283.04/10, Warsaw, September 2008.
[7] OLPIŃSKI W.: Automatic line block SHL-12 version 02 computer system. Technical opinion, CNTK, task 4362.04.10, Warsaw, March 2008.
[8] Principles of Technical Approval for Signalling and Communications Technology - Mu 8004, Deutsche Bundesbahn.
[9] Safety requirements for railway signalling systems introduced as binding by General Direction of Polish State Railways document no. KA2b-5400-01/98, Warsaw, February 1998.