Synthesis of safety functions for railway automation and telemechanics systems

Michael N. Vasilenko**,** Peter A. Vasilenko, Valentin A. Hodakovskij

Department of "Automation and telemechanics on railways"
Petersburg State Transport University
Emperor Alexander I

Abstract
The language of description of track objects (LTO) is a powerful tool for working with electronic technical documentation of railway automation and telemechanics. The principles of construction, areas of application, syntax and semantics of LTO were described in a previously published article [1,2]. The software implementation of this language in the object format of technical documentation in the XML extensible markup language is described in [3]. The analysis of the systems of railway automation and telemechanics from the point of view of functional safety, based on the application of the logical principles of the language of track objects. An approach is given for the formation of a complete set of safety functions for station automation systems, based on the technical documentation of the railway.

Keywords
electronic technical documentation, language for describing track objects, schematic plan of the station, dependency table, letters, words and sentences of LTO, safety functions, train traffic safety

1. Introduction

The principles of constructing the language for describing path objects (LTO) and its application areas, syntax and semantics are described in [1,2]. [3] describes the software implementation of LTO in the branch format of technical documentation (IFTD) used in computer-aided design and technical documentation systems and provides examples of grammatical constructions of LTO in the extensible markup XML language for a schematic plan of a station (SSP) and a table of interdependence of arrows and signals (TD). This article is devoted to the formation of a complete set of safety functions for ATS using the basic conditions defined in the theory of construction of safe RATS.

The algorithm for the synthesis of a complete set of safety functions is developed on the basis of LTO and digital models of SSP and TD.

2. Basic set of security features

The theory of synthesis of safe systems of railway automation and telemechanics (RATS) provides a solution to two main problems [4-6]:

1. Automation of train traffic control.
2. Ensuring the safety of train traffic.

To ensure the safety of train traffic, scientists of the Department of Automation and Telemechanics on Railways of the St. Petersburg State University of Railways of Emperor Alexander 1 developed a theory of safety [4-6] and determined the conditions for systems ensuring functional safety, the fulfillment of which is necessary for organizing train traffic at a station equipped with electrical interlocking system (EC) - regardless of the technical implementation (relay, relay-processor, microprocessor)

These conditions were first formulated in [6] for all technological operations with routes (Table 1). The list of implementation given in [4, 5] will be called the basic set of safety functions (BSSF).

Because of traffic safety violations, a threat to life and health of people is created, significant material damage is inflicted on the state, cargo is lost, expensive equipment is put out of action.

Table 1

Basic set of security functions

№	Security features
1	control of the end position of the running switches;
2	control of the correct position of the guard switches;
3	control of lack of transfer of switches to local control;
4	checking the absence of closure switches in other routes;
5	control of the free running sections;
6	control of the freedom of oversized sections;
7	checking for no cancellation of routes;
8	checking the absence of artificial cutting;
9	checking the actual closure of sections in a given route;
10	checking the opening of sections when canceling the route according to the specified algorithm;
11	checking the opening of sections during artificial cutting according to a given algorithm;
12	protection of closed sections from premature opening when applying and removing a shunt on the rail circuit;
13	protection of closed sections from premature opening when switching power feeders;
14	protection of closed sections against premature opening in case of loss of a shunt for a specified time;
15	control of the freedom of the receiving and dispatching track; front contact of path relay П;
16	control of the absence of assignment of hostile (frontal) routes in the opposite throat of the station before assigning a route to this receiving-departure route;
17	verification of the absence of transfer of the receiving-departure track to the local control in the opposite throat;
18	checking the absence of inclusion of the fence of the receiving and dispatching track;
19	checking the actual exclusion of frontal routes for a given receiving and departure route after setting the route;
20	control of the freeness of the first block removal section during auto-blocking;
21	control of the presence of the wand key in the control apparatus;
22	control of the correctly set direction of movement with two-way auto-blocking;
23	checking the actual closure of the direction change circuit with two-way auto-blocking;
24	control of the freedom of the haul with semi-automatic blocking;
25	control of compliance of the signal indication of the traffic light with the Instruction for signaling on the railways of the Russian Federation;
26	control of the absence of inclusion of an invitation signal indication at a traffic light;
27	control of the closed state of hostile traffic lights;
28	checking the closed state of obstruction traffic lights (control of the absence of activation of the obstruction alarm at the crossing);
29	checking the inclusion of permissive signal indications at a traffic light with a time delay sufficient to close the movement at the crossing;

BSSF is mandatory for most stations equipped with EC on any element base. This set is minimal and describes only the basic safety functions of the station systems of the railway. In the event that the station is equipped with additional RAT devices (for example, a rolling stock derailment control device, control and gauge devices, and others), the BSSF should be supplemented with appropriate safety functions.

In [1,2], the LTO alphabet and its correspondence to the SSP elements are defined, and in [3], a description of LTO in XML is defined. The safety functions in Table 1 can be compared with respect to the letters LTO (elements of the SSP), such a correspondence is given in Table 2.

Table 2
Compliance of security functions with the letters of LTO

Element of SSP	Element of LTO	Number of SF (from table 1)
Switch	S	1,2,3,4
Traffic lights	F	25,26,27
Block joint	C	5, 6, 7, 8, 9, 10, 11, 12, 13, 14
Path section	L	
Crossing	P	28,29

Since the BSSF (Table 1) contains a description of the specific elements of the SSP (for example, the receiving-departure track in LTO is a subspecies of the track section), Table 2 can be specified using the non-terminal LTO dictionary. (Table 3).

Table 3
Correspondence between SF and LTO using a nonterminal dictionary.

Element of SSP	Element of LTO	Number of SF (from table 1)
Traffic lights	F	{25, 26, 27}
Crossing	P	{28, 29}
Centralized switches	S	{1, 2, 3, 4}
Switch and non-switch section of the path	L,C	{5, 6, 7, 8, 9, 10, 11, 12, 13, 14}
Receiving and sending way	<RSW>	{15, 16, 17, 18, 19}
Area of approach and removal	<AAR>	{20, 21, 22, 23, 24}

Table 4 shows the correspondence of the LTO letters to the XML attributes and security functions.

Table 4
Correspondence of SSP elements to the letters of LTO, XML and SF attributes

Element of SSP	Element of LTO	Attribute XML	Number of SF (from table 1)
Traffic lights	F	<Traffic lights Id = "" (identifier) X = ""(coordinate x) Y = "" (coordinate y) PurposeLight = "" Typeoftrafficlight = "" NumofLights = "" … Signaling = ""/>	{25, 26, 27}
Crossing	P	<Crossing Id = ""(identifier) X = ""(coordinate x) Y = "" (coordinate y)	{28, 29}

		Serviced = "" Category = "" Length = "" … LatencyACS = ""/>	
Centralized switches	S	<Switch Id = ""(identifier) X = ""(coordinate x) Y = ""(coordinate y) SwitchType = "" RailType = "" BrandCrosspieces= "" … RadiusCurve =""/>	{1, 2, 3, 4}
Switch and non-switch section of the path	L,C	< Path section Id = ""(identifier) X = ""(coordinate x) Y = ""(coordinate y) Appointment = "" Specialization = "" NonstopPass ="" … High-speed movement =""/>	{5, 6, 7, 8, 9, 10, 11, 12, 13, 14}
Receiving and sending way	< RSW >	<Path section Id = ""(identifier) X = ""(coordinate x) Y = ""(coordinate y) Specialization = " receiving and dispatching" Specialization = "" Nonstop Pass ="" … High-speed movement =""/>	{15, 16, 17, 18, 19}
Area of approach and removal	<AAR>	<Path section Id = ""(identifier) X = ""(coordinate x) Y = ""(coordinate y) Specialization = "approximation removal" Specialization = "" Nonstop Pass ="" … High-speed movement =""/>	{20, 21, 22, 23, 24}

The movement of trains at stations equipped with EC systems is routed and, therefore, all routes have a clear set of properties, which include: Route type, technological operations with the route, route components. During the movement of trains, four types of routes are distinguished (proposals of LTO): departure , reception, transfer, shunting. The implementation of the LTO proposals corresponding to certain routes in the TD

3. Algorithm for the synthesis of a complete set of safety functions.

Using the digital model of TD and SSP in the IFTD format, it is possible to form a complete set of security functions (FSSF). To do this, it is necessary to write down the SF of all letters and formation module and the description of the parameters in XML is given in [3].

words (elements of the SSP) for all LTO proposals (TD routes). The FSSF synthesis algorithm is shown in Figure 2. FSSF is recorded as a table of safety functions (TD) for all routes.
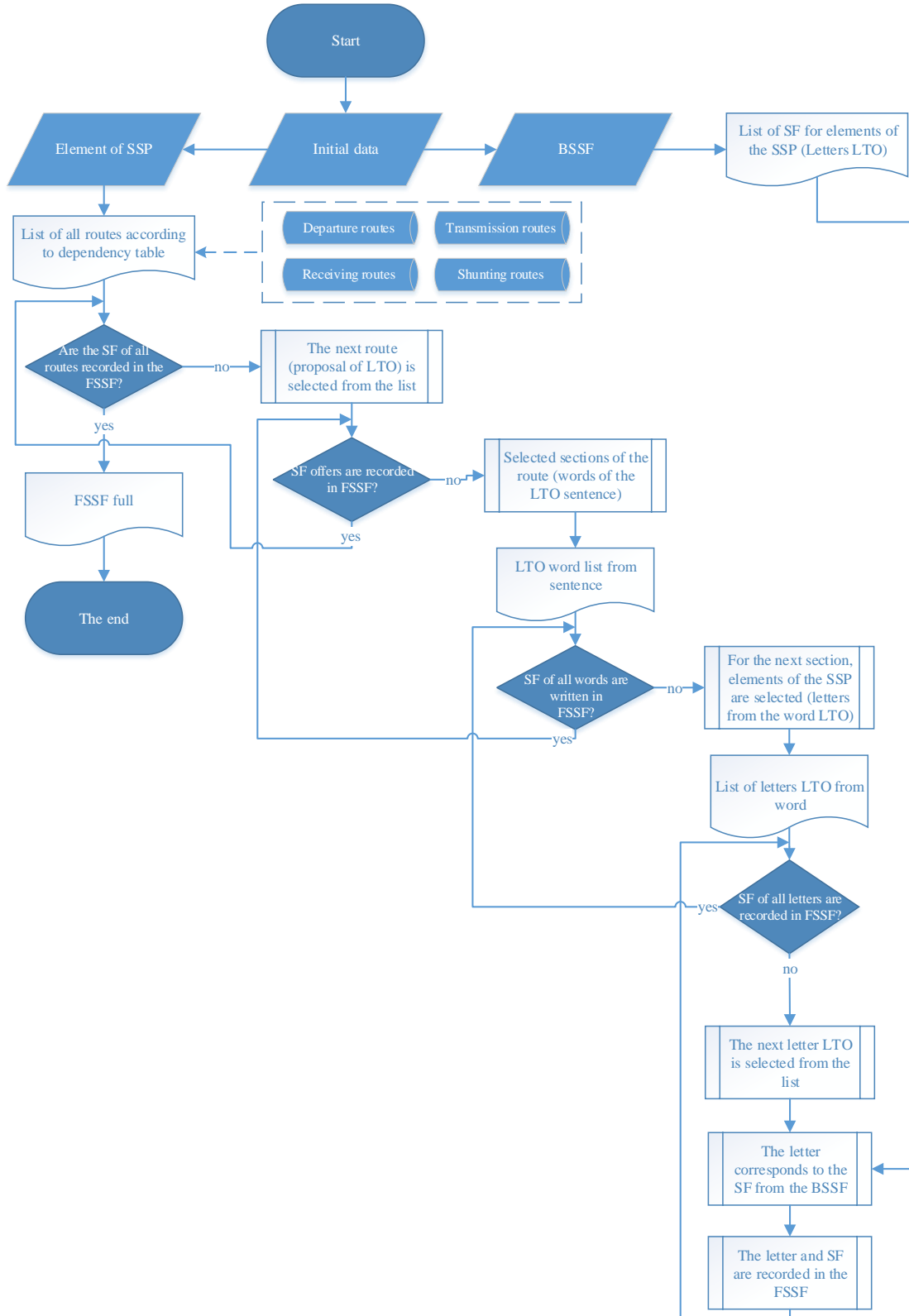
Figure 1: Algorithm for the formation of FSSF

4.   Conclusions

The concept of a basic set of safety functions for EC systems is introduced, which can be supplemented with the development and modernization of systems.

It is shown that the expansion of the basic set into a full set of safety functions for a particular plant can be achieved on the basis of a formal synthesis algorithm using technical documentation for the RAT systems.

References

1. Vasilenko M.N., Vasilenko P.A., Telezhenko T.A Principles of construction and application of the language for describing track objects of railway automation and telemechanics // Automation, communication, informatics. 2020. No. 5. S. 23-29.
2. Vasilenko M. N., Vasilenko P. A., Telezhenko T. A. Principles of construction and application of the language for describing track objects of railway automation and telemechanics // Automation, communication, informatics. 2020. No. 7. P. 15-21.
3. Vasilenko M.N, Vasilenko P. A., Bulavsky P. E. Software implementation of the language of track objects in the automated workstation for maintaining technical documentation // Automation, communication, informatics. 2020. No. 8. S. 29-33.
4. Works on the theory of synthesis and diagnosis of finite automata and relay devices / Ed. V.V.Sapozhnikova, Vl. V. Sapozhnikov - SPB: "ELMOR", 2009 - 900 p.
5. Microprocessor centralization systems: textbook. for technical schools and colleges of railway transport / Vl. V. Sapozhnikov, V. A. Kononov, S. A. Kurenkov and others; ed. Vl. V. Sapozhnikov. - M .: UMTs ZhDT, 2008, - 398 p.
6. Basics of designing electrical interlocking of intermediate stations / Kononov V.A., Lykov A.A., Nikitin A.B. - Ed. Route 2003, -315s.
7. Vasilenko MN, Bubnov VP, Bulavskiy PE, Vasilenko PA Errors in technical documentation of railway automation and telemechanics and their impact on the safety of train traffic. Automation in transport. 2019. No. 1. Volume 5.S. 94-112.