Synthesis of Full Functional Check Programs for Train Traffic Management Systems on a Railway Station

M A Gordon¹, P A Vasilenko², D V Sedykh²

¹ Institute "Giprotranssignalsvyaz" – Department of JSC "Roszheldorproject", Saint-Petersburg, Russia
² Emperor Alexander I St. Petersburg State Transport University, Saint-Petersburg, Russia
gordon_ma@mail.ru

Abstract. The article describes the technology for synthesis of full functional check programs for train traffic management systems. Algorithms for synthesis of a full set of safety functions and synthesis of minimized set of safety functions are also presented.

1. Introduction

Railway Signaling and Interlocking systems are required to ensure safe control of railway train traffic. These systems, regardless of the hardware base (relay or microprocessor) are discrete, i.e. they are described by Boolean expressions [1].

To synthesize programs for full functional checks of the interlocking system, one can use the main drawings of the technical documentation for this system that describes all the functionality, - a Schematic Plan of the Station (SPS) and a Table of Correlation (ToC) in a formalized form [2, 3].

In order to determine conditions for safe functioning of interlocking systems, it is reasonable to use topological formulas wherein the following symbols are introduced.

\[ A = \{a_1, a_2, \ldots, a_N\} \]

\[ |N| = |S_i| + |S_w| + |T_s| + |T_r| + |T_d| + |W| + |B| + |U| + |G| + |C_s| + |C_d| \]

The check program is written as a sequence of actions at the control unit of the interlocking system and correct (reference) produce response of the system to this action \( Z_{\text{ref}} \). If the actual produced response coincides with the reference response \( Z_{\text{ref}} \), the check shall be considered completed and the transition to the next check shall be performed. In case of noncoincidence \( Z_{\text{ref}} \neq Z_{\text{act}} \), the check program stops until the cause of the noncoincidence is eliminated (diagnostics of the noncoincidence cause to be undertaken and the cause to be eliminated).

The main means to conduct checks is the control unit of interlocking systems (monitor, display, devices to monitor state of objects, etc.). The control unit shall ensure comprehensive check of interlocking systems by simulating various technological situations at the station when setting, cancelling, releasing...
and emergency releasing of routes. The comprehensive check must also include a list of checked tasks and functions, approved by the Technical specification for the object.

The following 2 groups of tasks are identified among the tasks determined in the Normative and Reference Documentation for interlocking systems that shall be checked during start-up & commissioning and acceptance tests:

– Control Automation Task (CAT);
– Functional Safety Task (FST).

Each task shall be described by a set of functions to be checked during the start-up and commissioning: \( \text{CAT} = \{f_1, f_2, \ldots f_i\} \), where \( f_i \) is the \( i \)-th function of the control automation task, \( i = \bar{1}, \bar{J} \). Total number of functions is 88. \( \text{FST} = \{b_1, b_2, \ldots b_j\} \), where \( b_j \) is the \( j \)-th function of the functional safety task, \( j = \bar{1}, \bar{J} \). Total number of functions is 29.

List of functions and tasks \( S = \{\text{CAT, FST}\} \) shall be developed and approved at the stage of design, getting agreements and approval of schematic plan of the station (SPS) and tables of correlation between the railway track switches and signal indications in routes (ToCs).

Control automation tasks are classified as per the controlled object as follows:

– Power switch control tasks;
– Railway signal light control tasks;
– Control tasks of fixed devices for securing wagons;
– Tasks of implementation of the specified train or shunting route;
– Tasks of interaction with various devices and systems;
– Tasks of monitoring technological condition of track objects;
– Joining traction stations control tasks.

According to control modes, functional safety tasks are classified as follows:

– Tasks of the primary mode of objects control. This mode shall be operated when the control devices are in good working condition. In the primary mode, safety conditions of railway traffic at the station shall be automatically checked;
– Tasks of secondary control mode. The interlocking system should switch to this mode if it is not impossible to automatically check of railway train traffic safety conditions to the extent required to enable clear signal at the traffic light. Route in the secondary mode shall be set without turning the clear signal of traffic light on;
– Tasks of emergency control mode. This mode shall be applied in case when use of the primary or secondary mode of route object control is impractical. Operation of the station system in emergency control mode shall be under responsibility of the railway station duty officer.

Standard test procedures have been developed for all interlocking systems (relay, relay-processor, and microprocessor). Standard Test Procedure (STP) is a document regulating procedure of conduction of “idle” individual testing and integrated tests of interlocking systems. The checks described in STP are the complete verification test for all Safety Functions (SF) of the system. A Safety Function is a function whose violation may lead to a dangerous situation during train traffic. In other words, STP is a combination of tests to be conducted during operational acceptance of interlocking system (as per all CAT, FST, etc. tasks) without reference to the controlled object (station, wayside equipment, route, etc.)

Basic Set of Safety Functions (BSSF) is determined in the normative and technical documentation [4]. Each function from the basic set \( b_i \) is compared with a certain element of the SPS (\( S, S_n, T_n, T_r \) and others) and indicated in the BSSF table. For this reason, synthesis of all safety functions of a given station is carried out according to the ToC and SPS model, which is described in XML language in the software implementation. This set of functions (set of all safety conditions for all routes applicable at the station) is called a Full Set of station Safety Functions (FSSF). Thus, FSSF is an analogy of the complete verification test for all Safety Functions of the system.

The minimized set of safety functions is the set obtained by reducing the FSSF considering criterion of the exclusion of repeated SFs when checking identical elements of the station schematic plan (SPS) in different routes. The Minimized Set of Safety Functions (MSSF) shall maintain completeness of checks for all elements of SPS.
For actual testing during start-up and commissioning, a performance criterion for each SF is required. This criterion shall be a strictly defined list of actions, upon completion of which fulfillment or non-fulfillment of the SF may be explicitly found. For BSSF, this is a Description of the Test Methods (DTMSF).

All tests specified in STP generate a set of tests $T = \{t_1, t_2, \ldots, t_n\}$, where $n = 1/\bar{N}$, $N$ is a number of tests. Each test has the following parameters:
- Tested Object: station, route, track section, track switch, signal light, crossing over.
- Technological Operation: setting, cancellation, releasing, emergency releasing of routes.
- Operating Mode: primary, secondary, emergency.

Each test described in the STP corresponds to a detailed description of the test procedure.

2. Synthesis of a full functional check program

Information structure of the synthesis of full functional check programs is shown in Figure 1.

![Figure 1](image)

The algorithm of synthesis of full functional check programs includes the following steps:

Step 1. Enter a new schematic plan of the station or edit the existing schematic plan of the station at the automated workstation where technical documentation is used. In this case, a specialized module for generation of a schematic plan with full compliance with the object format of the technical documentation is used.

Step 2. Use the specialized module to synthesize the ToC automatically. Since the resulted ToC includes all possible routes, their number is reduced based on the routes that will be actually used for movement at the station. After that, the ToC shall be approved.

Step 3. If required, make amendments in BSSF. Amendments in BSSF shall be made depending on the specific features of interlocking systems and devices used at the station.

Step 4. Synthesize FSSF based on BSSF and approved ToC.

Step 5. Synthesize MSSF: minimize FSSF as per the criterion of exclusion of repeated FSs when checking identical elements of SPS in different routes.
Step 6. Synthesize Description of Test Methods for Safety Functions (DTMSF).

Step 7. Generate an electronic test logbook (ETL) based on MSSF and DTMSF. In ETL, each SF from MSSF corresponds to DTMSF. If the actual response of the system coincides with the reference one for all lines of ETL, the testing may be accepted as satisfactory. Otherwise, stop the testing until diagnostics of the reason for such noncoincidence is made and the same is eliminated.

3. Synthesis of a full set of safety functions

For synthesis of FSSF – algorithm shown in Figure 2 is used.

![Figure 2. Algorithm of FSSF synthesis.](image)

Input data for the algorithm are:

- SSP in a formalized form.
– ToC synthesized based on SPS.
– BSSF.

Main steps of algorithm are:
Step 1. Based on ToC, a list shall be generated to include all routes, and all sections for each route that are covered by the route, and all SPS elements for each section that are covered by the section.
Step 2. For each element from the list, a SF from BSSF shall be brought to correspondence with each element from the list.
Step 3. Combination of each element with a SF shall be recorded into FSSF being a table where every SPS element corresponds to a SF.

4. Synthesis of minimized set of safety functions
To synthesize MSSF, use the algorithm shown in Figure 3.

Figure 3 Synthesis of MSSF.
Input data for the algorithm is FSSF.

Main steps of algorithm are:

Step 1. From the FSSF list, obtain a list of all SPS elements with SFs corresponding to them.
Step 2. Make a template of MSSF Table and enter the first FSSF element into this Table.
Step 3. Perform identification for each element from the Table: check if there is an element with similar ID and SF in the MSSF Table; if yes, skip the element, if no, add the element to MSSF. After identification of the last element, the resulted Table presents MSSF.

5. Conclusion
Based on SPS and ToC, the authors have developed algorithms for generation of a full and minimized set of safety functions (FSSF and MSSF), and an electronic test logbook (ETL) has been developed to display the checks.
The worked out solutions enable excluding the human factor in development of check programs and not missing any of the safety conditions, which is critical for the train traffic safety systems.

References
[1] Theeg G, Vlasenko S (eds.) et al 2018 Railway Signalling & Interlocking: International Compendium 2nd revised edition, ed G Theeg and S Vlasenko (Leverkusen: PMC Media House GmbH) p 458
[2] Sedykh D, Gordon M and Efanov D 2018 Computer-Aided Design of Railway Signalling Systems in Russian Federation Proceedings 2018 International Conference on Industrial Engineering, Applications and Manufacturing (ICIEAM) (Moscow: Moscow Polytechnic University) pp 1-7
[3] 2017 GOST 33894-2016. Railway automatics and telemechanics systems on railway stations. Safety requirements and methods of checking (Moscow: Standartinform) p 30
[4] Winter K, Johnston W, Robinson P, Strooper P and Vanden Berg L 2005 Tool Support for Checking Railway Interlocking Designs Proceeding of the 10th Australian Workshop on Safety Related Programmable Systems (SCS'05) (Canberra: Australian Computer Science Communications) pp 101-107
[5] Sedykh D V, Vasilenko P A and Gordon M A 2019 Report on Research & Development Work: "Research of Methods of Automation for Synthesis of Full Functional Check Programs for RAT Systems" (Saint-Petersburg: GK Imsat OOO) p 125