Pamukkale Üniversitesi Mühendislik Bilimleri Dergisi

Pamukkale University Journal of Engineering Sciences

THE APPLICATION OF AUTOMATION THEORY TO RAILWAY SIGNALING SYSTEMS: THE TURKISH NATIONAL RAILWAY SIGNALING PROJECT

OTOMASYON TEORİSİNİN DEMİRYOLU SİNYALİZASYON SİSTEMLERİNE UYGULANMASI: ULUSAL DEMİRYOLU SİNYALİZASYON PROJESİ

Mustafa Seçkin DURMUŞ [1], Uğur YILDIRIM[1], Mehmet Turan SÖYLEMEZ[1]*

[1]Control Engineering Department, Istanbul Technical University, TR-34469, İstanbul, Turkey.
durmusmu@itu.edu.tr, yildirimu@itu.edu.tr, soylemezm@itu.edu.tr

Received/Geliş Tarihi: 04.01.2013, Accepted /Kabul Tarihi: 28.02.2013 doi: 10.5505/pajes.2013.14633
*Corresponding author/Yazışılan yazar

Abstract

When compared with the other transportation systems, railway systems are economical, safer and more environment friendly. Despite all these features, investments on railways in Turkey remained quite restricted in comparison to other European countries. The initial construction costs of railways are high and developing its signaling system also requires a lot of attention. Signaling system is the vital part of a railway system which ensures safe travel and transportation on railways. One of the main reasons that make a signaling system critical and hard to develop is to satisfy the recommendations of related functional safety standards such as EN 50128 and EN 61508-3. In this study, functional safety requirements used in railway signaling systems are stated and the use of recommended methods in the Turkish National Railway Signaling Project (TNRSP) are explained. Especially, the software development process and the use of several programming techniques in determination of the software architectures are discussed.
Keywords: Railway signaling system, Railway interlocking system, Functional safety, Petri nets.

Özet

Diğer ulaşım sistemleri ile karşılaştırıldığında, demiryolu sistemleri ekonomik, daha güvenli ve çevrecidir. Tüm bu özelliklerine rağmen, diğer Avrupa ülkeleri ile karşılaştırıldığında Türkiye'de demiryollarına yapılan yatırım oldukça kısıtlı kalmıştır. Demiryollarının ilk inşaat maliyetleri yüksek olup sinyalizasyon sisteminin geliştirilmesi çok büyük dikkat gerektirmektedir. Sinyalizasyon sistemi, bir demiryolu sisteminde güvenli ulaşım ve taşıma yapılabilmesini sağlayan en önemli bileşendir. Sinyalizasyon sisteminin bu denli önemli ve zor geliştirilebilir olmasının temel sebeplerinden bir tanesi, EN 50128 ve EN 61508-3 gibi ilgili fonksiyonel güvenlik standartlarının tavsiyelerinin yerine getirilmesidir. Bu çalışmada, demiryolu sinyalizasyon sistemlerine ilişkin fonksiyonel güvenlik gereksinimleri belirtilmiş ve bu tavsiyelerin Ulusal Demiryolu Sinyalizasyon Projesi (UDSP)'nde kullanılışı açıklanmıştır. Özellikle, yazılım geliştirme süreci ve çeşitli programlama yöntemlerinin yazılım mimarisinin belirlenmesinde kullanımı tartışılmıştır.
Anahtar kelimeler: Demiryolu sinyalizasyon sistemleri, Demiryolu anklaşman sistemi, Fonksiyonel güvenlik, Petri ağları.

1 Introduction

Railways provide more economical and environmental solutions [1] even their initial costs are relatively high. Among different transportation alternatives, for a passenger who travels from Rome to Paris, traveling by train causes less carbon dioxide emission and energy consumption as illustrated in Figure 1. Researches also prove that the lifetime risk of death caused by railways is very low according to different transportation alternatives. For example in the UK, the risk of death for 100 million vehicles per kilometer for travelling by car is 6,780 while it is 520 in railways. Similarly, odds of dying in average year for traveling by airplane are 1 in 4,082,474 while it is 1 in 9,848,485 for railways [2]. As a result of these advantages and the rise in population, the demand on railways increases day by day.

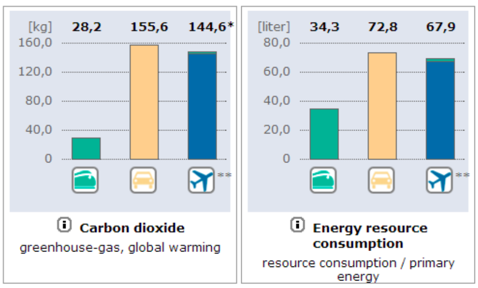


Figure 1. Typical emission and energy consumption [1].

Former railway systems where railway traffic and density were not too much as today did not need any signaling systems. Train drivers are warned about the obstruction in front of their way by the railway guards who show red flag or lamps. By the development of railways in those years, many accidents occurred because of either human (railway guards or even drivers themselves) or nonhuman (component malfunctions) errors. In order to eliminate all these problems, the first interlocking system was established in 1843 in UK [3].

The need of reliable and safe signaling system is much more today than in the past because sometimes failures may result in fatal accidents [4]. In addition to mechanical interlocking systems where the railway traffic operations were realized by signalboxes manually [3], railway control systems such as SMILE [5], STERNOL [6], ELEKTRA [7] and microprocessor-based systems [8] were also used. Many studies on modeling, design and verification of railway signaling and interlocking systems can be found in the literature [9]-[18].

Nowadays, as an alternative way, already certified COTS (Commercial off-the-shelf) solutions are also available in the market provided by several companies [19]-[24].

On the other hand, signaling systems are expected to satisfy safety related standards such as CENELEC (European Committee for Electrotechnical Standardization) standards in Europe. The European standard IEC 61508 [25] is developed for functional safety requirements of all kinds of electronic and programmable devices. In addition to the umbrella standard

IEC 61508, EN 50126 describes the functional safety requirements related with all kinds of railway applications where Reliability, Availability, Maintenance and Safety analysis (RAMS) are determined. EN 50128 (similar to EN 61508-3) determines methodologies for building software for railway control and applications and EN 50129 (similar to EN 61508-2) defines requirements for the hardware of electric, electronic and programmable devices.

A well-known definition arises within these standards known as Safety Integrity Level (SIL). SIL is the probability for the system to execute the safety functions required in all specified input conditions within a specified time interval [26]. For railway interlocking systems, safety integrity level is expected to be at least SIL 3 [27], which will be explained in detail in section 3.

International agreements such as deployment of European Rail Traffic Management System (ERTMS), Turkish State Railways and so development of railway systems in Turkey accelerated. Construction of the railways compatible with ERTMS still continues and the Turkish Government has already planned new investments for future extensions. Within this perspective, developing original, reliable and fail-safe interlocking systems, which constitute one of the most vital parts of the railway signaling systems, is of great importance for Turkey.

The paper is organized as follows. Brief descriptions of railway components are given in the next section. Section 3 describes the determination of SIL and the software design process is explained in section 4. Software tests are explained in section 5 and finally, conclusions are given in section 6.

2 Components of Railway Signaling System

In this section, the definitions of the components that are used in the TNRSP are explained.

2.1 Traffic Command Center (TCC)

All operations on railways such as monitoring the railway traffic and situation of the railway field components (e.g. positions of switches, colors of signals) and scheduling of trains are in the responsibility of the TCC. All railway traffic is managed by the help of the officers (the dispatchers) who request routes for incoming and outgoing trains. In case of an emergency situation, the dispatchers can also talk directly with the train drivers.

2.2 The Interlocking System

The interlocking system can be considered as decision-making software because it checks the incoming requests from the TCC and compares these requests with the actual situation of the railway field equipments. An incoming request is accepted, if all safety criteria are met, or rejected if there are any conflicts or the request is improper. Instead of relay-based interlocking systems (where vital relays are used as interlocking fail-safe components) fail-safe Programmable Logic Controllers (PLCs) [28] and computer-based solutions [22] are already in use for railway signaling systems.

2.3 Signals

Railway signals (or optical wayside signals) are established along the rail line on specific points to inform the train driver about the occupation of the next railway block. Train drivers have to pay attention to the signals on the right side with respect to their direction of movement.

Similar to road traffic lights, red color means that the next block is occupied, so the train must stop. Yellow color means that the next block is free but not the block after that (i.e. the next signal is red, so the train should stop at the next signal). Green color means at least the next two blocks are free, so the train can proceed within speed limits. Unlike road signal lights, however, some railway signals can have four aspects especially near station areas. The fourth aspect, which is a bottom yellow color for the Turkish State Railways, designate a line change ahead (so the train should proceed with reduced speed on switch regions). On the station exits where there is always a line change ahead, dwarf signals are used instead of four aspect signals.

2.4 Switches (Point Machines)

Since railway vehicles do not have any steering mechanism like the road vehicles, they need switches in order to change track when maneuvering in a railway area. Switches have two location indications named *normal* and *reverse*. In case of a route request or a manual request from the TCC, switches are controlled by the interlocking system. An example schematic representation of a scissor crossover switch (or scissor crossing) is given in Figure 2.

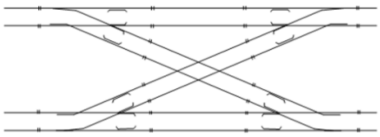


Figure 2. Scissor crossover switch.

2.5 Track Circuits

Track circuits are used to detect trains on railways. They inform the TCC about the absence or the presence of the train. A railway block may contain one or more track circuits that are connected in series depending on the length of the rail line. By the entrance of a train onto a railway block as given in Figure 3, the track circuit is short-circuited by the axles of the train. The track circuit then sends appropriate indication signals to the interlocking system.

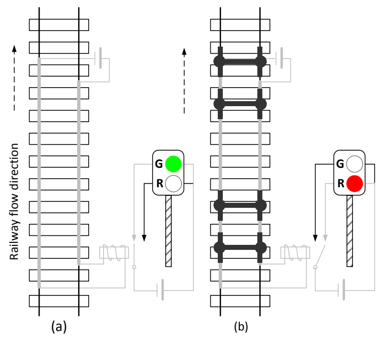


Figure 3. a) Unoccupied track circuit, (b) Occupied track circuit.

2.6 Level Crossing

Level crossings are intersection points of road traffic and railway traffic. Normally when there is no route reservation or route request, the interlocking system send inactive signal to level crossing barriers to keep it open and allow road traffic. After a route reservation, inactive signal is ended by the interlocking system to close the barriers of the level crossing and to activate the flashing red lights of the level crossing. More explanations and related fail-safe Petri models of the level crossing can be found in [29].

3 Influence of Functional Safety Requirements on the Interlocking Software Development

In order to design a fail-safe interlocking system, railway related safety standards developed by CENELEC should be considered by the designers. While developing a railway application in accordance with the CENELEC standards, as a first step, required SIL have to be determined. The required SIL for a given system can be determined by using the Figure D.1, the Figure D.2 and the Table D.1 in EN 61508-5. SIL determination is realized by using different parameters such as consequence of risk (C), frequency and exposure time of risk (F), possibility of failing to avoid hazardous event (P) and probability of the unwanted occurrence of risk (W) [27].

The consequence risk parameter (C) can be chosen as C_C level for the interlocking systems since system failures can result in death of several people. Similarly, the risk parameter (F) is chosen as frequent to permanent exposure in the hazardous zone (F_B). Since avoiding from hazardous events are possible under certain conditions, possibility of falling to avoid hazard risk (P) is chosen as P_A and lastly, due to high probability of unwanted risk occurrence, probability of the unwanted occurrence of risk (W) is chosen as W_3. By the help of these observations, it is possible to claim that the required SIL should be at least 3 for the interlocking systems. SIL determination process is given in Figure 4 and the relation between the expected range of failure per hour (λ) and SIL can be seen from Table 1 [27].

Table 1. Relationship between SIL, λ and MTTF.

SIL	High Demand or Continuous Operation Mode (Range of λ)	Low Demand Operation Mode Range of MTTF (Mean Time to Failure)
4	$10^{-9} \leq \lambda < 10^{-8}$	100000 ≥ MTTF ≥ 10000
3	$10^{-8} \leq \lambda < 10^{-7}$	10000 ≥ MTTF ≥ 1000
2	$10^{-7} \leq \lambda < 10^{-6}$	1000 ≥ MTTF ≥ 100
1	$10^{-6} \leq \lambda < 10^{-5}$	100 ≥ MTTF ≥ 10

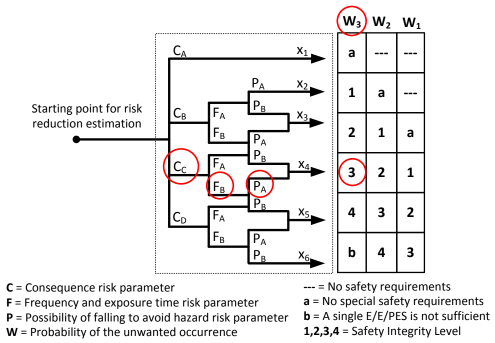


Figure 4. SIL determination process for the interlocking software according to EN 61508-5 [27].

On high demand or continuous operation mode, the λ value for a SIL3 system has to be between $10^{-8} \leq \lambda < 10^{-7}$. Similarly on low demand mode of operation, the railway interlocking system is expected to work minimum 1000 years without falling into a dangerous failure state. In order to satisfy the values given in Table 1, development of hardware and software for the system need to be considered as a whole. Different architectures such as 1oo2, 2oo2, 2oo3 or parallel redundant structures can be used as a solution [30]. Instead of hardware development process, more effort was made on the software development and testing process in the TNRSP.

3.1 Interlocking Software Architecture

The EN 50128 safety standard proposes several techniques for forming the architecture of safety critical software. Defensive Programming (DefP), Failure Assertion Programming (FAP), and Diverse Programming (DivP) techniques have been used to achieve a SIL 3 software in the TNRSP [27].

The aim of DefP is to detect abnormal control flow, data flow or data values during their execution and react to these in a predetermined and acceptable manner [31]. In other words, designer has to put several extra control points to check the validity of results and/or variables of the program. For instance, if a railway block is occupied, the entrance signal of this block cannot be yellow or green. Similarly, movement of a switch must not be allowed when there is a train on the same railway block. Such simple general rules can be checked independently, regardless of the current state of the program, just before sending output signals to the railway field.

In FAP, the main idea is to check pre-conditions (checking the initial conditions for validity before execution of a command) and post-conditions (checking all results after the execution of a command) in the execution of safety critical commands. For example, position indication of a switch before and after a movement request should be checked to ensure correct functioning of the switch. Similarly, a signal cannot be red and green at the same time. If red and green color indications are received from a signal at the same time, this must be considered as a failure by the interlocking software.

Finally, the aim of DivP is to detect and mask software design faults during execution of a program in order to prevent safety critical failures of the system and continue operation with high reliability [31]. In this technique, at least two independent groups develop the software with the same specifications using different techniques. The outputs of algorithms provided by separate groups are compared online to make a safety critical decision. For a safety critical signal (e.g. a position change command for a particular switch) to be sent to the railway field, all algorithms must agree. If a disagreement occurs then the system remains in the predetermined safe-state (the switch is not allowed to be moved). The architecture of the interlocking system is given in Figure 5.

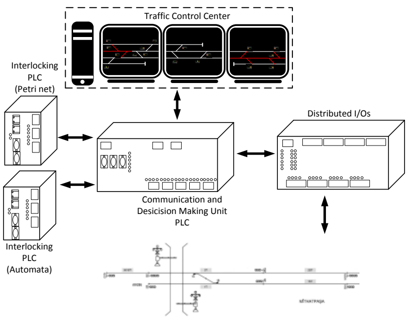


Figure 5. The architecture of the interlocking system.

Two independent groups from Istanbul Technical University (ITU) have developed interlocking software using automatons and Petri nets in the TNRSP. Both of these algorithms are expected to be used for diverse programming purposes. Although it increases safety integrity level of a program, the main disadvantage with diverse programming is that the system can fall into safe-state unexpectedly (causing operation distractions), when the algorithms do not produce the same results at the same time. Possible ways to overcome this shortcoming is documenting software specifications very clearly and using a careful synchronization between controllers.

4 Interlocking Software Development Process

The steps of the software development process used in the TNRSP are explained in this section. For this purpose, a recommended software development model named V-model is used (see Figure 6).

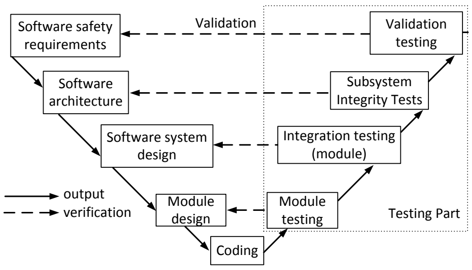


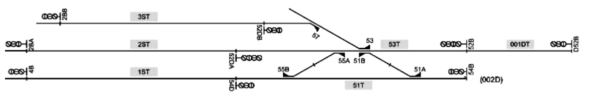
Figure 6. The V- Model [31].

As it is obvious from the Figure 6, as an initial step, the designer should obtain system specifications along with the software specifications. Actually, forming an interlocking table is the first formal step towards modeling an interlocking system. Software specifications are defined by Turkish State Railways. An example railway yard and a part of its interlocking table are given in Figure 7.

Some of the possible route requests (e.g. 001DT-1ST, 001DT-2ST), related signal colors with these possible route requests and the required conditions of the other railway field components (to be able to reserve the route) are defined in this table. For example, if route 001DT-2ST is requested switches 51, 53 and 55 have to be in normal position, signals 52DB, 52DA have to be red and entrance signal of this route 52B can be green (if the next signal 2BA is yellow), yellow (if the next signal 2BA is red) or yellow-red (if the block 2ST is occupied by another train).

The second step in the V-model is to choose the appropriate combination of the software architectures. The chosen architecture was described in section 3.1.

After this process, related system sub models (the modules) have to be obtained. In order to maximize the diversity, the components of the railway signaling system explained in section 2 are modeled separately by two different workgroups using two different methods: Automatons [32] and Petri nets [33]. Both methods are mentioned in IEC 61508 and EN 50128 safety standards as semi-formal modeling tools and highly recommended to obtain SIL 3 software.



DEFINITION			SIGNAL ID		SIGNAL CONDITION		LOCKS		BLOCK CONTROL	ROUTE LOCK
NAME	ROUTE NUMBER	ROUTE					SWITCHES	RELATED SIGNALS		
ENTRANCE SIGNAL	rt25	001DT - 1ST	52B	1S	YG	4B Y	51 53 55	52DB 52DA 54B 54D 2D1 4D1	53T 51T 1ST	(53T) (51T)
					YY	4B R, YR				
					YR				53T 51T 1ST	
	rt26	001DT - 2ST		2S	G	2BA Y	51 53 55	52DB 52DA 2D2	53T 2ST	(53T)
					Y	2BA R				
					YR				53T 2ST	
	rt27	001DT - 3ST		3S	YG	2BB Y	51 53 55 57	52DA 52DB 2D3	53T 3ST	(53T)
					YY	2BB R, FY				
					YR				53T 3ST	

Figure 7. The interlocking table, (G-Green, Y-Yellow, R-Red, YY-Yellow-Yellow, YR-Yellow-Red).

Several applications including both methods can be found in [34]-[40]. Modeling each component separately enables designers to prevent state explosion problems, allows easy error tracking, makes the verification and validation stages much easier and provides flexible programming. Therefore the whole railway field is modeled as a combination of parallel working sub-models. The Petri net models will be given in section 4.2. Additionally, for more information about automata models, the reader is referred to [41] and [42].

4.1 Petri Nets

Petri nets are defined in the literature by [33].

$$\mathrm{PN} = \mathrm{P,T,F,W,M_0} \tag{1}$$

where

- *P*: {P_1, P_2, ..., P_n}, finite set of places,
- *T*: {t_1, t_2, ..., t_m}, finite set of transitions,
- $F \subseteq (P \times T) \cup (T \times P)$ is a set of arcs,
- *W*: $F \rightarrow \{1, 2, 3, \ldots\}$ is a weight function,
- $\mathrm{M_0}$: $P \rightarrow \{0, 1, 2, 3, \ldots\}$ is the initial marking,
- $P \cap T = \emptyset$ and $P \cup T \neq \emptyset$.

4.1.1 Basic Properties of Petri nets [33]

- A transition *t* is said to be enabled if each input place *P* of *t* is marked at least *W(P, t)* tokens, where *W(P, t)* is the weight of arc from place *P* to transition *t*.

$$x(P_i) \geq W(P_i, t_j)\ for\ all\ P_i \in I(t_j) \tag{2}$$

where $x(P_i)$ is the number of tokens on ith place and $I(t_j)$ is the sets of input places of transition t_j.

- An enabled transition may or may not fire (depending on whether or not the event actually takes place).
- A firing of an enabled transition *t* removes *W(P, t)* tokens from each input place *P* of *t* and adds *W(t, P)* tokens to each output place *P* of *t*, where *W(t, P)* is the weight of the arc from *t* to *P*.

$$x'(P_i) \geq x(P_i) - W(P_i, t_j) + W(t_j, P_i) \tag{3}$$

where $x'(P_i)$ is the number of tokens on ith place after the firing of transition j. Petri nets can also represented in matrix form known as incidence matrix.

$$\mathbf{A} = [a_{ij}] \Rightarrow a_{ij} = a_{ij}^{+} - a_{ij}^{-} = W(P_i, t_j) + W(t_j, P_i) \tag{4}$$

In this matrix form, the new marking after a transition is calculated as follows:

$$M_k = M_{k-1} + A^T u_k \tag{5}$$

where $\mathbf{u_k}$ is the kth firing vector, $\mathbf{M_k}$ is the new marking which is an m x 1 column vector.

A PN is said to be pure if it has no self-loops and a PN is said to be ordinary if all of its arc weights are 1. For more details about PNs and its specification, features and types, [33] can be seen.

4.2 Modeling of the Railway Field Components

Basic Petri net models of the railway field components are given in the following figures from Figure 8 to Figure 13 and definitions of the Petri net models can be found in Table 2 and Table 3. All Petri net models given in figures are safe (or 1-bounded) Petri nets since there exists one, and only one, token available in the Petri net at any given time.

Since the routes given in Figure 7 intersect with each other, only one route reservation can be made in order to prevent collisions. More than one route reservation can be made when there is no intersection between the routes.

At the beginning, switches are assumed to be on initial position (P_5). After an incoming position command or a route request from TCC, switch moves to the desired position (normal or reverse) and stays there until a new position command or route request is received (the interlocking software locks the switch electronically). If the switch did not reach to desired position in a predetermined time, which is assumed as 7 sec for Turkish State Railways, it is considered as an error and the token moves to place P_E. Similar error states are also taken into account for the other component models but due to space restrictions, only the simplified models are given here.

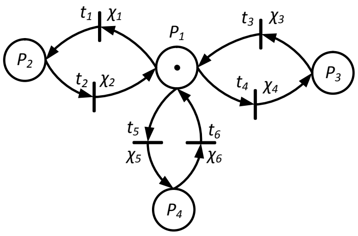


Figure 8. Petri net model for the route reservations given by the interlocking table in Figure 6.

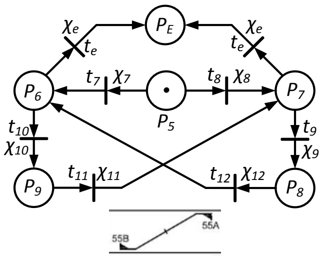


Figure 9. Petri net model for the switch.

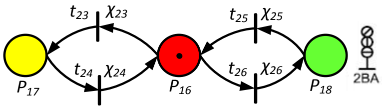


Figure 10. Petri net model for the three aspect tall signal.

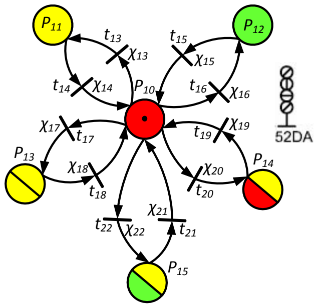


Figure 11. Petri net model for the four aspect tall signal.

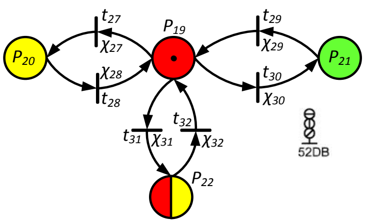


Figure 12. Petri net model for the three aspect dwarf signal.

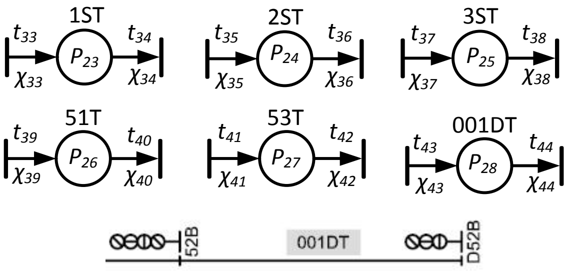


Figure 13. Petri net model for the track circuits.

Railway track circuits are modeled just single places with one input and one output because only one train can occupy a track circuit at the same time. If a train enters onto a track circuit than related transition is fired and a token put on its related place. In addition to this, while train is moving on a reserved route, the interlocking system counts the entrance and the exit of trains on to track circuits which also allows detecting unexpected occupation of track circuits. More explanations on modeling of the railway field components can be found in [39]-[42]. Please note that, the Petri net models given in this paper only explains the basic operation principles of the related railway field components.

Depending on the route reservation and the occupation of the next block, signal colors are adjusted to inform the train drivers. If a train passes a signal when it is red, then the train is stopped by Automatic Train Stop (ATS) or Automatic Train Protection (ATP) systems, which are out of the scope of this paper.

Table 2. Definition of the places given in Figure 8 to Figure 13.

Place	Definition
P_1	No reservation for the railway yard
P_2	001DT - 1ST route is reserved
P_3	001DT - 2ST route is reserved
P_4	001DT - 3ST route is reserved
P_5	Switch starting position
P_6	Switch is moving from Normal to Reverse position
P_7	Switch is moving from Reverse to Normal position
P_8	Switch is on Reverse position
P_9	Switch is on Normal position
P_{10}	Signal is Red
P_{11}	Signal is Yellow
P_{12}	Signal is Green
P_{13}	Signal is Yellow-Yellow
P_{14}	Signal is Yellow-Red
P_{15}	Signal is Yellow-Green
P_{16}	Signal is Red
P_{17}	Signal is Yellow
P_{18}	Signal is Green
P_{19}	Signal is Red
P_{20}	Signal is Yellow
P_{21}	Signal is Green
P_{22}	Signal is Yellow-Red
P_{23}	Track circuit 1ST
P_{24}	Track circuit 2ST
P_{25}	Track circuit 3ST
P_{26}	Track circuit 51T
P_{27}	Track circuit 53T
P_{28}	Track circuit 001DT
P_e	Error State

Table 3. Definition of the transitions given in Figure 8 to Figure 13.

Transition	Definition
t_1 (t_3, t_5)	Route 001DT - 1ST (001DT - 2ST, 001DT - 3ST) is reserved
t_2 (t_4, t_6)	Route 001DT - 1ST (001DT - 2ST, 001DT - 3ST) is released
t_7 (t_8)	Normal (Reverse) position request for switch
t_9 (t_{10})	Switch arrives on Reverse (Normal) position
t_{11} (t_{12})	Switch is moving from Reverse Reverse (Normal) to Normal (Reverse) position
t_{13} (t_{15}, t_{17}, t_{19}, t_{21})	Yellow (Green, Yellow-Yellow, Yellow-Red, Yellow-Green) color request for signal
t_{14} (t_{16}, t_{18}, t_{20}, t_{22})	Red color request for signal
t_{23} (t_{25})	Yellow (Green) color request for signal
t_{24} (t_{26})	Red color request for signal
t_{27} (t_{29}, t_{31})	Yellow (Green, Yellow-Red) color request for signal
t_{28} (t_{30}, t_{32})	Red color request for signal
t_{33} (t_{35}, t_{37}, t_{39}, t_{41}, t_{43})	Track circuit 1ST (2ST, 3ST, 51T, 53T, 001DT) is occupied
t_{34} (t_{36}, t_{38}, t_{40}, t_{42}, t_{44})	Track circuit 1ST (2ST, 3ST, 51T, 53T, 001DT) is unoccupied
t_e	Switch indication error

4.3 Generation of PLC Codes from Models

Converting the Petri net models to a useful PLC code is simpler by using Sequential Function Charts (SFCs) which is one of the five languages defined by IEC 61131-3 standard. Instead of widely used techniques like Ladder Diagrams (LD) or Function Block Diagrams (FBD), SFC is directly related with safe Petri nets and automatons. Besides, several formal conversion techniques are also available in the literature to convert Petri nets to PLC codes [43]-[46]. A snapshot of a part of a SFC code is given in Figure 14.

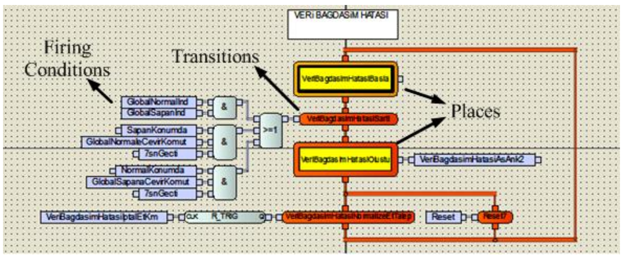


Figure 14. Snapshot of a part of a PLC code.

4.4 An Example (Route Reservation Procedure)

Assume that route request for 001DT-3ST is made from TCC. If there is no route reservation intersecting with the route 001DT-3ST or existence of another conflicting condition, the interlocking software will accept the request. In this case, in the first step, transition t_5, which moves the token on place P_1 to place P_4, will be fired. In the second step, the switches related with route 001DT-3ST have to be arranged in accordance with the interlocking table given on Figure 7. Switches 51 and 55 have to be on normal position, whereas switches 53 and 57 have to be on reverse position. If all these conditions are satisfied, the interlocking software sends related signal (which is 52B for this route) appropriate color information given on the interlocking table (signal 52B is assumed to be yellow for this example). Finally, the train movement is monitored via track circuits by the interlocking system. After route reservation is made, trains have to pass the track circuits one by one in a predetermined order. The block diagram of this example is given in Figure 15.

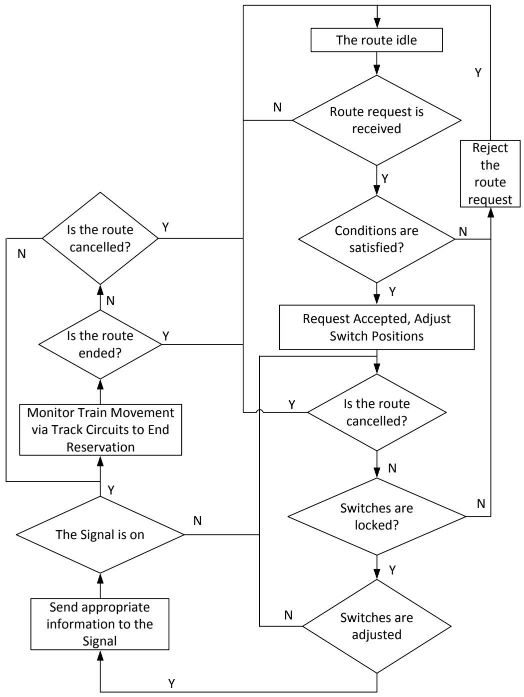


Figure 15. Route reservation procedure (Y-Yes, N-No).

5 Software Tests

Testing interlocking software is at least as important as developing it. The standards (EN 61508-3 and EN 50128) provide several guidelines for testing such crucial software. Testing of the interlocking software is achieved in five steps.

5.1 Interlocking Software Module Tests (Verification)

Module tests (testing program modules separately as mentioned in V-model given in Figure. 6) are realized by using the Interlocking Test Program (ITP) developed by the Department of Control Engineering of Istanbul Technical University (ITU). In this program, a basic simulator is used to imitate the signals in the field. An automatic testing procedure (2~3 weeks) was applied to each interlocking module.

5.2 Interlocking Software Simulator Tests (Validation)

Validation was realized by using a complex software simulator which is connected to the interlocking software. Simulator was connected to the interlocking software through a second PLC set using digital I/O modules, and all possible signals in the field are imitated by this second PLC. Complex train movements with several stress tests can be performed by the software simulator [47].

5.3 Hardware Simulator Tests (Commissioning)

A hardware simulator, which is 1:87 scaled model of the real railway field, is used to provide an even more realistic simulation. The signals collected from the model field are delivered to the interlocking system using a set of PLCs in this simulation model [48]. The hardware simulator was established in the Industrial Automation Laboratory of the Control Engineering Department of ITU.

5.4 Factory Acceptance Tests (FAT)

These tests are also realized in the Industrial Automation Laboratory of the Control Engineering Department of ITU, under the observation of a group of delegates from Turkish State Railways. The whole system (including the interlocking and TCC software, which was developed by TÜBİTAK-BİLGEM) has been validated in these tests.

5.5 Field Acceptance Tests

The final field acceptance tests are realized by Turkish State Railways in Mithatpaşa railway station in Sakarya, Turkey in January, 2012. All the tests are passed successfully. It should also be noted that the tests are executed by independent groups and documented carefully as suggested by the CENELEC standards.

6 Conclusion

In this study, the development of a railway interlocking system was explained. The railway related functional safety requirements of CENELEC standards, especially EN 61508 and EN 50128, are also considered. The voting system, which is a part of the developed interlocking system, consists of two fail-safe PLCs with the running codes determined by using Automata and Petri net methods regarded as semi-formal methods by EN 50128. Communication between the Traffic Control Center, the railway field and the interlocking PLCs are achieved by a master controller where all decisions are compared, considered and executed. Obtained interlocking software is tested and verified by both using a simulator called Interlocking Test Program (ITP) and a small-scaled hardware simulator of railway yard established in Istanbul Technical University Industrial Automation Laboratory.

Automatic construction of the interlocking tables, automatic generation of supervisors for the control of railway field component models, automatic PLC code generation for the interlocking software that is fully compatible with European Rail Traffic Management System (ERTMS) Level 1-3 issues can be classified as possible future works.

7 Acknowledgement

This work is supported by The Scientific and Technological Research Council of Turkey (TÜBİTAK) project number 108G186 – The National Railway Signaling Project.

8 References

[1] URL: www.ecopassenger.org. (Reached on: 08.03.2013).
[2] URL: http://www.medicine.ox.ac.uk/bandolier/booth/Risk/transporttrav.html. (Reached on: 08.03.2013).
[3] Hall, S., *Modern Signalling Handbook*, Ian Allan Publishing, England, 2001.
[4] Kuepper, G.J., “150 years of train-disasters - practical approaches for emergency responders”, *9-1-1 Magazine*, September/October, 30-33, 1999.
[5] Akita, K., Watanabe, T., Nakamura, H., and Okumura, I., “Computerized Interlocking System for Railway Signalling Control: SMILE”, *IEEE Transactions on Industry Applications*, Vol. IA-21-4, 826-834, 1985.
[6] Petersen, J.L., “Automatic Verification of Railway Interlocking Systems: A Case Study”, *Proc. of the 2nd Workshop on Formal Methods in Software Practice*, 1998, 1-6.
[7] Kantz, H. and Koza C., “The ELEKTRA Railway Signalling-System: Field Experience with an Actively Replicated System with Diversity”, *Proc. of the 25th International Symposium on Fault-Tolerant Computing*, 1995, 453-458.
[8] Rao, V.P. and Venkatachalam, P.A., “Microprocessor-Based Railway Interlocking Control with Low Accident Probability”, *IEEE Trans. on Vehicular Technology*, Vol. VT-353, 141-147, 1987.
[9] Hartonas-Garmhausen, V., Campos, S., Cimatti, A., Clarke, E. and Giunchiglia, F., “Verification of a Safety-Critical Railway Interlocking System with Real-time Constraints”, *Science of Computer Programming*, Vol. 36, 2000, 53-64.
[10] Nakamatsu, K., Kiuchi, Y., Chen, W.Y. and Chung, S.L., “Intelligent Railway Interlocking Safety Verification Based on Annotated Logic Program and its Simulator”, *Proc. of the IEEE Int. Conf. on Networking, Sensing&Control*, 694-700, 2004.
[11] Dipoppa, G., D’Alessandro, G., Semprini, R. and Tronci, E., “Integrating Automatic Verification of Safety Requirements in Railway Interlocking System Design”, *Proc. of 6th IEEE Int. Symp. on High Assurance Systems Engineering*, 209-219, 2001.
[12] Roanes-Lozano, E., Roanes-Macias, E. and Laita, L.M., “Railway Interlocking Systems and Gröbner bases”, *Mathematics and Computers in Simulation*, 51, 473-481, 2000.
[13] She, X., Sha, Y., Chen, Q. and Yang, J., “The Application of Graph Theory on Railway Yard Interlocking Control System”, *Proc. of the IEEE Intelligent Vehicles Symposium*, 883-888, 2007.
[14] Banci, M., Fantechi, A. and Ginesi, S., “The Role of Formal Methods in Developing a Distributed Railway Interlocking System”, *Proc. of the 5th Symp. on Formal Methods for Automation and Safety in Railway and Automotive Systems*, 220-230, 2004.
[15] Banci, M., Fantechi, A. and Ginesi, S., “Some Experiences on Formal Specification of Railway Interlocking Systems using Statecharts”, *Train International Workshop at SEFM2005*, 2005.
[16] Bohn, J., Damm, W., Klose, J., Moik, A. and Wittke, H., “Modeling and Validating Train System Applications Using Statemate and Live Sequence Charts”, *Proc. of the Conf. on Integrated Design and Process Technology*, 2002.
[17] Hei, X., Takahashi, S. and Nakamura, H., “Distributed Interlocking System and Its Safety Verification”, *Proc. of the 6th World Congress on Intelligent Control and Automation*, 8612-8615, 2006.
[18] Hei, X., Takahashi, S. and Nakamura, H., “Toward Developing a Decentralized Railway Signalling System Using Petri nets”, *Proc. of the IEEE Conf. on Robotics, Automation and Mechatronics*, 851-855, 2008.
[19] URL:http://www.thalesgroup.com/Pages/Solution.aspx?id=2493&pid=1568. (Reached on: 08.03.2013).
[20] URL:http://www.mobility.siemens.com/mobility/en/pub/urban_mobility/rail_solutions/rail_automation/electronic_interlockings.htm. (Reached on: 08.03.2013).
[21] URL:http://www.funkwerk-it.com/wEnglisch/produkte/signaltechnik/alister-stellwerk.shtml. (Reached on: 08.03.2013).
[22] URL:http://www.ansaldo-sts.com/en/activities-and-services/business-segments/computer-based-interlocking. (Reached on: 08.03.2013).
[23] URL: http://www.alstom.com/transport/products-and-services/signalling/smartlock-interlocking. (Reached on: 08.03.2013).

[24] URL:http://www.bombardier.com/en/transportation/products-services/rail-control-solutions?docID=0901260d8000a67e. (Reached on: 08.03.2013).

[25] IEC 61508-3, "Functional Safety of Electrical / Electronic / Programmable electronic safety-related systems, Part 5: Examples of methods for the determination of safety integrity levels", 1997.

[26] Spellemaeker, M. and Witrant, L., "How to Determine the Safety Integrity Level (SIL) of a Safety System", URL: http://www.indsci.com/docs/Press/PIN_0907.pdf. (Reached on: 08.03.2013).

[27] Söylemez, M.T., Durmuş, M.S. and Yıldırım, U., "Functional Safety Application on Railway Systems: Turkish National Railway Signalization Project", *Proc of the 24th Int. Cong. on Condition Monitoring and Diagnostics Engineering Management*, 1683-1692, 2011.

[28] URL: http://www.hima.com/_filenet/Download.asp?ID=003674672:1&Tag=Rail%20Flyer%20en. (Reached on: 08.03.2013).

[29] Durmuş, M.S., Yıldırım, U., Kurşun A., and Söylemez, M.T, "Fail-safe signalization design for a railway yard: A level crossing case", *The 10th International Workshop on Discrete Event Systems*, 337-342, 2010.

[30] Börcsök, J., *Functional Safety*, Hüthig Verlag, Germany, 2007.

[31] EN 50128, "Railway Applications, Communications, signalling and processing systems, Software for railway control and protection systems", 2001.

[32] Ramadge, P.J. and Wonham, W.M., "The Control of Discrete Event Systems", *Proc. of IEEE*, Vol. 77, No. 1, 1989, 81-98.

[33] Murata, T., "Petri nets: Properties, Analysis and Applications", *Proc. of IEEE*, Vol. 77, No.4, 1989, 541-580.

[34] Giua, A. and Seatzu, C., "Modeling and Supervisory Control of Railway Networks Using Petri nets", *IEEE Trans. On Automation Science and Engineering*, Vol.5, No.3, 2008, 431-445.

[35] Hagalisletto, A.M., Bjork, J., Yu, I.C. and Enger, P., "Constructing and Refining Large-Scale Railway Models Represented by Petri nets", *IEEE Trans. On System, Man and Cybernetics-Part C: Applications and Reviews*, Vol.37, No.4, 2007, 444-460.

[36] Zurawski, R. and Zhou, M.C., "Petri nets and Industrial Applications: A Tutorial", *IEEE Trans. on Industrial Electronics*, Vol. 41, No.6, 1994, 567-583.

[37] Febbraro, A.D., Porta, G. and Sacco, N., "A Petri net modelling approach of intermodal terminals based on Metrocargo© system", *Proc. of the IEEE Intelligent Transportation Systems Conference*, 1442-1447, 2006.

[38] Hasdemir, İ.T., Kurtulan, S. and Gören, L., "An implementation methodology for supervisory control theory", *International Journal of Advanced Manufacturing Technology*, Vol. 36, No.3-4, 373-385, 2008.

[39] Durmuş, M.S., Yıldırım, U., and Söylemez, M.T., "Application of Functional Safety on Railways Part I: Modelling & Design", *Proc. of the 8th Asian Control Conference*, 2011, 1090-1095.

[40] Yıldırım, U., Durmuş, M.S. and Söylemez, M.T., "Application of Functional Safety on Railways Part II: Software Development", *Proc. of the 8th Asian Control Conference*, 2011, 1096-1101.

[41] Dincel, E. and Kurtulan, S., "Interlocking and Automatic Operating System Design with Automaton Method", *Proc. of the 13th IFAC Symposium on Control in Transportation Systems*, 2012, 191-196.

[42] Kaymakçı, Ö.T., Üstoğlu, İ. and Anık, V.G., "A Local Modular Supervisory Controller for a Real Signalling System", *Proc. of the 5th IET International System Safety Conference*, 2010, 1-6.

[43] Uzam, M., *Petri-net-based Supervisory Control of Discrete Event Systems and Their Ladder Logic Diagram Implementations*, PhD. dissertation, University of Salford, 1998.

[44] Thapa, D., Dangol, S. and Wang, G.N., "Transformation from Petri nets Model to Programmable Logic Controller using One-to-One Mapping Technique", *Proc. of the Int. Conf. on Computational Intelligence for Modelling, Control and Automation and Int. Conf. on Intelligent Agents, Web Technologies and Internet Commerce*, 2005, 228-233.

[45] Frey, G., "Automatic Implementation of Petri net Based Control Algorithms on PLC", *American Control Conference*, 2000, 2819-2823.

[46] Genter, G., Bogdan, S., Kovacic, A. and Grubisic, I., "Software tool for modeling, simulation and real-time implementation of Petri net-based supervisors", *16th IEEE International Conference on Control Applications*, 2007, 664-669.

[47] Mutlu, İ., Ovatman, T., Söylemez, M.T. and Gören-Sümer, L., ‚A New Test Environment for PLC Based Interlocking Systems,, *Proc. of the International Conference on Transportation, Mechanical and Electrical Engineering*, 2011, 1123-1127.

[48] Mutlu, İ., Ergenç, A.F., Ovatman, T. and Söylemez, M.T., "Design of a Hardware and Software based Test Bed for Railway Signalization System", *Proc. of the 13th IFAC Symposium on Control in Transportation Systems*, 2012, 185-190.