IEEJ TRANSACTIONS ON ELECTRICAL AND ELECTRONIC ENGINEERING
IEEJ Trans 2014; **9**: 523–531
Published online in Wiley Online Library (wileyonlinelibrary.com). DOI:10.1002/tee.22001

Paper

Fault Diagnosis in Fixed-Block Railway Signaling Systems: A Discrete Event Systems Approach

Mustafa S Durmuş*, Non-member
Shigemasa Takai**[a], Non-member
Mehmet T Söylemez*, Non-member

In conventional railway systems (or fixed-block railway signaling systems), railway lines are divided into subsections, called *railway blocks*, which start and end with a signal. In order to prevent collisions, only one train is allowed in each railway block at a time. Since the occupancy of the next block is indicated by the signals, train drivers have to pay attention to the signals during their journey. In spite of the conventional railway systems having several drawbacks such as the reduction in railway line capacity and the same safe braking distances for all kinds of trains, they have been in use since the mid-1800s. In this paper, we study fault diagnosis in fixed-block railway signaling systems from the discrete event systems point of view: first the signaling system equipment are modeled by using Petri nets, and next a diagnoser is designed to show the diagnosability of the system.

Keywords: fixed-block railway signaling systems, Petri nets, fault diagnosis

Received 4 July 2013; Revised 15 October 2013

1. Introduction

Failure is defined as termination of the ability of a functional unit to provide a required function or operation of a functional unit in any way other than as required, whereas fault is defined as the abnormal condition that may cause a reduction in, or loss of, the capability of a functional unit to perform a required function [1]. A safety-critical system is defined in [2] as a system where human safety is dependent upon the correct operation of the system. Also, a system is said to be safety-critical in [3] if the failure of a system could lead to results that are determined to be undesirable. Based on these definitions, air traffic control systems, nuclear power reactor control systems, and railway signaling systems can be classified as safety-critical systems because sometimes possible failures may lead to the death of many people [4].

In fixed-block railway signaling systems, the railway lines are divided into fixed railway blocks. Each block has entrance and exit signals of different types depending on the location of the signal [5]. The lengths of the railway blocks are determined on the basis of different variables such as the permitted line speed and the gradient of the railway line. Furthermore, the signaling system is one of the most important components of the fixed-block railway systems, which ensures safe transportation and travel. From the engineering point of view, to comply with the requirements of the safety-related standards and to achieve the desired safety level (referred to as the *safety integrity level* or SIL in [1]), railway signaling engineers have to pay great attention to both signaling software development and signaling software testing when designing signaling software for fixed-block railways [6–9].

Besides, from the theoretical point of view, fixed-block railway systems are regarded as discrete event systems (DESs) because of their features like non-determinism, asynchronism, event-driven mode, and simultaneity [10]. Representation of such a system with a model is necessary as in the conventional control theory. Modeling tools for DESs must be suitable to cover all their different features. Several methods have been introduced as DES modeling tools, such as Grafcet [11], automata [12] and, of course, Petri nets [13]. For more details about DES theory, the reader is referred to Ref. [10].

Events in DESs can be classified as observable and unobservable events. A system is said to be diagnosable if it is possible to detect, with a finite delay, occurrences of certain unobservable events which are referred to as failure events [14]. The diagnoser is built from the system model itself and performs diagnostics when it observes online the behavior of the system. States of the diagnoser carry failure information, and occurrences of failures can be detected with a finite delay by inspecting these states [15].

The pioneering study on failure diagnosis of DESs is the work of Sampath *et al*. [14, 15], which is an automata-based approach. They gave the definition of diagnosability and presented a necessary and sufficient condition for the system to be diagnosable. They also proposed a diagnoser design method for an experimental simple heating, ventilation, and air conditioning (HVAC) system. In Ref. [16], the authors developed a diagnoser design procedure for active diagnosis of DESs which presents an integrated approach to control and diagnosis. As an alternative to automata-based modeling, Ushio *et al*. proposed a diagnoser for a system modeled by a Petri net where only the marking of some of the places, called observable places, is observable [17]. Chung [18] extended the above work [17] by assuming that some of the transitions are also observable in addition to observable places. In Ref. [19], an approach to test diagnosability by checking the structure property of the diagnoser was proposed on the basis of the method of Ref. [17]. More topics and approaches on diagnosis of Petri nets can be found in Refs [20–23].

In this paper, fault diagnosis in fixed-block railway signaling systems is studied from the DES point of view: first the signaling system components are modeled by using Petri nets, and next a diagnoser is designed to show the diagnosability of the system.

[a] Correspondence to: Shigemasa Takai.
E-mail: takai@eei.eng.osaka-u.ac.jp

* Control Engineering Department, Istanbul Technical University, Maslak 34469, Istanbul, Turkey

** Division of Electrical, Electronic and Information Engineering, Osaka University, 2-1 Yamada-Oka, Suita, Osaka 565-0871, Japan

Briefly, the main aim of using the DES modeling tools such as automata and Petri nets in fixed-block railway signaling systems is to model the specifications of the system and to evaluate the operational requirements by analysis and redesign [24]. In fact, the use of these DES modeling tools is highly recommended in Table B.5 of Ref. [6] and in Table A.16 of Ref. [7] as a modeling technique to design the SIL3 or SIL4 safety-critical software.

There are several works on the safety of railway signaling systems (see, e.g.[25–28]). SMILE [25] is an early signaling system software application where fail-safe microcomputer systems are used, and STERNOL was developed by ABB Signal [26]. Additionally, microprocessor-based interlocking systems including accident probabilities [27] and graph-based railway interlocking applications [28] were also studied. The purpose of most existing studies was to develop a control mechanism (signaling software) and to verify the software. On the other hand, the main purpose of this work is to check the diagnosability of the constructed railway signaling system models (e.g., Petri net models) before the development and testing of the safety software.

Also, railway systems have been studied in the framework of Petri nets. For example, the use of colored Petri nets with object-oriented programming [29] and a Petri net modeling technique with a supervisory control scheme [30] can be found in the literature. However, in these studies, faulty conditions were not included in the Petri net models, nor was a fault diagnosis approach considered. In Ref. [31], a time Petri net modeling technique with an online monitoring approach to estimate and monitor train movement in a small model railway layout was examined, and certain sufficient conditions for diagnosability, which take temporal information into account, were obtained. As possible faults, point machine (PM) faults were considered there. In this paper, in addition to PM faults, the route reservation procedure and faulty conditions in wayside signals are considered, and the diagnosability property is verified on the basis of the necessary and sufficient condition of [14] in the untimed setting.

The rest of the paper is organized as follows. In Section 2, the basic definitions of Petri nets and the concept of fault diagnosis are given. The definitions of the basic components of fixed-block railway signaling systems are given in Section 3. Specifications of fixed-block railway systems are explained in Section 4. Modeling of the components and the fault diagnosis approach are explained in Section 5, and, finally, the paper ends with a brief conclusion in Section 6.

2. Preliminaries

2.1. Petri nets

A Petri net [13] is defined as

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

Where

- $P = \{p_1, p_2, \ldots, p_k\}$ is the finite set of places,
- $T = \{t_1, t_2, \ldots, t_z\}$ is the finite set of transitions,
- $F \subseteq (P \times T) \cup (T \times P)$ is the set of arcs,
- $W: F \to \{1, 2, 3, \ldots\}$ is the weight function,
- $M_0: P \to \{0, 1, 2, 3, \ldots\}$ is the initial marking,
- $P \cap T = \emptyset$ and $P \cup T \neq \emptyset$.

We use $I(t_j)$ and $O(t_j)$ to represent the sets of input places and output places of transition t_j, respectively, as

$$I(t_j) = \{p_i \in P : (p_i, t_j) \in F\} \tag{2}$$

$$O(t_j) = \{p_i \in P : (t_j, p_i) \in F\} \tag{3}$$

For a marking $M : P \to \{1, 2, 3, \ldots\}$, $M(p_i) = n$ means that the ith place has n tokens [13]. A marking M can also be represented by a vector with k elements where k is the total number of places.

DEFINITION 1 [10]: *A transition t_j is said to be enabled at a marking M if each input place p_i of t_j has at least $W(p_i, t_j)$ tokens, where $W(p_i, t_j)$ is the weight of the arc from place p_i to transition t_j, that is, $M(p_i) \geq W(p_i, t_j)$ for all $p_i \in I(t_j)$.*

Note that, if $I(t_j) = \emptyset$, transition t_j is always enabled. An enabled transition may or may not fire (depending on whether or not the event actually takes place). The firing of an enabled transition t_j removes $W(p_i, t_j)$ tokens from each $p_i \in I(t_j)$ and adds $W(t_j, p_i)$ tokens to each $p_i \in O(t_j)$, where $W(t_j, p_i)$ is the weight of the arc from t_j to p_i. That is,

$$M'(p_i) = M(p_i) - W(p_i, t_j) + W(t_j, p_i) \tag{4}$$

where $M'(p_i)$ is the number of tokens in the ith place after the firing of transition t_j. The notation $M[t_j >$ denotes that a transition t_j is enabled at a marking M. Also, $M[t_j > M'$ denotes that, after the firing of t_j at M, the resulting marking is M'. These notations can be extended to a sequence of transitions.

DEFINITION 2 [13]: *A Petri net PN is said to be pure if it has no self-loops and said to be ordinary if all of its arc weights are 1.*

DEFINITION 3 [13]: *A marking M_n is reachable from the initial marking M_0 in a Petri net PN if there exists a sequence of transitions $t_1 t_2 \ldots t_n$ such that $M_0[t_1 > M_1\ [t_2 > \ldots M_{n-1}\ [t_n > M_n$ and $R(M_0)$ denotes the set of all reachable markings from M_0.*

DEFINITION 4 [13]: *A Petri net PN is said to be m-bounded if the number of tokens in each place does not exceed a finite number m, that is, $\forall M_k \in R(M_0), \forall p_i \in P : M_k(p_i) \leq m$. Additionally, PN is safe if it is 1-bounded.*

DEFINITION 5 [13, 32]: *A Petri net PN is said to be deadlock-free (complete absence of deadlocks) if at least one transition is enabled at every reachable marking $M_k \in R(M_0)$.*

The set P of places is partitioned into the set P_o of observable places and the set P_{uo} of unobservable places [17]. Similarly, the set T of transitions is partitioned into the set T_o of observable transitions and the set T_{uo} of unobservable transitions. That is,

$$P = P_o \cup P_{uo} \text{ and } P_o \cap P_{uo} = \emptyset \tag{5}$$

$$T = T_o \cup T_{uo} \text{ and } T_o \cap T_{uo} = \emptyset \tag{6}$$

Also, a subset T_F of T_{uo} represents the set of faulty transitions. It is assumed that there are n different failure types, and $\Delta_F = \{F_1, F_2, \ldots, F_n\}$ is the set of failure types. That is,

$$T_F = T_{F_1} \cup T_{F_2} \cup \cdots \cup T_{F_n} \tag{7}$$

where $T_{F_i} \cap T_{F_j} = \emptyset$ if $i \neq j$. The label set is defined as $\Delta = \{N\} \cup 2^{\Delta_F}$ where N denotes the label "normal", which indicates that no faulty transition has fired, and 2^{Δ_F} denotes the power set of Δ_F, that is, 2^{Δ_F} is the set of all subsets of Δ_F. In the rest of the paper, unobservable places and unobservable transitions are represented by striped places and striped transitions, as shown in Fig. 1.

2.2. Fault diagnosis based on Petri net models

Because of the existence of unobservable places, some markings cannot be distinguished. We denote $M_1 \equiv M_2$ if $M_1(p_i) = M_2(p_i)$ for any $p_i \in P_o$; in other words, the observations of markings M_1 and M_2 are the same. It is useful to define the quotient set

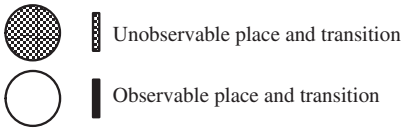


Fig. 1. Representation of places and transitions

$\hat{R}(M_0)$ as in Ref. [18] with respect to the equivalence relation ($\equiv$); $\hat{R}(M_0) := \hat{R}(M_0)/\equiv := \{\hat{M}_0, \ldots, \hat{M}_n, \ldots\}$ where $M_0 \in \hat{M}_0$. An element of $\hat{R}(M_0)$ is referred to the observation of a marking or an observable marking.

For simplicity, we impose the following two assumptions in this paper.

ASSUMPTION 1 [14, 17]: *A Petri net system PN defined by (1) is bounded and deadlock-free.*

ASSUMPTION 2 [14, 17]: *There does not exist a sequence of unobservable transitions whose firing generates a cycle of markings which have the same observation: that is, for any* $M_i \in R(M_0)$ *and* $t_i \in T_{uo}, i = 1, 2, \ldots, n, M_1[t_1 > M_2 \quad [t_2 > \ldots M_n \quad [t_n > M_1 \Rightarrow \exists i, j \in \{1, 2, \ldots, n\}: M_i \not\equiv M_j$.

We define a diagnoser [14, 17, 18] for a Petri net system *PN*. A state q_d of the diagnoser is of the form $q_d = \{(M_1, l_1), (M_2, l_2), \ldots, (M_n, l_n)\}$, which consists of pairs of a marking $M_i \in R(M_0)$ and a label $l_i \in \Delta$. The notation $Q = 2^{R(M_0)\times\Delta}$ denotes the power set of $R(M_0) \times \Delta$, that is, each element of Q is a subset of $R(M_0) \times \Delta$ and is of the form $\{(M_1, l_1), (M_2, l_2), \ldots, (M_n, l_n)\}$. The diagnoser is an automaton given by

$$G_d = (Q_d, \Sigma_o, \delta_d, q_0) \tag{8}$$

where $Q_d \subseteq Q$ is the set of states, $\Sigma_o = \hat{R}(M_0) \cup T_o$ is the set of events, $\delta_d : Q_d \times \Sigma_o \to Q_d$ is the partial state transition function, and $q_0 = \{(M_0, N)\}$ is the initial state. The state set Q_d is the set of states in Q that are reachable from the initial state q_0 under the state transition function δ_d. Each observed event $\sigma_o \in \Sigma_o$ represents the observation of a marking in $\hat{R}(M_0)$ or an observable transition in T_o. The transition function δ_d is defined by using the label propagation function and the range function. The label propagation function $LP : R(M_0) \times \Delta \times T^* \to \Delta$ propagates the label (normal or faulty) over a sequence $s \in T^*$ of transitions, where T^* is the set of all finite sequences of elements of T, as follows [14, 17]:

$$LP(M, l, s) = \begin{cases} N, & \text{if}(l = N) \wedge (\forall F_i \in \Delta_F : T_{F_i} \notin s) \\ \{F_i : F_i \in l \vee T_{F_i} \in s\}, & \text{otherwise,} \end{cases} \tag{9}$$

where $T_{F_i} \in s$ (respectively, $T_{F_i} \notin s$) indicates that a sequence $s \in T^*$ of transitions contains (respectively, does not contain) a faulty transition with failure type F_i. Briefly, if the sequence of transitions does not include any faulty transition, then the label attached to the resulting marking is normal (N). If the sequence of transitions includes a faulty transition, then the label includes the corresponding failure type. Then, the range function $LR : Q \times \Sigma_o \to Q$ is obtained by modifying its definition [18] as follows:

$$LR(q, \sigma_o) = \cup_{(M,l)\in q} \cup_{s\in T^*(M,\sigma_o)} \{(M', LP(M, l, s))\} \tag{10}$$

where $M[s > M'$, and $T^*(M, \sigma_o) \subseteq T^*$ is defined in the following two cases:

1. If $\sigma_o \in \hat{R}(M_0)$,

$$T^*(M, \sigma_o) = \begin{cases} \emptyset, & \text{if } M \in \sigma_o \\ \{s \in T^*_{uo} : (M_s \in \sigma_o) \\ \wedge(\forall s'(\neq s) \in \bar{s} : M_{s'} \equiv M)\}, & \text{otherwise,} \end{cases} \tag{11}$$

where $M[s > M_s, M[s' > M_{s'}$, and $\bar{s}$ denotes the set of all prefixes of s. In (11), the case of $M \notin \sigma_o$ corresponds to a change of the observable marking. In this case, $T^*(M, \sigma_o)$ is the set of sequences $s \in T^*_{uo}$ of unobservable transitions such that, during the firing of s, all of the interval markings except the last one in σ_o have the same observation.

2. If $\sigma_o \in T_o$,

$$T^*(M, \sigma_o) = \{s \in T^*_{uo} \cdot \{\sigma_o\} : (M[s>) \wedge (\forall s'(\neq s) \in \bar{s} : M_{s'} \equiv M)\} \tag{12}$$

where $M[s' > M_{s'}$. When the firing of an observable transition $\sigma_o \in T_o$ is observed, $T^*(M, \sigma_o)$ is the set of sequences of unobservable transitions followed by σ_o such that all of the interval observable markings except the last one are the same.

That is, $T^*(M, \sigma_o)$ is the set of possible transition sequences from M which are consistent with the observed event σ_o.

Remark 1: *In this paper, we modify the definition of* $T^*(M, \sigma_o)$ *of [18] as follows:*

- When $M \in \sigma_o \in \hat{R}(M_0)$, we let $T^*(M, \sigma_o) = \emptyset$, instead of $T^*(M, \sigma_o) = \{\varepsilon\}$ [18], to avoid the self-loop labeled by the current observable marking in G_d.
- When $\sigma_o \in T_o$, $M \in \sigma_o$ is impossible, so this case is not considered.

Finally, the transition function $\delta_d : Q_d \times \Sigma_o \to Q_d$ is defined as follows [14, 17]:

$$\delta_d(q, \sigma_o) = \begin{cases} LR(q, \sigma_o), & \text{if } LR(q, \sigma_o) \neq \emptyset \\ \text{undefined}, & \text{otherwise.} \end{cases} \tag{13}$$

2.3. Diagnosability A Petri net system *PN* is said to be diagnosable [17] if the type of the fault is always detected within a uniformly bounded number of firings of transitions after the occurrence of the fault. It is possible to classify states in Q_d as follows:

1. A state $q \in Q_d$ is said to be F_i-certain if $F_i \in l$ for any $(M, l) \in q$.
2. A state $q \in Q_d$ is said to be F_i-uncertain if there exist (M, l) and $(M', l') \in q$ such that $F_i \in l$ and $F_i \notin l'$.

If the system is diagnosable, then, after the occurrence of a faulty transition (e.g. $t \in T_{F_i}$), the state of the diagnoser reaches an F_i-certain state within a finite number of firings of transitions [17]. A set $\{q_1, q_2, \ldots, q_n\} \subseteq Q_d$ of F_i-uncertain states are named an F_i-indeterminate cycle [14, 17] if the following conditions hold:

1. The states $q_1, q_2, \ldots, q_n \in Q_d$ constitute a cycle in G_d, that is, there exist $\sigma_1, \sigma_2, \ldots, \sigma_n \in \Sigma_o$ such that, $\delta_d(q_j, \sigma_j) = q_{j+1}$ for each $j = 1, 2, \ldots, n-1$ and $\delta_d(q_n, \sigma_n) = q_1$.

2. For each $j = 1, 2, \ldots, n, k = 1, 2, \ldots, m$, and $r = 1, 2, \ldots, m'$, there exist $(M_j^k, l_j^k), (\tilde{M}_j^r, \tilde{l}_j^r) \in q_j$ which satisfy the following two conditions:

(a) For any $j = 1, 2, \ldots, n, k = 1, 2, \ldots, m$, and $r = 1, 2, \ldots, m'$, $F_i \in l_j^k$ and $F_i \notin \tilde{l}_j^r$.

(b) Markings $M_j^k (j = 1, 2, \ldots, n, k = 1, 2, \ldots, m)$ and $\tilde{M}_j^r$ $(j = 1, 2, \ldots, n, r = 1, 2, \ldots, m')$ satisfy the following conditions:

$$\exists s_j^k \in T^*(M_j^k, \sigma_j) : M_j^k[s_j^k > M_{j+1}^k \quad (j = 1, 2, \ldots, n-1, k = 1, 2, \ldots, m),$$

$$\exists s_n^k \in T^*(M_n^k, \sigma_n) : M_n^k[s_n^k > M_1^{k+1} (k = 1, 2, \ldots, m-1),$$

$$\exists s_n^m \in T^*(M_n^m, \sigma_n) : M_n^m[s_n^m > M_1^1,$$

$$\exists \tilde{s}_j^r \in T^*(\tilde{M}_j^r, \sigma_j) : \tilde{M}_j^r[\tilde{s}_j^r > \tilde{M}_{j+1}^r \quad (j = 1, 2, \ldots, n-1, r = 1, 2, \ldots, m'),$$

$$\exists \tilde{s}_n^r \in T^*(\tilde{M}_n^r, \sigma_n) : \tilde{M}_n^r[\tilde{s}_n^r > \tilde{M}_1^{r+1} (r = 1, 2, \ldots, m'-1),$$

$$\exists \tilde{s}_n^{m'} \in T^*(\tilde{M}_n^{m'}, \sigma_n) : \tilde{M}_n^{m'}[\tilde{s}_n^{m'} > \tilde{M}_1^1.$$

Remark 2: *The above definition of an F_i-indeterminate cycle is obtained by slightly modifying the definition of [17] by taking the existence of observable transitions into account.*

THEOREM 1 [14, 17]: *A Petri net system PN is diagnosable if and only if the diagnoser given by (8) does not contain an F_i-indeterminate cycle for any failure type F_i.*

The proof of this theorem can be found in [14].

3. Basic Components of the Fixed-Block Signaling Systems

Similar to Refs [5, 33], a brief description of the components of fixed-block signaling systems is given in this section.

3.1. Traffic control center The traffic control center (TCC) is responsible for the whole train traffic in its region. The components of the railway field can be controlled and monitored by the TCC. All operations are managed by the dispatchers (officers in the TCC).

3.2. Signaling system control software The signaling system control software, namely the interlocking system, evaluates the requests of the dispatchers and sends proper commands to the railway field equipment, if necessary. The most important task of the signaling system control software is to provide system safety at all times.

3.3. Signals Since every country has its own signaling principles and safety standards, the use of colors of railway signals may vary from country to country. Railway signals inform train drivers of the occupation of the next block. For example, in the Turkish State Railways, the meaning of the red color is that the next block is occupied, whereas the yellow color means that the next block is free but not after the next block. The yellow color also permits a train to proceed with reduced speed. The green color indicates that the next two blocks are free and the train can proceed. The Japanese Railways uses red, yellow, and green signals with their combinations, and the North American Railways uses purple and amber signals. Signals are located at the entrance and exit of the railway blocks (with fixed length).

3.4. Point machines (Railway switches) The PMs enable the railway vehicles to change from one track to another. They have two location indicators known as *normal* and *reverse*. The positions of the PM can be controlled by the TCC either manually or automatically.

3.5. Railway blocks The occupation of a train in a railway block is detected with the help of track circuits or axle counters. Depending on the length of the block, one or more track circuits are used. Track circuits operate according to the short-circuit principle. By the entrance of a train into a railway block, the track circuit is short-circuited by the axles of the train. On the other hand, axle counters count the incoming and outgoing axles of trains. The general block diagram of the whole system is given in Fig. 2.

4. Specifications of the Fixed-Block Signaling System

The train movement in a fixed-block railway system mainly relies on restrictions and prohibitions. The specifications will be explained by the help of an example railway field shown in Fig. 3,

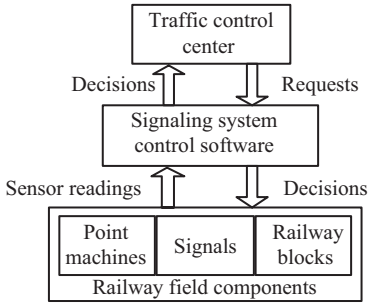


Fig. 2. The general block diagram of the system

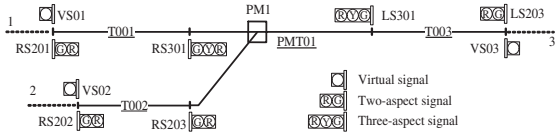


Fig. 3. An example railway field

which includes four railway blocks T001, T002, PMT01, and T003.

The given railway field layout in Fig. 3 is general enough in the sense that it includes the main railway field components such as a PM, track circuits, and railway wayside signals. For example, regardless of the scale of a railway field, the operational logic of a signal is the same. For example, the red signal always means that a train must stop, and the green signal is used to indicate that the next railway block is free. The signaling system control software always checks the incoming requests and the condition of the railway field equipment. When there is no reserved route, all signals must be red. If any signal in the field becomes any other color than red, the signaling system control software sends a warning message to the TCC. Furthermore, the given railway field including these equipment can be easily extended to check diagnosability of large railway fields.

First of all, a route must be reserved for a single train to allow its movement and prevent it from colliding with others. Several conditions have to be checked before and after the route reservation. As an initial condition, to accept a route request which is made by the TCC, there must not be any intersecting pre-reserved route. For instance, if the route 1–3 is requested by the TCC, the routes 3–1, 2–3, or 3–2 must not be pre-reserved. All these restrictions can be summarized in a table known as the *interlocking table* [33].

After the acceptance of a route request, the signaling control software sends proper commands to adjust the position of the PM. In Fig. 3, if the route request from 2 to 3 or 3 to 2 is accepted, then PM1 has to be adjusted to the reverse position. Later, when the PM has the proper position related to the requested route, the signaling software sends appropriate information to the entrance signal of the route. The entrance signals of the routes 1–3, 3–1, 2–3, and 3–2 are RS301, LS301, RS203, and LS301, respectively. If all components have proper conditions (the PM is in the proper position and the entrance signal shows the right color), then the signaling control software reserves the route and electronically locks the components of the route. This electronic locking of the components can be regarded as an additional protection of the components. For example, in order to prevent a train from derailment, the PM must keep its position while its railway block is occupied by a train.

Another important issue is to check the condition of the field components periodically such as the color information shown by the signals, the positions of the PMs, etc. As a world-wide operational condition, a PM has to change its position in a predefined time, which is 7 s in the Turkish State Railways, and a

PM must not remain in the middle of the movement when it starts to change its position. On the other hand, malfunctions such as wrong signal color indication and no signal color indication can occur. All these unwanted situations have to be taken into account by the signaling control software and the safety of the system has to be provided immediately. For more explanations, the reader is referred to Ref. [34].

Finally, the signals VS01, VS02, and VS03 in Fig. 3 indicate the virtual signals that do not exist in the railway field but are used for the route reservations from signal to signal by the dispatchers.

5. Modeling of the Railway Field Components and Fault Diagnosis Approach

5.1. Modeling by Petri nets In this section, compact Petri net models of the railway field components are explained. The Petri net models given in this section are *ordinary* and *safe*. Since there are four possible route reservations intersecting with each other for the given railway field in Fig. 3, the Petri net model related to the route reservations can be represented by five places (Fig. 4). The meanings of the places and transitions for all Petri net models are given in Table I in this section.

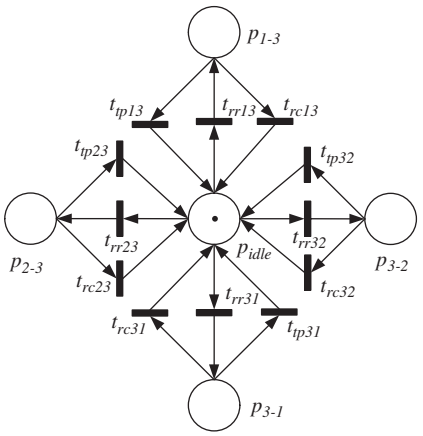


Fig. 4. Petri net model of the route reservations

Table I. Meanings of places and transitions in the models given in Figs 4–7

Place	Meaning	Transition	Meaning
p_{idle}	There is no route reservation	t_1	PM left normal position
p_{1-3}	The route 1–3 is reserved	t_2	PM reached reverse position
p_{2-3}	The route 2–3 is reserved	t_3	PM left reverse position
p_{3-1}	The route 3–1 is reserved	t_4	PM reached normal position
p_{3-2}	The route 3–2 is reserved	t_5	7 s passed
p_1	PM is in normal position	t_6	Move PM to normal position
p_2	PM is in reverse position	t_7	Move PM to reverse position
p_3	PM is moving from reverse position to normal position	t_8	7 s passed
p_4	PM is moving from normal position to reverse position	t_9	Turn signal to red
p_5	PM does not reach desired position	t_{10}	Turn signal to green
p_6	Two-aspect signal is red	t_{11}	Signal fault acknowledged
p_7	Two-aspect signal is green	t_{12}	Turn signal to green
p_8	Three-aspect signal is red	t_{13}	Turn signal to red
p_9	Three-aspect signal is green	t_{14}	Turn signal to yellow
p_{10}	Three-aspect signal is yellow	t_{15}	Turn signal to red
p_{11}	Railway block T001 is occupied	t_{16}	Signal fault acknowledged
p_{12}	Railway block PMT01 is occupied	t_{17}	Signal fault acknowledged
p_{13}	Railway block T002 is occupied	t_{18} (t_{21})	Occupy railway block T001
p_{14}	Railway block T003 is occupied	t_{19} (t_{20})	Vacate railway block T001
p_{f1}	PM did not reach reverse position	t_{22} (t_{24})	Occupy railway block T002
p_{f2}	PM did not reach normal position	t_{23} (t_{25})	Vacate railway block T002
p_{11_1}	Restriction of T001	t_{26_1}–t_{26_3} (t_{28})	Occupy railway block PMT01
p_{12_1}	Restriction of PMT01	t_{27} (t_{29})	Vacate railway block PMT01
p_{13_1}	Restriction of T002	t_{30} (t_{32})	Occupy railway block T003
p_{14_1}	Restriction of T003	t_{31} (t_{33})	Vacate railway block T003
		t_{f1}	Fault occurs while PM is moving from normal position to reverse position
		t_{f2}	Fault occurs while PM is moving from reverse position to normal position
		t_{f3}	Faulty green color in the signal
		t_{f4}	Faulty yellow color in the signal
		t_{f5}	Faulty green color in the signal
		t_{tp32}	Train has passed the route 3–2
		t_{rr32}	Reserve the route 3–2
		t_{rc32}	Cancel the route 3–2
		t_{rc31}	Cancel the route 3–1
		t_{tp13}	Train has passed the route 1–3
		t_{rr13}	Reserve the route 1–3
		t_{rc13}	Cancel the route 1–3
		t_{tp23}	Train has passed the route 2–3
		t_{rr23}	Reserve the route 2–3
		t_{rc23}	Cancel the route 2–3
		t_{tp31}	Train has passed the route 3–1
		t_{rr31}	Reserve the route 3–1

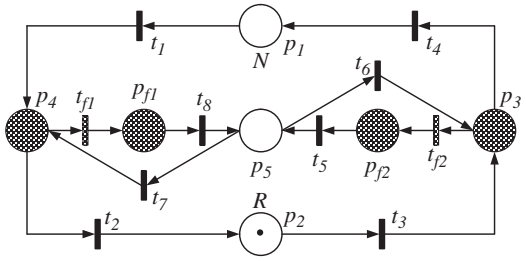
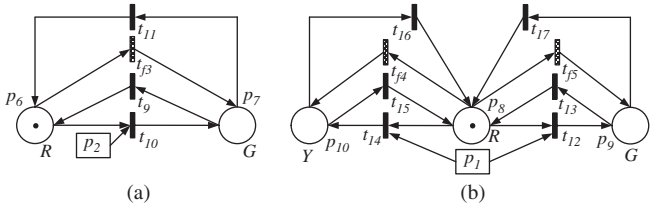


Fig. 5. Petri net model of the PM



(a) (b)

Fig. 6. Petri net models of the signals. (a) Two-aspect signal. (b) Three-aspect signal

As can be seen from Fig. 4, only one route reservation is permitted to prevent the trains from collisions.

The Petri net model of the PM is given in Fig. 5. As represented in Fig. 1, some places and some transitions are assumed as unobservable. The position of the PM can be detected with the help of the position sensors. So the movement of the PM from one position to another is assumed as unobservable (the switch is in the middle of movement). As an operational restriction, the PM has to change its position in 7 s. When the PM begins to change its position, the token in p_2 (or p_1) moves to the unobservable place p_3 (or p_4) over the transition t_3 (or t_1). If the PM does not reach its new position in 7 s, then the faulty transition t_{f2} (or t_{f1}) fires and the token in the unobservable place p_3 (or p_4) moves to p_{f2} (or p_{f1}) over the transition t_{f2} (or t_{f1}). On the other hand, if the PM reaches its new position, the token in p_3 (or p_4) moves to p_1 (or p_2) over the transition t_4 (or t_2).

The Petri net models of the signals are given in Fig. 6. Initially, all signals in the railway field are red. Signals can show proper color indications other than red, according to route reservations. Assume that it is desired to reserve the route 1–3. When the route 1–3 is reserved, a train occupies the blocks T001, PMT01, and T003, respectively. The Petri net models given in Fig. 6 represent the signals RS203 and RS301. R, Y, and G indicate red, yellow, and green colors, respectively. After the acceptance of the related route request, it is expected that the PM is in the normal position. If it is not in the proper position, then the signaling control software sends an appropriate command to the PM. When the PM is in the proper position, the token in the place p_8 moves to the place p_9 by the firing of the transition t_{12}. The places p_1 and p_2 denoted by rectangles in Fig. 6 represent such conditions. The signal RS203 can be green (p_7) if the PM is in the reverse position (p_2). Similarly, the signal RS301 can be green (p_9) or yellow (p_{10}) if the PM is in the normal position (p_1). The signal RS301 remains to be green until a train enters the railway block PMT01 or a route cancellation request from the TCC is received.

The unobservable transitions t_{f3}, t_{f4}, and t_{f5} represent the faulty transitions that can be encountered in signal malfunctions. In some cases, signals can show wrong color indications because of electromagnetic fields and cable short circuits. When such a fault occurs, it has to be detected immediately by the signaling control software, and depending on the condition of the other components, the system moves to the safe state (e.g., all route requests are rejected and all signals related to the faulty signal become red).

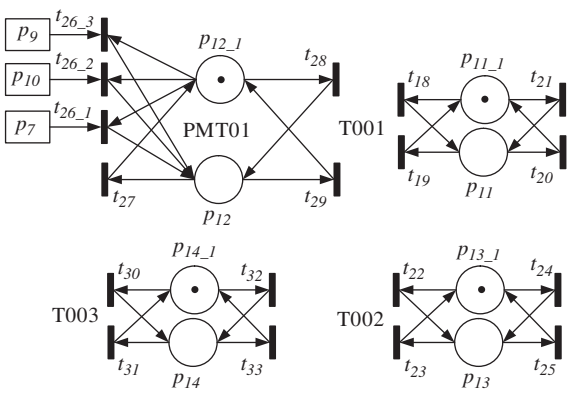


Fig. 7. Petri net models of the railway blocks

Finally, the train movement is monitored and detected with the help of the track circuits, and each railway block is modeled by a single place with entrance and exit transitions which represent the direction of the movement (Fig. 7). The train is expected to enter and exit the railway blocks in order. When a train enters the related railway block, a token is put in its related place (e.g., for T001, a token is added to the place p_{11} by the firing of t_{18} or t_{21}) depending on the direction of movement. The token in the place p_{11} is removed by the firing of t_{20} (or t_{19}) when the train exits the track T001. The places p_{11_1}, p_{12_1}, p_{13_1} and p_{14_1} are used to restrict the train's entry into the railway blocks while the corresponding block is occupied by another train. Additionally, the entry of each railway block is enabled by the signal colors. The entry of a train to T001 and T003 is enabled by the signals RS201 and LS203, respectively, as shown in Fig. 3. Similarly, for the routes 1–3 or 2–3, the entry of a train to PMT01 is enabled by the signals RS301 or RS203. After the route 1–3 is reserved, a train in T001 can enter PMT01 when the signal RS301 is yellow or green. The places p_7, p_9, and p_{10}, denoted by rectangles in Fig. 7, represent the restriction of the entry of the train to PMT01 by the signals RS301 (p_9, p_{10}) or RS203 (p_7). Depending on the condition of the railway field, the entry into PMT01 is enabled by the proper signal colors. Similar restrictions have to be added to each railway block Petri net model, but they are not shown here for simplification.

Note that the Petri net models of the railway field components given in this paper are compact models which just represent the main operational behavior of the components. These models can then be converted to software blocks by using different approaches [35–37]. For the railway field shown in Fig. 3, the software contains six signals, one PM, and four railway blocks including their relations.

5.2. Definition of some possible failures In railway signaling systems, in order to provide a safe and effective transportation, failures can be classified according to their importance. Some failures can be overcome by just informing the TCC and the train drivers of their occurrences, whereas some failures cannot. In the latter case, the whole system has to be stopped. For instance, when a PM malfunction occurs, the signaling system informs the TCC of the occurrence and does not permit the train movement in the PM area. Furthermore, trains can be guided to alternative routes. Likewise, if a track circuit (or an axle counter) malfunction occurs, such as the disappearance of the train on the railway line, the signaling system has to stop trains immediately and also inform the TCC. The former case, for which raising an alarm is enough, is referred to an *alarm condition*, whereas the latter case, for which trains have to stop, is referred to as *safe-state condition*. For the railway field of Fig. 3, some possible failures and their results can be summarized as follows:

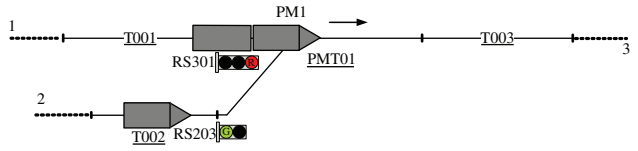


Fig. 8. Catastrophic failure

1. Alarm conditions:

   - A signal that is in the opposite direction for the route shows any color other than red after the route is reserved. Assume that the route 1–3 is reserved and the entry signal RS301 is green. Then the signals LS301, LS203, and RS203 must be red. For instance, assume that the signal LS301 becomes green instead of red after the route 1–3 is reserved. In this situation, the route 1–3 have to be cancelled immediately and the entry signal of the route (RS301) must be red if the train has not entered yet. On the other hand, if the train has entered the route when the fault occurs at the signal LS301, the TCC must inform all other incoming trains of the occurrence of the fault because the route cannot be cancelled while a train is moving. A similar scenario can be explained with the help of the example railway yard given in Fig. 8. If a fault occurs at the signal RS203 when the route 1–3 is not reserved and the block T002 is free, raising an alarm is enough to provide system safety.
   - The position of the PM is corrupted after a route is reserved. Assume that the route 3–2 is reserved, the PM is in the reverse position, and the entry signal LS301 is yellow. The position of the PM must be locked in reverse until the route is cancelled or a train has passed. When the position of the PM is corrupted, the route has to be cancelled if there is no train in the route. If a train is moving in the route when the fault occurs in the PM, the train driver must be informed by the TCC about the occurrence of the fault. In both cases, an alarm signal is also produced to inform the dispatchers.

2. Safe-state conditions:

   - A signal that is in the opposite direction for the route shows any color other than red after the route is reserved and the railway block is occupied. Assume that the route 1–3 is reserved and the train occupies the blocks T001 and PMT01. In this situation, the entry signal RS301 is red because the train has entered PMT01. Assume also that the railway block T002 is also occupied by another train. If the color of the signal RS203 becomes green by the occurrence of a fault (while a train is moving in the route 1–3), then the whole system has to move to the safe state where all signals must be red and all trains have to be stopped immediately in order to prevent collisions. This scenario is illustrated in Fig. 8.

5.3. The diagnoser design The diagnoser is designed by using the procedure given in Refs [14, 17–19]. Although there are four possible route reservations for the railway field given in Fig. 3, only a part of the diagnoser for the reservation of the route 1–3 is given in Fig. 9. The diagnoser in Fig. 9 partially represents the route reservation process after the route 1–3 is requested from the TCC and accepted by the signaling control software. The other route reservations are not mentioned here but they can be dealt with in a similar manner.

Each state represented by a rectangle consists of a pair of a marking of places p_1 to p_{14}, p_{f1}, and p_{f2} and a label N or $F_i (i \in \{1,2,3,4,5\})$. That is, in the part of the diagnoser, a marking just after an observed event is uniquely determined. Also, multiple failures are not dealt with for simplicity. Each failure type F_i is related with the faulty transition t_{fi}. Each state transition is labeled by the observation of a marking or a pair of the observations of a marking and an observable transition with a slight abuse of notation. (According to the definition of (8), each state transition is labeled by the observation of a marking or an observable transition. In Fig. 9, for ease of understanding, the observation of a marking is also attached in the latter case.) The former corresponds to the case where only the change of the observation of a marking is observed, whereas the latter corresponds to the case where the firing of an observable transition is observed with the observation of a marking. For instance, at the initial state of the diagnoser, the event label $\hat{M}1 - t_3$ indicates that the firing of an observable transition t_3 is observed with the observation $\hat{M}1$ of the resulting marking. Also, at the state ((1,0,0,0,0,1,0,1,0,0,0,0,1,0,0,0),N) with the observable marking $\hat{M}20$, the event label $\hat{M}23$ represents that the observable marking $\hat{M}20$ changes to $\hat{M}23$ by the firing of an unobservable transition t_{f5} which is not indicated in the event label.

According to Theorem 1 given in Section 2.3 and the part of the diagnoser given in Fig. 9, there is no F_i-indeterminate cycle for

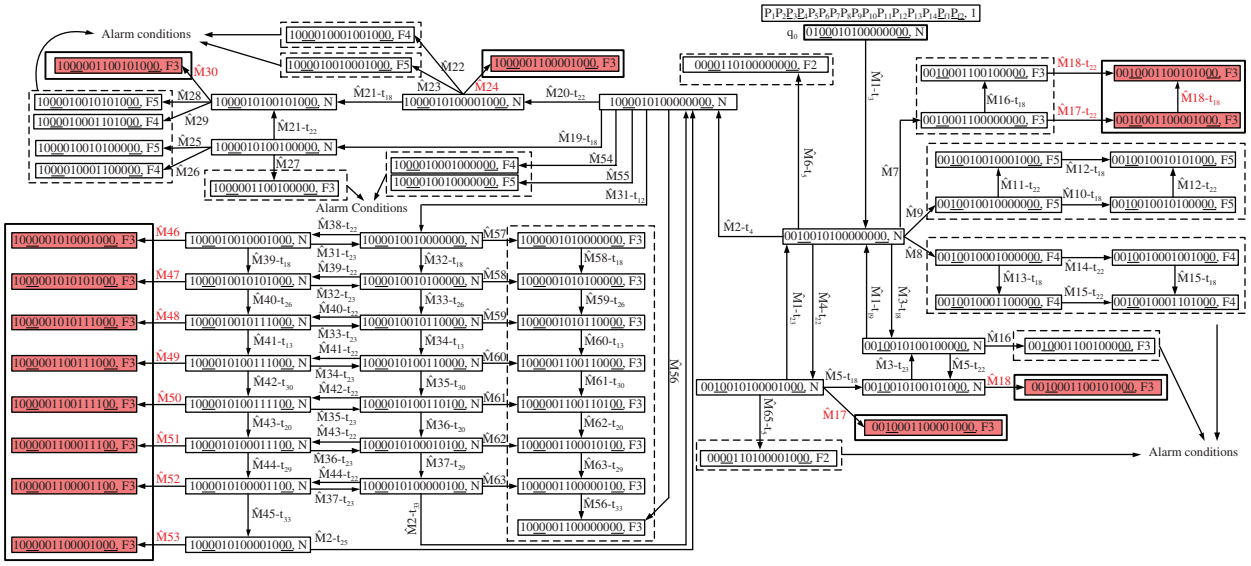


Fig. 9. A part of the diagnoser for the route 1–3

any failure type F_i and the system is diagnosable in the considered situation (Note that we can verify that the system is entirely diagnosable.). For safety reasons, it should be an expected result. In Fig. 9, the thick rectangles indicate the safe-state conditions whereas the dashed rectangles indicate alarm conditions.

While reserving the route 1–3, if a fault occurs in the PM movement (the faulty transition t_{f2} in Fig. 5 fires), an alarm is raised and the route reservation is cancelled. This situation is represented by the state ((0,0,0,0,1,1,0,1,0,0,0,0,0,0,0,0),F_2) with the observable marking $\hat{M}6$, which means that the PM did not reach the desired position in 7 s. At this state, the dispatcher in the TCC can request the PM to be moved either to the reverse or to the normal position. When the PM moves to the proper position for the route 1–3 and is locked, if a fault occurs at the entrance signal of the route (the signal RS301) or at the signal RS203 (the faulty transitions t_{f3}, t_{f4}, or t_{f5} fires), the route reservation is also cancelled. This situation is represented by the state ((0,0,1,0,0,0,1,1,0,0,0,0,0,0,0,0),F_3) with the observable marking $\hat{M}7$, ((0,0,1,0,0,1,0,0,0,1,0,0,0,0,0,0),F_4) with the observable marking $\hat{M}8$, or ((0,0,1,0,0,1,0,0,1,0,0,0,0,0,0,0),F_5) with the observable marking $\hat{M}9$. The safe-state condition may occur if, after the route 1–3 is reserved, the railway block T002 is occupied and a train is moving in the route. These are indicated as thick rectangles in Fig. 9. In such a situation, the trains have to stop by the help of the automatic train protection (ATP) and automatic rain stop (ATS) equipment, which is out of the scope of this paper.

A benefit of such a diagnoser design is that it enables us to check the adequacy of the constructed Petri net models. While developing signaling control software (Fig. 2), the designers have to perform a worst case analysis, which can also be considered as a tradeoff between the system safety and ease of operations. Since the Petri net models have to be simple for easy error tracking of the software and also reliable for safe transportation, the designers have to cope with both simplicity and reliability specifications. For example, if the signaling control software is developed by just considering the safety issues at first sight, then the whole system may fall into the safe-state condition in case of any simple failure, such as the stoppage of the whole train traffic with a simple signal malfunction. This will result in long delays in railway operations and wastage of time. On the other hand, if safety issues are not considered adequately, then accidents may occur, which is also an unwanted situation. The design of a diagnoser using the DES approach helps us to decide what should be done in case of each failure. For some failures, just raising an alarm would be enough to provide the system safety (e.g., ((1,0,0,0,0,1,0,0,0,1,0,0,1,0,0,0),F_4) with the observable marking $\hat{M}22$ and ((1,0,0,0,0,1,0,0,1,0,0,0,1,0,0,0),F_5) with the observable marking $\hat{M}23$ in Fig. 9), whereas in some cases the whole system has to move into the safe-state where all signals are red, all PMs are locked, and all trains have to be stopped immediately (e.g., ((0,0,1,0,0,0,1,1,0,0,0,0,1,0,0,0),F_3) with the observable marking $\hat{M}17$ and ((0,0,1,0,0,0,1,1,0,0,1,0,1,0,0,0),F_3) with the observable marking $\hat{M}18$ in Fig. 9). Briefly, designing a diagnoser can be considered as an additional safety procedure, which allows designers to verify the accuracy of the related Petri net models and also the developed software.

6. Conclusion

The structure of the fixed-block railway signaling systems enables signaling software designers to study these systems as DESs. Since the railway systems fall in the class of safety-critical systems where human life is in question, the detection of the occurrence of a failure as soon as possible and preventing the system from possible faulty conditions is the most important issue. The safety of the entire system has to be guaranteed at all times. In this study, a sample railway field is modeled by using a well-known modeling tool Petri nets, and the DES approach is applied to design a diagnoser. Designing a diagnoser can be time consuming but enables signaling software designers to verify their models before testing the developed signaling system software.

Acknowledgement

This work was supported by JSPS RONPAKU (Dissertation Ph.D.) Program and the Okawa Foundation for Information and Telecommunication.

References

(1) IEC 61508-4, Functional Safety of Electrical/Electronic/Programmable electronic safety-related systems, Part 4: Definitions and abbreviations. 2010.
(2) An introduction to Safety Critical Systems. IPL intelligent business. 2011. http://www.ipl.com/pdf/p0826.pdf. Accessed June, 2013
(3) Knight JC. Safety critical systems: challenges and directions. *Proceedings of the 24th International Conference on Software Engineering*, Orlando, Florida, USA, 2002;547–550.
(4) Kuepper GJ, 150 years of train-disasters - Practical approaches for emergency responders *9-1-1 Magazine* 1999; **(September/October issue)**:30–33.
(5) Hall S. *Modern Signalling Handbook.* Ian Allan Publishing: Birmingham, UK; 2001.
(6) IEC 61508-3, Functional Safety of Electrical/Electronic/Programmable electronic safety-related systems, Part 3: Software requirements. 2010.
(7) EN 50128, Railway Applications, Communications, signalling and processing systems, Software for railway control and protection systems. 2001.
(8) Söylemez MT, Durmuş MS, Yıldırım U. Functional safety application on railway systems: Turkish National Railway Signalization Project. *Proceedings of the 24th International Congress on Condition Monitoring and Diagnostics Engineering Management* 2011;1683–1692.
(9) Kaymakçı Ö, Anık VG, Üstoğlu İ. A local modular supervisory controller for a real signalling system. *Proceedings of the 5th IET International System Safety Conference*, Manchester, UK, 2010.
(10) Cassandras CG, Lafortune S. *Introduction to Discrete Event Systems.* Kluwer Academic Publishers: Norwell, MA; 1999.
(11) David R. Grafcet: a powerful tool for specification of logic controllers. *IEEE Transactions on Control Systems Technology* 1995; **3(3):**253–268.
(12) Ramadge PJ, Wonham WM. The control of discrete event systems. *Proceedings of the IEEE* 1989; **77(1):**81–98.
(13) Murata T. Petri nets: properties, analysis and applications. *Proceedings of the IEEE* 1989; **77(4):**541–580.
(14) Sampath M, Sengupta R, Lafortune S, Sinnamohideen K, Teneketzis D. Diagnosability of discrete-event systems. *IEEE Transactions on Automatic Control* 1995; **40(9):**1555–1575.
(15) Sampath M, Sengupta R, Lafortune S, Sinnamohideen K, Teneketzis D. Failure diagnosis using discrete-event models. *IEEE Transactions on Control Systems Technology* 1996; **4(2)**:105–124.
(16) Sampath M, Lafortune S, Teneketzis D. Active diagnosis of discrete event systems. *IEEE Transactions on Automatic Control* 1998; **43(7):**908–929.
(17) Ushio T, Onishi I, Okuda K. Fault detection based on Petri net models with faulty behaviors. *Proceedings of the 1998 IEEE International Conference on Systems, Man and Cybernetics* 1998; 113–118.
(18) Chung SL. Diagnosing PN-based models with partial observable transitions. *International Journal of Computer Integrated Manufacturing* 2005; **18(2–3)**: 158–169.
(19) Wen YL, Jeng MD. Diagnosability of Petri nets. *Proceedings of the 2004 IEEE International Conference on Systems, Man and Cybernetics* 2004; 4891–4896.
(20) Ramirez-Trevino A, Ruiz-Beltran E, Rivera-Rangel I, Lopez-Mellado E. Online fault diagnosis of discrete event systems. A Petri net-based

approach. *IEEE Transactions on Automation Science and Engineering* 2007; **4(1)**: 31–39.
(21) Lefebvre D, Delherm C. Diagnosis of DES with Petri net models. *IEEE Transactions on Automation Science and Engineering* 2007; **4(1)**: 114–118.
(22) Cabasino MP, Giua A, Seatzu C. Fault detection for discrete event systems using Petri nets with unobservable transitions. *Automatica* 2010; **46(9)**: 1531–1539.
(23) Cabasino MP, Giua A, Lafortune S, Seatzu C. A new approach for diagnosability analysis of Petri nets using verifier nets. *IEEE Transactions on Automatic Control* 2012; **57(12):** 3104–3117.
(24) IEC 61508-7, Functional Safety of Electrical/Electronic/Programmable electronic safety-related systems, Part 7: Overview of techniques and measures. 2010.
(25) Akita K, Watanabe T, Nakamura H, Okumura I. Computerized Interlocking System for Railway Signalling Control: SMILE. *IEEE Transactions on Industry Applications* 1985; **21(3)**: 826–834.
(26) Petersen JL. Automatic verification of railway interlocking systems: a case study. *Proceedings of the 2nd Workshop on Formal methods in Software Practice* 1998; 1–6.
(27) Rao VP, Venkatachalam PA. Microprocessor-based railway interlocking control with low accident probability. *IEEE Transactions on Vehicular Technology* 1987; **36(3)**: 141–147.
(28) Roanes-Lozano E, Roanes-Macias E, Laita LM. Railway interlocking systems and Gröbner bases. *Mathematics and Computers in Simulation* 2000; **51(5)**: 473–481.
(29) Kristoffersen T, Moen A, Hansen HA. Extracting high-level information from Petri nets: a railroad case. *Proceedings of the Estonian Academy of Sciences, Physics and Mathematics* 2003; **52(4)**: 378–393.
(30) Giua A, Seatzu C. Modeling and supervisory control of railway networks using Petri nets. *IEEE Transacions on Automation Science and Engineering* 2008; **5(3)**: 431–445.
(31) Ghazel M. Monitoring and diagnosis of discrete event systems using time Petri nets: a railway case study. *Fault Detection: Theory, Methods and Systems* 2011; 69–95.
(32) Li ZW, Zhou MC, Wu NQ. A survey and comparison of Petri net-based deadlock prevention policies for flexible manufacturing systems. *IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews* 2008; **38(2)**: 173–188.
(33) Yıldırım U, Durmuş MS, Söylemez MT. Automatic interlocking table generation for railway stations using symbolic algebra. *Proceedings of the 13th IFAC Symposium on Control in Transportation Systems* 2012; 171–176.
(34) White C. Interlocking principles. *IET Professional Development Course on Railway Signalling and Control Systems* 2010; 65–78.
(35) Uzam M, Jones AH. Discrete event control system design using automation Petri nets and their ladder diagram implementation. *The International Journal of Advanced Manufacturing Technology* 1998; **14(10)**: 716–728.
(36) Thapa D, Dangol S, Wang GN. Transformation from Petri nets model to programmable logic controller using one-to-one mapping technique. *Proceedings of the International Conference on Computational Intelligence for Modelling, Control and Automation and International Conference on Intelligent Agents, Web Technologies and Internet Commerce* 2005; 228–233.
(37) Frey G. Automatic implementation of Petri net based control algorithms on PLC. *Proceedings of the 2000 American Control Conference* 2000; 2819–2823.

Mustafa Seçkin DURMUŞ (Non-member) received the B.S. and M.S. degrees from Pamukkale University, Denizli, Turkey, in 2002 and 2005, respectively. He is currently pursuing the Ph.D. degree at the Istanbul Technical University (ITU), Turkey, and also a Ronpaku Fellow of the Japan Society for the Promotion of Science and studying at the Division of Electrical, Electronic and Information Engineering, Osaka University, Japan. Since 2007, he has been a Research and Teaching Assistant in the Department of Control Engineering, ITU. His research interests include railway signaling systems and fault diagnosis of discrete event systems. Mr. Durmuş is a student member of the IEEE.

Shigemasa TAKAI (Non-member) received the B.E. and M.E. degrees from Kobe University, Hyogo, Japan, in 1989 and 1991, respectively, and the Ph.D. degree from Osaka University, Osaka, Japan, in 1995. From 1992 to 1998, he was a Research Associate with Osaka University. In 1998, he joined Wakayama University as a Lecturer, and in 1999 became an Associate Professor. From 2004 to 2009, he was an Associate Professor with the Kyoto Institute of Technology. Since 2009, he has been a Professor with the Division of Electrical, Electronic and Information Engineering, Osaka University. His research interests include supervisory control and fault diagnosis of discrete event systems. Prof. Takai is a member of the IEICE, SICE, ISCIE, and IEEE.

Mehmet Turan SÖYLEMEZ (Non-member) is a Professor with Department of Control Engineering, Istanbul Technical University. His research interests include pole assignment (pole placement, pole shifting, eigenstructure assignment), linear control systems theory, multivariable systems, robust control, matrix theory, computer algebra, computer-aided control system design (CACSD), numerical analysis, optimization, genetic algorithms, PID controllers, low-order controller design, simulation of DC traction railway systems, railway signaling systems, flight control systems, and emergency management systems.