Available online at www.sciencedirect.com

ScienceDirect

IFAC-PapersOnLine 49-3 (2016) 459–464

Modular Fault Diagnosis in Fixed-Block Railway Signaling Systems

Mustafa S. Durmus*, İlker Ustoglu, Roman Y. Tsarev***, Michael Schwarz******

**Electrical and Electronics Engineering Department, Pamukkale University,
Denizli, TURKEY (e-mail: msdurmus@pau.edu.tr).
**Control and Automation Engineering Department, Yildiz Technical University,
Istanbul, TURKEY (e-mail: ustoglu@yildiz.edu.tr) **
***Institute of Space and Information Technology, Siberian Federal University,
Krasnoyarsk, RUSSIA (e-mail: tsarev.sfu@mail.ru)
****Computer Architecture and System Programming, Kassel University,
Kassel, GERMANY (e-mail: m.schwarz@uni-kassel.de)*

Abstract: The diagnosis of possible faults in railway signaling systems is an important issue to provide safe travel and transportation in railways. Signaling system designers have to consider the possible faults which may occur in railway field components both on the requirements preparation phase and on the development phase of the signaling system software or namely, the interlocking system. Although the diagnosis of different unobservable faults is relatively hard, especially for large scale railway fields, this complexity can be overcome by using the Discrete Event System (DES) based modular diagnosis approach which is explained in this paper. The main advantage of using such modular approach for fault diagnosis in fixed-block signaling systems is the inspection of the diagnosability of the whole system with respect to its subsystems (railway field components). In this study, the diagnosability of the railway field equipment and the whole system is also explained with a case study.

Keywords: Discrete Event Systems, Modular Fault Diagnosis, Fixed-Block Railway Signaling Systems.

1. INTRODUCTION

The use of railway transportation among different alternatives (e.g. road and air transportation) brings many profits such as less carbon dioxide emission and energy consumption. Although the infrastructure and the signaling costs of railways are high, they provide more environmental friendly and affordable solutions.

Railway signaling systems are divided into two main categories named as fixed-block (conventional) and moving-block signaling systems. Train movements are rely on route reservation procedure in fixed-block signaling systems. The requirements of each route including the railway field equipment are pre-defined in the interlocking table. Railway lines are divided into fixed-length rail blocks. Each railway block consists of an entrance signal and an exit signal. These signals inform the train driver about the situation of the next railway block. Although the use of the fixed-block signaling systems decreases the efficient use of the existing railway lines, it has been in use since mid-1800s in all over the world.

As with all other safety-critical applications, standards are defined to combine different safety requirements and concepts for railways. Software development process for fixed-block signaling systems including the choice of hardware and the communication protocols are defined by the EN 50126, EN 50128 and EN 50129 standards. In addition to the requirements and recommendations of railway related functional safety standards, signaling system engineers should take fault diagnosis into account while developing the signaling system software, or in other words, the interlocking system. (IEC 61508-7) describes fault diagnosis as the process of determining if a system is in a faulty state or not and it should be performed at the smallest subsystem level because smaller subsystems allow a more detailed diagnosis of faults.

Detecting faults in railway signaling systems, especially the faults which may occur in field components (e.g. points, signals) is a vital issue due to its harsh results. Therefore, fault diagnosis and condition monitoring studies on railway point mechanisms can be found in the literature (Rouvray et al. 1998; Roberts et al. 2002; Garcia Marquez et al. 2003; Zattoni 2006). However, these studies are addressed the fault diagnosis problem from a different perspective.

Due to having DES-like features in their structure (Cassandras and Lafortune 2008), and the recommendation of railway related safety standards such as (IEC 61508-3) and (EN 50128), fixed-block signaling systems can be regarded as discrete event systems (DESs) and the DES based modeling and fault diagnosis methods are applicable to fixed-block signaling systems.

However, diagnosability is described by (Sampath et al. 1995) as the detection with a finite delay occurrence of failures of any type using the record of observable events. The diagnoser is obtained by using the system model itself and it observes online the behavior of the system (Sampath et al. 1996). The studies of (Sampath et al. 1995) and (Sampath et al. 1996) defined the basics of DES based fault diagnosis and these basics further developed by many workgroups and

10.1016/j.ifacol.2016.07.077

studied as online (Ramirez-Trevino et al. 2007), centralized (Ushio et al. 1998; Chung 2005), decentralized (Debouk et al. 2000; Cabasino et al. 2013) and so on. As an application of DES based fault diagnosis to fixed-block railway signaling systems, (Durmuş et al. 2014) considers diagnosability analysis as an intermediate step between modeling the system and testing the developed software which enables signaling system designers to preliminary check their models. On the other hand, for large and complex systems, diagnosis of faults becomes a critical and stringent task. As pointed in (Giua and Seatzu 2014), due to the state explosion problem in DESs, the use of theoretical results while dealing with the real-world applications becomes complicated and sometimes inapplicable.

Therefore, instead of constructing a diagnoser for the whole system and checking its diagnosability, similar to (Debouk 2003) and (Contant et al. 2006), we will study the system model with respect to its subsystems and check the diagnosability of each subsystem (diagnosability of the modules) to show the overall diagnosability. The reader is referred to (Zaytoon and Lafortune 2013; Takai 2008; Zhou et al. 2008), for the overview of DES based fault diagnosis methods and for detailed explanation on modular fault diagnosis.

2. PRELIMINARIES

2.1 Fixed-Block Signaling System Components

The traffic control center is responsible for all railway traffic by providing an interface between the interlocking system and the dispatchers. Dispatchers (responsible officer) may send several requests to the interlocking system for evaluation such as route reservation request, point machine position request or field component blocking requests. Another main responsibility of the traffic control center is to log and monitor the train movements.

The interlocking system receives the requests of the traffic control center, and evaluates these requests for a final decision. The requests of the dispatchers can be accepted or rejected according to the safety restrictions. The design, development and the testing process of the interlocking system should be carefully handled and realized with respect to the related functional safety requirements (Durmuş et al. 2013, Durmuş et al. 2015a).

Railway blocks (RBs) are the subsections of the railway lines with fixed-length. The entrance and exit of a *RB* is equipped with signals to inform train drivers. The location of the trains are detecting by using simple electrical circuits know as track circuits or devices known as axle counters.

Signals (SLs) are used to inform the train drivers about the situation of their way. Even different colours and their combinations are in use and differ from country to country, the red colour and the green colour have similar meanings. Turkish State Railways use the red colour to denote the next two *RBs* are occupied whereas the green colour denotes the next two *RBs* are free. The yellow colour denotes the next *RB* is unoccupied but not the *RB* after the next. Depending on the topology of the railway field, an additional yellow colour is also used by Turkish State Railway to denote the line change. Generally, this additional yellow colour is placed at the bottom of the signal before entering point machine regions.

Point machines (PMs) are devices which enable trains to pass from one railway line to another. A *PM* can be operated either by a route reservation request or manually via traffic control center. The position of a *PM* can be also adjusted from the railway feld by the responsible officers (shunter) by using a lever.

General representation of a fixed-block signaling system is illustrated in Fig. 1. More detailed definitions of the components of fixed-block railway signaling systems can be found in (Hall 2001).

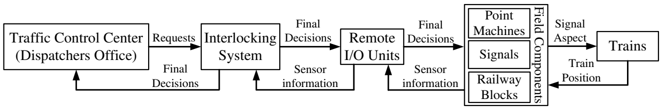

Fig. 1. General representation of a fixed-block signaling system.

2.2 Petri nets

A Petri net is defined by Murata (1989) as

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

where

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

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

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

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

For a marking $M : P \rightarrow \{0, 1, 2, 3, ...\}$, $M(p_i) = n$ means that the ith place has n tokens (Murata 1989). A marking M can also be represented by a vector with k elements where k is the total number of places.

Definition 2.2.1 (Cassandras and Lafortune 2008): 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 $I(t_j)=\varnothing$, 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, and we let $W(p_i,t_j)=0$ if $(p_i,t_j)\notin F$ and $W(t_j,p_i)=0$ if $(t_j,p_i)\notin F$. 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 2.2.2 (Murata 1989): 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 2.2.3 (Murata 1989): A marking M_n is reachable from the initial marking M_0 in a Petri net *PN* if there exists a sequence of transitions $t_1t_2\ldots t_n$ 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 2.2.4 (Murata 1989): 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, $\forall M_k \in R(M_0),\ \forall p_i \in P : M_k(p_i)\le m$. Additionally, a Petri net *PN* is *safe* if it is 1-bounded.

Definition 2.2.5 (Murata 1989; Li et al. 2008): 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 (Ushio et al. 1998). 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,

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

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

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 $T_{F_i}\cap T_{F_j}=\varnothing$ if $i\neq j$. The label set is defined as $\Delta=\{N\}\bigcup 2^{\Delta_F}$ 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. 2.

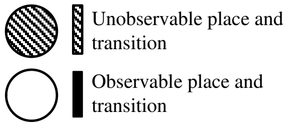
Unobservable place and transition
Observable place and transition

Fig. 2. Representations of places and transitions.

2.3 Fault Diagnosis and The Modular Architecture

As mentioned by (Sampath et al. 1995) and (Ushio et al. 1998), a Petri net system *PN* is diagnosable, if it is possible to detect the type of the fault within a finite number of firings of transitions after the occurrence of the fault. Due to the existence of unobservable places, some markings cannot be distinguished and therefore, the quotient set $\hat{R}(M_0)$ is defined with respect to the equivalence relation $(\equiv)$; $\hat{R}(M_0):={}^{R(M_0)}\!/\!_{\equiv}:=\{\hat{M}_0,\ \ldots,\ \hat{M}_n,\ \ldots\}$ where $M_0\in\hat{M}_0$ (Wen et al. 2004). An element of $\hat{R}(M_0)$ is referred to the observation of a marking or an observable marking. $M_1\equiv M_2$ denotes that the observations of markings M_1 and M_2 are the same for any $p_i\in P_o$, if $M_1(p_i)=M_2(p_i)$. The diagnoser of the whole system 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 which are reachable from the initial state q_0 under the state transition function δ_d, $\Sigma_o=\hat{R}(M_0)\cup T_o$ 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 diagnoser state q_d 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 $l_i\in\Delta$. 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 detailed explanation of the label propagation function and the modified range function of (Chung 2005) can be found in (Durmuş et al. 2014).

As mentioned in (Debouk 2003) and (Contant et al. 2006), instead of dealing with the state explosion problem of the diagnoser and checking the diagnosability of the whole system, the diagnosability of the Petri net system *PN* can be examined with respect to its subsystems. Before the definition of the modular diagnosability approach we impose the following two assumptions in this paper.

Assumption 2.3.1 (Sampath et al. 1995; Ushio et al. 1998): A Petri net system *PN* defined by (1) is *bounded* and *deadlock-free*.

Assumption 2.3.2 (Sampath et al. 1995; Ushio et al. 1998): 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,...,n*.

$$M_1[t_1 > M_2[t_2 > \dots M_n[t_n > M_1 \Rightarrow \exists i,j \in \{1,2,\dots,n\}: M_i \not\equiv M_j$$

As described by (IEC 61508-7), the aim of the modular approach is the decomposition of a software system into small comprehensible parts in order to limit the complexity of the system. By considering the recommendations of the (IEC 61508-3) where the use of modular approach and the use of *PN* formalism are highly recommended (see Table A.4 of IEC 61508-3), and the theory of the DES based fault diagnosis approach, the structure of the interlocking system can be separated into subsystems (or modules) as given in Fig. 3. Each module consists of the *PN* model and the diagnoser of each railway field component. These modules are linked with the other related component modules according to the interlocking table to form the whole system. As an advantage of the use of the modular approach, even if there can be more than one component with the same type, it is adequate to use a single module (a single *PN* model and its diagnoser) to represent the operational behavior of the component. For instance, there can be more than one point machine in the field but developing a single generic module for the point machine is sufficient.

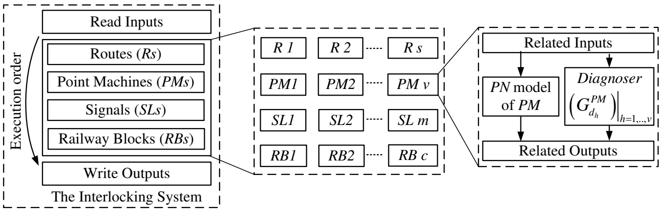

Fig. 3. The modular structure of the interlocking system.

The overall system and its diagnoser with respect to its subsystems can be extended as follows:

$$PN = PN_R \cup PN_{PM} \cup PN_{SL} \cup PN_{RB}, \tag{9}$$

$$G_{d_h}^{type} = \left(Q_{d_h}^{type},\ \Sigma_{o_h}^{type},\ \delta_{d_h}^{type},\ q_{0_h}^{type}\right), \tag{10}$$

where

- $PN_R = \{PN_{R1}, PN_{R2}, ..., PN_{Rs}\}$ are the *PN* models of the routes,
- $PN_{PM} = \{PN_{PM1}, PN_{PM2}, ..., PN_{PMv}\}$ are the *PN* models of the point machines,
- $PN_{SL} = \{PN_{SL1}, PN_{SL2}, ..., PN_{SLm}\}$ are the *PN* models of the signals,
- $PN_{RB} = \{PN_{RB1}, PN_{RB2}, ..., PN_{RBc}\}$ are the *PN* models of the railway blocks,

and similarly, $G_{d_h}^{type}$ is the diagnoser of any module with,

$$h = \begin{cases} \{1,2,...,s\} & \text{if, the } \textit{type} \text{ of the component is } R \\ \{1,2,...,v\} & \text{if, the } \textit{type} \text{ of the component is } PM \\ \{1,2,...,m\} & \text{if, the } \textit{type} \text{ of the component is } SL \\ \{1,2,...,c\} & \text{if, the } \textit{type} \text{ of the component is } RB \end{cases} \tag{11}$$

- $Q_{d_h}^{type}$ is the set of reachable states of the related modules,
- $\Sigma_{o_h}^{type}$ is the set of events of the related modules,
- $\delta_{d_h}^{type}$ is the set of partial state transition functions of the related modules,
- $q_{0_h}^{type}$ is set of initial states of the related modules,

The set of the diagnoser states $q_{h_n}^{type}$ consists of pairs of a marking $M_{h_n}^{type} \in R\left(M_{0_n}^{type}\right)$ and a label $l_{h_n} \in \Delta_F^{type}$ where *h* is given by (11) and *n* represents the number of the diagnoser states (see Assumption 2.3.2). Instead of using label $l_{h_n}^{type}$, we used label l_{h_n} because components and so as the diagnosers do not share any failure type. Each observed event $\sigma_{h_n}^{type} \in \Sigma_{o_h}^{type}$ represents the observation of a marking in $\hat{R}\left(M_{0_n}^{type}\right)$ or an observable transition in T_o^{type}.

Assume that a railway field consists of two point machines and assume also that each *PM* diagnoser has five states,

$$G_{d_2}^{PM} = \left\{ \underbrace{\left(Q_{d_1}^{PM},\ \Sigma_{o_1}^{PM},\ \delta_{d_1}^{PM},\ q_{0_1}^{PM}\right)}_{Diagnoser\ of\ PM1}, \underbrace{\left(Q_{d_2}^{PM},\ \Sigma_{o_2}^{PM},\ \delta_{d_2}^{PM},\ q_{0_2}^{PM}\right)}_{Diagnoser\ of\ PM2} \right\}$$

$$q_{h_n}^{PM} \Rightarrow q_{2_5}^{PM} = \left\{q_{1_5}^{PM}, q_{2_5}^{PM}\right\}$$

$$Q_{d_2}^{PM} = \begin{bmatrix} q_{1_5}^{PM} \\ --- \\ q_{2_5}^{PM} \end{bmatrix}$$

$$= \begin{bmatrix} \overbrace{\left(M_{1_5}^{PM1}, l_{1_5}\right), \left(M_{2_5}^{PM1}, l_{2_5}\right), \left(M_{3_5}^{PM1}, l_{3_5}\right), \left(M_{4_5}^{PM1}, l_{4_5}\right), \left(M_{5_5}^{PM1}, l_{5_5}\right)}^{Diagnoser\ states\ of\ PM1} \\ ------------------------------ \\ \underbrace{\left(M_{1_5}^{PM2}, l_{1_5}\right), \left(M_{2_5}^{PM2}, l_{2_5}\right), \left(M_{3_5}^{PM2}, l_{3_5}\right), \left(M_{4_5}^{PM2}, l_{4_5}\right), \left(M_{5_5}^{PM2}, l_{5_5}\right)}_{Diagnoser\ states\ of\ PM2} \end{bmatrix} \tag{12}$$

where $M_{h_n}^{PM} \in R\left(M_{0_n}^{PM}\right)$ and $l_{h_n} \in \Delta_F^{PM}$. For instance, the pair $\left(M_{1_5}^{PM1}, l_{1_5}\right)$ is used to denote the marking of the first state of the diagnoser of *PM* 1 and its label whereas the initial state is denoted by $q_{0_2}^{PM} = \left\{q_{0_1}^{PM}, q_{0_2}^{PM}\right\} = \left\{\left(M_{0_5}^{PM1}, l_{0_5}\right), \left(M_{0_5}^{PM1}, l_{0_5}\right)\right\}$.

According to (Contant et al. 2006) and (Durmuş et al. 2014), it is possible to classify states in $Q_{d_h}^{type}$ as follows:

1. A state $q_{h_n}^{type} \in Q_{d_h}^{type}$ is said to be F_i^{type}-certain if $F_i^{type} \in l_{h_n}$ for any $\left(M_{h_n}^{type}, l_{h_n}\right) \in q_{h_n}^{type}$.

2. A state $q_{h_n}^{type} \in Q_{d_h}^{type}$ is said to be F_i^{type}-uncertain if there exist $\left(M_{h_n}^{type}, l_{h_n}\right)$ and $\left(M_{h_n}'^{type}, l_{h_n}'\right)$ such that $F_i^{type} \in l_{h_n}$ and $F_i^{type} \notin l_{h_n}'$.

Theorem 2.3.1 (Sampath et al. 1995; Ushio et al. 1998; Contant et al. 2006): A Petri net subsystem (module) is diagnosable if and only if the diagnoser of any component of the subsystem does not contain an F_i^{type}-indeterminate cycle for any failure type F_i^{type}. As omitted by (Contant et al. 2006), the proof of this theorem is also omitted here and can be found in (Sampath et al. 1995).

3. MODELING the SYSTEM COMPONENTS: SIGNALS

In this section, the Petri net models of the signals and their diagnosers which are used in the railway field given in Fig. 4. with its interlocking table given in Table 1.

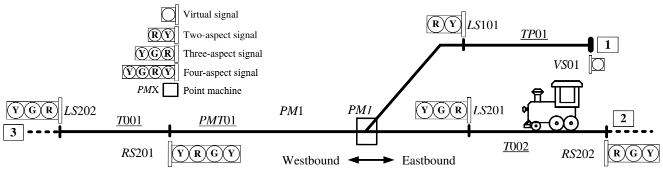

Fig. 4. A sample railway field (R-Red, Y-Yellow and G-Green).

Table 1. Part of the interlocking table of the railway field given in Fig. 4

Definition		Entrance Signal ID	Entrance Signal Colour		Lock	
Route Number	Route					
Route 1 (1-3)	*TP*01-*T*001	*LS*101	Y	*LS*202 - Y, G	1 Reverse	*LS*201, *RS*201
Route 2 (2-3)	*T*002-*T*001	*LS*201	G	*LS*202 - Y, G	1 Normal	*LS*101, *RS*201
			Y	*LS*202 - R		

3.1 Signals

The *PN* models and the diagnosers for the signals LS201 is illustrated in Fig. 5. The definitions of the transitions and the places of the *PN* model is given in Table 2. The places such as p_{pm1_1} and p_{RS201_R} denoted by rectangles are the additional conditions of related transitions. For instance, the color of the signal *LS*201 can be yellow when the *PM*1 is in normal position and the signals *RS*201 and LS101 are red. Representations of the *PN* model shown in Fig. 5 is as follows:

$$PN_{SL} = \left\{ \underbrace{PN_{RS201}}_{1}, \underbrace{PN_{LS202}}_{2}, \underbrace{PN_{LS101}}_{3}, \underbrace{PN_{LS201}}_{4}, \underbrace{PN_{RS202}}_{5} \right\},$$

$$P_o^{LS201} = \left\{ p_{LS201\_1}, p_{LS201\_2}, p_{LS201\_3}, p_{LS201\_6}, p_{LS201\_7}, p_{LS201\_9} \right\},$$

$$P_{uo}^{LS201} = \left\{ p_{LS201\_4}, p_{LS201\_5}, p_{LS201\_8}, \right\},$$

$$T_o^{LS201} = \{ t_{LS201\_1}, t_{LS201\_21}, t_{LS201\_22}, t_{LS201\_3}, t_{LS201\_4}, \\ t_{LS201\_5}, t_{LS201\_6}, t_{LS201\_8} \},$$

$$T_{uo}^{LS201} = \left\{ t_{LS201\_f5}, t_{LS201\_f6}, t_{LS201\_f7} \right\},$$

$$M_{0_6}^{LS201} = \Big(M_{0_6}^{LS201}\left(p_{LS201\_1}\right), M_{0_6}^{LS201}\left(p_{LS201\_2}\right), M_{0_6}^{LS201}\left(p_{LS201\_3}\right), \\ M_{0_6}^{LS201}\left(p_{LS101\_4}\right), M_{0_6}^{LS201}\left(p_{LS101\_5}\right), M_{0_6}^{LS201}\left(p_{LS101\_6}\right), \\ M_{0_6}^{LS201}\left(p_{LS101\_7}\right), M_{0_6}^{LS201}\left(p_{LS101\_8}\right), M_{0_6}^{LS201}\left(p_{LS101\_9}\right) \Big), \\ = \left(1,0,0,\underline{1},\underline{1},0,0,\underline{1},0\right).$$

The underlined numbers indicate the marking of the unobservable places.

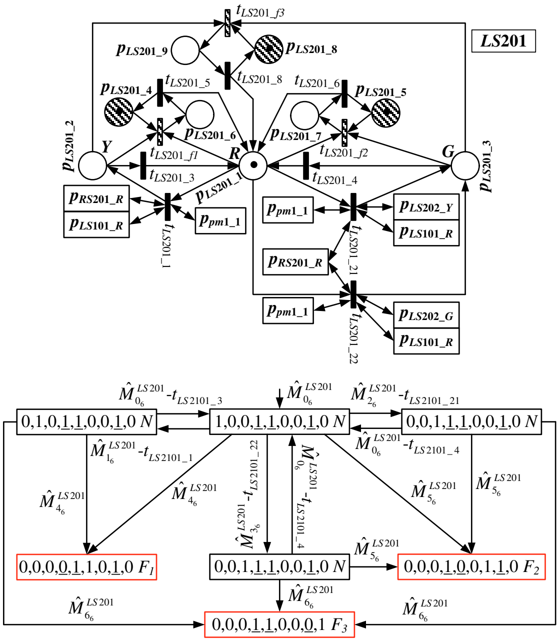
t_{LS201_f3}
LS201
p_{LS201_9}
p_{LS201_8}
t_{LS201_8}
p_{LS201_4}
t_{LS201_5}
t_{LS201_6}
p_{LS201_5}
p_{LS201_6}
p_{LS201_7}
p_{LS201_2}
Y
t_{LS201_f1}
R
t_{LS201_f2}
G
p_{LS201_3}
t_{LS201_3}
t_{LS201_4}
p_{LS201_1}
p_{RS201_R}
p_{LS101_R}
p_{pm1_1}
t_{LS201_1}
p_{pm1_1}
p_{LS202_Y}
p_{LS101_R}
t_{LS201_21}
p_{RS201_R}
p_{pm1_1}
p_{LS202_G}
p_{LS101_R}
t_{LS201_22}
$\hat{M}_{0_6}^{LS201}$-t_{LS2101_3}
$\hat{M}_{0_6}^{LS201}$
$\hat{M}_{2_6}^{LS201}$-t_{LS2101_21}
0,1,0,$\underline{1}$,$\underline{1}$,0,0,$\underline{1}$,0 N
1,0,0,$\underline{1}$,$\underline{1}$,0,0,$\underline{1}$,0 N
0,0,1,$\underline{1}$,$\underline{1}$,0,0,$\underline{1}$,0 N
$\hat{M}_{1_6}^{LS201}$-t_{LS2101_1}
$\hat{M}_{0_6}^{LS201}$-t_{LS2101_4}
$\hat{M}_{4_6}^{LS201}$
$\hat{M}_{4_6}^{LS201}$
$\hat{M}_{3_6}^{LS201}$-t_{LS2101_22}
$\hat{M}_{0_6}^{LS201}$-t_{LS2101_4}
$\hat{M}_{5_6}^{LS201}$
$\hat{M}_{5_6}^{LS201}$
0,0,0,$\underline{0}$,$\underline{1}$,1,0,$\underline{1}$,0 F_1
0,0,1,$\underline{1}$,$\underline{1}$,0,0,$\underline{1}$,0 N
$\hat{M}_{5_6}^{LS201}$
0,0,0,$\underline{1}$,$\underline{0}$,0,1,$\underline{1}$,0 F_2
$\hat{M}_{6_6}^{LS201}$
$\hat{M}_{6_6}^{LS201}$
$\hat{M}_{6_6}^{LS201}$
0,0,0,$\underline{1}$,$\underline{1}$,0,0,$\underline{0}$,1 F_3

Fig.5. PN model and diagnoser of the SL LS201.

Table 2. Meanings of places and transitions in the model given in Fig. 5 and Fig. 6

Place	Meaning	Transition	Meaning
p_{LS201_1}	Signal is red	t_{LS201_1}	Turn signal to yellow
p_{LS201_2}	Signal is yellow	t_{LS201_3}, t_{LS201_4}	Turn signal to red
p_{LS201_3}	Signal is green	$_{LS201\_21}$, (t_{LS201_22})	Turn signal to green
p_{LS201_4}, p_{LS201_5}, p_{LS201_8}	Color fault restriction of signal	t_{LS201_5}, t_{LS201_6}, t_{LS201_8}	Signal color fault acknowledged
p_{LS201_6}, p_{LS201_7}, p_{LS201_9}	Signal color fault has occurred	(t_{LS201_f1}, t_{LS201_f2}, t_{LS201_f3}	Faulty color aspect in the signal

For the *PN* models in Fig. 5 and Fig. 6, it is assumed that there are three different failure types $\Delta_F^{SL} = \{F_1, F_2, F_3\}$, where, $T_{F_1}^{SL} = \{t_{LS201\_f1}\}$, $T_{F_2}^{SL} = \{t_{LS201\_f2}\}$ and $T_{F_3}^{SL} = \{t_{LS201\_f3}\}$. Even though failures F_1, F_2, F_3 and F_4 are identical which mean that related signal has wrong color indication (e.g. signal aspect is green and red at the same time), separate failure labels are used to specify the exact failures between colors.

The diagnoser given in Fig. 5 consists of three states. Initially, the color of the signal LS201 is red and illustrated by the initial state $\{(1,0,0,\underline{1},\underline{1},0,0,\underline{1},0,N)\}$. The color of the signal LS201 can be yellow by an incoming route reservation command from the traffic control center (eg. route request from 2 to 3). At this situation, the state of the diagnoser will be $\{(0,1,0,\underline{1},\underline{1},0,0,\underline{1},0,N)\}$ by observing the marking $\hat{M}_{1_6}^{LS201}$ and the observable transition t_{LS2101_1}. If the signal LS201 will be red and yellow at the same time, or in other words, if the marking $\hat{M}_{4_6}^{LS201}$ is observed, the state of the diagnoser becomes $\{(0,0,0,\underline{0},\underline{1},1,0,\underline{1},0,F_1)\}$ In this state, the interlocking system will inform the traffic control center and provides the safety of the railway field.

According to Theorem 2.3.1 given in Subchapter 2.3 and the diagnoser given in Fig. 5, there is no F_i^{type}-indeterminate cycle for any failure type in Δ_F^{type} and the components of the modules are diagnosable in the considered situation. Note that, it is also possible to verify that the modules and the overall system are entirely diagnosable and this method is also applicable to systems which can be modeled as modules as presented in this paper. Even if a single model is used to represent the behavior of each component, the name of the transitions and places should be labeled carefully while converting all models to software blocks. After the software blocks has obtained, each block should linked with the other software blocks according to the interlocking table.

4. CONCLUSIONS

Developing a signaling system for large-scale fixed-block railway fields becomes a hard task by using the recommended methods in the railway related functional safety standards due to the exponential growth of the state space. On the other hand, inspecting the fixed-block signaling systems with respect to its subsystems (railway field components) makes the designing step which includes the modeling and the fault diagnosis much easier. The application of modular fault diagnosis approach of DES enables designers to cope with the large-scale fixed-block railway fields in an easy way due to their modular structure. This approach allows designers to check the adequacy of their models before passing to the testing phase and the developed system should be tested by using several methods for different scenarios to provide the required safety integrity level.

ACKNOWLEDGEMENT

This work is supported by The Scientific and Technological Research Council of Turkey (TÜBİTAK) project number 115E394 – Fail-Safe PLC implementation of Interlocking System Design with Fault Diagnosis capability for Fixed-block Railway Signaling Systems.

REFERENCES

Cabasino, M.P., Giua, A., Paoli, A. and Seatzu, C. (2013). Decentralized Diagnosis of Discrete Event Systems Using Labeled Petri Nets. *IEEE Transactions on Systems, Man and Cybernetics: Systems,* 43(6), 1477-1485.

Cassandras, C.G. and Lafortune, S. (2008). *Introduction to discrete event systems*, 2nd ed., Springer.

Chung, S.L. (2005). Diagnosing PN-based models with partial observable transitions. *International Journal of Computer Integrated Manufacturing,* 18(2-3), 158-169.

Contant, O., Lafortune, S. and Teneketzis, D. (2006). Diagnosability of Discrete Event Systems with Modular Structure. *Discrete Event Dynamic Systems: Theory and Applications,* 16, 9-37.

Debouk, R., Lafortune ,S. and Tenektzis, D. (2000). Coordinated decentralized protocols for failure diagnosis of discrete event systems. *Discrete Event Dynamic Systems: Theory and Applications,* 10(1-2), 33-86.

Debouk, R. (2003). Diagnosis of Discrete Event Systems: A Modular Approach. Proceedings of the IEEE International Conference on System, Man and Cybernetics, 306-311.

Durmuş, M.S., Yıldırım, U. and Söylemez, M.T. (2013). The Application of Automation Theory to Railway Signaling Systems: The Turkish National Railway Signaling Project. *Pamukkale University Journal of Engineering Sciences,* 19(5), 216-223.

Durmuş, M.S., Takai, S. and Söylemez, M.T. (2014). Fault Diagnosis in Fixed-Block Railway Signaling Systems: A Discrete Event Systems Approach. *IEEJ Transactions on Electrical and Electronic Engineering,* 9(5), 523-531.

Durmuş MS, Eriş O, Yıldırım U, Söylemez M T (2015a) A new bitwise voting strategy for safety-critical systems with binary decisions. *Turkish Journal of Electrical Engineering and Computer Sciences,* 23(5), 1507-1521.

Durmuş, M.S., Takai, S. and Söylemez, M.T. (2015b). Decision making strategies in fixed-block railway signaling systems: A discrete event systems approach. *IEEJ Transactions on Electrical and Electronic Engineering*, 10(2), 186-194.

EN 50128. (2011). Railway Applications, Communications, signalling and processing systems, Software for railway control and protection systems. *European Committee for Electrotechnical Standardization*, Brussels.

Garcia Marquez, F.P., Schmid, F. and Collado, J.C. (2003). A Reliability Centered Approach to Remote Condition Monitoring: A Railway Points Case Study. *Reliability Engineering and System Safety,* 80, 33-40.

Giua, A. and Seatzu, C. (2014). Petri nets for the Control of Discrete Event Systems. *Software & Systems Modeling*, 14(2), 692-701.

Hall, S. (2001). *Modern Signalling Handbook*, Ian Allan Publishing, England.

IEC 61508-3. (2010). Functional Safety of Electrical/Electronic/Programmable electronic safety-related systems, Part 3: Software requirements. *European Committee for Electrotechnical Standardization*, Brussels.

IEC 61508-7. (2010). Functional safety of electrical/electronic/programmable electronic safety-related systems, Part 7: Overview of techniques and measures. *European Committee for Electrotechnical Standardization*, Brussels.

Li, Z.W., Zhou, M.C. and Wu, N.Q. (2008). 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* 38(2), 173-188.

Murata, T. (1989). Petri nets: Properties, Analysis and Applications. *Proceedings of IEEE,* 77, 541-580.

Ramirez-Trevino, A., Ruiz-Beltran, E., Rivera-Rangel, I. and Lopez-Mellado, E. (2007). Online fault diagnosis of discrete event systems. A Petri net-based approach. *IEEE Transactions on Automation Science and Engineering* 4(1), 31-39.

Roberts, C., Dassanayake, H.P.B., Lehrasab, N. and Goodman, C.J. (2002). Distributed Quantitative and Qualitative Fault Diagnosis: Railway Junction Case Study. *Control Engineering Practice,* 10, 419-429.

Rouvray, P., Hallam, P., Danaher, S. and Thorpe, M.G. (1998). The application of Matlab to railway signaling system fault modelling. IEE colloquium on the use of systems analysis and modelling tools: experiences and applications, 7/1–7/8, London, UK.

Sampath, M., Sengupta, R., Lafortune, S., Sinnamohideen, K. and Teneketzis, D. (1995). Diagnosability of discrete event systems. *IEEE Transactions on Automatic Control,* 40(9), 1555-1575.

Sampath, M., Sengupta, R., Lafortune, S., Sinnamohideen, K. and Teneketzis, D. (1996) Failure diagnosis using discrete-event models. *IEEE Transactions on Control Systems Technology,* 4(2), 105-124.

Takai, S. (2008). A Sufficient Condition for Diagnosability of Large-Scale Discrete Event Systems. Proceedings of the 23rd International Technical Conference on Circuits/System, Computers and Communications, 321-324, Shimonoseki City, Yamaguchi-Pref., Japan.

Ushio, T., Onishi, I. and Okuda, K. (1998). Fault detection based on Petri net models with faulty behaviors. Proceedings of the IEEE International Conference on System, Man and Cybernetics 113-118, San Diego, California, USA.

Wen, Y.L. and Jeng, M.D. (2004). Diagnosability of Petri nets. Proceedings of the IEEE International Conference on System, Man and Cybernetics, 4891-4896, The Hague, Netherlands.

Zattoni, E. (2006). Detection of Incipient Failures by Using an H2-norm Criterion: Application to Railway Switching Points. *Control Engineering Practice,* 14, 885-895.

Zaytoon, J. and Lafortune, S. (2013). Overview of Fault Diagnosis Methods for Discrete Event Systems. *Annual Reviews in Control,* 37(2), 308-320.

Zhou, C., Kumar, R. and Sreenivas, R.S. (2008). Decentralized Modular Diagnosis of Concurrent Discrete Event Systems, Proceedings of the 9th IFAC International Workshop on Discrete Event Systems, 388-393, Göteborg, Sweden.