

# Fail-Safe Signalization Design for a Railway Yard: A Level Crossing Case

Durmuş M.S. \*, Yıldırım U.\*\*, Kurşun A.\*\*, Söylemez M.T.\*\*

\*Control Engineering Department, İstanbul Technical University,  
İstanbul, Turkey, (Tel: +90-505-2102113; e-mail: durmusmu@itu.edu.tr).

\*\*Control Engineering Department, İstanbul Technical University,  
İstanbul, Turkey, (e-mail: {yildirimu, kursuna, soylemezm}@itu.edu.tr)}

---

**Abstract:** Level crossings (grade crossings or railroad crossings) are one of the most crucial parts of the railway lines as two different types of transportation intersect at these points. Human failures including ignorance of warning signs, device troubles or carelessness can easily result in accidents especially at such cross-sections. In order to decrease the possibility of accidents on level crossings, several standards have been developed. In accordance with these standards, formal methods are required to be used specially in the development of interlocking systems that control safe operation of such crossings. In this study, a railway yard with a level crossing is modeled by Automation Petri Nets in order to design a fail-safe signalization system. A SCADA testbed is also developed to test several possible failure situations. The methods proposed in the design are expected to be used as part of an interlocking system in a railway station in Turkey.

**Keywords:** Level Crossing, Automation Petri Nets, Signalization.

---

## 1. INTRODUCTION

Providing *safe transportation* is one of the most important aims of railway systems. Although new technologies (Rumsey, 2006) and upgrades can overcome some of the problems on railways; sometimes they lead to fatal accidents (Kuepper, 1999, Wikipedia, 2010).

New standards are also developed to reduce such accidents (Burrage, 1995, National Railway Level Crossing Safety Strategy 2010-2020, 2010, Reder, 2006). The problem of level crossing (CarrsQ, 2008) safety is considered using several methods like probabilistic risk assessment (Anandarao and Martland, 1998), fault tree analysis (Reif et al., 2000), suitable software specifications (Jansen and Schneider, 2000) or Petri Nets - PNs (Einer et al., 2000, Kluge, 2003), which are widely used for modeling and design of railway signalization systems (Durmuş and Söylemez, 2009).

Most of the PN models in the literature do not consider failure modes (Ren and Zhou, 1995, Uzam and Jones, 1998, Uzam, 1998), Hörste, 1999, Peng, 2002, Febraro et al., 2006, Giua and Seatzu, 2008, Hagalisletto et al, 2007), which a machine or a system can encounter in daily life. However, improving system safety and reliability by taking possible failure situations into account and doing the worst case analysis is crucial especially in application areas like railways, where human life is in question.

A fail-safe system has to be capable of detecting failures or malfunctions that occur on a running system and take the whole or a part of the system in a predetermined *safe mode* when necessary. For instance, when switch position indicators show that a switch is on both normal and reverse positions at the same time, or a level crossing barrier is not closed when it is supposed to be closed for a railway system,

the whole system has to go into the safe mode (all components are supposed to be doing predetermined (*safe*) tasks when the system enters to safe mode). For instance, if the barrier is not closed the drivers have to be warned by an extra notice and the signals to the incoming trains should be turned to red.

In this study, a sample railway yard with a level crossing is modeled by PNs and Automation Petri Nets (APNs) while considering possible failures of some of the components. The resulting model is then converted to (Function Block Diagram) FBD using Token Passing Logic (TPL) technique (Uzam and Jones, 1998, Uzam 1998)) and implemented on a fail-safe PLC to satisfy a certain Safety Integrity Level (SIL) described by EN 50126, EN 50128, EN 50129 and IEC 61508 standards.

## 2. COMPONENTS of RAILWAY SIGNALLING and INTERLOCKING

*Traffic Command Center (TCC)* is a place where all train traffic is controlled and route reservations are made by dispatchers. The commands of dispatcher, which are mostly route reservation requests, are sent to the interlocking system, where they are checked considering the current state of the railway yard. The interlocking allows only commands that do not endanger the safety of the system, and hence is usually considered as the most crucial part of the signalization system. This is illustrated in Fig. 1.

When, a route reservation required by the dispatcher is possible, interlocking adjusts all equipments related with that route reservation (colours of signal lights, position of switches and gate barriers etc.).

*Track circuits (TCs)* are simple electrical equipments which are used to detect trains on railways. Both DC and AC TCs are used in Turkish railways. On some regions axel counters

are also used to detect trains. These equipments inform interlocking and also TCC about the absence or presence of the train (Hall, 2001, Palmer, 2006).

Similar to the road traffic, *colour signal lights* are used to inform the driver of the trains if the next railway block is occupied or not. Meanings of colour signals used in Turkish Railways are given in Table 1.

*Switches* are used on railways to allow the trains to change lines. Switches are also controlled by the interlocking system and have to be on *normal* or *reverse* position. If the switch is on neither normal nor reverse position or the position indicators show both positions at the same time, it is assumed that the switch is on a faulty state.

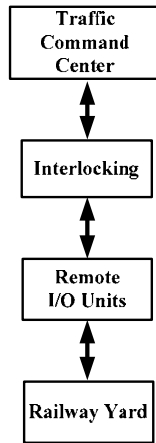


Fig. 1. Block diagram of signalization system.

*Flashing lights and gate barriers* are used for active protection of level crossings (Hall, 2001). They have three states: active, which means barrier is closed to allow train traffic, inactive, which means barrier is open to allow road traffic, and faulty, which means crossing is being opened or closed, or a fault has occurred (Anandarao and Martland, 1998).

### 3. AUTOMATION PETRI NETS (APNs)

An extension of the Petri Net (PN) definition in (Murata, 1989) can be done easily by adding inhibitor arcs ( $\dashv$ ), enabling arcs ( $\dashv$ ), firing conditions ( $\chi$ ) and actions ( $Q$ ) to ordinary PNs and known as APNs (Uzam and Jones, 1998, Uzam 1998) defined in the literature by (1).

$$APN = (P, T, Pre, Post, In, En, \chi, Q, M_0) \quad (1)$$

- **P** :  $\{p_1, p_2, \dots, p_n\}$ , finite set of places.
- **T** :  $\{t_1, t_2, \dots, t_n\}$ , finite set of transitions.
- **Pre** :  $(PxT) \rightarrow N$ , directed ordinary arcs from places to transitions ( $N$  is a set of nonnegative integers).
- **Post** :  $(TxP) \rightarrow N$ , directed ordinary arcs from transitions to places.
- **$M_0$**  :  $P \rightarrow N$ , initial marking
- **In** :  $(PxT) \rightarrow N$ , inhibitor arcs from places to transitions.
- **En** :  $(PxT) \rightarrow N$ , enabling arcs from places to transitions.
- **$\chi$**  :  $\{\chi_1, \chi_2, \dots, \chi_m\}$ , firing conditions associated with the transitions.
- **Q** :  $\{q_1, q_2, \dots, q_n\}$ , finite set of actions that might be assigned to the places.

Enabling and inhibitor arcs do not have any effect on number of tokens since they are used to enable or inhibit a transition. In fact these arcs and firing conditions add extra condition to fire a transition. For example, in order to fire a transition the number of tokens on a place has to be equal or greater than the number of the outgoing arcs to that transition. More details can be found in (Uzam and Jones, 1998, Uzam 1998).

### 4. MODELLING THE RAILWAY YARD

Railway yard shown in Fig. 2 is modelled by APNs to be used for fail-safe signalization design. This railway yard consist of three entrances (two on the east side and one on the west side), four railway blocks named 001BT, 1T, 1ST and 2ST (a block can contain more than one track circuit if necessary), six signal lights (B2D, 2D, 52DA, 54D, 2BA and 4B) and one level crossing. There are four possible routes that incoming trains can use to travel. These are from 001BT to 1ST, from 001BT to 2ST, from 1ST to 001BT, and from 2ST to 001BT.

All components of the railway yard given in Fig. 2 are modelled separately. The model of the railway blocks are given in Fig. 3. If there is a train on a railway block, a token is put in its related place. When the train moves to another block, its corresponding token also moves.

However, a train can occupy more than one TC at the same time. Because of this reason, railway blocks are modelled separately as given in Fig. 3 to check the presence or absence of trains on related blocks. That is to say, trains are modelled as tokens and railway blocks are modelled as places.

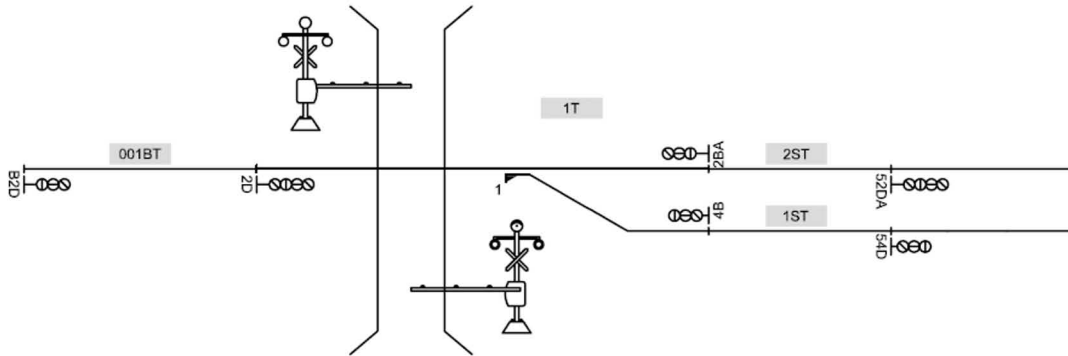


Fig. 2. Railway yard.

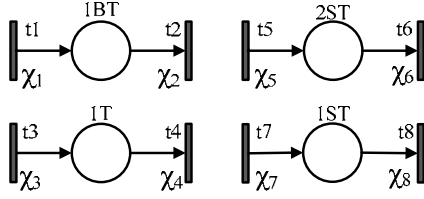


Fig. 3. PN model of the railway blocks.

Reservations are also modelled as places for all possible routes in the TCC model. Only one of the routes is allowed to be reserved at any time in order to prevent collision of trains. The corresponding PN is given in Fig. 4.

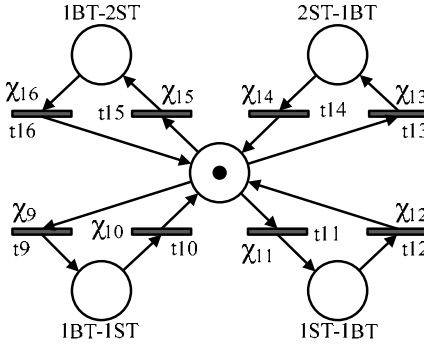


Fig. 4. PN model of TCC.

The APN models of the level crossing, the barrier and the flashing lights are given in Fig. 5, Fig. 6 and Fig. 7, respectively.

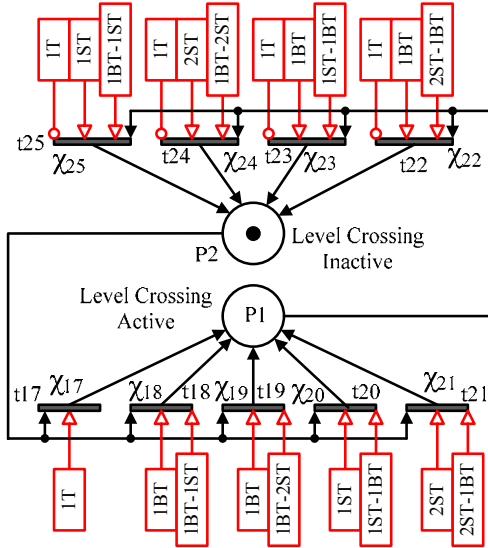


Fig. 5. APN model of the level crossing.

Normally (when there is no reservation), barrier of the level crossing is opened (it can be seen from Fig. 5 that P2 has a token, which means an inactive signal is being sent to the level crossing system by the interlocking). For instance, when the path 001BT-1ST is reserved by the TCC, the token moves to place 1BT-1ST in Fig. 4. The inactive signal (token on P2) does not terminate until a train enters the block 001BT. When a train enters to the block 001BT the level crossing becomes

active (token passes to place P1, when firing condition  $\chi_{18}$  is satisfied).

After t18 on Fig. 5 is fired, the barrier which is normally on open position begins to close by firing t26 as shown in Fig. 6 (token on P3 passes to P4) and the lights begin to flash at the same time (token on P8 passes to P9). If the barrier does not close in a predefined time, transition t30 (firing condition  $\chi_{30}$  is satisfied) is fired and token on P4 passes to P7 (fail state), in which interlocking informs TCC about this failure. When this failure is fixed transition t31 will be fired and the barrier begins to close again (token on P7 passes to P4). If the barrier is closed without any problems in a predefined time transition t27 will be fired, which allows token on P4 to pass to P5. Similarly, when the level crossing is set as inactive again, the token passes to P6 from P5, the barrier starts to open and the lights turn off. If a problem occurs during this process transition t32 will be fired and token on P6 passes to P7 (fail state). When this failure is fixed transition t33 will be fired and the barrier begins to open again. If the barrier is opened correctly in a predefined time transition t29 will be fired, which allows token on P6 to pass to P3 again.

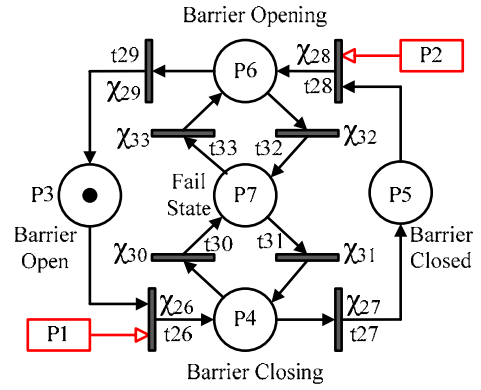


Fig. 6. APN model of the barrier.

In the failure situation (token on P7), the signal lights turn to yellow-red immediately to warn the train driver. When the problem is fixed, the token passes to its previous place. Places connected to enabling and inhibitor arcs are shown by rectangles in order to reduce the complexity of the figures.

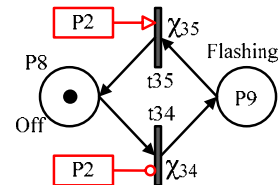


Fig. 7. APN model of the flashing lights.

APN model of switch 1 is given in Fig. 8. Similar to Fig. 6, if the switch does not reach to the desired position in a predefined time  $t$  then the token passes to fail-state. For instance, if switch 1 is on normal position and TCC makes the reservation 1BT-1ST, which requires the switch to go to the reverse position, t36 will be fired and token on SW1n passes to place SW1nr. SW1nr means switch 1 is moving from normal position to reverse position. However, if the

switch stays in SW1nr more than a predefined time  $t_{40}$  will be fired to cause the token to pass into SW1f state, which is considered as the failure state of the switch. In this case interlocking moves switch back to normal position by firing  $t_{43}$  (token on SW1f passes to SW1nr) and warns the TCC. Switches can be controlled directly or indirectly (by route reservations).

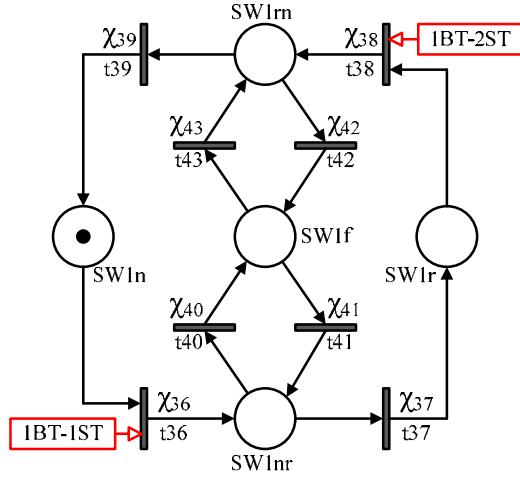


Fig. 8. APN model of the switch 1.

Finally, models of colour signal lights are given in Fig. 9. Signal light 54D is a three aspect dwarf signal and 52DA is a four aspect tall signal light. As it is obvious from Fig. 9 that all signals are on red when there is no reservation. By a route reservation, relevant signal lights change their colours depending on their subsequent signal lights. Definitions of some firing conditions ( $\chi$ ) are given on Table 2.

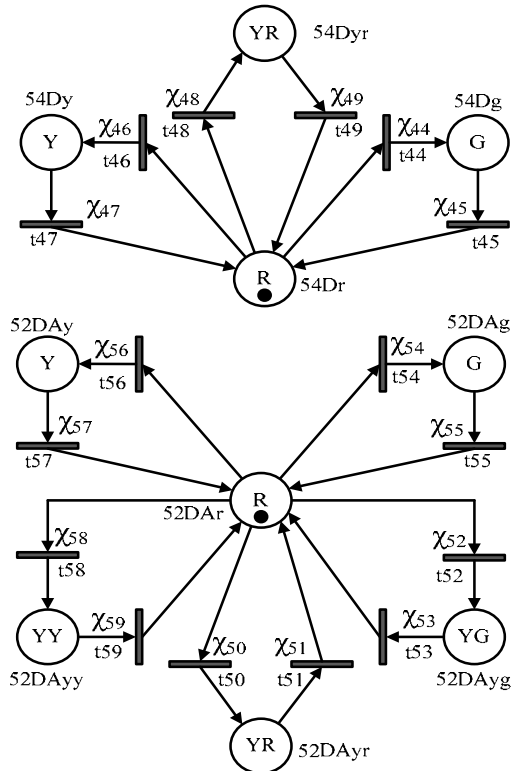


Fig. 9. PN models of colour signal lights 54D and 52DA.

These models are then converted to PLC code (FBD code) by using TPL (Token Passing Logic) technique given on (Uzam and Jones, 1998, Uzam 1998).

## 5. RESULTS

In this study, a railway yard with a level crossing is modeled with APNs where possible failures are also considered. Unlike other PN or APN models in the literature, the model becomes more comprehensive and capable in dealing with failures or device malfunctions using a formal approach. Considering failure situations will also improve safety and reliability of the design. The model obtained is converted to Function Block Diagram (FBD) and implemented on a failsafe PLC. These models can then connect to each other for modelling more complex railways. Different scenarios are tested in order to verify the correctness of the model and the resulting PLC code by the help of a SCADA testbed. An example scenario is also illustrated in Fig. 10. More generic modelling of fail-safe operations of such railway equipments, and applying formal checking algorithms to such designs should be the topic of further studies. Moreover, this study can be considered as an application of a formal method to a real railway station.

## ACKNOWLEDGMENT

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

## REFERENCES

- Anandarao, S., Martland, C.D. (1998). Level Crossing Safety on East Japan Railway Company: Application of Probabilistic Risk Assessment Techniques. *Transportation*, Vol(25), pp. 265-286.
- Burrage, K.W. (1995). Railway Safety Standards. In *IEEE Conference on Electric Railways in a United Europe*, pp. 153-157.
- CarrsQ. (2008). State of The Road: Railway Level Crossing Safety Fact Sheet.
- Durmuş, M.S. and Söylemez, M.T. (2009). Railway Signalization and Interlocking Design via Automation Petri Nets. *The 7<sup>th</sup> Asian Control Conf. (ASCC'09)*, Hong Kong, China.
- Einer, S., Slovak, R., Schneider, E. (2000). Modeling Train Control Systems with Petri Nets - An Operational Specification, In *IEEE Conference on Systems, Man and Cybernetics*, Vol (5), pp. 3207-3211.
- Febbraro, A., Porta, G., Sacco, N. (2006). A Petri Net Modeling approach of Intermodal Terminals Based on Metrocarga<sup>®</sup> System, In *Proceedings of The IEEE Intelligent Transportation Systems Conference*, Toronto, Canada, pp. 1442-1447.
- Giua, A. and Seatzu, C. (2008). Modeling and Supervisory Control of Railway Networks Using Petri Nets. *IEEE Trans. on Automation Science and Engineering*, Vol(5), pp. 431-445.
- Hagalisletto, A.M., Bjork, J., Yu, I.C. and Enger P. (2007). Constructing and Refining Large-Scale Railway Models Represented by Petri Nets. *IEEE Trans. On System, Man*

- and Cybernetics-Part C: Applications and Reviews, Vol(37), pp. 444-460.
- Hall, S. (2001). *Modern Signalling Handbook*, Ian Allan Publishing, England.
- Hörste M.M. (1999). Modeling and Simulation of Train Control Systems using Petri Nets, In *Proceedings of 3<sup>rd</sup> FMRail Workshop*.
- Jansen, L., Schneider, E. (2000). Traffic Control Systems Case Study: Problem Description and a Note on Domain-Based Software Specification, In *INT2000: Integration of Specification Techniques with Applications in Engineering*, pp. 41-47.
- Kluge, O. (2003). Modelling a Railway Crossing with Message Sequence Charts and Petri Nets. *Lecture Notes in Computer Science*, Vol (2472), pp.197-218.
- Kuepper, G.J. (1999). 150 Years of Train-Disasters - Practical Approaches for Emergency Responders. In *9-1-1 Magazine September/October issue*, pp. 30-33.
- Murata, T. (1989). Petri Nets: Properties, Analysis and Applications, *Proceeding of IEEE*, Vol(77), pp. 541-580.
- National Railway Level Crossing Safety Strategy (2010-2020), (2010) Australian Transport Council, Rail Level Crossing Group.
- Uzam, M. and Jones, A. H. (1998). Discrete Event Control System Design Using Automation Petri Nets and Their Ladder Diagram Implementation. *The International Journal of Advanced Manufacturing Technology*, Vol(14), pp. 716-728.
- Uzam, M. (1998). Petri-net-based Supervisory Control of Discrete Event Systems and Their Ladder Logic Diagram Implementations, PhD. Thesis, University of Salford, SALFORD, M5 4WT, UK.
- Palmer, J. (2006). The Need for Train Detection. *The 11<sup>th</sup> IET Professional Development Course on Railway Signalling and Control Systems*, York, UK, pp. 47-53.
- Peng, S., Zhou, M.C. (2002). Sensor-Based Petri Net Modeling for PLC Stage Programming of Discrete-Event Control Design, In *Proceedings of The IEEE International Conference on Robotics & Automation*, Washington, DC, pp. 1907-1912.
- Reder, H.J. (2006). Cross Acceptance of Safety Approvals in The Rail Industry: A Manufacturer's Viewpoint. In *The 1<sup>st</sup> IET International Conference on System Safety*, London, UK, pp. 338-343.
- Reif, W., Schellhorn, G., Thums, A. (2000). Safety Analysis of a Radio-Based Crossing Control System Using Formal Methods. In *9<sup>th</sup> IFAC Symposium Control in Transportation Systems*.
- Ren, X., Zhou, M.C. (1995). Tactical Scheduling of Rail Operations: A Petri Net Approach, In *IEEE Conference on Systems, Man and Cybernetics*, pp. 3087-3092.
- Rumsey, A.F. (2006). Developments in Train Control Worldwide. *The 11<sup>th</sup> IET Professional Development Course on Railway Signalling and Control Systems*, York, UK, pp. 223-232.
- Wikipedia. (2010). [http:// en.wikipedia.org / wiki / List\\_of\\_level\\_crossing\\_accidents](http://en.wikipedia.org/wiki/List_of_level_crossing_accidents). (15.03.2010).

Table 1. Definitions of colour signal lights




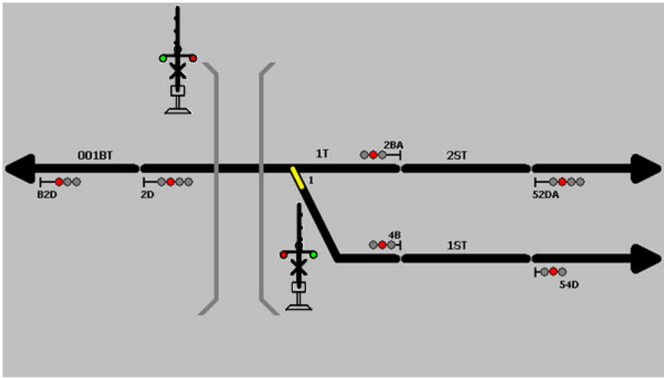
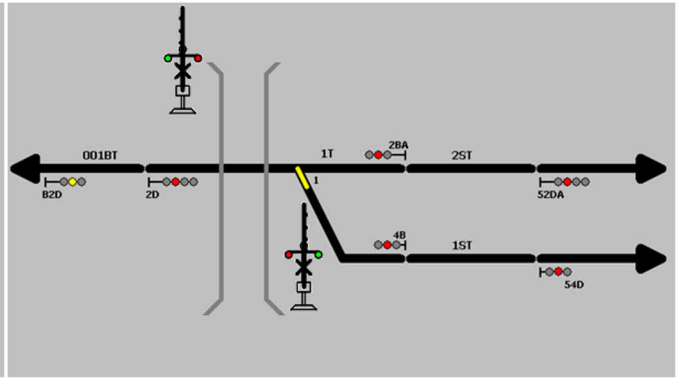
	Four Aspect Tall Signal Lights	Green : Next two blocks are free, train can proceed. Yellow : Next block is free, but the second block is occupied. Proceed carefully. Red : Stop, next block is occupied. Yellow-Green : There is a turning and next two blocks are free. Proceed with a predefined speed. Yellow-Yellow : There is a turning and next block is free, but the second block is busy. Yellow-Red : Proceed carefully (stop if necessary).
	Three Aspect Tall Signal Lights	Green : Next two blocks are free, train can proceed. Yellow : Next block is free, but the second block is occupied. Proceed carefully. Red : Stop, next block is occupied.
	Three Aspect Dwarf Signals	Green : Next two blocks are free, train can proceed. Yellow : Next block is free, but the second block is occupied. Proceed carefully. Red : Stop, next block is occupied. Yellow-Red : Proceed carefully (stop if necessary).

Table 2. Definitions of firing conditions

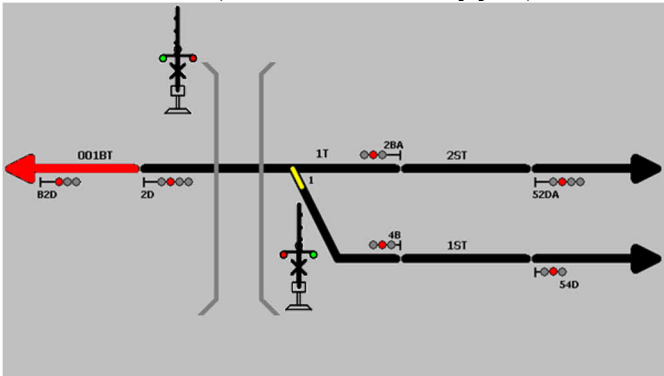
$\chi_1$ : Train movement to 001BT $\chi_2$ : Train movement from 001BT $\chi_9$ : Reserve route 001BT to 1ST $\chi_{10}$ : Reservation route 001BT to 1ST is terminated $\chi_{18}$ : Set level crossing as active (if 1BT is busy and 1BT-1ST is reserved) $\chi_{22}$ : Set level crossing as inactive (if route 2ST-1BT is reserved, 1T is free and 1BT is busy) $\chi_{26}$ : Close barrier $\chi_{27}$ : Barrier closed $\chi_{28}$ : Open barrier $\chi_{29}$ : Barrier opened $\chi_{30}$ : Barrier has not been closed in time $t_b$ $\chi_{31}$ : Close barrier again $\chi_{32}$ : Barrier has not been opened in time $t_b$	$\chi_{33}$ : Open barrier again $\chi_{34}$ : Set flashing lights $\chi_{35}$ : Reset flashing lights $\chi_{36}$ : Change position of switch to reverse position $\chi_{37}$ : Switch is set to reverse position $\chi_{38}$ : Change position of switch to normal position $\chi_{39}$ : Switch is set to normal position $\chi_{40}$ : Switch has not been set to reverse position in time $t_s$ $\chi_{41}$ : Take switch back to reverse position $\chi_{42}$ : Switch has not been set to normal position in time $t_s$ $\chi_{43}$ : Take switch back to normal position $\chi_{44}$ : set 54D red to green $\chi_{45}$ : set 54D green to red $\chi_{50}$ : set 52DA red to yellow-red $\chi_{51}$ : set 52DA yellow-red to red
---	--



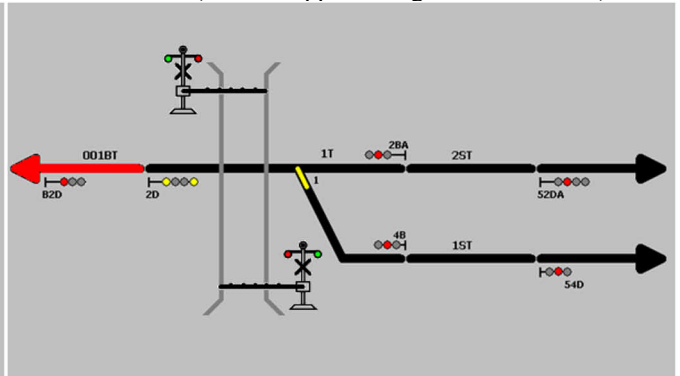
10.1 (No train on the railway yard)



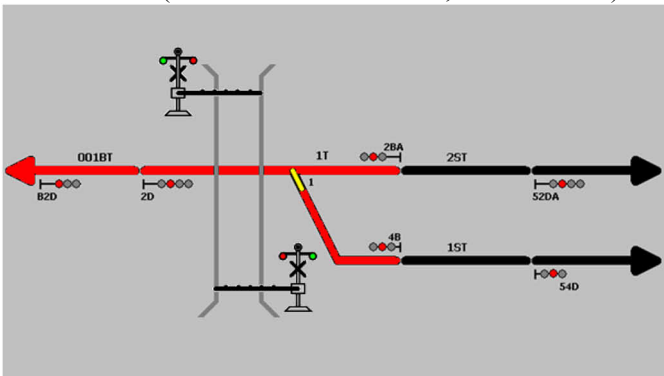
10.2 (Train is approaching to block 001BT)



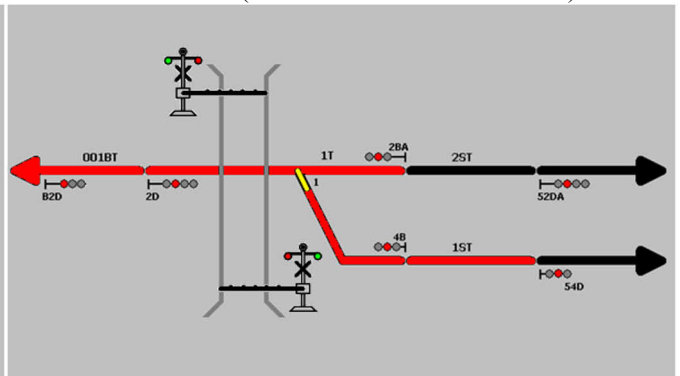
10.3 (Train enters block 001BT, no reservation)



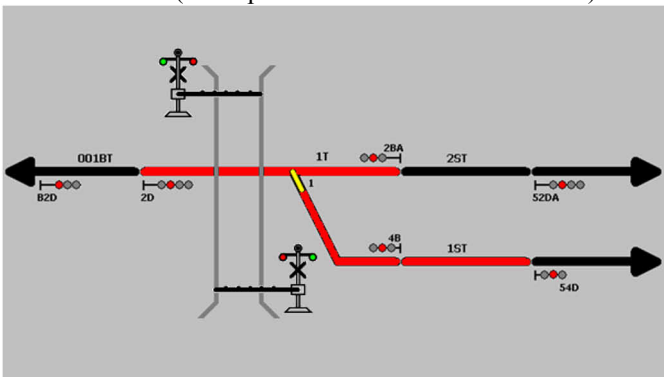
10.4 (Route 001BT-1ST is reserved)



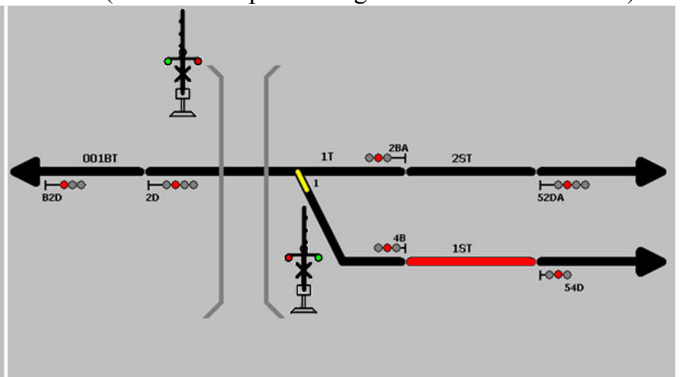
10.5 (Train proceeds and enters to block 1T)



10.6 (Train is still proceeding and enters to block 1ST)



10.7 (Train is still proceeding and leaves block 001BT)



10.8 (Train is on block 1ST)

Fig. 10. SCADA interface for the railway yard given in Fig. 2.