Modeling of the Safety and the Performance of Railway Operation via Stochastic Petri Nets

Robert Nicolae[1] Florin Moldoveanu[1] Mihai Cernat[1]
Roman Slovák[2] Eckehart Schnieder[2]

[1]*Transilvania* University of Brasov, Faculty of Electrical Engineering and Computer Science
Blvd. Eroilor No. 29, RO-500036 Brasov, Romania
Tel., Fax: +40-268-474718, e-mail: cernat@leda.unitbv.ro

[2]Technical University of Braunschweig
Institute for Traffic Safety and Automation Engineering
Langer Kamp 8, 38106 Braunschweig, Germany
e-mail: {slovak | schnieder}@iva.ing.tu-bs.de

***Abstract* – The objective of the paper is to investigate the applicability of stochastic Petri nets for the safety and performance analysis of a railway operation control system. The problem chosen by the applied reference case study is a decentralized radio-based control system for a railway level crossing, where a single track railway line and a road are crossing each other. A model was created, using the PROFUND methodical concept, integrating the operational PROcess, system FUNctionality and Dependability.**

***Index Tems* – Key words: Stochastic Petri Nets, Railway Operation Control System, Modelling, Reference Case Study Radio based Level Crossing.**

I. Introduction

Nowadays diverse railway safety organisational structures, strategies and operational practices are still used in many European countries. Each national railway authority and industry has developed its own strategy, requirements and operational procedures to obtain a safe system. They have also implemented systems and measures in accordance to their philosophy of safety as well as their national restrictions. To harmonise the technical and the operational systems, the European Union has a set of CENELEC Standards with the aim of providing direction and guidance in the areas of RAMS (Reliability, Availability, Maintainability and Safety) [1 - 4].

Up to now, the safety relevant train control systems were designed with the aim to reach the highest possible safety level based on the requirements of absolute safety. One new feature of CENELEC Standards is the definition of safety targets for all components of the railway operation control system based on the risk evaluation as a result of its operational requirements. This approach allows the designers to reach the required safety level of railway operation by cost effective means. This approach fits to the vision of a future intelligent traffic system.

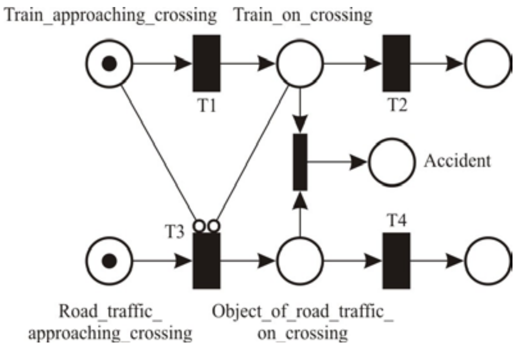
Train_approaching_crossing
Train_on_crossing
T1
T2
Accident
T3
T4
Road_traffic_ approaching_crossing
Object_of_road_traffic_ on_crossing

Fig. 1. Petri nets model of a railway level crossing.

II. Reference Case Study

The problem chosen for the reference case study [5] is a decentralized radio–based control system for a railway level crossing, where a single track railway line and a road are crossing at the same level. The intersection area of the road and the railway line is called „Danger zone“, since the trains and road traffic must not enter it at the same time to avoid collision.

Fig. 1 shows a Petri nets model of a railway level crossing, where a single track railway line and a road are crossing at the same level.

The railway crossing is equipped with barriers and road traffic lights. Traffic lights at the level crossing consist of a red and a yellow light. When the yellow light is shown road users (drivers, cyclists, pedestrians etc.) shall stop at the level crossing if possible. The red light means that the level crossing has been closed for road traffic and must not be entered. The yellow and red light must never be shown together. When both lights are off, the crossing area may be entered by road users. Half arm barriers are used to block the entry lane on either side of the level crossing.

The traffic lights and barriers at the level crossing are controlled by the level crossing control system. It will be activated when a train is approaching the level crossing. In the activated mode the level crossing control system performs a sequence of actions at a specific timing in order to safely close the crossing and to ensure the „Danger zone“ to be free of road traffic. First, the traffic lights are switched on such as to show the yellow light, then after 3 seconds they are switched to red. After some further 9 seconds the barriers start to be lowered. If the barriers have been completely lowered within a maximum time of 6 seconds the level crossing control system signals the safe state of the level crossing, thus allowing the train to pass the level crossing. When the train has completely passed the crossing area the level crossing may be opened for road traffic again and the level crossing control system switches back to the deactivated mode. The approaching of a train to the level crossing, is typically detected by line equipment or signal staff in order for the level crossing to be closed on time, to let the train pass through without any delay or braking action. In modern radio-based train control systems, the activation of the level crossing is based on continuous self-localisation of the train and the mobile communication between the train and the central level crossing control system. A route map on board of the train contains the positions of the potential danger points at the level crossings and provides additional information for the train when or where to send an activation order to the corresponding level crossing control system.

When the on-board system detects that the train is approaching a level crossing it will send an activation order to the level crossing control system to switch on the road traffic lights and to lower the crossing barriers. It will also set a braking curve for speed supervision, making the train stop at the potential danger point in a failure situation.

The level crossing control system acknowledges the receipt of the activation order to the train. After the receipt of the acknowledgment the on-board system waits for an appropriate time for the level crossing to be closed and then sends a status request to the level crossing control system. If the level crossing is in its safe state, a status report message will be sent to the train. This allows the train to cancel the braking curve and safely pass over the level crossing. Triggering the vehicle sensor at the rear of the level crossing will allow the barriers to be opened again and the traffic lights to be switched off. he scenario presented above can be also exemplified through Fig. 2. The figure contains two parts: one containing a diagram with the braking curve of the train and the other one containing the communication process between the train and the level crossing control system. The figure also exemplifies all five steps of the process: 1) activation order; 2) acknowledgement; 3) status request; 4) status report; 5) deactivation signal.

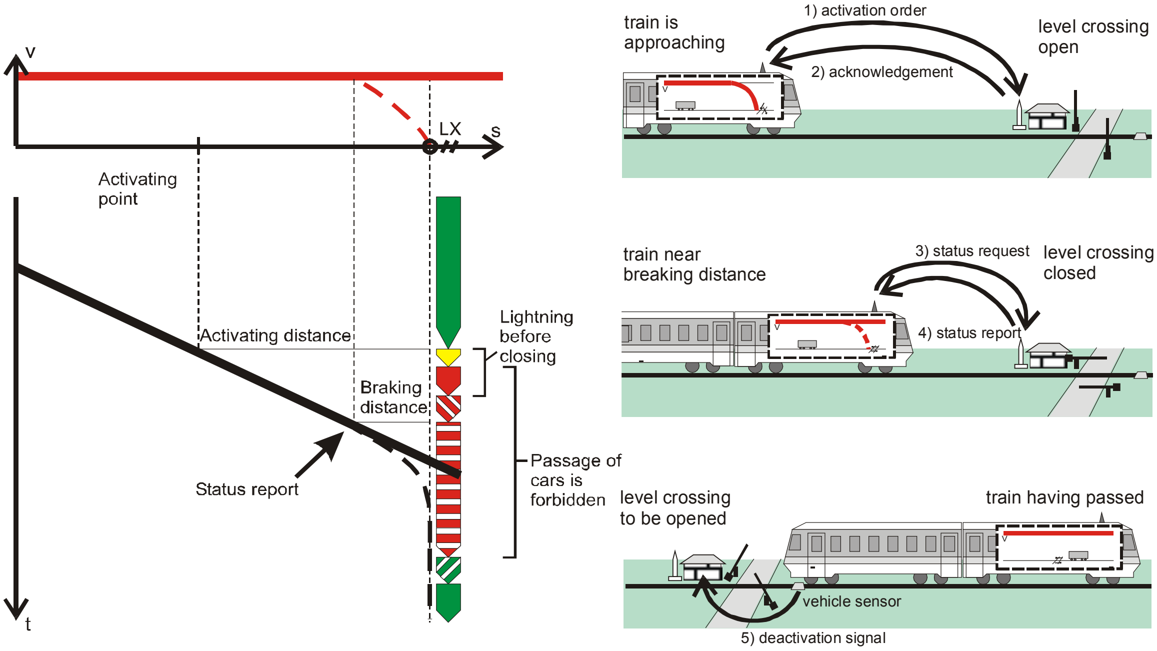

Fig. 2. The regular scenario of the operational railway process

Possible failure conditions have to be taken into account for a safe control of the level crossing and the train. A main cause of failures is the malfunctioning of the sensors and actuators. Defects may also occur in the main physical structures. Failures of communication systems may affect communication between control systems and devices as described above for radio networks and mobile communication. Last but not least the control systems themselves may fail. Defected devices will be repaired after some time, so that the occurrences of both failures and repairs have to be taken into account. While failures may occur at any time, repair of defected devices in case of non-recoverable failures will not take place when a train is approaching or passing the level crossing.

In the studied case only a limited number of failures are regarded: failures of the yellow or red traffic light (regarded separately), the barriers, the vehicle sensor and the delay or loss of the telegrams on the radio network. The traffic lights and the vehicle sensor are constantly supervised and defects are immediately reported to the level crossing control system. Failures of the barriers can only be detected by time-out, when barriers fail to reach the upper or lower end position in time or at all. The required behaviour of the control systems under failure conditions will be described below, according to the temporal sequence of failure occurrences and control reactions.

After having sent the activation order to the level crossing, the train waits for an acknowledgement. The train will send no status request until the acknowledgement has been received. If in the sequel, the train does not receive the status report with the safe state of the level crossing before entering its braking curve, the on-board system will apply the brakes until the status report has been received, or the train has come to a stand still. If the status report has been received before stand still, the brakes are released and the train can continue its run. Otherwise a request is prompted on the driver's display to make sure that the level crossing can be passed safely and to confirm the safe state on the display. If meanwhile the status report has been received, the message is cancelled from the display, the brakes are released and the train does not need to confirm anymore. Else the driver has to confirm the safe state of the level crossing in order to release the brakes and continue its run. Fig. 3 presents the technical faults which have to be considered in the operational process and also a possibility to resolve these faults. The example shows the complexity of the operational process which leads to a large number of test cases which have to be specified for validation of the control code.

III. Modelling Language

Petri nets were selected for the modelling language [6]. In Petri nets the conditioning of a transition means generally that the transition is enabled, but it is not forced to. In order to describe temporal relationships between events, Petri nets can be extended by time formalisms. The transition time parameter Θ indicates when, after conditioning, the transition will switch (fire).

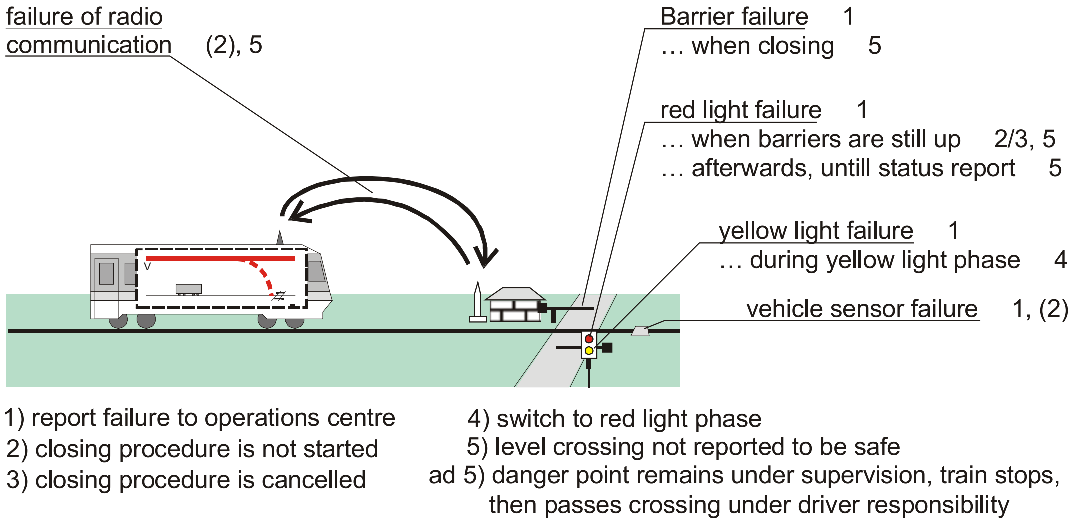
failure of radio communication (2), 5
Barrier failure 1
… when closing 5
red light failure 1
… when barriers are still up 2/3, 5
… afterwards, untill status report 5
yellow light failure 1
… during yellow light phase 4
vehicle sensor failure 1, (2)
1) report failure to operations centre
2) closing procedure is not started
3) closing procedure is cancelled
4) switch to red light phase
5) level crossing not reported to be safe
ad 5) danger point remains under supervision, train stops, then passes crossing under driver responsibility

Fig. 3. Technical faults to consider within the operational process.

During the time between conditioning and the switching of a certain transition the tokens are still visible for the whole net, i.e. they can still be removed by other events and so prevent the switching of the transition. The software used for the control system modelling is TimeNET3.0 developed by the Institute for Technical Informatics of the Technical University of Berlin [7, 8].

In the Extended Deterministic and Stochastic Petri Nets (EDSPN), which we used to describe our process, four types of time parameters Θ are defined [2, 5]:

- $\Theta = 0$.The transition switches immediately after conditioning without any delay (immediate transition). Such a transition has always priority over transitions of other types.
- $\Theta =$ const. The transition switches a constant time after conditioning (deterministic transition).
- $P(\Theta \le t) = 1 - e^{-\lambda t}$, with λ as rate of an exponential distribution function. The firing time of this transition is distributed exponentially with mean time 1/λ (exponential transition).
- $P(\Theta \le t) = \Phi(t),$ where $\Phi(t)$ is a general stochastic distribution function. The time elapsed after meeting the input conditions until occurrence of the transition is described by a probability distribution function (general stochastic transition).

Fig. 4 shows the graphical representation of the elements in an EDSPN net.

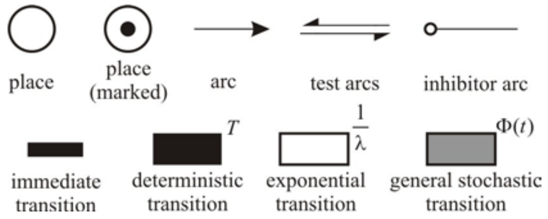

Fig. 4. Graphical elements of EDSPN.

IV. Modelling of the Reference Case Study

A model must be created for describing the applicability of stochastic Petri nets for safety analysis of a railway operation control system (ROCS).. This model, as a component part of the PROFUND methodical design concept [11] should contain the three essential parts: the PROcess, the FUNctional model; the Dependability model. For the beginning the model will contain only the process and the functional models. This means that the model will be an ideal model, where no failures were considered. In the real world this model can however not be found, thus an extension of this model must be created. This extension is represented by the dependability model which will complete the ideal model and also will give a more accurate case study close to the reality.

The ideal model is presented in Fig. 5, where the process and also the functional models can be seen.

A. Transportation Process

This model describes the movement of the train (TR) from the moment when it is outside the "Activating Area", the movement through the "Activating Area", followed by the movement through the "Danger zone" (DZ) and finally the movement outside "Danger zone". In the beginning, the train is out of the "Danger zone", which represents the zone where the accident is possible to occur. By advancing, the train will get into the "Activating Area" (TR_at_LX_activation), where it will start to send the activating order to the level crossing (LX). Continuing its movement (TR_approaching), the train will enter the next zone called "Approaching Area" (TR_before_DZ) where the status of the level crossing should have been already received from the Level Crossing Control System (LXCS). It means that the train has the "Movement Authority" (MA). With MA, the train is able to enter the "Danger zone" (TR_enters_DZ) without braking (TR_in_DZ_AUTOM) and after a certain time it will leave the zone (TR_leaves_DZ_when_OK) and will continue its movement.

B. System Functionality

1) *Train.* First, the "Train On-Board Functional Model" will be described. In Fig. 4 it can be seen, that after the "Activation Signal" was sent (ACT_sent_to_LX and ACT_sent) the train waits for a specified time for the level crossing to close (TR_waits_LX_close).

The train will ask the "Status Request" (TR_asks_SRQ) only if it has received the "Acknowledge Signal" from the level crossing (TR_recev_ACK) which means that the level crossing has received the interrogation from the train. After sending the "Status Request" the train will wait for the "Status Report" from the LXCS. If the "Status Report" says, that it is safe for the train to enter into the "Danger Zone", the train will have the MA to proceed further without braking (TR_with_MA).

2) *Communication.* The next functional model is the "Communication Functional Model", is represented in Fig. 5. The communication represents in this case the radio contact between the train and the level crossing control system (LXCS). 3) *Level Crossing*. The last functional model is the "Level Crossing Functional Model". At the beginning the level crossing is unsafe (LX_unsafe), which means that the barriers are up.

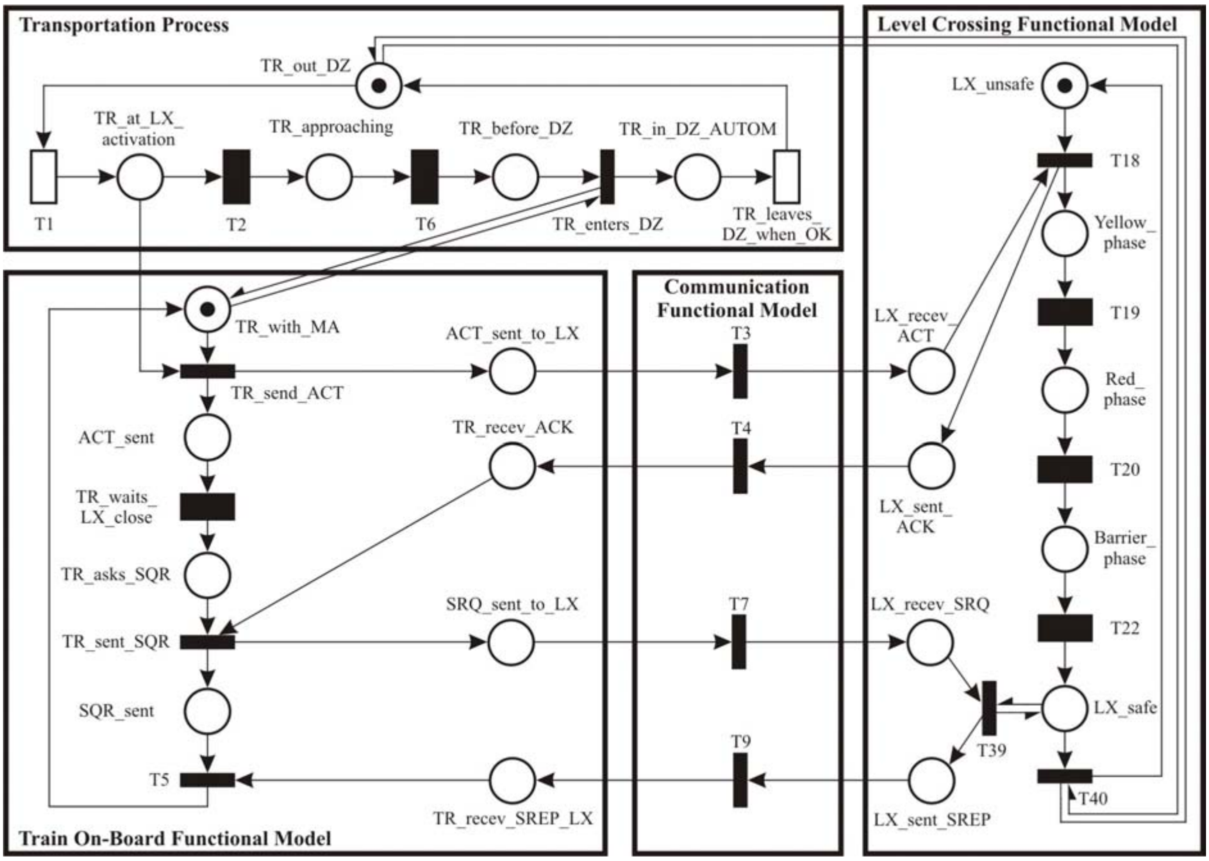

Fig. 5. Representation of the Transportation Process and of the System Functionality.

When the LXCS receives the “Activation Signal” from the train, the level crossing passes into the yellow phase meaning that the yellow light is switched on (Yellow_phase). The level crossing control system will also send back the “Acknowledge Signal” (LX_sent_ACK) for the train to know that it has received the “Activation Signal”. After three seconds of the yellow phase, the level crossing passes into the red phase (Red_phase), hence the red light is switched on. This phase will only take nine seconds and after the time is elapsed the barrier will start lowering (Barrier_phase). The estimated time for the barrier to lower is six seconds. Normally, when this time is elapsed the barrier should be lowered and the level crossing safe (LX_safe). The LXCS will be interrogated by the train about its status through a “Status Request” message (LX_recev_SRQ) and will send to the train a “Status Report” message with the actual state of the LX (LX_sent_SREP). When the train will leave the “Danger Zone”, the level crossing will be automatically opened and the traffic lights will be switched off.

C. *System Dependability Model Extension*

If in the ideal model, represented in Fig. 5, no failures were taken in consideration, the extended model will regard a number of possible failures as: failures of the yellow or red traffic light (regarded separately), the barriers, the vehicle sensor and the delay or loss of the telegrams on the radio network. This extended model is called “System dependability model extension”. Fig. 6 shows a representation of the extended model with the following component parts: 1) Transportation Process, which is a new form of the model presented in Fig. 5; 2) Train Dependability Model and Train On-Board Functional Model are regarded as one part, for a better understanding of the described components; 3) Radio Communication Dependability Model and Communication Functional Model are also regarded as one part, and the last two components 4) Level Crossing Functional Model and Level Crossing Dependability Model.

1) *Transportation Process Extension.* Small changes in the model can be observed: a new place appeared, called TR_in_DZ_manually. Unlike the first model, where the train was not forced to stop, because the apparition of an error was null, in the Process extension, the appearing of an error will necessarily determine the stop of the train by the train driver.

The stop of the train involves that the train driver will get off the train and manually safe the level crossing. When the level crossing will be safe, the train will be able to continue on its way and leave the „Danger zone“ (TR_leaves_DZ_safed_manually).

2) *Train Dependability Model.* To explain the dependability model of the train it is necessary to describe the model together with the train functionality model. The Train On-Board Functional Model suffers no changes in relation to the ideal model presented in Fig. 4, but now the possibility has occurred that the model components could fail. It is possible, also, that the train is not detected by the detection system (DET_NOK), meaning that it is possible for the train to enter the „Danger zone“ when the level crossing it is not assured by the barriers. The situation generated in this manner could lead to a possible accident. In case that the detection is functional (DET_OK), the transmission of the activation radio signal will be normal (ACT_sent_to_LX) and the level crossing control system will be noticed to begin the lowering process of the barriers. The Train Dependability Model includes three possible cases when the train will be required to stop before getting into the „Danger zone“ and manually safe the level crossing.

The first case is, when the train, after having waited for a specified time for the barriers to be closed, sends a “Status Request” to the level crossing control system to interrogate it about the status of the barriers (TR_asks_SRQ). If the train did not receive any acknowledge message from the level crossing (TR_recev_ACK) it will be forced to brake and than to stop.

In the second case, after the “Status Request” was sent (SRQ_sent_to_LX and SRQ_sent), it is necessary that the response from the level crossing is returned in a specified known time. If this time is overdue, the train must brake and finally stop.

The third case is when the response form the level crossing system control indicates the existence of a failure in some point (TR_recev_SREP_LX_defect) and the level crossing can not be safely assured. After this message is received the train will immediately start to brake. This can be seen in Fig. 6 where transition T4 it is an immediate and not a timed transition.

3) *Communication Dependability Model.* Like the Train Dependability Model, the Radio Communication Dependability Model is also closely connected with Communication Functional Model. Fig. 6 shows, starting from the upper left corner, the propagation of the radio messages from the train to the level crossing system control and back. A place named “TELEGRAM” was introduced in the model with an important function for the radio communication between the train and the level crossing system communication. At any time, this place admits only one token or none. Therefore the role of this place is to ensure that, at any time, only one radio message can be sent the possibility of two radio messages existing simultaneously at one moment being null. The RADIO is represented by two places: one with RADIO_OK, when the radio is functional and the other one with RADIO_NOK when the radio is defect. The transition from the functional state to the defect state is made through an exponential transition and from the defect state to the functional state through a general transition. The choice of general transitions is explained in [9], [10].

The Communication Functional Model suffered a small change. The transitions, which in the first variant were immediate transitions, are now exponential transitions. These transitions are more suitable for the Communication Functional Model because the radio transmission can not take place instantly and determines a specified delay. The time of transmission should be known by the train on-board system and by the LXCS, because the train should brake in case it has not received the radio messages in a specified time, and the level crossing needs also some adequate time to lower the barriers and to become safe.

4) *Level Crossing Dependability Model.* The last dependability model contains the Level Crossing Dependability Model and the Level Crossing Functional Model. The functional model did not suffer any changes from the first variant. The most important part is represented by the Level Crossing Dependability Model.

If initially the ideal model had no failures (Fig. 5), now, the model contains four possible fault like: yellow and red light failure, barrier motor failure and sensor failure. The functional model contains only the model without failures. For starting, if the level crossing is unsafe and the yellow light is ok, the level crossing passes into the yellow phase (Yellow_phase). If the yellow light is defect than the level crossing will pass directly to the red phase (Red_phase). It can be seen, that the failure of the yellow light does not put the model into the defect state (LX_defect) because the failure of this light is not vital for the level crossing. If the level crossing is in the yellow phase or the red phase and the red light is defect than the model will pass into the defect state (LX_defect).

The red phase is followed by the barrier phase (Barrier_phase) when the barrier will start to lower. The model will pass into the barrier phase, in a specified time, if the yellow light is ok or defect, the red light however being required to be functional.

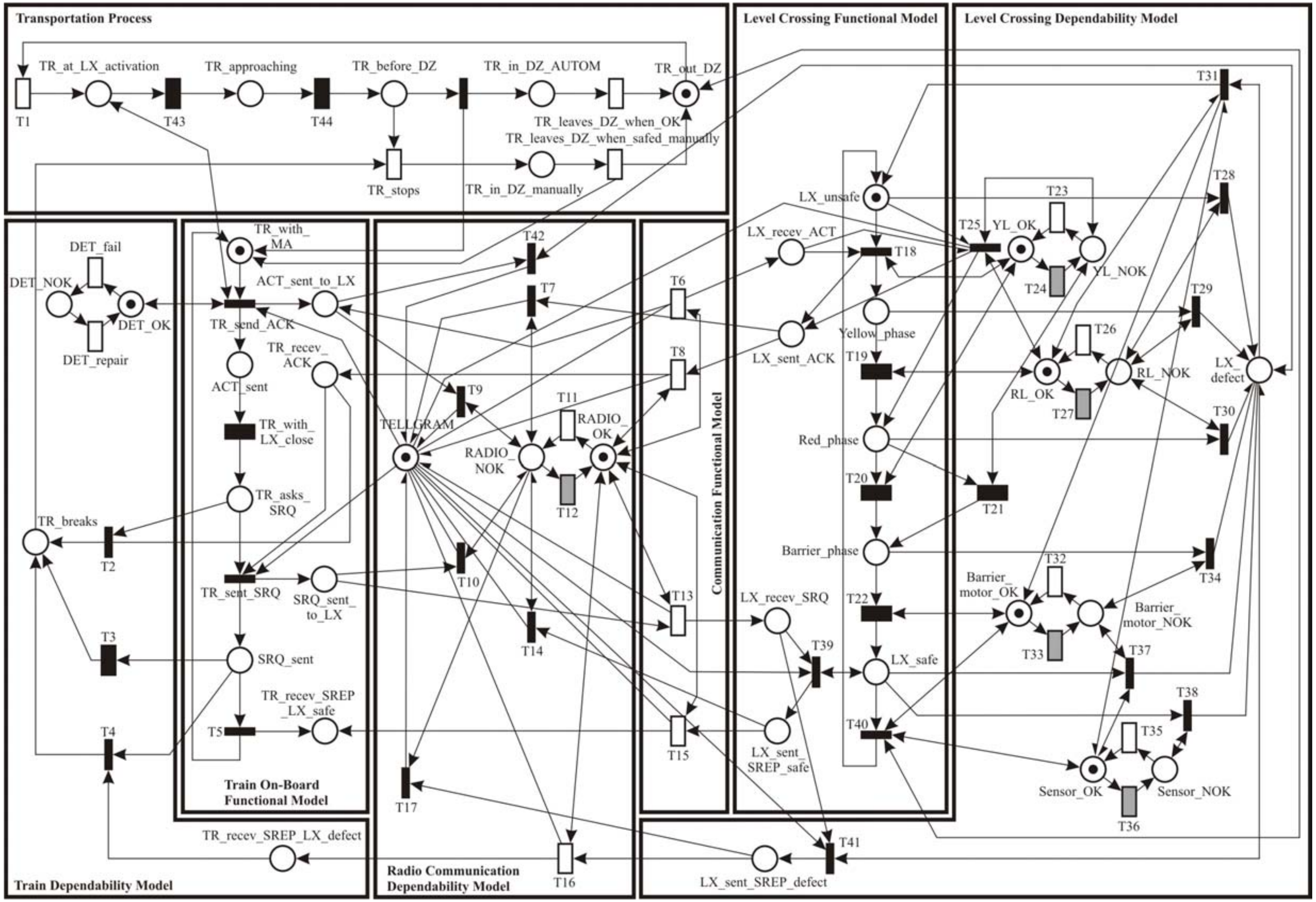

Fig. 6. Representation of the Transportation Process and of the System Functionality and Dependability.

If the barrier motor has no defection (Barrier_motor_OK) the level crossing will become safe. When the level crossing is in the barrier phase but the barrier motor is defect (Barrier_motor_NOK) the model will pass into the defect state. If level crossing is safe, and the "Status Request" from the train has arrived, the level crossing system control will send to the train a "Status Report" radio message where it specifies its safe status (LX_sent_SREP_safe). But if the level crossing is defect (LX_defect) the message will specify the defect status which will cause the train to start braking. After the train will leave the „Danger zone" a sensor will be activated by the train. When this sensor is activated, it will determine the barrier to lift and the level crossing will become unsafe. This is possible only when the sensor is ok (Sensor_OK), a possible failure however having to be taken in consideration. If the sensor is defect (Sensor_NOK) the barrier will remain lowered and the level crossing will be signalled as defect (LX_defect).

V. Conclusions

The problem chosen for the reference case study [3] is a decentralized radio–based control system for a railway level crossing, where a single track railway line and a road are crossing at the same level. For the purpose of safety and performance analysis a formal model was created, using the PROFUND methodical concept, consisting of three essential parts: the PROcess, the FUNctional model and the Dependability model.

Modelling was achieved by using the formal description with Extended Deterministic and Stochastic Petri Nets (EDSPN).

The presented stochastic Petri net model corresponds to the example definition according to the referred case study. In the real application the number of considered failures is to be extended according to the relevance for safety or performance analysis.

The four different types of transitions used in EDSPN allow the describing of the causal as well as of the temporal deterministic or stochastic system behaviour, which is the object of the aimed performance and safety analysis.

References

[1] EN 50216: Railway applications: "The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS)", Brussels, 1998.

[2] R. Slovak, J. May, P. Tomasov, E. Schnieder, "Approach to the Quantitative Risk Analysis of a Level Crossing Traffic Process by Means of Stochastic Petri Nets", *Transport* 2002, Sofia, 2002.

[3] L. Jansen, E. Schnieder, "Traffic Control System Case Study: Problem Description and a Note on Domain-based Software Specification", *INT* 2000, Berlin, Germany.

[4] St. Einer, H. Schrom, R. Slovak, E. Schnieder, "Experimental Validation of Train Control Systems by Using a Railway Model", Allan, J. et al., Hrsg., *Computers in Railways* VIII, S. 925-934, Ashurt Lodge, Ashurt, Southampton, SO40 7AA, UK, 2002.

[5] R. Slovak, S. Einer, P. Tomasov, "A Petri Net Based Method for Proof of Safety of Railway Operation Control System, Integrated Design and Process Technology", *IDPT*-2002, June 2002, U.S.A.

[6] F. Bause, P. S. Kritzinger, *Stochastic Petri Nets, An Introduction to the Theory*, 2nd Edition, Verlag Vieweg, 2002.

[7] A. Zimmerman, *TimeNET 3.0 User Manual. A Software Tool for the Performability Evaluation with Stochastic Petri Nets, Performance Evaluation Group*, TU Berlin, June 2001.

[8] http://pdv.cs.tu-berlin.de/~timenet/

[9] R. Nicolae, :Modelling with Stochastic Petri Nets for Safety Analysis of a Railway Operation Control System. Diploma Thesis", *Transilvania* University of Brasov, 2003.

[10] R. Nicolae, et al., "Analysis of the Safety and the Performance of Railway Operation via Stochastic Petri Nets". *The 9th International Conference on Optimzation of Electrical and Electronic Equipment, OPTIM* '04, Brasov, May 20-24, 2004.

[11] R. Slovák, J. May, and E. Schnieder, "PROFUND Modelling for Holistic Risk and Availability Analysis by Means of Stochastic Petri Nets Applied to a Level Crossing Control System". *Proc. of Formal Methods for Railway Operation and Control Systems* (G. Tarnai and E. Schnieder Eds), L'Harmattan Budapest, 2003, 221-232.

[12] W. Schneeweiss, *Petri Nets for Reliability Modeling*. Verlag LiLoLe, Hagen, 1999.