Experience using Coloured Petri Nets to Model Railway Interlocking Tables*

Somsak Vanit-Anunchai
School of Telecommunication Engineering
Institute of Engineering
Suranaree University of Technology
Muang, Nakhon Ratchasima, Thailand
somsav@sut.ac.th

Interlocking tables are the functional specification defining the routes on which the passage of the train is allowed. Associated with the route, the states and actions of all related signalling equipment are also specified. It is well-known that designing and verifying the interlocking tables are labour intensive, tedious and prone to errors. To assist the verification process and detect errors rapidly, we formally model and analyse the interlocking tables using Coloured Petri Nets (CPNs). Although a large interlocking table can be easily modelled, analysing the model is rather difficult due to the state explosion problem and undesired safe deadlocks. The safe deadlocks are when no train collides but the train traffic cannot proceed any further. For ease of analysis we incorporate automatic route setting and automatic route cancelling functions into the model. These help reducing the number of the deadlocks. We also exploit the new features of CPN Tools; prioritized transitions; inhibitor arcs; and reset arcs. These help reducing the size of the state space. We also include a fail safe specification called flank protection into the interlocking model.

1 Introduction

1.1 Background

In the railway signaling domain, an interlocking table is a tabular representation comprising the sections or routes that the train is allowed to enter together with the required states and actions of all related equipment along the routes. The interlocking tables play such an important role that operating procedures and train movement must be complied with it. This document also acts as a legal agreement between the railway administrators and the contractors. Designing a large interlocking table is a difficult task partly because the railway signalling system is required to be *fail safe*. The *fail safe* means that, in the event of failure, the system shall respond in a no harmful way or no danger to persons. In the railway signalling domain an important event of failure is when a train overruns the stop signal.

Railway signalling contractors usually have software tools generating the interlocking table from the track layout and track side equipments. However the generated table is not unique. It depends upon the signalling principle or regulation of each railway administrator. After the interlocking tables are designed and checked by the contractors, they need to be rechecked by signal engineers. In the past we manually inspected the submitted interlocking tables without any software tools. Thus the checking process was very slow, labour intensive and prone to errors. To reduce the manpower and time consumed in the checking process the State Railway of Thailand has been using formal methods and CPN Tools since 2009.

*Supported by National Research Council of Thailand Grant no. PorKor/2551-153

To appear in EPTCS.

1.2 Motivation

Previously, we modelled and analysed in [11] a single track railway station using Coloured Petri Nets (CPNs). We created a static model where CPN structure was used to mimic the signalling layout and the train movements. A generic CPN model of the signal operation was also developed. The content of the interlocking table coded into ML functions which are used on arc inscriptions. Modelling interlocking tables of other railway stations was simply done by changing the content of the ML functions. These ML functions were automatically generated. After the contractors submitted the interlocking table files in Microsoft-EXCEL format, the tables were transformed to XML and then to ML functions using Extensible Stylesheet Language Transformations (XSLT). The interlocking tables were formally verified by exhaustively searching for the states where trains collide. [11] had two important problems. Firstly, when we had many signalling devices working together, the CPN diagram became too complicated. It also took 2-3 days to create a new CPN model of the signalling layout for a large station. Secondly, [11] focused on only interlocking tables. Although the system was safe, the signalman could give the sequences of instructions (route setting) that leaded the train traffic into deadlocks. Using state space generation, our CPN model generated a lot of safe terminal markings that had no train collision but the train traffic was in deadlock. It was very inconvenient to investigate all terminal markings in [11].

To solve the first problem, we modeled in [12] the signalling layout by encoding the geographic information into *tokens* with a complex data structure. When signaling layout was modified or rebuilt, we simply change the initial marking. To solve the second problem, this paper introduces the automatic route setting and automatic route canceling functions into the CPN model. Although these two procedures are not in the interlocking tables, both are standard operating procedures normally conducted by signalmen. After applying these two procedures, the sequences of route setting commands that lead to traffic deadlocks could be avoided.

1.3 Contributions

The contribution of this paper is three fold. Firstly, to ease of analysis and get rid of the undesired, safe terminal markings, the automatic route setting and automatic route canceling functions are included in the model. Secondly, when we considered a double track station in [12], we encountered the state explosion. To alleviate the state explosion problem, we revise the CPN model by exploiting the recently introduced features of CPN Tools version 4.0.0 [13] that are prioritized transitions; inhibitor arcs; and reset arcs. Thirdly, preventing an accident when a train overruns the stop signal, a fail safe condition called “Flank Protection” is required. This condition has not been included in [11] and [12] because it does not affect the normal functional behaviour as long as no fault occurs in the braking system and the train driver still obeys the signal. This paper has included the flank protection into the model.

The rest of this paper is organised as follows. Section 2 briefly explains the concept of railway signalling system and interlocking tables. Section 3 reviews related work. The CPN model is discussed in Section 4. Analysis results are reported in Section 5. Section 6 presents conclusion and outlines suggested future work.

2 Railway Signalling Systems and Interlocking Tables

2.1 Signalling Systems

In general the railway lines are divided into *sections*. To avoid collision, only one train is allowed in one *section* at a time. The train can enter or leave the *section* when the driver receives authorization from a signalman via a signal indicator. Before the signalman issues the authorization, he needs to ensure

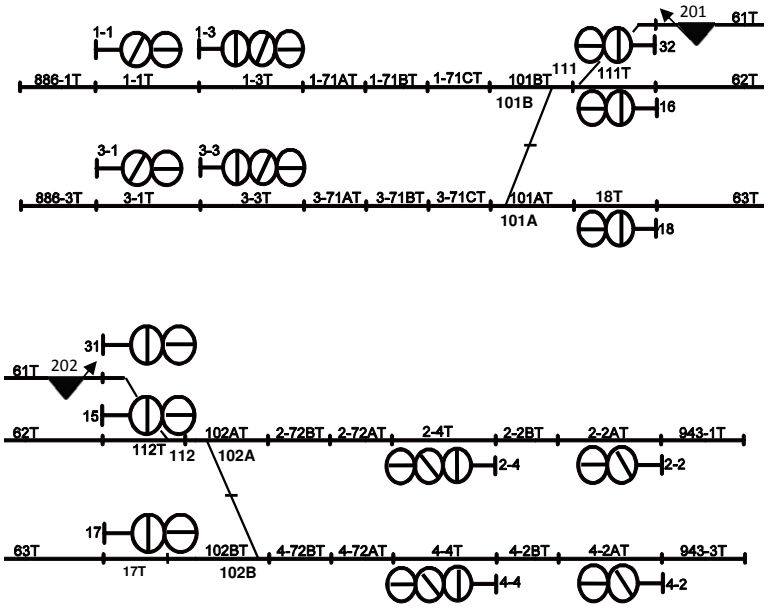

Figure 1: Signalling layout of the Panthong Station (double track)

that no object blocks the passage of the train. The *section* between two railway stations, which involves two signal men, is called "*block section*". To prevent human error that may lead to collisions, the strict operation on a *block section* is controlled by equipment called "Block Instruments". Figure 1 shows the signalling layout of a double track station named "Panthong". The signalling layout comprises a collection of railway tracks and signalling equipment such as track circuits, points and signals. (e.g. signal no.1-3 and signal no.2-4). Each piece of signalling equipment has an identification number and holds a certain state as follows.

Track Circuits A track circuit is an electrical device used to detect the presence of a train. A track circuit (e.g. 61T, 1-3T) is either *clear* indicating no train on the track or *occupied* indicating the possible[1] presence of a train.

Warner signals A warner signal (e.g. 1-1, 2-2, 3-1,4-2) has two aspects: *yellow* or *green*. It informs drivers about the status of the next signal.

Home signals A home signal (e.g. 1-3, 2-4, 3-3, 4-4) has three aspects: *red*, *yellow* or *green*. It displays *red* when the train is forbidden to enter the *station area*. It displays *yellow* giving the driver authority to move the train into the *station area* and prepare to stop at the next signal. It displays *green* giving the driver authority to move the train passing the *station* and enter the next *block section*.

Starter signals A starter (e.g. 15, 16, 17, 18, 31, 32) has two aspects: *red* or *green*. It displays *red* when forbidding the train to enter the *block section*. It displays *green* when giving the driver authority to move the train into the *block section*.

Point A point (e.g. 101A, 101B, 111, 112, 102A, 102B) or railway switch or turnout is a mechanical installation used to guide a train from one track to another. A point usually has a straight through track called "main-line" and a diverging track called loop line. A point is right-hand when a moving train from

[1]When the track circuit fails, its state is occupied even if there is no train.

a joint track diverges to the right of the straight track. Similarly a left-hand point has the diverging track on the opposite side of a right-hand point. When a point diverges the train, it is in reverse position. When a point lets the train move straight through, it is in normal position.

Derailer A derailer (e.g. 201, 202) is a mechanical installation used to prevent unauthorized movements of trains or unattended rolling stock. The train is derailed when it rolls over the derailer. The normal position is the derailing position.

2.2 Interlocking Tables

A collection of track circuits along the reserved *section* is called "*route*". An entry signal shall be clear to let the train enter the route. Although the request to clear the entry signal is issued by the signalman, the route entry permission is decided by the interlocking system using safety rules and control methods specified in the agreed Interlocking Tables. Tables 1, 2, and 3 are the Interlocking Tables (partial) for Panthong station of which the signalling layout is shown in Fig. 1. Data in the first column, "From", is the route identifications which are labelled by the entry signal: 1-3(1); 1-3(2); 3-3(1); 3-3(2); 3-3(3); 2-4(1); 2-4(2); 4-4(1); 4-4(2); 4-4(3); 15(1); 15(2); 16(1); 16(2); 31(1);31(2); 32(1);32(2); 17 and 18. Due to space limitation we show only 4 routes in Tables 1, 2 and 3. Each row in the tables represents the requirement how to set and release each route. For example, route 3-3(3) comprises the track circuits 3-3T, 3-71AT, 3-71BT,3-71CT,101AT, 18T, 63T, 17T and requires that the point 101 is in normal position. Routes 3-3(1), 3-3(2) and 3-3(3) distinguish that behind signal 3-3 three routes are possible. Similar rule applies to routes 1-3; 2-4; and 4-4. The column "Requires Route Normal" shows conflict routes. A route cannot be set if any conflicting routes have been set and not yet released. For route 3-3(3) the conflicting routes are 16(2), 32(2), 3-3(1), 3-3(2), 18, and 4-4(3). The exit (starter) signal of this route is 17, and if home signal 3-3 shows green, then starter signal 17 shows green.

Different Interlocking systems from different manufacturers may have different control methods. However there are four basic control methods widely accepted and used among railway companies.

Route locking Route setting involves a collection of adjacent track circuits, points and signals. A route can be set and reserved for a passage of a train along this route. To assure the safety, firstly, the interlocking system verifies that the route does not conflict with other routes previously set. Secondly, the points along the route are locked in the correct positions. If the related points are not in the correct positions, the controller will attempt to set and lock them in the correct positions. Thirdly, the track circuits along the required route are all clear or unoccupied so that nothing obstructs the passage of the train. Then the entry signal can be cleared (showing yellow or green).

Table 1: An Interlocking Table for Panthong station (part 1:Route locking)

ROUTE		INTERLOCKING			CONTROLS		
		REQUIRES	SET & LOCKS POINTS		ASPECT	SIGNAL AHEAD	REQUIRES TC
FROM	TO	ROUTE NORMAL	NORMAL	REVERSE			CLEAR
3-3(1)	31	16(1) , 16(2) ,32(1) , 32(2) , 3-3(2) , 3-3(3), 18 , 1-3(1) , 1-3(2) , 2-4(1) , 2-4(2), 4-4(1) , 4-4(2)		101,111,112, 201, 202	Y	31 AT R#	3-3T, 3-71AT, 3-71BT , 3-71CT, 101AT, 101BT, 111T, 61T, 112T
3-3(2)	15	16(1) ,16(2) ,32(1) ,32(2), 3-3(1) ,3-3(3) ,18 ,1-3(1),1-3(2) , 2-4(1), 2-4(2) , 4-4(1) , 4-4(2)	111,112	101	Y	15 AT R#	3-3T,3-71AT, 3-71BT, 3-71CT, 101AT, 101BT, 111T, 62T, 112T
3-3(3)	17	16(2) , 32(2) , 3-3(1) , 3-3(2) , 18 ,4-4(3)	101		Y G	17 AT R# 17 AT G#	3-3T, 3-71AT, 3-71BT, 3-71CT, 101AT, 18T,63T,17T
15(2)	DOWN BLOCK SECTION 4	31(1),31(2), 15(1) , 2-4(1), 2-4(2) , 4-4(1) , 4-4(2),4-4(3)	112	102	G		17T, 102BT, 4-72BT,4-72AT, 4-4T, 4-2BT,4-2AT,943-3T

Table 2: An Interlocking Table for Panthong station (part 2:Approach locking)

ROUTE		CONTROL						
		APPROACH LOCKED WHEN SIGNAL CLEARED & AND		ROUTE RELEASED BY				Notes
				TC	TC OCC	TC OCC	OR	AND / OR
From	TO	TC OCC	OR TIME	CLEAR	& CLEAR		Emergency RELEASE AFTER	REMARKS
3-3(1)	31	3-1T	120 sec	3-3T,3-71AT , 3-71BT, 3-71CT 101AT, 101BT	111T	61T	240 sec	DOWN BLOCK 3 NOT SET
3-3(2)	15	3-1T	120 sec	3-3T,3-71AT , 3-71BT, 3-71CT 101AT, 101BT	111T	62T	240 sec	DOWN BLOCK 3 NOT SET
3-3(3)	17	3-1T	120 sec	3-3T,3-71AT ,3-71BT, 3-71CT,101AT	18T	63T	240 sec	DOWN BLOCK 3 NOT SET
15(2)	DOWN BLOCK SECTION 4	63T	120 sec	63T,17T, 102BT, 4-72BT,4-72AT,	4-4T	4-2BT	240 sec	DOWN BLOCK4 SET

Table 3: An Interlocking Table for Panthong station (part 3:Flank Protection)

ROUTE		INTERLOCKING		CONTROLS
		SET & LOCKS POINTS		REQUIRE TRACK AT TIME OF CLEARING ONLY
From	TO	NORMAL	REVERSE	TC CLEAR
3-3(1)	31	102		62T
3-3(2)	15	102 201, 202		
3-3(3)	17	102		
15(2)	DOWN BLOCK SECTION 4	202		63T

Approach locking After a route is set; the point is locked; and the entry signal is cleared, if the track circuit in front of (approaching) the entry signal is occupied, then the signalman cannot cancel the route and the entry signal by the normal procedure. Approach locking prevents the train driver from the sudden change of signal aspect from green or yellow to red. Column 3 in Table 2, "APPROACH LOCKED WHEN SIGNAL CLEARED & TC OCC", presents locking when a route is set and the approach track circuit is occupied. For example, route 3-3(3) will be approach locked if the route is set and track 3-1T is occupied.

Route released After the passage of the train, the reserved route is released automatically. Column "Route Released by" in Table 2 presents route released mechanism for the signalling layout in Fig. 1. Route 3-3(3) will be released when the track circuits 3-3T, 3-71AT, 3-71BT, 3-71CT, 101AT are clear; the track circuit 18T is occupied and then clear; and the track circuit 63T is occupied. The reserved route can be emergency released but the release action will be delayed for 4 minutes after the signalman issues the "emergency route released" command.

Flank protection This is an important class of fail safe requirement. The equipment within the surrounding area of the reserved route that may cause an accident shall be protected even if no train is expected to pass such a signal or such points. Points should be in such positions that they do not give immediate access to the route. Even though those flank points and derailers are not located on the required route, when the route is set, they shall be locked in the safe position until the route is released. Table 3 shows the flank protection requirements for routes 3-3(1), 3-3(2), 3-3(3) and 15(2) of the Panthong's interlocking table. For example route 3-3(3) requires the points 102 (both 102A and 102B), which are not on the route, be locked in the normal position. Route 15(2) requires the track circuits 63T, which is not in the route 15(2), be unoccupied. Route 15(2) also requires the derailer 202, which is not in the route 15(2), be locked in the derail position. Because routes 3-3(3) and 15(2) are not in conflict, trains may enter these two routes at the same time. However arriving on 63T, the train on

route 3-3(3) could overrun the red signal no. 17 and collide with the train on route 15(2) at point 102. To prevent this accident, route 3-3(3) requires flank protection, point 102 be locked in the normal position. Meanwhile Route 15(2) cannot be set as long as 102 in the normal position.

3 Related Work

In [6], Fokkink and Hollingshead divide the railway signalling system into three layers: infrastructure, interlocking and logistics layers. The infrastructure layer involves objects or equipment used in the yard. The work in this category, for instance [1,4], ties closely with the manufacturer's products. The logistics layer involves human operation and train scheduling which aims at efficiency and absence of deadlocks. It involves the operation of the whole railway network (e.g. [7,9]) thus the state space explosion problem is often encountered. The interlocking layer provides the interface between logistics and infrastructure layers. It prevents us from accidents caused by human errors or equipment failure. The work in this category models the interlocking tables and verifies them against the signalling principles. For example [6, 15] uses theorem prover and [16] uses NuSMV. Hansen [8] presented a VDM model of a railway interlocking system, and validate it through simulation using Meta Language (ML). The work focuses on the principles and concepts of Danish systems rather than a particular interlocking system. He also pointed out that Interlocking systems from other countries may be different from the Interlocking described in [8]. Winter et al [14] proposed to create two formal models during the design process of interlockings. One is the formal model of the Signalling Principles called Principle model. The other is the formal model of the functional specification for a specific track-layout called Interlocking model. The Control Tables are translated into an interlocking model and then checked against the Principle model. At first she used CSP (Communicating Sequential Processes) as a modelling language but later found that the CSP models of the interlocking system and the signalling principle are difficult to understand and validate. Thus [16] used ASM (Abstract State Machine) notation to model the semantics of control tables. The ASM model is then automatically transformed to NuSMV code [5] while the safety properties are modeled in CTL (Computational Tree Logic). Basten [2] simulated and analysed railway interlocking specification using ExSpect which is a software tool based on high level Petri Nets. However formal verification of railway interlockings were not possible because they were too complex for the technology at that time. Hagalisletto et al [7] modelled signalling equipment such as track circuits and turnouts using Coloured Petri Nets. But their aim is to simulate the train schedule rather than to verify the interlocking.

4 The CPN Model of the Panthong's Interlocking Table

Coloured Petri Nets (CPNs) [10] are a graphical modelling language for design, verification and analysis of distributed, concurrent and complex systems. CPNs include hierarchical constructs that allow modular specifications to be created. CPN Tools [10] is a software tool used to create, maintain, simulate and analyse CPNs. We use CPN Tools version 4 [13] to create our railway signaling model and analyse them using reachabilty analysis. Due to space limitation we choose to explain only two CPN pages: `UserCommand` and `Move_Track_ to_Track`.

4.1 Modelling Scope and Assumptions

To reduce the complexity of the model as well as avoid the state explosion problem when analysing railway networks [7, 16], we need to make the following assumptions regarding train movement and

signalling operations:

1. We assume that a train has no length and it occupies one track at a time. The train moves in only one direction. Train shunting is not considered.
2. Our model does not include the auxiliary signals such as Call-on, Shunting and Junction indicators.
3. Our model does not include level crossings.
4. Our model includes high level abstraction of block systems but we do not model their operations in detail.
5. Our model does not include timers.
6. The train must not move through a track circuit so fast that the interlocking cannot detect the presence of the train. We use *prioritized transitions* to model this condition.
7. Unlike [12], our CPN model includes the flank protection.

4.2 Examples of the CPN Model

This section provides two examples of CPN pages. Due to space limitation we choose to explain only the `UserCommand` and `Move_Track_ to_Track` pages because these pages play important roles in the model. For global declarations and other details regarding our CPN model of the interlocking table, see [11] and [12].

4.2.1 UserCommand page

The `UserCommand` page shown in Fig. 2 models the action after a route request command is issued (e.g. 3-3(3)). Transition `SetRoute` checks whether it is plausible to set the requested route. Taking tokens from fusion places `RouteNormal` and `TrackPool`, transition `SetRoute` checks if

1. No conflict route is being set (modelled by function require_route_normal).
2. The relevant tracks are unoccupied (modelled by functions require_track_clear and require_flank_track_clear).

If all conditions are met, transitions `SetNormalLock` and `SetReverseLock` will attempt to set and lock points in the correct position. The two conditions and the states of the relevant point machines and derailers will be rechecked again by Substitution transition `RouteSetting`.

Actually the above model description is enough to satisfy the specification requirement. However when the CPN model was analysed, we found many deadlocks which were safe terminal states. It is inconvenient to investigate all deadlocks so we attempt to reduce them by introducing automatic route setting and automatic route canceling. These two functions are not specified in the interlocking table because they are normally conducted by the signal man. The automatic route setting condition is that the preselected route setting command can be issued only when the track in front of the entry signal is occupied. This is modelled by the ML function `approach_set`. After the transition `SetRoute` fires, it will be disabled by the inhibitor arc from place `RouteSuccess?`. When the route setting process is not complete, no other route can be set. Transitions `SetNormalLock` and `SetReverseLock` attempt to set and lock the points in the position specified in the interlocking table. Because transition `SetNormalLock` has a higher priority, the actions of transition `SetNormalLock` do not interleave with the actions of transition `SetReverseLock`.

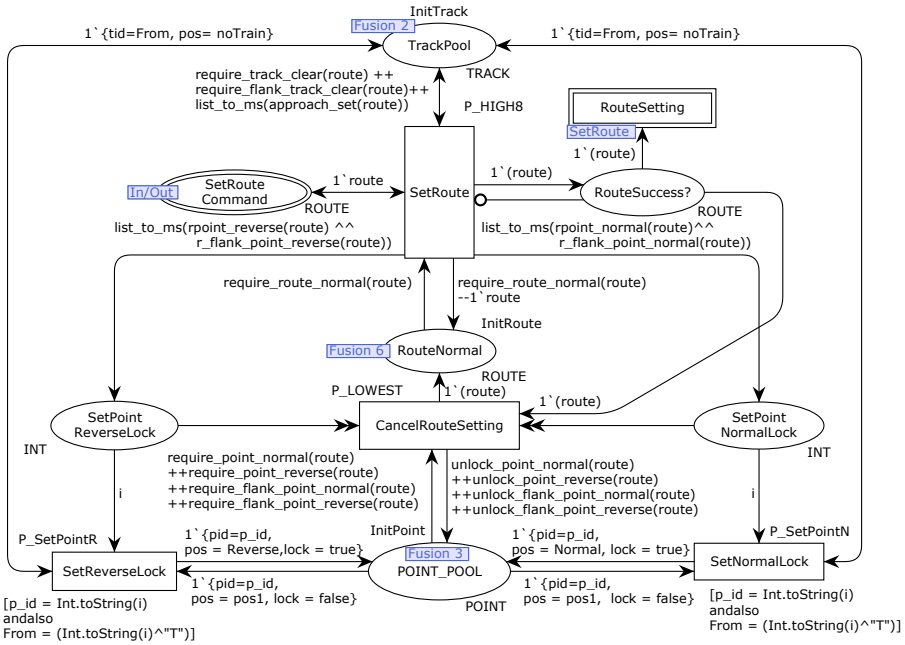

Figure 2: CPN model: UserCommand page

When the route setting cannot be completed and no more action can occur in the model, the incomplete route setting will be canceled using transition `CancelRouteSetting` (lowest priority). This transition clears all tokens in the places `SetPointReverseLock` and `SetPointNormalLock` by the reset arcs (two arrow arcs) in a single instance. Using prioritized transitions, inhibitor arcs and reset arcs can alleviate the state explosion problem. The automatic route setting and automatic route cancelation can eliminate deadlocks due to the wrong sequence of route setting commands given by the signal man.

4.2.2 Move_Track_ to_Track page

Figure 3 shows the CPN diagram modelling the simple train movements between two adjacent tracks. Place `Config` stores tokens representing signalling layout as discussed in [12]. In addition to the layout, the train movement requires information regarding the status of signalling equipment stored in places `TrackPools`, `SignalPool`, and `PointPool1`. Transition `MoveT2T` represents the movement across adjacent straight tracks. Transition `MoveTST` behaves similar to Transition `MoveT2T` but there is an entry signal post between the adjacent tracks. However the train moves toward the back of the signal. The train movement facing the front of the entry signal was modelled in another CPN page illustrated in [12]. The movement across points is captured by Transition `MoveTPT`. For ease of analysis we also add two places `AccidentH2T_H2H` and `AccidentHead2Side` for detecting train collision.

5 Analysis

5.1 Desired Property

A basic safety property that railway signalling shall provide is to prevent train collision and derailment. Places `AccidentH2T_H2H` and `AccidentHead2Side` shall be empty when no collision occurs. Checking derailment is in other CPN pages that we do not discussed in this paper. To convince us of the correctness

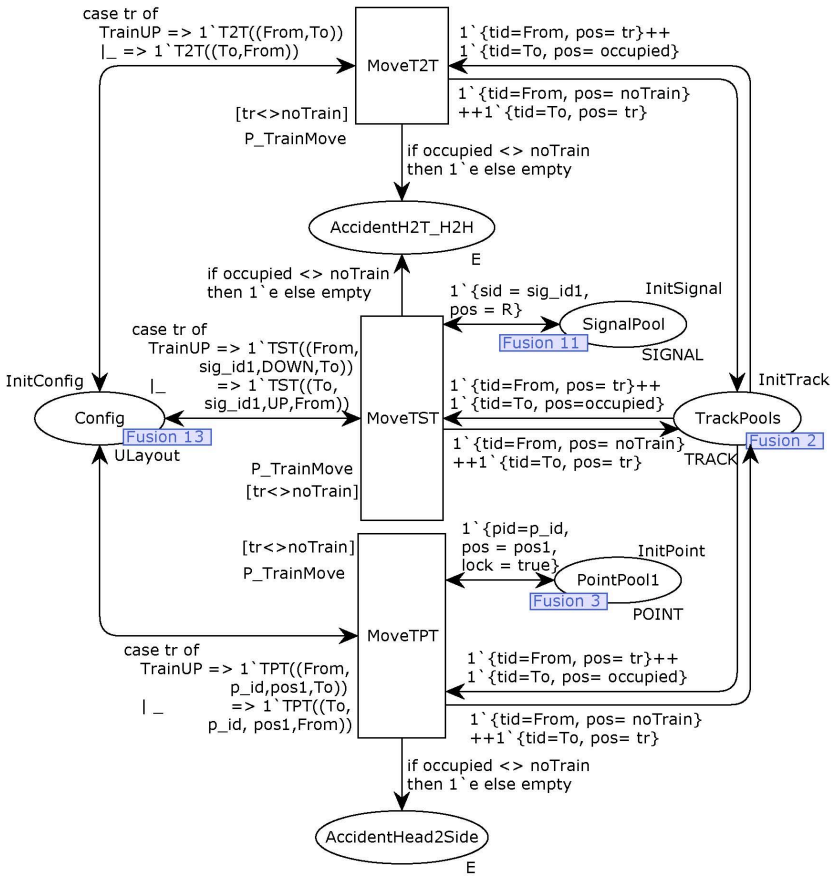

Figure 3: CPN model: Move Track to Track page

of our CPN model and the interlocking table, the CPN model is analysed using reachability analysis in CPN Tools version 4.0.0. The investigation of the generated reachability graph is conducted on Windows XP using a AMD9650 computer with 2.30 GHz and 3.5 GB of RAM. After generating each entire graph, we use ML query functions searching for the markings that have tokens in places[2] `AccidentH2T_H2H` or `AccidentHead2Side`. For ease of investigating the terminal markings, we wish to execute the model until there is no train left in the model. This can be done using automatic route setting and automatic route cancelation. However there are still possible deadlocks left as shown in Section 5.3.

5.2 Initial Configurations

Despite the fact that we can analyse various scenarios by changing the initial markings, due to space limitation, we select to discuss only six cases with the initial configurations shown in Table 4. The initial configurations are:

1. Case A is when three trains are on the platform tracks.
2. Case B is when two trains are on the platform tracks 62T and 63T.
3. Case C1,C2, and C3 are when one train is on the platform track 61T, 62T, and 63T respectively.
4. Case D is when no train is on the platform tracks.

[2]Of course we also need to check other accident places in other CPN pages that are not discussed in this paper.

Table 4: Initial configurations of track circuits.

Case	886-1T	886-3T	61T	62T	63T	943-1T	943-3T
A	TrainUP	TrainUP	TrainUP	TrainDOWN	TrainUP	TrainDOWN	TrainDOWN
B	TrainUP	TrainUP	NoTrain	TrainDown	TrainUP	TrainDOWN	TrainDOWN
C1	TrainUP	TrainUP	TrainUP	noTrain	noTrain	TrainDOWN	TrainDOWN
C2	TrainUP	TrainUP	noTrain	TrainUP	noTrain	TrainDOWN	TrainDOWN
C3	TrainUP	TrainUP	noTrain	noTrain	TrainUP	TrainDOWN	TrainDOWN
D	TrainUP	TrainUP	noTrain	noTrain	noTrain	TrainDOWN	TrainDOWN

In all initial markings, four trains are coming from the north and south directions and other track circuits are unoccupied; all points are in `Normal` position and unlocked; all derailers are `Normal` and locked. All signals are in normal states.

5.3 Analysis Results

Tables 5 and 6 show analysis results: state space sizes; execution time; and the number of deadlocks. All markings are safe (no train collision). In particular, Tables 5 illustrates that our approach can reduce the state space sizes.

1. B[Coor2010] was the old analysis result from [12].
2. B[no Flank Protection] is a new result when the CPN model is revised not only using prioritized transitions; inhibitor arcs; and reset arcs but also including the automatic route setting and automatic route canceling functions. However B[no Flank Protection] has not included the flank protection requirement. This result shows that our proposed reduces the number of states to about 70%. The number of terminal marking is also reduced significantly.
3. B[with Flank Protect] is the result when we add the flank protection requirement into the model. Because of this restriction, the non-conflicting routes in [12] that has no overlapped section now become conflicted so that the state space size is reduced drastically .

Revising model structure with the flank protection requirement, we are able to analyse the scenarios that we cannot reach before (Case C1, C2, C3 and D). The details of the terminal markings are listed in Table 7. They show the occupancies of trains on the tracks in front of the entry signal. In all terminal markings other tracks are unoccupied. All points are `Normal` and unlocked. All derailers are `Normal` and locked. All signals are in the normal states. Terminal markings no. 5 of Case C1 and no. 7 of Case D suggest that the signal man can manage the traffic such that no deadlock occurs. For the traffic of Case C2 and C3 there always be deadlocks so that the emergency procedure shall be carefully conducted to solve the deadlocks.

Table 5: Comparison of the state space sizes (with [12]).

Case	Node	Arc	Time(hh:mm:ss)	No. of Terminal Markings
A[Coor2010]	36	84	00:01:01	1
A[no FlankProtection]	16	32	00:00:11	1
A[with FlankProtection]	16	32	00:00:11	1
B[Coor2010]	261,522	1,189,280	11:28:44	57
B[no FlankProtection]	187,016	288,549	09:49:01	3
B[with FlankProtection]	16	32	00:00:12	1

Table 6: Summary of state space results.

Case	Nodes	Arc	Time (hh:mm:ss)	No. of Deadlocks
C1	24,133	45,704	00:55:03	5
C2	196	348	00:01:11	2
C3	2,004	4,788	00:05:35	3
D	76,257	137,398	04:07:27	7

Table 7: Terminal Markings.

Case	No.	1-1T	3-1T	61T	62T	63T	4-2BT	2-2BT
C1	1	noTrain	noTrain	TrainUP	TrainUP	TrainUP	TrainDOWN	TrainDOWN
	2	TrainUP	TrainUP	TrainUP	TrainDOWN	TrainDOWN	noTrain	noTrain
	3	noTrain	TrainUP	TrainUP	TrainUP	TrainDOWN	noTrain	TrainDOWN
	4	TrainUP	noTrain	TrainUP	TrainDOWN	TrainUP	TrainDOWN	noTrain
	5	noTrain	noTrain	noTrain	noTrain	noTrain	noTrain	noTrain
C2	1	TrainUP	TrainUP	noTrain	TrainUP	TrainDOWN	noTrain	TrainDOWN
	2	TrainUP	noTrain	noTrain	TrainUP	TrainUP	TrainDOWN	TrainDOWN
C3	1	noTrain	TrainUP	noTrain	noTrain	TrainUP	TrainDOWN	noTrain
	2	noTrain	TrainUP	noTrain	TrainUP	TrainUP	TrainDOWN	TrainDOWN
	3	TrainUP	TrainUP	noTrain	TrainDOWN	TrainUP	TrainDOWN	noTrain
D	1	TrainUP	noTrain	noTrain	TrainDOWN	TrainUP	TrainDOWN	noTrain
	2	noTrain	TrainUP	noTrain	TrainUP	TrainDOWN	noTrain	TrainDOWN
	3	noTrain	noTrain	noTrain	TrainUP	TrainUP	TrainDOWN	TrainDOWN
	4	TrainUP	TrainUP	noTrain	TrainDOWN	TrainDOWN	noTrain	noTrain
	5	noTrain	noTrain	noTrain	noTrain	TrainUP	TrainDOWN	noTrain
	6	noTrain	TrainUP	noTrain	noTrain	TrainDOWN	noTrain	noTrain
	7	noTrain	noTrain	noTrain	noTrain	noTrain	noTrain	noTrain

6 Conclusion and Suggested Work

This paper restructures the previous CPN model in [12] to make the analysis process easier and alleviate the state explosion problem. We also include the flank protection requirement specified in the interlocking table (Table 3).

From a modelling perspective it is easy to add the flank protection requirement but from analysis perspective it is not so easy to be verified. The flank protection is a fail safe requirement preventing an accident when equipment fails or a train passes a signal at danger. This dangerous scenario normally cannot be reached in our regular CPN model. To verify the flank protection and reach the states that are normally unreachable, the CPN model needs to allow the train pass a signal at danger. Thus, we suggest to conduct experiments by deleting the signal from the signalling layout and let the train pass over. This can be easily done by modify the configuration tokens that represent geographic information. This *modified* CPN models are used to generate the reachability graphs. When we search the entire graphs, we expect no train collision. However, if those points are not related to the required route at all, accidents definitely do not occur regardless of the point positions either normal or reverse. Thus, to prove the safety properties of the flank protection requirement we need to prove two properties. Firstly, if the flank protection works correctly, no train collision occurs. Secondly, if the model does not include the flank protection, trains will collide.

When verifying the flank protection in the interlocking table, we always assume that the flank points are known. However, for a large and complex station layout, it is difficult to identify the flank points without any errors. To facilitate the design and verification tasks, we suggest to use the modified CPN model generating train collision scenarios. Tracing the markings before trains collide should help us identify the flank points and their correct positions.

References

[1] K. Czarnecki et al (2008): *The Future of Train Signaling*. In: *Proceedings of MoDELS 2008, Lecture Notes in Computer Science* 5301, Springer Verlag, pp. 128–142.

[2] T. Basten, R. Bol & M. Voorhoeve (1995): *Simulating and Analyzing Railway Interlockings in ExSpec*. *IEEE Parallel & Distributed Technology, Systems & Applications* 3(3), pp. 50–62.

[3] J. Bjørk, A. M. Hagalisletto & P. Enger (June 2006): *Large Scale simulations of Railroad Nets*. In: *Proceedings of the Fourth International Workshop on Modelling of Objects, Components and Agents, MOCA'06,Bericht 272, FBI-HH-B-272/06*, pp. 45–101.

[4] C. Chevilat, D. Carrington, P. Strooper, J. G. Süß & L. Wildman (2008): *Model-Based Generation of Interlocking Controller Software from Control Tables*. In: *Proceeding of ECMDA-FA 2008, Lecture Notes in Computer Science* 5095, Springer, Heidelberg, pp. 349–360.

[5] A. Cimatti, E. E. Clarke, F. Giunchiglia & M. Roveri (1999): *NuSMV: A new symbolic model verifier*. In: *Proceedings of International Conference on Computer Aided Verification, CAV'99, Lecture Notes in Computer Science* 1633, Springer Verlag, pp. 495–499.

[6] W.J. Fokkink & P.R. Hollingshead (May 1998): *Verification of Interlockings: from Control Tables to Ladder Logic Diagrams*. In: *Proceedings of 3rd Workshop on Formal Methods for Industrial Critical Systems (FMICS'98)*, Stichting Mathematisch Centrum, Amsterdam, pp. 171–185.

[7] A. M. Hagalisletto, J. Bjørk, I. C. Yu & P. Enger (2007): *Constructing and Refining Large-Scale Railway Models Represented by Petri Nets*. *IEEE Transactions on Systems, Man, and Cybernetics, Part C* 37(4), pp. 444–460.

[8] K. M. Hansen (1994): *Formalizing Railway Interlocking Systems*. In: *Nordic Seminar on Dependable Computing Systems*, Department of Computer Science, Technical University of Denmark, pp. 83–94.

[9] C. W. Janczura (1998): *Modelling and Analysis of Railway Network Control Logic using Coloured Petri Nets*. Ph.D. thesis, School of Mathematics and Institute for Telecommunications Research, University of South Australia, Adelaide, Australia.

[10] K. Jensen, L.M. Kristensen & L. Wells (2007): *Coloured Petri Nets and CPN Tools for Modelling and Validation of Concurrent Systems*. *International Journal on Software Tools for Technology Transfer* 9(3-4), pp. 213–254.

[11] S. Vanit-Anunchai (2009): *Verification of Railway Interlocking Tables using Coloured Petri Nets*. In: *the tenth Workshop and Tutorial on Practical Use of Coloured Petri Nets and the CPN Tools*, DAIMI PB 590, Department of Computer Science, University of Aarhus, pp. 139–158.

[12] S. Vanit-Anunchai (2010): *Modelling Railway Interlocking Table Using Coloured Petri Nets*. In D. Clarke & G. Agha, editors: *Proceedings of the 12th International Conference on Coordination Models and Languages, (Coordination 2010), Lecture Notes in Computer Science* 6116, Springer, Heidelberg, Amsterdam, Netherlands, pp. 137–151.

[13] Michael Westergaard (2013): *CPN Tools 4: Multi-formalism and Extensibility*. In José Manuel Colom & Jörg Desel, editors: *Petri Nets, Lecture Notes in Computer Science* 7927, Springer, pp. 400–409. Available at `http://dx.doi.org/10.1007/978-3-642-38697-8_22`.

[14] K. Winter (2002): *Model Checking Railway Interlocking Systems*. In: *Proceeding of the 25th Australian Computer Science Conference (ACSC 2002)*.

[15] K. Winter, W. Johnston, P. Robinson, P. Strooper & L. van den Berg (2005): *Tool Support for Checking Railway Interlocking Designs*. In: *Proceeding of the 10th Australian Workshop on Safety Related Programmable Systems (SCS'05)*, Australian Computer Science Communications, pp. 101–107.

[16] K. Winter & N. Robinson (2003): *Modelling Large Railway Interlockings and Model Checking Small Ones*. In: *Proceeding of the Australian Cumputer Science Conference (ACSC 2003)*.