TRANSPORT PROBLEMS 2009
PROBLEMY TRANSPORTU Tom 4 Zeszyt 1

Ahmad MIRABADI*, Mohammad B. YAZDI
Iran University of Science and Technology, School of Railway Engineering (S.R.E)
Iran,Tehran, Narmak
**Corresponding author*. E-mail: mirabadi@iust.ac.ir

AUTOMATIC GENERATION AND VERIFICATION OF RAILWAY INTERLOCKING CONTROL TABLES USING FSM AND NUSMV

Summary. Due to their important role in providing safe conditions for train movements, railway interlocking systems are considered as safety critical systems. The reliability, safety and integrity of these systems, relies on reliability and integrity of all stages in their lifecycle including the design, verification, manufacture, test, operation and maintenance.

In this paper, the Automatic generation and verification of interlocking control tables, as one of the most important stages in the interlocking design process has been focused on, by the safety critical research group in the School of Railway Engineering, SRE. Three different subsystems including a graphical signalling layout planner, a Control table generator and a Control table verifier, have been introduced. Using NuSMV model checker, the control table verifier analyses the contents of control table besides the safe train movement conditions and checks for any conflicting settings in the table. This includes settings for conflicting routes, signals, points and also settings for route isolation and single and multiple overlap situations. The latest two settings, as route isolation and multiple overlap situations are from new outcomes of the work comparing to works represented on the subject recently.

AUTOMATYCZNA GENERACJA I SPRAWDZANIE TABLIC ZALEŻNOŚCI DLA SYSTEMU STEROWANIA RUCHEM KOLEJOWYM Z WYKORZYSTANIEM METODY AUTOMATÓW SKOŃCZONYCH I FORMALNYCH TECHNIK WERYFIKACJI

Streszczenie. Ze względu na konieczność zapewnienia bezpiecznych warunków dla ruchu pociągów, systemy sterowania ruchem kolejowym muszą być rozpatrywane jako systemy bezpieczeństwa krytycznego. Niezawodność i bezpieczeństwo tych systemów opiera się na niezawodności i integralności wszystkich etapów cyklu ich powstawania, zawierającego projektowanie, weryfikację, produkcję, testowanie, pracę i utrzymanie.

W artykule została przedstawiona automatyczna generacja i weryfikacja tablic zależności jako jeden z najważniejszych etapów w procesie projektowania urządzeń SRK, opracowana przez grupę badawczą ze Szkoły Inżynierii Kolejowej, SRE. Wprowadzono trzy różne podsystemy: planowanie układu sygnalizacji, generator i weryfikator tablic. Używając technik formalnych, weryfikator tablic analizuje ich zawartość (bezpieczne warunków ruchu pociągu) i sprawdza przebiegi kolizyjne. Obejmuje to ustawienia sprzecznych tras, jak również punktów dla pojedynczych i wielokrotnych sytuacji zachodzenia przebiegów.

1. INTRODUCTION

Railway interlocking systems are categorized as safety critical systems with SIL-4, based on EN50126 and IEC61508 standards. Functional specification of the railway interlocking systems is introduced in interlocking control tables. Control tables have an important role in the signalling design process since

They clarify what conditions must be met before a train move can be permitted on the railway lines and stations. Control tables are considered as an interlocking design specification, to be used by the interlocking designers and also as a test specification, to be used by tester. These tables contain the key functional safety requirements for the interlocking system. The development process of these interlocking tables, especially for medium to large scale stations, is labour intensive and requires specialized skills and currently is an entirely manual process. Obviously this can cause a major source of human's errors in the design process of interlocking system. Mechanization of the generation and verification of the control tables can be an efficient approach to improve the reliability of the overall interlocking system. The work introduced in this paper is an introduction to a toolset, designed for automatic generation and verification of control tables.

In contrast to the works represented by other researchers such as Eisner [1], Simpson et al. [2] and Hubber [3], this paper proposes an easier approach in modelling the interlocking system and its verification and comparing to the work represented by Tombs et al. [4] a further step in identifying the settings for route isolation and flank protection.

2. INTERLOCKING CONTROL TABLE

In signalling point of view, a railway station consists of a collection of functions including different types of signals, track sections (monitored by train detection systems such as track circuits and axle counters), points, level crossing equipment and etc. Each of the objects in a railway can attain a certain number of states:

- a track section can be either occupied or clear;
- a three-aspect main signal can be red (ON), yellow or green (OFF);
- a point can be in reverse or normal position;

Figure 1 depicts a schematic view of signaling objects arrangement (signalling layout plan) in a typical railway station. Each separated object in this figure is provided with a unique identification code. The layout plan of the stations is considered as the first stage of the interlocking design, based on the operation requirements provided by the railway operator.

In setting a route for a particular train movement (i.e. a signal to become green or yellow) the followings are the minimum pre-settings, required to be implemented and verified [5]:

- all tracks in the route and in the overlap should be clear
- all points in the route and in the overlap should be set, clear, locked and checked
- all conflicting signals and opposing signals should be ON (red)
- all in-route signals should be OFF (clear)
- the route should be isolated from all potential conflicting movements

An interlocking control table is a structured, tabular presentation of the rules and pre-settings, governing route settings. It is used as a reference for identification of interrelation between different signaling functions (i.e. signals, points and track sections) in generation and verification of interlocking.

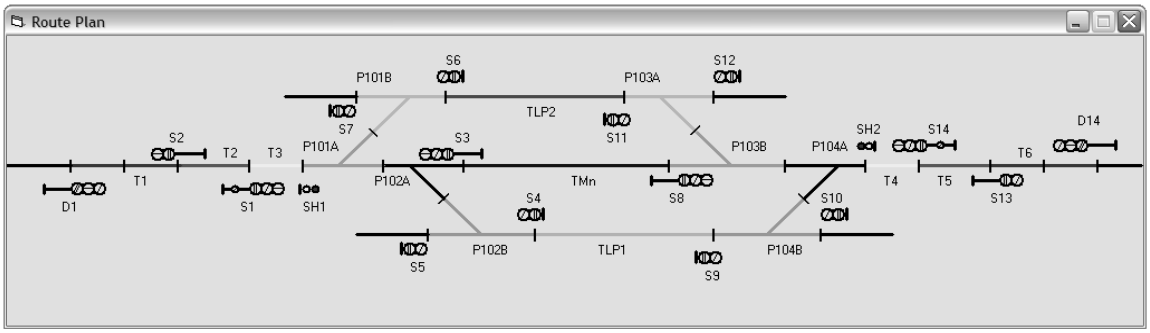

Fig. 1. Signalling layout plan for a typical simple railway station
Rys. 1. Układ torowy i plan sygnalizacji dla typowej, prostej stacji kolejowej

All possible and required routes in the stations, which are derived from the signalling layout plans, are represented in the route table of the stations.

Generation and verification of control table is the design stage after the route table generation and before the wiring diagram designing in relay based interlocking systems (or software flowchart development in computer based interlocking). The format and contents of tables is not standardized, and may vary even within the same railway administration. Nevertheless, general principles of control table design are evident.

A route is defined by an entrance signal and exit signal. Each row of the table consists of the pre-settings required by one particular route which can be defined in the station. The required settings for a route between signals S1 and S9 in figure1, as one row of the interlocking control table, is shown in table 1.

Table 1

A row of C. T. for the station shown in figure 1

Start Signal	Route name	Exit Signal	Signals		Points		Track Section		Overlap	Conf. Routes	Flank Protection	
			ON	OFF	Normal	Rev.	Clear	Occ.			Normal	Rev.
S1	S1(m1)	S9	S9 S3 S4 S5 S6 …	S1 Sh1	P101A	P102A P102B	T3 TLP1	T2	P104B[N]	S3(m1) S4(m1) S5(m1) S5(m2) S6 (m1) …	P101A P104A	P103B

3. AUTOMATIC C. T. GENERATION AND VERIFICATION

Figure 2 shows the flow diagram of an automatic C. T. generation and verification system. The system is basically designed in three subsystems as:

- Graphical Signalling Layout Planner (SLP)
- Route Table Generator (RTG)
- Control Table Generator (CTG)
- Control Table Verifier (CTV)

3.1. Signalling Layout Planner, SLP

SLP is a software tool to plan the signalling layout of any given station, based on its topographic map, using a user friendly graphical interface. Using SLP, the user is able to generate a model of the station as a combination of track sections and then position the signalling objects (i.e. signals, points…) on the specified locations, based on the operational and signalling safety requirements.

SLP provides the signalling layout plan in Extensible Markup Language (XML) format.

3.2. Route Table Generator, RTG

RTG is a software system to analyze the signalling layout plan and identify all routes possible to be defined in the station. Each route is defined as the distance between a start and an exit signal. The system is able to identify routes initiated from main, colling-on and subsidiary signals in the station. The operator will be able to alter the table according to operational requirements and limitations.

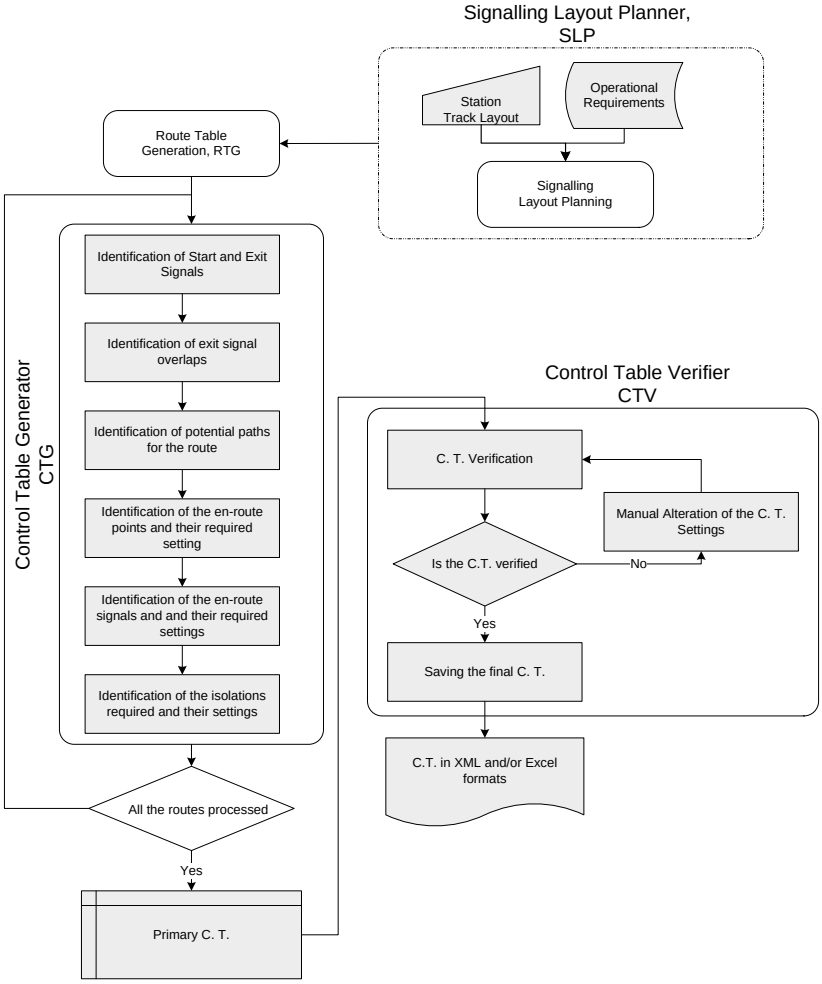

Fig. 2. Flow diagram of automatic C. T. generation and verification
Rys. 2. Schemat (algorytm) automatycznej generacji i weryfikacji

3.3. Control Table Generator, CTG

The Control Table Generator determines all required settings for each particular route specified in the route table. For this purpose, CTG scans the route between the entrance and the exit signals, and identifies all track sections, signals and points which have filled the route. In other word, the CTG algorithm identifies the sequence of track sections, points and signals within each route and its overlap and their corresponding situations (Normal or Reverse).

Since in some situations, there are more than one path to reach from entrance signal to the exit signal (e.g. S1 to S13 in figure 1), CTG algorithm is designed in a way to identify and record both paths as two different routes.

Running the CTG over the route table and the signalling layout plan, a majority of control table field, including the followings will be completed:

- overlaps
- track sections within the route and overlap that should be clear or occupy
- points lying in the route and overlap and their direction
- signal replacement track sections (track sections witch are placed after the entry signal)
- en-route shunt signals

Table 2 shows a sample of CTG output for the route connecting signals S1 and S9.

Table 2

Sample of control table, generated by CTG

Start Signal	Route name	Exit Signal	Signals		Points		Track Circuits		Overlap
			ON	OFF	Normal	reverse	Clear	Occupied	
S1	S1(m1)	S9	S9	S1	P101A	P102A P102B	T3, TLP1	T2	P104B[N]
S1	S1(m2)	S9	S9	S1	P101A	P102A P102B	T3, TLP1	T2	P104B[R]

3.4. Control Table Verifier, CTV

After generation of primary control table that consist of basic setting for all routes identified by RTG or by the user, CTV will check the generated control table against a set of signalling principles, to ensure the integrity of the settings and also to fill the remaining fields of the control table.

For this purpose, CTV benefits from the NuSMV model checker. CTV checks the possibility of a collision a train moving on a particular route with all other routes identified in the station.

4. CONTROL TABLE VERIFICATION

Automatic verification of control tables is one of the key functions of the signaling design toolset. In this toolset, the automatic verification is performed by using the formal language Finite State Machines (FSM) and also the symbolic model checker NuSMV.

FSM in here is used to model the train movement as a sequence of states which train should go through from entrance signal to the exit signal, while NuSMV is used for detection of any conflict between the routes, in the same or in the opposite directions.

The input language of NuSMV is designed to allow for the description of Finite State Machines (FSM) as transition relations. This relation describes the evolutions of the FSM states.

4.1. CTL Model Checking

In order to check that the model developed for a system, satisfies the desired properties and conditions specified by the user, a model checker is used. These specifications need to be defined for the system in a suitable manner. In NuSMV, the specifications to be checked can be expressed in two different temporal logics: the Computation Tree Logic (CTL) and Linear Temporal Logic (LTL). The specifications represented in CTL or LTL will be evaluated by NuSMV, which determines whether they are true or false in FSM. If the NuSMV recognizes that a specification is false, it will provide the trace of the FSM that falsifies that property, as an output. In this paper CTL is used to express the specifications of the model.

CTL provides the opportunity for expressing the properties that should hold for all the paths, starting in a particular state and also properties that should hold just for some paths. As an example,

consider for instance the formula AF p in CTL. It expresses the condition that, for all the paths (A) starting from a state, eventually in the future (F) condition p must hold. That is, all the possible evolutions of the system will eventually reach a state satisfying condition p. The EF p formula in CTL, on the other hand, requires that there exists some paths (E) that eventually in the future satisfies p.

Similarly, formula AG p requires that condition p is always, or globally, true in all the states of all the possible paths, while formula EG p requires that there exist some paths along which condition p is globally true. More information on CTL logic can be found in [6] and [7].

4.2. Verification of The Safety Requirements

The general safety requirements of railway interlocking system are explained in section 2 of this paper. In order to formalize the problem a train moving on each particular route, moving from one state to another is considered, while at the same time a second train is moving on all other routes sequentially. The specifications will be verified if there will be collision between the two mentioned trains.

A train collision is simply specified as two trains (t1 and t2) occupying the same track section in the station. The CTL formulas for ensuring train movement without collision and derailment are given in the following table.

Table 3

A sample of CTL formula

AG! (t1.location = t2.location)
AG! (t1.location = derailment)
AG! (t2.location = derailment)
AF (t1.locatin = last track & t2.locatin = last track)

Where AG! can be read as never and AF as at least one time. These formulas guarantee that:

- Two trains should never be located in the same track section, otherwise a collision will happen.
- A train should occupy all the track sections of the route and its overlaps, sequentially, until it reaches the last track section. In other word, trains should completely pass the routes, without any collision or derailment.

After finishing the above checking for all routes in the station, all detected conflicts will be represented as a list of conflicting routes.

The control table and consequently the interlocking system should provide all necessary settings in order to ensure that no two conflicting routes can be set at the same time. During the checking the FSM model, the NuSMV model checker goes through each route of the route table. The conflicting routes are detected and represented as counter-example outputs by the NuSMV. A counter-example is a list of states that lead to a state violating the checked safety requirements (i.e. in this case a front-to-front collision).

For each state only the changes from the previous state are given. Figure 3 shows the key parts of states that finally lead to a collision of trains t1 and t2 on the track P101A (see state 1.4).

```
-- specification AG !(t1.location = t2.location)  is false
-- as demonstrated by the following execution sequence
Trace Description: CTL Counterexample
Trace Type: Counterexample
-> State: 1.1 <-
  t1.location = T3
  t2.location = TLP1
-> Input: 1.2 <-
  _process_selector_ = t1
  running = 0
  t2.running = 0
  t1.running = 1
-> State: 1.2 <-
  t1.location = P101A
-> Input: 1.3 <-
  _process_selector_ = t2
  running = 0
  t2.running = 1
  t1.running = 0
-> State: 1.3 <-
  t2.location = P101B
-> Input: 1.4 <-
  _process_selector_ = t2
  running = 0
  t2.running = 1
  t1.running = 0
-> State: 1.4 <-
  t2.location = P101A
-- specification AF (t1.location = TLP2 & t2.location = T3)  is true
-- specification AG !(t1.location = derailment)  is true
-- specification AG !(t2.location = derailment)  is true
```

Fig. 3. Counter-example output by NuSMV
Rys. 3. Przykładowe obliczone dane wyjściowe

The last stage of the process, through which the primary control table will be completed, new settings for the control table, to ensure that no two conflicting routes will be set at the same time, will be added.

As a result of the model checking implementation, the detected conflicting routes are added to the associated list and then all required settings for isolation of the specified route, such as point settings, will be identified and added to the control table.

In other word control table verifier, not only verifies the settings in the primary control table, also completes the table with settings concerning route isolation as one of the safety requirements.

Table 4 shows the new control table, with additional information in bold, which have been added by the verified program.

Table 4

Additional columns filled after the verification process by CTV

Enter Signal	Route name	Exit Signal	Signals		Points		Track Circuits		Overlap	Conflicting Routes	Flank Protection	
			N	R	N	R	Clear	Occ.			N	R
S1	S1(m1)	S9	S9, S3, S4, S5, S6, …	S1, SH1	P101A	P102A P102B	T3, TLP1	T2	P104B[N]	**S3(m1), S4(m1), S5(m1), S5(m2), S6 (m1), …**	**P101A P104A**	**P103B**

5. CONCLUSION

This paper introduces an algorithm for generation and verification of interlocking control table. Required settings for route isolation and also multiple overlaps are from problems this paper has tried to solve. Using the toolset developed by the safety critical research group in the school of railway engineering (SRE), the human interference in the design, development and verification of control table has been minimized.

Bibliography

1. Eisner C.: *Using symbolic model checking to verify the railway stations of hoornkersenboogerd and heerhugowaard*. Proc. of Conf. on Correct Hardware Design and Verification Methods (CHARME'99)', Vol. 1703 of LNCS, Springer-Verlag, 1999.
2. Simpson A., Woodcock J., Davies J.: *The mechanical verification of solid state interlocking geographic data*. Proc. of Formal Methods Pacific (FMP'97)', Discrete Mathematics and Theoretical Computer Science Series, Springer-Verlag, 1997, p. 223-243.
3. Hubber M.: *Towards an industrially applicable model checker for railway signalling data*. Masters thesis, University of York, 2001.
4. Tombs D., Robinson N., Nikandros G.: *Signalling control table generation and verification*. Proc. of the Conference on Railway Engineering (CORW2000)', Railway Technical Society of Australasia, November, 2002.
5. *Office of rail regulation: Railway safety principles and guidance*. Section D, guidance on signalling, April, 2006.
6. Cavada R., et al.: *NuSMV 2.2 Tutorial*. ITC-irst - Via Sommarive 18, 38055 Povo (Trento). Italy, 2006.
7. Emerson E.: *Temporal and modal logic. Handbook of Theoretical Computer Science*, Vol. b, Elsevier Science Publishers, 1990.

Received 7.07.2008; accepted in revised form 14.03.2009