Smart Control of Automatic Level Crossings with Communication Facilities

M. Ghazel

Univ Gustave Eiffel, COSYS-ESTAS
France

Abstract

The study discussed in the present paper seeks to develop a new LC control/command architecture in the ERTMS L2/3 operation context, which allows for preventing some identified risky scenarios. The main motivation that underlines the developed control scheme is to make a step change on the LC control operation, by switching from a rudimentary passive control to a new paradigm that advocates for a supervised control-command which takes in consideration the dynamics within the LC zone as a whole. In addition to its advantages in terms of safety, the established architecture scheme seeks for dispensing with train sensing devices, thus making getting maintenance saving possible, as well as improving the system's reliability. We should also notice that this is perfectly in line with the increasing willingness to minimize track equipment and, hence, to ensure substantial savings in terms of installation and maintenance. In order to establish the LC control architecture, we have set up a formal framework which enables expressing the various constraints to be ensured, and we have illustrated how formal models and analytic techniques can be advantageously utilized for designing and validating control architectures for safety critical railway systems. Besides, the important debugging phase witnesses how developing such a control model can hide some fine features which are intractable without the support of automated checking tools. It is interesting to recall here that using such formal techniques is more and more recommended for the design, the verification and the validation of critical complex systems, particularly in railways (14). Although further setups still need to be undertaken before an actual implementation, the discussed contribution paves the way towards developing a control architecture which efficiently integrates LCs in the ERTMS/ETCS operation framework.

1   Introduction

Safety at Level Crossings (LC) has always been a challenging issue for railway stakeholders. Level Crossing (LC) accidents account for about one third of the total number of railway accidents in Europe, causing more than 300 deaths every year (1), (2). In general, these accidents are the cause of a complex combination of interrelated technical, organizational, operational andhuman-related causes. The collisions occurring at LCs give rise to serious material damage and important traffic disturbances. Besides, they seriously tarnish the safety reputation of railways although the main causes are generally related to errors committed by road users (about 95% of the whole LC accidents). It is worth noticing that although a major part of LC accidents are related to human factor errors, such errors are generally related or accentuated by some technical considerations. That is to say that some technical settings of the LC control may have a direct impact on road users' behaviour.

On the other hand, ERTMS (European Rail Traffic Management System) is the standard railway control-command and signaling (CCS) system being currently implemented in Europe and elsewhere. The aim of ERTMS is to guarantee railway interoperability while keeping the highest safety standards. Moreover, having a standard railway CCS system is key to enhance the competitiveness of the railway sector. Regarding LCs, it should be noted that the ERTMS specifications only provide a rough description regarding level crossing control.

As mentioned earlier in this section, some accident scenarios are the result of the combination of technical settings and human errors. Tackling human errors proves to be complex since, by nature, human errors are generally non-deterministic and difficult to predict. Nonetheless, we believe that there is room for safety LC improvement by means of fine tuning some technical settings in such a way as to anticipate or event prevent some hazardous behaviours by road users.

The present study elaborates on a functional control architecture for automatic LCs in the context of ERTMS operation Levels 2 and 3. Indeed, these operation levels ensure a continuous tracking of train location thanks to the GSM-R (Global System for Mobile communications - Railways) link between trains and Radio Block Center (RBC). Namely, the established LC control scheme aims to ensure an optimal LC command based on the information regarding the train location and, thereby, prevent some potential risky scenarios and improve the global safety at LCs. In particular, the current study focuses on two main risky scenarios that occur at LCs and which have caused an important number of train/car collisions. Namely, this is about 1) unnecessary long LC closure cycles, and 2) too short LC opening duration between two successive closure cycles. In fact, when analyzing LC accident scenarios some typical situations arise while, to a large extent, errors from the road users are

impugned. In particular, the scenario consisting in bypassing the half barriers to cross the LC when it is closed for the road traffic (zigzag) has been identified to be a major scenario behind LC collisions. This happens in 2-half-barriers LCs which constitute the major proportion of automatic guarded LCs, in particular in France. Moreover, several studies focusing on human factors in LC areas have pointed out that this misbehavior is often related to the long duration of LC closure. In fact, the sensors responsible for announcing the train's approach to the local control system are implemented in such a way as to ensure that the LC closure is triggered to ensure a minimum given delay prior to the train arrival at the intersection zone. Therefore, the (static) location of the train sensor which detects the train arrival is set according to the maximum speed limit of the track section. Nevertheless, different train categories, such as freight and passenger trains, with different speed, may pass on the section where the LC is located. Moreover, some operational considerations such as stopping at nearby station, may lead to speed decrease. As a consequence, such a LC control scheme leads to unnecessarily long closure delays in the case of slow trains. For instance, let us consider a maximum authorized train speed 1 of 160 km $*$ h -1 and a nominal closing duration of 22 s. It follows that if a freight train running at 50 km $*$ h -1 approaches the LC, the LC closure will be triggered 70 seconds prior to the train arrival at the LC intersection. Such a long closure duration could prompt impatient vehicle drivers who may run the risk of bypassing the lowered half-barriers. Several studies on LC safety pointed out that the imprudence and impatience of road users are the major factors behind LC accidents/incidents. For instance, in the 2007 report conducted by the Australian National Railway Level Crossing Behavioral Coordination Group (BCG), it is stated that among more than 4400 road users who participated in a survey that measures awareness and impatience at LCs, one quarter reported having engaged in illegal usage of a LC at least once (3). Moreover, some observation campaigns regarding LC road users' behavior that we have undertaken in the framework of the PANSAFER project (4), showed long LC closure cycles as a main factor behind zigzagging.

On the other hand, in the case of LCs located on double-track lines, although the trains that come from the same side are sufficiently spaced apart, those circulating from the opposite direction may arrive at the LC independently of each other. Hence, successive LC closure cycles may be too close to each other. That is to say that the LC is opened to road traffic when the first passing train leaves the intersection zone, then when a few seconds later an approaching train is detected from the opposite direction, the LC is closed down again. This situation has also been identified as a hazardous scenario which can cause misbehavior from road users, especially w.r.t. to the panic of car drivers, as reported in (5). It should be noticed that various systems have been elaborated, worldwide, to help improving LC safety. In (6), a control system for 4-half-barrier LCs is elaborated in such a way as to prevent scenarios where cars are trapped between the entry and exit barriers. The system was tested in Illinois (U.S) then implemented in numerous LCs throughout the United States. Further some systems that allow obstacle detection at LCs have been developed; (7) discusses a stereo vision based system that have been tested in Japan. The authors of (8) develop an ultra-wideband radar system that makes it possible to detect vehicles trapped in the

LC intersection zone, while (9) discusses a multi-sensory architecture that can detect obstacles on the tracks, especially at LCs. The system consists of two emitting and receiving barriers, which are placed on opposing sides of the railway, and use infrared and ultrasonic sensors. Diverse techniques of data fusion are then used to ensure a highly reliable detection. In (10), techniques that allow train travel time prediction are used to mitigate congestion at level crossings while (11) assesses various innovative solutions for pedestrian level crossing treatments. This last study is part of a list of projects launched by the Federal railway Agency (U.S.) to improve safety at LCs, as summarized in (12). Such projects investigate a diversity of options, including innovative technical solutions, infrastructure arrangements, training, etc.

2   Methods

To develop a control model that allows for tackling the two risky scenarios, a generic methodology is employed. Firstly, a formal behavioral model is developed using the Time Petri Net (TPN) notation. The benefits of such formal model is that it allows for specifying a number of dynamical features in a rigorous and unequivocal way. More importantly, a number of tools are available to automatically check behavioural properties on this model.

In order to set up a behavioral model that depicts the LC dynamics, a modular modeling approach, that is similar to the one developed in (15), is adopted. This consists in decomposing the whole system in modules, then establishing elementary behavioral models for these modules, before integrating the developed models while taking into account the various interactions. Such a process is quite convenient for dealing with complex systems, as the modelling problem is decomposed into smaller sub-problems. In our case, the LC system will be decomposed into two modules; on the one hand, there is the local control system, which is in charge of controlling the barriers closure/opening, the road traffic lights and the sound alarms; on the other hand, we have the rail traffic monitoring which triggers the LC closing/opening cycles by activating approaching/departure train sensors, respectively. For the sake of simplicity, we will consider that the LC local control module reacts in a passive way to the stimulus of the railway traffic, and we will report the various constraints on the model of the rail traffic module. Without loss of generality, we will consider a 2-half-barrier LC (2-HB) with two railway tracks, that run in opposite directions. Note that the control of 4-half-barriers LCs is slightly different. In addition, we assume that no interleaving occurs between LC closing cycles due to successive trains running in the same direction; this basically transcribes the track sections layout. Finally, it is assumed that the control system is failure-free.

Once the structure of the LC control model is established, we need to set the actual parameters in our control architecture with the goal to meet the operational and safety requirements so as to tackle the risky scenarios mentioned above. The different distances that intervene in our control scheme are detailed in [16] where a preliminary control scheme is outlined.

Finally, the validation phase consists in checking whether or not the pre-defined requirements are met, and provide adequate evidence. In safety critical applications, design validation is a crucial step that is required prior to any further developments. In general terms, validation consists in checking the design against various kinds of properties (safety, reactivity, liveness, etc.). Different techniques can be utilized to accomplish the validation process, depending on several parameters such as, for instance, the type of system description (dynamic model, static model, general characterization, etc.) and the available expertise. When the system behavior is described as a dynamic model, simulation and analytic methods are the most used techniques for analysis. Whereas simulation has some advantages in terms of ease of use, it remains quite limited when it comes to dealing with complex systems, since simulation does not guarantee an exhaustive analysis of the system behavior, as errors can be related to very specific scenarios that may not be elucidated by simulation. This is the reason why formal methods are more and more recommended to deal with complex systems (13). In particular, Model-Checking (MC) is an automatic verification technique that ensures an exhaustive analysis of the system behavior. As a result, when checking some properties through MC, the obtained result is, either YES or NO, unequivocally. Besides, various free MC software tools (called model-checkers) are available and implement efficient MC algorithms that can handle large systems (up to 10 100 states). In practice, a model-checker automatically verifies a property stated as a formula in temporal logic on a discrete event model that describes the system behavior. In the current study, we used the model-checking facilities of the TINA tool (20) to investigate various requirements on the developed control scheme.

3 Results

The developed behavioural model
For the lack of space, we will not represent the various elementary models that have been established to depict the behaviour of the different identified sub-systems involved in the LC control, the authors can refer to (16) for more details.

As mentioned earlier, TPN notation will be used to develop models for the dynamics within the LC zone. A TPN can be formally defined as follows:

Let $T \subset Q +$ be a temporal domain, a Time Petri Net (17) on domain T is a tuple N = <P, T, B, F, M 0 , SIM > s.t:
• N = < P, T, B, F, M 0 > is a marked Petri Net (PN), (B as backward and F as forward),
• SIM : T → T × T ∞ , where T ∞ = T ∪ {∞} is the Static Interval Mapping, which assigns to each transition in T its static firing interval with rational lower bound of firing (as $T \subset Q$).

In general, to obtain a finite representation of the state space of a given TPN, (18) proposed the State Class paradigm, which is the key feature of the enumerative method that allows reachability analysis for TPNs. In fact, a state class is the maximal aggregation of states E = (M, I) that can be obtained from each other by time

translation. Hence, for bounded TPN, it is possible to derive a finite representation of its state space called State Class Graph (SCG). For more details on the way to compute the SCG of a bounded TPN on the basis of the enumerative approach, the reader can refer to (19). It is moreover worth noticing that there exists a tool called TINA (TIme petri Net Analyzer) (20), which implements the enumerative approach and allows for establishing the state class graph from a textual or graphic description of a TPN. One can recall in this respect that SCG preserves the linear properties of the TPN. Moreover, TINA offers facilities to derive further TPN state space representations, which are variants of the SCG that offer the advantage of preserving further property types, namely branching properties (CTL / CTL* properties). Since each abstract state space representation preserves more or less features on the system behavior, the choice between these representations mainly relies on the properties to be checked on the model. Finally, it should be noticed that, besides analyzing TPN reachability, TINA tool offers interesting model-checking facilities such as, for instance checking state/event LTL properties, CTL* and μ-calculus formulas and path analysis.

The global behavioral model shall integrate the elementary dynamics of the involved subsystems. It has then to embed the various interactions between the dynamics of these subsystems. In particular, the following high-level requirements are to be considered so as the opening cycle can be launched:

1. The train-approaching announcement has to be emitted at the appropriate moment in such a way as to ensure a fixed delay (of α seconds) before the train reaches the intersection zone.

2. When the LC is open for the road traffic, as soon as a train-approaching announcement is emitted, the closing cycle is launched.

3. As soon as the crossing train is ensured to have left the intersection zone (by means of the train sensor in the leaving direction), the opening is launched only if:
(a) no train in the opposite direction is crossing
(b) no train in the arrival direction from the opposite side will launch a closing cycle within less than γ seconds, which is implemented through the anticipated-announcement.

The above requirements will be implemented in our global behavioral model, by introducing additional elements (places, transitions and arcs) which will couple the elementary models accordingly. Moreover, as mentioned earlier, some modifications will be made in these models so as to fulfill the various behavioral constraints. The overall model is consists in a time petri net model, where the transitions depicted by thin line stand for immediate transitions, i.e. to which a [0, 0] firing interval is assigned. In what follows, we will discuss the various modeling choices that have been made.

6

The various behavioral requirements have been finely implemented within our model, so as to obtain a trustworthy representation of the behavior. Yet, a validation phase is still required to ensure that all the safety and functional requirements are well met.

<u>Validation phase</u>
To perform the validation phase, we reformulate the two risky scenarios as temporal logical formulas so as MC automatic technique can be brought into play for their checking. By referring to our behavioural model, it proves to be complex to generate formal properties that express the investigated scenarios in a straightforward way. To allow expressing these properties in an intuitive way, we have enriched our behavioural model with some observers, which serve as watch-dogs for our properties. In practice, checking a property amounts to examine whether or not a dedicated violation state can be reached. In the following we will illustrate how the expressed properties look like.

• Short opening duration: Thanks to the developed observer, verifying whether or not two subsequent cycles could be launched less than 30 seconds after each other, can be achieved simply by checking if place P O1−2 can be marked. Using the model-checking facilities of TINA, namely its SELT model-checker, one has to check the following property: $\Phi 1 : AG(\neg P\ O1{-}2)$ which can be written using the TINA syntax: [ ](−P O1−2). This property has been checked on the re-computed state class graph, following the integration of the observer model. SELT shows that such a property is well satisfied.

• Unnecessarily long closing duration: As mentioned earlier, using an observer to monitor a specific feature allows for considerably simplifying the actual property to be checked on the model. In particular, in our case, such a property can be expressed as an LTL formula: $\Phi 2 : AG(\neg P\ O2{-}1)$, which can be written using the TINA syntax: [ ](−P O2−1). This property has been checked on the re-computed state class graph, following the integration of the second observer model. SELT shows that such a property is well satisfied.

The reader can refer to [16] where a preliminary version of the study is discussed and where the technical details regarding the V&V phase can be found.

4   Conclusions and Contributions

The study discussed in the present paper seeks to develop a new LC control/command architecture in the ERTMS L2/3 operation context, which allows for preventing some identified risky scenarios. The underlying idea behind the developed control scheme was to make a step change on the LC control operation, by switching from a rudimentary passive control to a new paradigm that advocates for a supervised control-command which takes in consideration the dynamics within the LC zone as a whole. Besides its advantages in terms of safety, the developed architecture scheme makes it possible to dispense with train sensing devices, thus making getting

maintenance saving possible, as well as improving the system's reliability. Furthermore, this is perfectly in line with the increasing willingness to minimize track equipment so as to ensure installation and maintenance savings. In order to establish the LC control architecture, we have set up a formal framework which allows for expressing the various constraints to be ensured and we have illustrated how formal models and analytic techniques can be advantageously utilized for designing and validating control architectures for safety critical railway systems. Besides, the important debugging phase witnesses how developing such a control model can hide some fine features which are intractable without the support of automated checking tools. It is interesting to recall here that using such formal techniques is more and more recommended for the design, the verification and the validation of critical complex systems, particularly in railways (14). Although further setups still need to be undertaken before an actual implementation, the discussed contribution paves the way towards developing a control architecture which efficiently integrates LCs in the ERTMS/ETCS operation framework.

References

[1] A.W. Evans, Fatal train accidents on Europe's railways: 1980-2009, Accident Analysis & Prevention, vol. 43(1), pp. 391-401, 2011.

[2] European Railway Agency (ERA), Report on Railway Safety and Interoperability in the EU, 2020.

[3] K. Taylor, Addressing road user behavioural changes at railway level crossings, in Proceedings of the ACRS-Travelsafe National Conference, Brisbane, Australia, 2008, pp. 368–375.

[4] L. Khoudour, P. Feltz, D. Bertrand, M. Ghazel, M. Heddebaut, S. Collart-Dutilleul, Y. Ruichek, A. Flanquart, PANsafer Project: Towards a safer level crossing, The 11 th World Level Crossing Symposium Toward further improvement of level crossing safety (GLX'2011), Tokyo, 2010.

[5] S. K. Merz, Adamstown Level Crossing - Operational Review Report, http://www.transport.nsw.gov.au/sites/default/files/b2b/news/Adamstown-Level-Crossing-Review.pdf

[6] F. Coleman, Y. J. Moon, Design of gate delay and gate interval time for four-quadrant gate system at railroad-highway grade crossings, Transportation Research Record: Journal of the Transportation Research Board, vol. 1553, 1996, pp. 124-131.

[7] M. Ohta, Level crossings obstacle detection system using stereo cameras, Quarterly Report of RTRI, vol. 46(2), pp. 110-117, 2005.

[8] S. P. Lohmeier, R. Rajaraman, V. C. Ramasami, Development of an ultra-wideband radar system for vehicle detection at railway crossings, In 2002 IEEE Conference on Ultra Wideband Systems and Technologies, pp. 207-211, 2002.

[9] J. J. Garcia, J. Urena, A. Hernandez, M. Mazo, J. A. Jiménez, F. J. Alvarez, C. De

Marziani, A. Jiménez, M. J. Diaz, C. Losada, E. Garcia, Efficient Multisensory Barrier for Obstacle Detection on Railways, IEEE Transactions on Intelligent Transportation Systems, vol. 11(3), pp. 702-713, 2010.

[10] M. Li, G. Wu, S. Johnston, W. B. Zhang, Analysis Toward Mitigation of Congestion and Conflicts at Light Rail Grade Crossings and Intersections, California PATH Research Report UCB-ITS-PRR-2009-9, ISSN 1055-1425, 2009.

[11] Federal Railroad Administration, Office of Research, Development and Technology - Washing-ton, Engineering Design for Pedestrian Safety at Highway-Rail Grade Crossings, Technical report DOT/FRA/ORD-16/24, June 2016.

[12] FRA/Volpe Center Highway-Rail Grade Crossing Safety and Trespass Prevention Research Program, Federal Railroad Administration, Office of Research, Development and Technology, 2015 National highway-rail grade crossing safety training conference, 2015.

[13] M. Ghazel, Formalizing a subset of ERTMS/ETCS specifications for verification purposes, Transportation Research Part C: Emerging Technologies, Elsevier, vol. 42, pp. 60-75, 2014.

[14] http://www.shift2rail.org

[15] M. Ghazel and E.-M. El-Koursi, Two-half-barrier level crossings versus four-half-barrier level crossings: a comparative risk analysis study, IEEE Transactions on Intelligent Transportation Systems, vol. 15 (3) pp. 1123-1133, 2014.

[16] M. Ghazel, A Control Scheme for Automatic Level Crossings under the ERTMS/ETCS Level 2/3 Operation, IEEE Transactions on Intelligent Transportation Systems, vol. 18 (10) pp. 2667-2680, 2017.

[17] P. M. Merlin, A study of the recoverability of computing systems, PhD thesis, University of California, Irvine, CA, 1974.

[18] B. Berthomieu and M. Diaz, Modeling and verification of time dependent systems using time Petri nets, IEEE Transactions on Software Engineering, vol. 17(3), pp. 259-273, 1991.

[19] M. Diaz, les réseaux de Petri - Modèles fondamenteaux, Hermes, 2001.

[20] B. Berthomieu, P. Ribet and F. Vernadat, The tool TINA - Construction of abstract state spaces for Petri nets and time Petri nets, International Journal of Production Research, vol. 42(14), pp. 2741-2756, 2004.