Proceedings of the 2009 IEEE International Conference on Systems, Man, and Cybernetics
San Antonio, TX, USA - October 2009

Aspects of the Safety Analysis of an On-board Automatic Train Operation Supervisor

Gary A. Bundell
School of Electrical, Electronic & Computer Engineering
University of Western Australia
35 Stirling Highway, Crawley, 6009, WA, Australia
email: bundell@ee.uwa.edu.au

***Abstract*—In today's train operations the driver may no longer be the primary guardian of the safety of the train, that function being taken over by various forms of Automatic Train Protection (ATP) systems. What is left for the driver is still an important safety supporting function which is their capacity to review the set of train control actions that they intend to apply, and match those with the current state of the train and current external conditions. And as many in the industry would know, ATP systems are not always perfect. In Automatic Train Operation (ATO), where the driver is to be replaced, this residual safety function must be automated also. Where this becomes particularly important is in long heavy-haul trains where the driver's experience and the undesirability of relying on the emergency braking capability provided by the ATP system is a much more significant issue. This paper focuses on the safety analysis of a train control supervisor for ATO using timed Petri nets as the modelling approach.**

***Keywords*—safety analysis, automatic train operation, supervisory control, timed petri nets**

I. INTRODUCTION

The type of train to be automatically supervised is a heavy-haul iron ore carrying train, typically made up of two to three 4500 HP locomotives at the front and two at the rear when loaded, and about 240 ore cars, all up of about 2.4km in length and weighing just under 30,000 tonnes when fully loaded. Such trains are operated by Rio Tinto Iron Ore and BHP Billiton Iron Ore in the Pilbara region of Western Australia (a region that exports about a third of the world's requirements for iron ore). Currently these trains operate with a driver, but a successful feasibility study to replace the driver with a fully automated system at Rio Tinto Iron Ore has been completed [2]. The final automated system is planned to drive the train the full length of the mainline track (up to a maximum of about 420 km) and was expected to be operational by 2012 [22], although very recently has been suspended until ore prices sufficiently recover.

Some aspects of this project have historical links to a much earlier project [8] that aimed to provide the driver with on-board advice on the best driving strategy to use. The function of the human driver can be considered at three levels: generating appropriate control actions for the train, reviewing the state of the train and that those control actions meet the requirements for safe operation of the train, and finally looking out for internal and external indications of hazards to the train. This paper only focuses on the highest level function of the driver: the review of the state of the train and the intended control actions to ensure that when a human driver is replaced, this key safety-related function of the driver is maintained at an acceptable level.

In the context of train safety it is important to be aware that many modern train control systems operate with some form of automatic train protection system (ATP), and this system (often certified to a high safety integrity level) will ultimately take action to bring the train to a stop (usually by using a largely independent emergency braking system). For many types of train, application of emergency braking is a low risk operation that brings the train to a halt very quickly. Whereas for long heavy-haul trains, application of emergency braking is to be avoided if at all possible due to the additional wear and tear on the train, and it is one of the primary functions of the driver to avoid this being necessary. As a result of this situation, an automated on-board supervisor that replaces a driver must assume this safety-related function (albeit at a much lower integrity than the ATP system). As with a driver, an on-board supervisor needs to assist in further reducing the overall risk of operating the train. The problem to be solved therefore is how to demonstrate that an appropriate safety integrity level has been achieved using the applicable standards (see the discussion on this aspect in Section II) and using appropriate design and development methodologies.

The distributed nature of what could be termed 'supervisory operational control' in the overall safety of railway operations has previously been considered [3], specifically in the context of off-board train supervision, and the key point is that the human train driver and human train controller currently provide functions supporting safety at many levels.

II. APPLICABLE STANDARDS

The standards that are most relevant to the introduction of new equipment to a railway system are the so called "CENELEC standards" all of which are now also IEC standards: IEC 62425 [11], IEC 62278 [12] and IEC 62279 [13]. The origin of these standards in the area of safety requirements is early drafts of IEC 61508 [14] although there are some notable differences. An important common concept is the notion of Safety Integrity Level (or SIL) which can be interpreted in both quantitative and qualitative terms. An example of a notable difference is that the SIL associated with software safety requirements in IEC 62279 [13] is the same for

978-1-4244-2794-9/09/$25.00 ©2009 IEEE

SILs of 1 & 2, and 3 & 4 rather than all SILs having different requirements as in IEC 61508 [14].

It is beyond the scope of this paper to assess the contribution the driver makes to risk reduction in the current system, but let us assume that a SIL of 1 is to be assigned to the on-board train supervisor which is to replace the driver. Such an assignment means that the contributions of this subsystem in its safety-related functions to the overall system safety are limited by the provisions of the standard [11] to a tolerable hazard rate of 10^{-5}/hour.

III. A MOTIVATING EXAMPLE

We will consider a simple example that helps to set the context of the main issues involved and which has the key characteristics of the safety requirements to be met. If the terrain profile in driving a long heavy-haul train was mostly flat, then the challenge of driving such a train would be quite modest, but in the Pilbara region of the North-West of Australia lies a mountain range between the many mines and the port. Thus a train journey taking a typical journey (but in an abstracted and not-to-scale form) has an elevation profile something like Fig. 1.

Of note, a 2% down gradient represents an approximate acceleration of 0.2 ms^{-2} and assuming that the retardation available from a emergency brake application is about 0.5 ms^{-2}, a fully-loaded train travelling at 60 Km/h would take nearly a minute to come to a stop. For a maximum service brake application the same retardation force is not immediately available and there is usually a considerable delay of up to 60 seconds or so as the brakes progressively apply down the train. Managing the magnitude of the application and timing is an important issue in not only bringing the train to a safe stop but to do so in a way that leaves it in a low risk state and also at a preferred location. This requirement is illustrated in Fig. 2 which shows a low-risk region of operation (the single cross-hatched region) between engaging ATP (the double cross-hatched region) and the actual speed profile within that (the solid line). Also shown in the Figure are the two top-level hazards which need to be avoided in train operations: exceeding any speed restrictions (Hazard 1) and exceeding any Limits of Authority or LOA (Hazard 2).

Of additional note is the deliberate discretisation of the bounding velocity profile, which mostly has significance in the right-most braking curve region. The key idea here is that the system dynamics for this type of train dictate that the maximum possible Δv in 5 seconds is less than 4 Km/h so a system that meets the discrete profile constraints (shown as small dots on the linear bounding profile in Fig. 2) will also necessarily meet it in continuous time. As we shall see in what follows, it is fundamentally for this reason that a discrete-event model is all

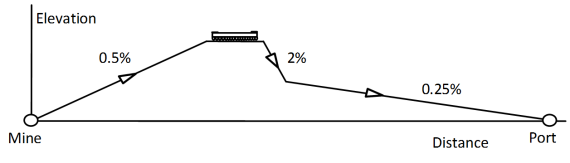

Figure 1. Elevation profile with approximate track gradients

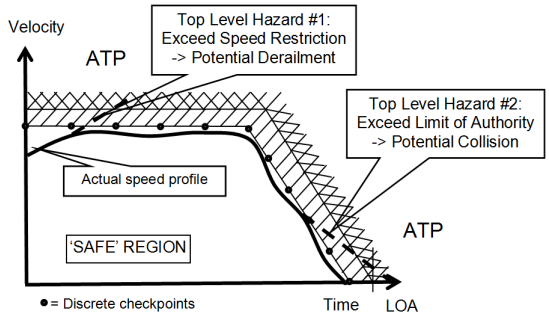

Figure 2. Speed profile and regions of operation with top level hazards

that is needed for verification of the safety properties of the system and a combined (or hybrid) model of the system is not necessary in this application.

IV. RELATED WORK

The research literature associated with the application of Petri Nets (PNs) to the modeling of safety critical systems can be traced back to the early work of Leveson & Stolzy [16] whose status is confirmed through an earlier version of that work being referenced in the guidelines for both standards [13][14]. Their work showed how PNs can be applied to modeling a simple railway crossing problem and the use of reachability analysis to identify 'unsafe states'. Although mentioning Timed PNs, their work only made limited use of temporal modeling for specification of the operation of a watchdog timer. There was little further work done on this approach until Goddard [10] used PNs (augmented with inhibitor arcs and condition places) for modeling a parking brake system. He also employed reachability trees for hazard analysis, and linked it to a more traditional failure modes and effects analysis (FMEA) approach. This work made no use of temporal modeling. Shortly after this Sacha [23] applied an extended PN model using transition variables and again used reachability trees to model the railway crossing problem.

After the abovementioned early work, Jansen et al. [15][17] worked on applying PN modeling techniques to the emerging European Train Control System (ETCS). Of note they were one of the first groups to realise the crucial importance of a much larger scale modeling and analysis tool to support this work, and they selected the (then named) Design CPN package [7]. While the above work was in progress, Padberg & Gajewski [20] again looked at the railway crossing example, but applied a more explicit temporal logic approach, and Colored Petri Net (CPN) models were also used employing the key idea of preserving the 'correctness' in transformation (in this case, the safety properties) of the models. Of particular interest is further work by Padberg, Schiller & Ehrig [21] that evaluated the approach to the CPN modeling of ETCS in [15][17], and was somewhat critical of the way in which hierarchy had been employed.

The most specific related work relevant to this current paper, is that of Meyer zu Horste & Schnieder [18] and also work by Einer, Slovak & Schnieder [9]. The first paper [18] describes a 'reference architecture' for modeling train control systems around a BASYSNET methodological framework. The

key idea here was to build a train control system from blocks, scenarios, processes and a top-most context level. It includes a breakdown of required functions in multi-train operations, such as train banking, shunting, and scheduling, and notes the common optimization requirements (of time, energy and train sequencing).

A companion paper [9] references the CENELEC standards in their original European Norm form, and uses the level crossing example showing how it can be mapped from a textual description through to a top-level system model. They employed an approximately-defined CPN type model at the top level, but usefully discussed failure modes of devices with the notion of different places carrying tokens for 'intact' or 'defective' operations of the device. They also discussed exceptions to normal behavior being modeled in the PN, but the only analysis requirement mentioned is liveness, with no focus on temporal properties.

Later, quite separate work by Monfalcone, Kaufman & Giras [19], identified that the Corridor Risk Assessment Model (CRAM) [24] and the PN modeling work of [17] was the "current state of the art for train safety models". There was also a claim made that neither of these approaches addressed system design level analysis of various "processor-based configurations".

A further development in the modeling of train control systems was the work by Berkenkotter et al. [4] in producing a hybrid type of UML-based model illustrated with an example of radio-based train control for stopping at level-crossings. This required management of the static velocity profile (speed restrictions) and the dynamic profile before stopping, and the key safety-critical objective being modeled was compliance with a target velocity curve.

The most recent work has been performed by Zimmermann & Hommel [26] who again used the ETCS system of a radio-based computerized control system (particularly the top-level 3, where all track side equipment is replaced and a moving block operation used). The train communications system (including movement authorities and protocols) was modeled using stochastic Petri Nets (SPNs) in the TimeNET package. In further work, Trowitzsch & Zimmermann [25] used transformations of UML state machines (using the UML RT profile) into SPNs.

In summary, in the last 20 years since the initial work of Leveson & Stolzy [16] there has been a modest amount of research on the modeling of train control systems with safety specifications, and much less on the serious application of TPN models to analyze and verify appropriate safety properties. Given the earlier mentioned recommendation on the use of TPNs for modeling in the relevant standards (particularly [13], where it is highly recommended at all SIL levels) this is surprising, although it is possible than little of this work has yet made its way into the open literature.

V. BUILDING A MODEL

There are a number of possible approaches to modeling the discrete-event properties of a system such as the one introduced in Section III, but the one that is not only specified as highly recommended in the relevant standards [13], and also supported by substantial research in the literature [10][15][16][20][23], is adopted here also. A Timed Petri Net [5][7] based model is able to adequately capture the concurrent temporal event-based behavior of both the physical system and the controlling software, and through a reachability analysis, can be used to verify the required safety properties of the on-board train supervisor's behavior.

Following a similar discretisation approach to that described in Section III, but in a spatial sense, the train itself may be divided up to approximate the distributed braking behavior of up to 240 ore cars, e.g. by dividing it into 12 segments of 20 ore cars each. Fig. 3 below shows a top level CPN model which groups together the model of the driver and locomotive as the first segment and the brakes system of the ore-cars as all the other segments (only two of these are shown in Fig. 3).

We are using CPNTools [7] primarily for its temporal and hierarchical modeling capabilities, and token 'color' (i.e. type or class) is not being used (for the deliberate reason that we would like the subsequent reachability analysis to be as direct as possible and not require unfolding of a type or class hierarchy). Also, while 'color' is a powerful additional modeling component, it isn't necessary for the type of models required.

We are also quite deliberately avoiding the use of 'inhibitor arcs', 'guards' or other advanced modeling features of high-level Petri nets in support of a direct (and ultimately bounded and deterministic) reachability analysis required for safety

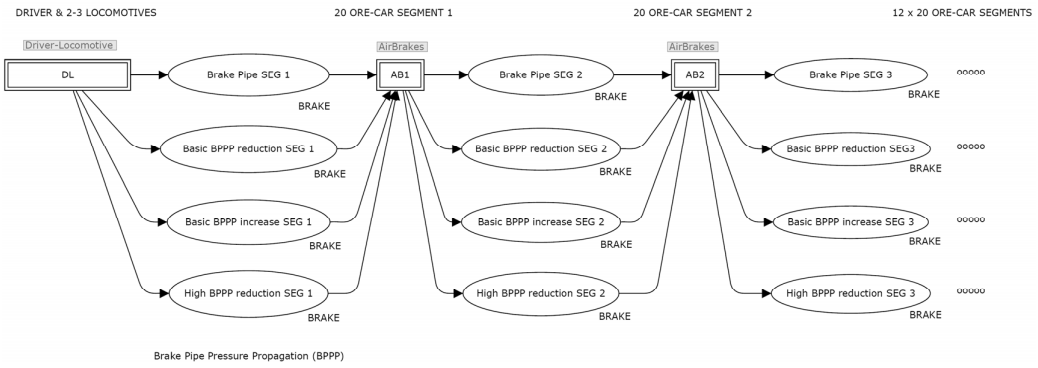

Figure 3. Top-level discrete-event train model

property determination.

Apart from the main segments of the model described earlier, the other feature of the model is the highly simplified representation of the 'signaling function' of the brake pipe. Rather than use a continuously variable air pressure (say in KPa) we are using a charged signal, basic reduction signal, basic increase signal, and a high reduction signal. The basic reductions and increases fall into the typical service brake range (e.g. 100 KPa) and the high pressure reduction is an emergency application (e.g. more than 300 KPa). We don't bother modeling recovery from an emergency brake application as that isn't time-critical. Other intermediate levels of braking could easily be modeled, but for the purposes of this example it is kept as simple as possible.

If we turn now to the two main segments of the model, Fig. 4 shows the first Driver/Locomotive segment (Block DL in Fig. 3), which describes a simple scenario of the driver applying the service brakes after 20 seconds, releasing them after 20 seconds, and then applying the emergency brakes a further 20 seconds after that (i.e. something must have gone wrong for the driver to need to follow this sequence). The only extra details in the locomotive model are: the initial charging of the brake pipe (which introduces a small delay), delays for brake applications and releases, and the operation of an equalising reservoir on the locomotive that requires charging.

Fig. 5 shows the brake model segment (Block AB in Fig. 3). It is a highly abstracted form of the model in one ore-car and the delays are appropriately scaled to correspond to a 20-ore car segment. The main features of the brake model are the triple-valve and its three operational and single initial states, the emergency and auxiliary reservoirs, and the brake cylinder itself. Of importance are the propagation delays, the most notable being the 5 seconds delay (250 msec x 20) for each ore car segment on brake pipe air pressure 'signals'. There are additional smaller delays for the valves and cylinders in the segment. This representation is based on the generic Westinghouse train air brakes model [6], but its key features are common to all train air brakes systems to this day. For the purposes of fitting these diagrams into a reasonable space, we restrict the model here to two ore-car segments only (in practice there would be 12 or potentially more).

VI. Analysis of the Model

Given this model, the next stage is to perform a reachability analysis, which in CPN Tools is performed with an Occurrence Graph. As shown in Fig. 6, the graph consists of 44 states, with a part of the final state token occupancy table also shown (all intermediate states in the tree can also be examined in CPN Tools). In the final state, which is arrived at after 66.4 seconds, we have an emergency brake application fully applied, and the brake cylinders extended in all ore-car segments (which is the primary safety state we are looking for from such a simple analysis). The model contains additional structural information that can be used to show well-behavedness properties derived from the reachability analysis (such as liveness and boundedness, but not reversibility in this case), and it also has more detailed timing information which can be useful for further temporal analysis.

It should also be noted here that CPN Tools (in the currently released V2.2.0 version used in this work [7]) has an acknowledged fault [7] when modeling temporal behavior in TPNs, i.e. token removal from decision places is non-deterministic and does not take into account time delays in the output transitions. This fault shows up clearly in the resulting occurrence graphs and the 'workaround' is to replace the timed non-deterministic decision structure from the model. Due to the avoidance of this structure in all the models used here, this fault hasn't had an impact, but in general if it cannot be removed, only additional (and thus redundant) behavior would be represented in the occurrence graph and no system behavior would be unmodeled.

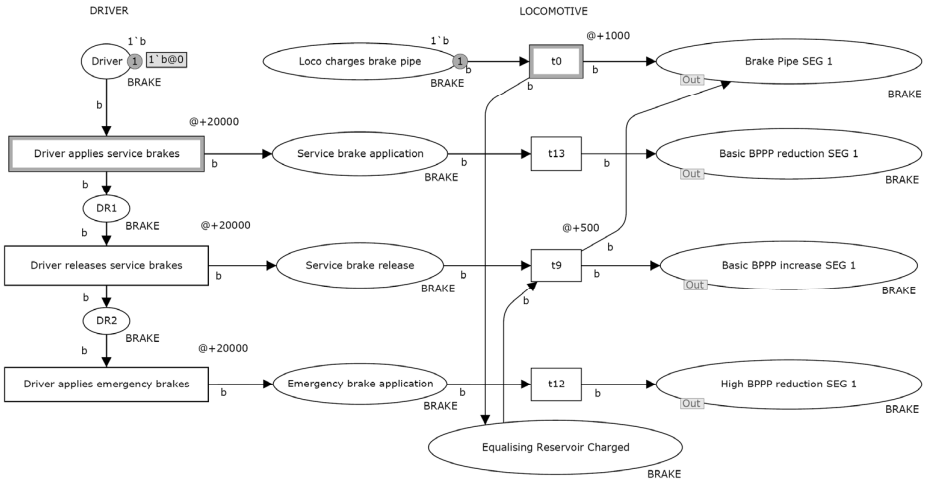

Figure 4. Simplified CPN model of typical driver braking actions and the corresponding locomotive brake signals (Block DL in Fig. 3)

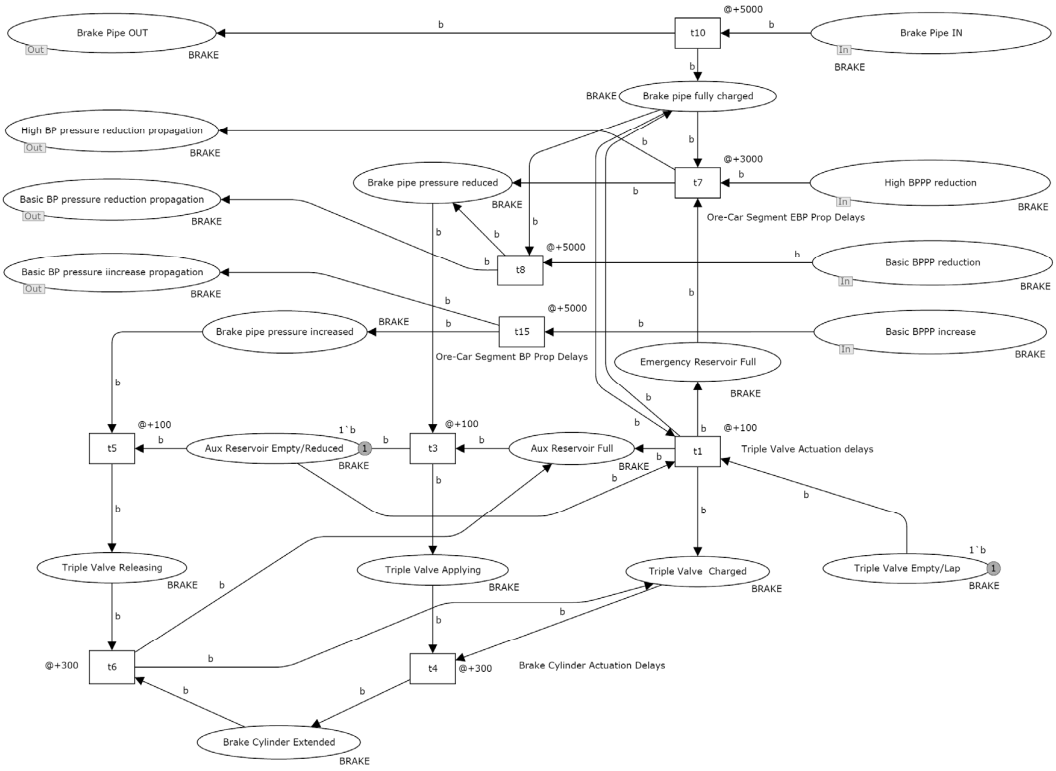

Figure 5. Simplified CPN model of an ore-car brakes system (Block AB in Fig. 3)

VII. REFINING THE MODEL

Now, although it is important that we have an analysis approach which allows ready confirmation of all the timing of key events, recollection of the two top-level hazards from Fig. 2, reminds us that for the specific problem here, we want to show that the on-board train supervisor is able to maintain operation within the 'safe region' using only service brakes. To apply this analysis approach we need to discretise the state space, and to illustrate this as simply as possible we take the situation where we are trying to maintain the speed within a limit of 70 Km/h. Time is indexed in 5 second intervals and brake applications are confined to three bands from 0 to 200 KPa. Let us suppose the train is on a 1.5% downgrade at an initial speed of 60 Km/h. As Fig. 7 shows, with no brake applications the speed quickly increases above the track limit which becomes potentially hazardous.

A brake application of 200 KPa is enough to quickly reduce the speed. Considering Table I, we can see that speed can be discretised into 3 regions characterised by five simple rules relating brake pressure (p), time (t) and speed (v):

1. $p = 0 \ \& \ t >= 20 \rightarrow v > 70$
2. $p = 0 \ \& \ t <= 15 \rightarrow v < 70$
3. $p >= 100 \rightarrow v < 70$
4. $p = 200 \rightarrow v <= 60$
5. $0 <= p <= 100 \rightarrow v > 60$

A simple supervisor safety-related function would thus be to respond to the speed exceeding 70 Km/h by applying a brake application of 200 KPa (which is excessive, but 100 KPa isn't adequate so it is the only choice in this simplified example). Because of the earlier mentioned limitation in CPN tools in temporally non-deterministic simulations, Fig. 7 shows a TINA TPN [5] implementation of the discretised model of the braking behavior of the system, and the simple supervisory function required to prevent the overspeed situation.

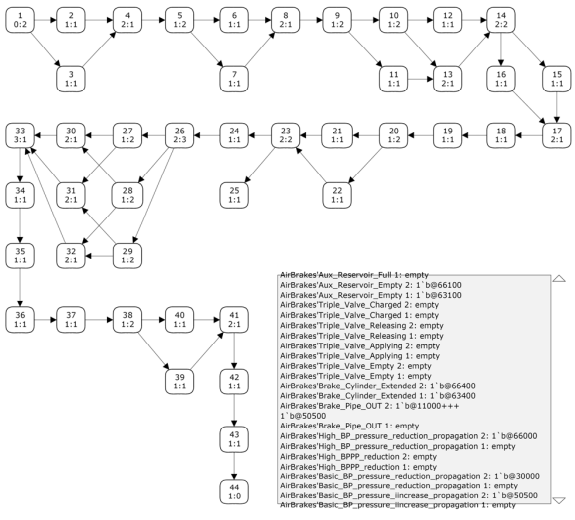

Figure 6. Occurrence Graph for the CPN train model

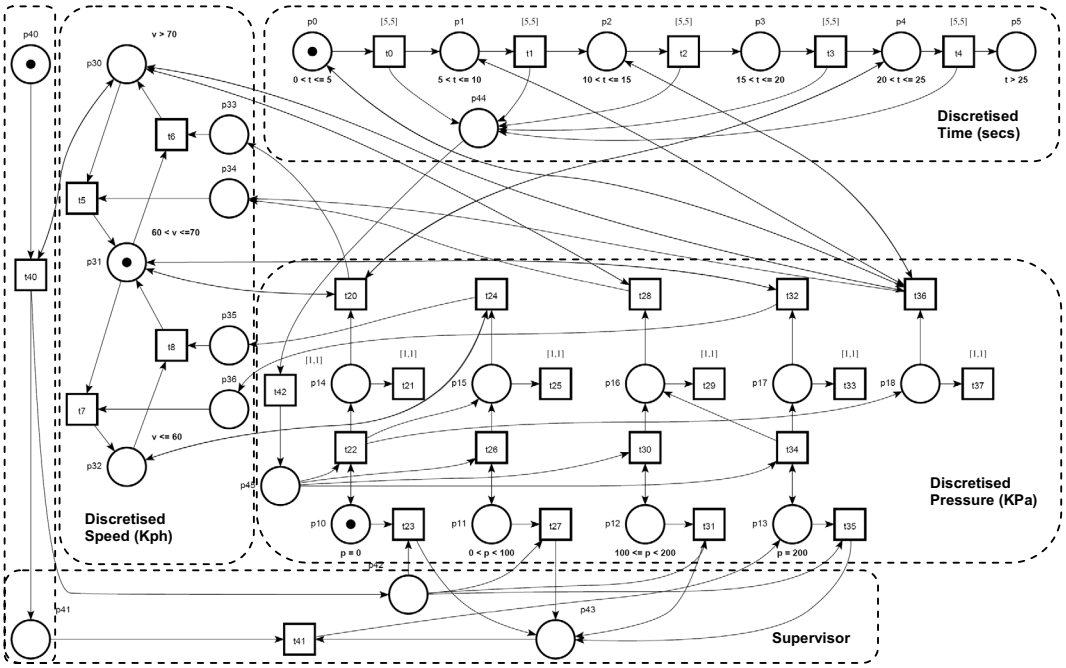

Figure 7. Simple PN model of the discretised braking behaviour of the train

A reachability tree can be drawn for the PN model which is shown in Fig. 8 (TINA provides a listing of all reachable states but not a diagram as such). In fact, the tree is produced for two cases, the first where no supervisory controller is enabled (with place p40 unmarked) and where there is a supervisory controller enabled (with place p40 marked). For the former case, when a token reaches place p30, which corresponds to the hazard state of v > 70 Km/h, it remains in this state. But with the latter case of the supervisory controller enabled, the hazard state is removed within 5 seconds of operation. Of course, this is a very simple example, but it clearly illustrates the approach to be taken in the more complex situations. A more realistic level of discretisation would be to use a Δv of 5 Km/h and 20 KPa brake applications. A full model is currently under development based on this approach which relies on the hierarchical modeling capabilities to keep the complexity manageable.

A final example to consider is how we would represent the braking curve part of Fig. 2 using the same approach. As shown in Fig. 9, speed is discretised from 0 Km/h to 70 Km/h and time between 0 and 180 seconds. The structure of the model is such that any violation of the braking curve (i.e. an excessive speed at a time when it isn't expected) results in a token in place p100 (and such a marking is very evident from the reachability tree). Fig. 9 shows the braking curve model and a very simple supervisor action to ensure the speed is reduced sufficiently quickly to comply with the braking model limits. The next stage of model development is to upgrade the model of the braking system to a form similar to that shown in Fig. 3 to Fig. 5 and to incorporate additional aspects of the on-board train supervisor structure as implemented.

TABLE I. DISCRETISED BRAKE APPLICATIONS, TIME AND SPEED

	Time (Seconds)					
Brake Application (KPa)	0	5	10	15	20	25
0	60.00	62.65	65.29	67.94	70.58	73.23
100	60.00	60.40	60.79	61.19	61.58	61.98
200	60.00	58.15	56.29	54.44	52.58	50.73

60 < v < 70 Kph
v > 70 Kph
v ≤ 60 Kph

In addition to a timed-based simulation of execution of the TPN, a reachability analysis is used to show that the braking curve constraints can be met by the on-board train supervisor. It then remains to show through design review, code walkthrough and testing of the actual supervisor that it faithfully implements the function and safety properties of the modeled supervisor.

VIII. CONCLUSIONS

The purpose of this paper, apart from reviewing the work in the last two decades on safety analysis of train control systems, has been to develop an approach using TPNs to model and analyze two of the key safety properties required of a long heavy-haul train. Modeling such a train requires specific attention to be given to the distributed brakes model and the safety functions of an on-board train supervisor that must work with a traditional ATP system when the driver is replaced. This requires an on-board train supervisor of low safety-integrity (relative to ATP), but it still has to be well defined and verifiable to the extent specified by the relevant standards [11][12][13]. It was also suggested in this paper that a hybrid approach (combining continuous-time and discrete even behavior) isn't required for the verification of safety properties, and further that such an approach (as has been seen in the literature) makes the use of a reachability type analysis far

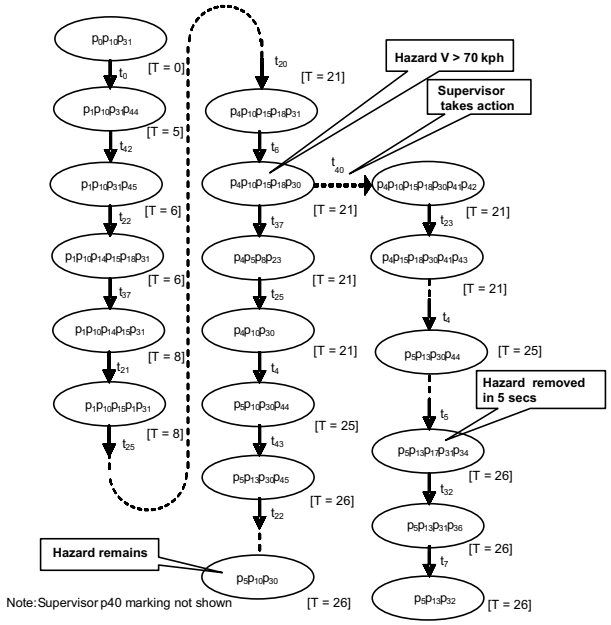

Figure 8. Reachability tree of the simple PN model of train braking

more difficult (if even still possible, as certainly the tool to perform this analysis becomes much more specialized).

Further, the approaches in the literature that seek to replace the lowest levels of the model with algebraic specifications also have little to recommend them since they similarly suffer from both difficulty of analysis and loss of the considerable visualization benefit of the PN graphical form. Similarly, with the various extensions of PN type models; particularly variables, inhibitor arcs, etc. It is the author's view that the clearest modeling and analysis environment is provided by simple TPNs, but then hierarchical modeling support is vital to manage the resulting complexity of the models produced. Of course, basic computational theory indicates that there is an inevitable tradeoff between ease of modeling (e.g. expressiveness) and difficulty of analysis (e.g. reachability, liveness, boundedness, etc) of the resulting models. It is also the author's view that HTPNs provide an intermediate balance that maintains the full analysis capabilities of PNs, although as mentioned there are some limitations with some current modeling tools (which could be expected to be overcome in due course).

Further work in this research direction is to develop a complete HTPN model of the automated on-board train supervisor for a long heavy-haul iron-ore train as an aid to demonstrating that the on-board train supervisor achieves the required safety integrity level. To support that aim, additional safety requirements have to be drawn into this modeling framework. For example, in addition to the two top-level hazards described earlier, the on-board train supervisor has secondary safety requirements, such as stopping the train at particular 'lower risk' locations (which consequently require certain power settings to be applied before braking action is taken), and further that certain control sequences must not be applied as they could potentially separate the train into smaller segments which may increase the risk of a derailment. The modeling of these situations is not inherently difficult in the HTPN environment, but the appropriate structuring of models and subsequent analysis has yet to be done. It is also hoped that a dedicated HTPN modeling tool does not need to be developed for this work, but a previous effort [1] may need to be revisited and re-used in this project.

ACKNOWLEDGMENTS

This work was supported in part by a UWA research contract funded by MRX Technologies, 24 Drummond Place, West Perth 6007, WA, Australia. The author would like to particularly thank Dr Jim Blair and Ross Norman of MRX Technologies, and Rob Wasley of Rio Tinto Iron Ore, Rail Division.

REFERENCES

[1] Ang, W.L. & Bundell, G.A., "Design and Analysis Using a Combined TAD-HTPN Real-Time System Modelling Approach", The 4th Australasian Conference on Parallel and Real-Time Systems, Newcastle, Australia, Sep 29-30, 1997, pp 250-261.

[2] Australian Mining, "Automated train driving", 24 Sept 2007, http://www.miningaustralia.com.au/articles/Automated-train-driving_z74718.htm.

[3] Belmonte, F., Boulanger, J.L., Schon, W. & Berkani, K. "Role of supervision systems in railway safety", COMPRAIL 2006 Conference, Prague, Czech Republic, 10-12 July 2006, pp 129-138.

[4] Berkenkötter, K., Bisanz, S., Hannemann, U. & Peleska, J., "Executable HybridUML and Its Application to Train Control Systems", Lecture Notes in Computer Science, Springer, Vol. 3147, Integration of Software Specification Techniques for Applications in Engineering, 2004, pp 145-173.

[5] Berthomieu, B. & Vernadat, F., "Time Petri Nets Analysis with TINA", Proc. 3rd International Conference on the Quantitative Evaluation of Systems (QEST'06), 2006, pp 123-124.

[6] Conner, P., "Air Brakes", Railroad.net, http://railroad.net/articles/railfanning/airbrakes/

[7] CPN Tools (previously known as Design CPN), http://wiki.daimi.au.dk/cpntools.

[8] Duncan, I.B., Winch, K.M. & Bundell, G.A., 'Driver Assist - Microprocessor Technology to aid in the Scheduling of Trains', COMPRAIL 1987 Conference, Stuttgart, Germany, July 1987, pp 133-148.

[9] Einer, S., Slovak, R. & Schnieder, E.; "Modeling train control systems with Petri nets - an operational specification", 2000 IEEE International Conference on Systems, Man, and Cybernetics, Vol. 4, 8-11 Oct. 2000, pp 3081-3086.

[10] Goddard, P.L., "A Combined Analysis Approach to Assessing Requirements For Safety Critical Real-Time Control Systems", 1996 Proceedings Annual Reliability and Maintainability Symposium, pp 110-115.

[11] IEC 62425:2007 Railway Applications - Communication, signalling and processing systems - Safety related electronic systems for signalling

[12] IEC 62278:2002 Railway applications - The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS)

[13] IEC 62279:2002, Railway applications – Communications, signalling and processing systems – Software for railway control and protection system

[14] IEC 61508-1:1998, Functional safety of electrical/electronic/programmable electronic safety-related systems, Part 1: General requirements

[15] Jansen, L., Meyer zu Hörste, M. & Schnieder, E., "Technical Issues in Modelling the European Train Control System (ETCS) Using Coloured Petri Nets and the Design/CPN Tools", CPN'98 Workshop on Practical

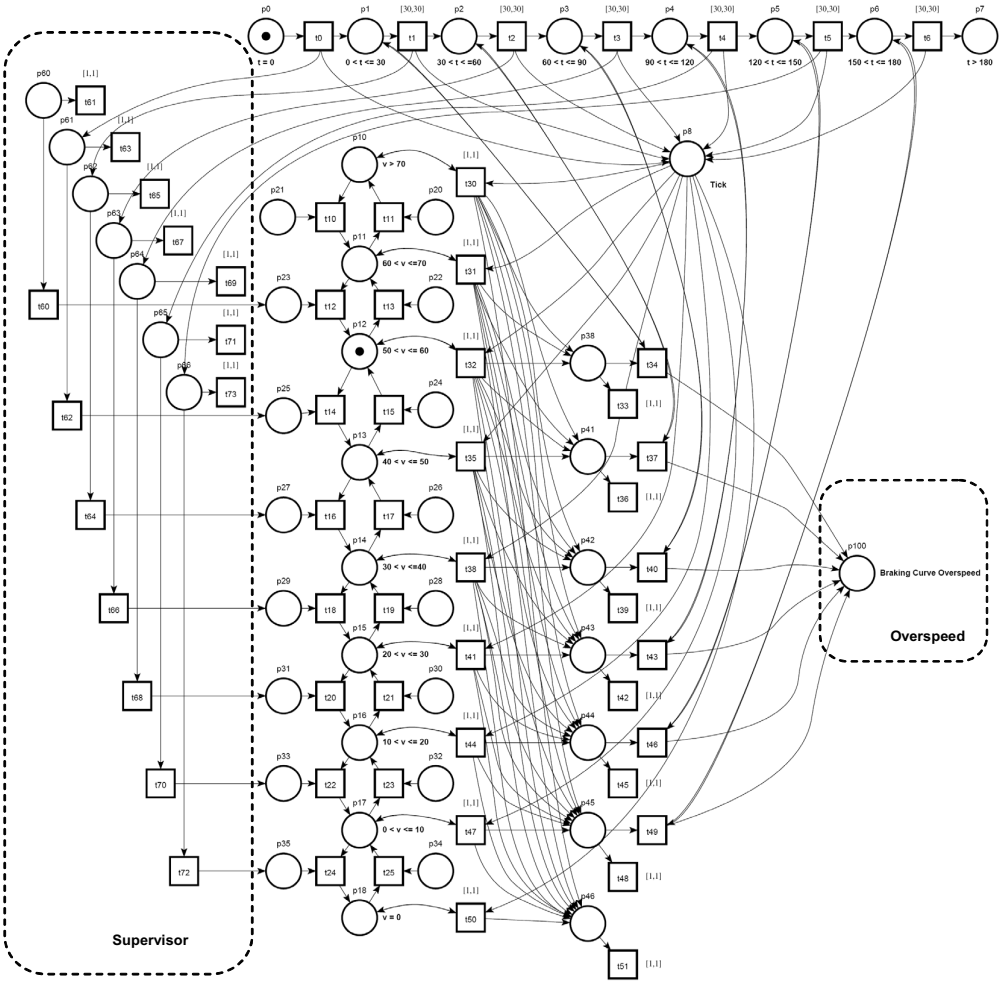

Figure 9. Extended PN model of the discretised braking behaviour of the train

Use of Coloured Petri Nets and Design/CPN, June 10-12, 1998, Aarhus, Denmark, pp 103-115.

[16] Leveson, N.G. & Stolzy, J.L., "Safety Analysis Using Petri Nets", IEEE Transactions on Software Engineering, Vol. SE-13, No. 3, March 1987, pp 386-397.

[17] Meyer zu Horste, M. & Schnieder, E., "Formal modelling and simulation of train control systems using petri nets", FM'99 World Congress on Formal Methods in the Development of Computing Systems, Lecture Notes in Computer Science, Vol. 1709, Springer-Verlag, 1999, p 1867.

[18] Meyer zu Horste, M. & Schnieder, E.; "Modeling train control systems with Petri nets - a functional reference architecture", 2000 IEEE International Conference on Systems, Man, and Cybernetics, Vol. 4, 8-11 Oct. 2000, pp 3207-3211.

[19] Monfalcone, M.E., Kaufman, L.M. & Giras, T.C., "Safety Modeling of a Direct Traffic Control (DTC) Train Control System Using the Axiomatic Safety-Critical Assessment Process (ASCAP)", 2001 Proceedings Annual Reliability and Maintainability Symposium, 2001, pp 352-357.

[20] Padberg, J. & Gajewski, M., "Rule-based refinement of Petri nets for modeling train control systems", IFAC Conference Control Systems Design, Bratislava, Slovakia, June 18-20, 2000, pages 299-304.

[21] Padberg, J., Schiller, P. & Ehrig, H., "New Concepts for High-Level Petri Nets in the Application Domain of Train Control Systems", Proc. Vol.2, 9th IFAC Symposium on Control in Transportation Systems 2000, pp 153-160.

[22] Railway Gazette International, "Rio Tinto to go driverless", 19 June 2008, http://www.railwaygazette.com/news_view/article/2008/06/8554/rio_tinto_to_go_driverless.html

[23] Sacha, K., "Safety Verification of Software Using Structured Petri Nets", Lecture Notes in Computer Science 1516, 1998, pp 329-342.

[24] US Department of Transportation, Federal Railroad Administration, "Case Studies in Collision Safety", Volumes 1 & 2, Oct. 1998.

[25] Trowitzsch, J. & Zimmermann, A., "Using UML state machines and Petri nets for the quantitative investigation of ETCS", Proceedings of the 1st international conference on performance evaluation methodologies and tools table of contents, Pisa, Italy, 2006.

[26] Zimmermann, A. & Hommel, G., "Towards modeling and evaluation of ETCS real-time communication and operation", Journal of Systems and Software, Vol.77, Issue 1, July 2005, Pages 47-54.