TRAIN DRIVER AUTOMATION STRATEGIES TO MITIGATE SIGNALS PASSED AT DANGER ON SOUTH AFRICAN RAILWAYS

J.H. van der Merwe\textsuperscript{1*} & B.P. Sunjka\textsuperscript{2}

\textsuperscript{1,2}School of Mechanical, Aeronautical and Industrial Engineering
University of the Witwatersrand, South Africa
\textsuperscript{1}jhvdmerwe@gmail.com, \textsuperscript{2}Bernadette.sunjka@wits.ac.za

ABSTRACT

Train derailments or collisions have the potential to result in catastrophic loss of life and/or destruction of property. Ever higher demands for train density (i.e. trains per hour for a given section of track) as well as the catastrophic results when accidents do occur have given rise to the development of railway signalling systems as mitigation measures.

Signals Passed At Danger (SPADs) refers to when a train driver passes a stop signal without authority and is one of the typical causes of such accidents resulting in significant damages reported within Transnet Freight Rail (TFR) in recent years. Studies have shown human train driver error and violation of signals to be a significant cause of SPAD events.

This study investigated the application of train driver automation as a mitigation measure against SPADs within the South African railway environment in general and TFR in particular. The study was qualitative in nature, following a model development methodology and used in-depth, semi-structured interviews with railway signalling engineers for data collection. The primary goal was defined to be the development of a train driver function automation method that could be considered the most appropriate within the TFR operational environment.

The study determined the most appropriate method to be that of having a human driver with technical supervision. In this arrangement, the human driver could remain in his conventional role of driving the train but with a technical supervision system superimposed that automatically intervenes if a train driver exceeds his movement authority (e.g. Automatic Train Protection or ATP). This approach mitigates many of the costs imposed by human failure associated with SPAD events, yet retains the value of human flexibility which is especially useful under abnormal circumstances.

*Corresponding author
1. INTRODUCTION

Since its construction in the 1860’s, the South African railway network has grown to roughly 23 273 route kilometers [19, 26, 28]. Of the major South African railway operators, Transnet Freight Rail (TFR), Metrorail and Gautrain, TFR is the most prominent, representing 20 953 route kilometers of infrastructure ownership [26] and 60.5% of train traffic - 73.2 million train kilometers registered on average, annually, for the period 2013 to 2016 [20,21]. TFR railway infrastructure is located in both urban and rural areas and its operational control systems facilitate both freight and passenger trains [18], causing the TFR environment to best represent the South African railway context as a whole.

Railway transportation concentrates large quantities of people or goods on networks between various destinations. Inherent in this method of transportation also lies its great weakness - train derailments or collisions which have the potential to result in catastrophic loss of life and/or destruction of property. The 4490 operational safety incidents reported over the period 2013 to 2016 resulted in 1845 injuries, 461 fatalities and R469 964 458 in direct economic losses (annual averages) [21]. Ever higher demands for train density (i.e. trains per hour for a given section of track) as well as the catastrophic results when accidents do occur, have given rise to the development of railway signalling systems as mitigation measures [22, 25].

While the South African Railway Safety Regulator regulatory framework distinguishes between several categories of operational incidents [21], Signals Passed At Danger (SPADs) is the subject of this particular study. Railway signals, most often taking the form of traffic-lights located next to the railway line, are used to coordinate train traffic and protect train movements by communicating to train drivers their current movement authorities. In Figure 1, train B has received a proceed signal (Sig Y) to move onto the top line while trains A and C are ordered to stop by signals X and Z. These signals, and the drivers obeying them, are the only things protecting train B from a possible collision.

![Figure 1 Signalling train movements](image)

Signals X and Z are said to be “at danger” (meaning stop) and an incident where a driver passes such a signal is called a Signal Passed At Danger or SPAD [7]. SPADs are considered the most serious precursors to railway accidents ascribable to operator error [10]. The average number of unauthorized movements, including SPADs, reported on South African railways for the period 2013 to 2016 is 102.7 (annual average) or 1.4 SPADs per million train kilometers traveled (normalization parameter) [20, 21]. This compares quite favourably to Australia at 1.5 [16] but less favourably to Great Britain at 0.5 [13, 14, 15] for the same period, illustrating that South African SPAD levels are not especially high. Yet, of the top five most costly incidents reported for 2014/15, three were related to train handling (associated damages R93 million) with the most costly incident directly attributed to a SPAD (Maputo train-on-train collision – R56 million) [20]. These numbers indicate that while SPADs are not the most common incidents, the associated costs when they do occur can be relatively high, presenting a significant risk.

The Independent Transport Safety Regulator (ITSR) body within the New South Wales Government in Australia, concluded that the causes of SPADs generally include technical deficiencies associated with rolling stock or infrastructure but also driver error and violation of authorities [7]. Driver errors and violations typically include unsafe actions by the train crew such as the misreading of signal aspects, disregard for cautionary signals, incorrect braking technique, failure to communicate correctly and a range of external and internal distractions. The ITSR also includes organizational factors, such as poor safety culture, poorly designed procedures and inadequate monitoring or supervision, as contributors to such violations.

The study, therefore, proposed to investigate the application of train driver automation as mitigation to SPAD incidents in the South African railway environment in general and TFR in particular.
2. LITERATURE REVIEW

2.1 Strategies and countermeasures in SPAD risk management

Theeg & Vlasenko [25] describe the functions of train protection and control systems, as falling into three categories i.e.

- cab signalling functions that constitute driver warnings and information displays located in the train cab and that typically include audible signal warnings, visual repetition of track side signals and dynamic speed information;
- supervision functions that constitute the monitoring of train conditions and driver behavior that typically include checks in driver ability, attentiveness and compliance with speed limits; and
- intervention functions that constitute automatic interventions that typically include forced-response driver warnings, disabling of traction power and the application of train service or emergency brakes, to slow the train or bring it to a complete standstill.

Based on a study performed in Australia and New Zealand, Naweed et al. [12] defined the two general categories of formal countermeasures and informal strategies to mitigate SPAD risk in train driving. Formal countermeasures typically include forced-response devices that promote driver awareness to SPAD risk (Automatic Warning System - AWS) as well as automatic intervention systems (Automatic Train Protection - ATP). Informal strategies focus on the driver’s intention to drive safely. These strategies are created by the drivers themselves to aid them in safely executing their duties - an exercise that can in and of itself be considered safety awareness or safety culture. According to Naweed et al. [12], these strategies became more important as systems like the AWS and ATP are increasingly not used as intended. Some drivers reported that they sometimes turn down the volume of the AWS system, considering it a distraction, even though such an action was against policy. Others reported using the ATP system as a general method of monitoring speed and not as a safety warning device.

The strategies identified, which were grouped as specifically applying to the context of service delivery or the context of the driver-signal dynamic were,

- **Assessment strategies** that focus on the driver’s own assessment of the train he is driving and the driver monitoring of his own fitness to drive safely [12]. The first entails the personal assessment by the driver of the state of the train he is driving. This would include knowledge of potential mechanical issues such as braking dynamics that may affect train handling. The second strategy entails the driver’s honest self-monitoring of his levels of emotional distraction and fatigue and reporting concerns about his fitness to drive prior to starting his shift.

- **Task prioritization strategies** that include the conscious decision to focus on tasks considered imperative to safe driving and the postponement of competing tasks [12]. A typical example would be ignoring an incoming call from the controller whilst navigating a difficult section in the route. When confronted with time table pressure, experienced drivers would consciously prioritize safety.

- **Automatic-attention strategies** that are built around cognitive processes and awareness strategies to assist drivers in automatically registering signals and changes in signals [12]. A typical example would be when a driver observes a signal switching from clear to caution, where that driver would then “turn on a switch” [12] in his head helping him to focus on the signal state and changes in that state. This becomes much more important in demanding situations.

- **Behavioral strategies** that include token actions that drivers devise as aids to help them overcome sighting restrictions, retain signal awareness and act as reminders during station dwells [12]. Such actions include consciously setting the direction switch to the neutral position during station dwells, or physically standing up in the cab when a caution signal is encountered.

To apply operator automation as a mitigation strategy in SPAD incidents in a South African railway context, the following areas of literature pertaining to train driver automation are explored:

2.2 Fundamental challenges to train driver automation

There are fundamental challenges or practical limitations to the concept of operator automation that should also be considered. These include certain ironic circumstances that have to be confronted when considering operator (train driver) automation as well the additional roles that train drivers fulfil above that of train control.
2.2.1 The ironies of automation

Bainbridge [1], a seminal author on the topic of operator automation, discusses the ironies faced by the system designer aiming to eliminate the operator from a control system due to his perceived unreliability or inefficiency. Bainbridge [1] considered it ironic that this same designer cannot control the errors that he himself introduces into the design of the automatic control system (designer unreliability). The operator then tends to end up with an arbitrary set of tasks that could not be easily or practically automated but that are also not really suited to the abilities of the operator (designer inefficiency). These tasks can generally be reduced to the categories of monitoring of the automatic system for correct operation and the intervention or “taking control” in the case of actual system failure. Bainbridge [1] suggested that if an operator is required to take control of a process and stabilize it, a certain measure of manual control skill is required. The same applies to fault diagnosis underpinning judgements on process shut down or recovery actions. Such judgements and actions require a certain measure of cognitive skill.

The manual control skills required to control a complex process can take a long time to master and deteriorate fairly quickly if not practiced regularly. This is evidenced by the fact that experienced operators tend to make step changes or transitions more smoothly, quickly and with fewer actions than less experienced operators [1]. More experienced operators tend to demonstrate an insight or intuition into what the effects of their actions will be. Contrary to this, inexperienced operators rely more on feedback and correction - a process that can be slow and result in significant oscillation or “back and forth” action. At the same time it will be more difficult for an inexperienced operator to be able to judge if the feedback received is the result of poor driving or system failure. It may require a very skilled operator to take over to cope without relying on the system. Train driving can be considered a good example of such a complex process. The driver has to adjust and control the speed of the train - a vehicle that has a lot of inertia and is, therefore, relatively unresponsive to his control actions. At the same time, the driver has to adjust for changing speed restrictions, keep to a strict time table, drive economically and avoid hazards [1].

The cognitive skills required, can be categorized into categories of “long-term knowledge” and “working storage”. Long-term knowledge represents the methods and strategies developed over time, while engaged in the control of a process [1]. These methods and strategies are developed during the long run performance of control actions, considering the feedback and retaining what works and works well while rejecting those methods that work less well or not well at all. Unfortunately, this knowledge cannot be acquired without practice and deteriorates if not practiced [1]. Working storage represents knowledge about the current state and behavior of the process on a given day. A train driver may have to adjust to driving a different kind of train or a train with a different makeup affecting the handling. There may be workmen on the track this week or line of sight may be affected by the weather resulting in the driver adjusting his approach to driving. This kind of knowledge will not be available to the operator when control has to be taken in the moment of need [1].

Bainbridge [1] also suggests that before relegating the role of the operator to that of only monitoring an automated process, it should be remembered that the operator was to be replaced by the automatic system because he was perceived to be inferior at the control task to that very same automatic system. Now the operator will be required to only monitor and judge if the automatic system is working effectively. The irony of the situation is again evident when considering the monitor has to remain vigilant for an abnormality or failure event that rarely occurs. Owing to the fact that human operators are not always competent at this, they tend to rely on the alarm system to highlight abnormalities. This prompts us to ask: Is the alarm system working correctly and how should the monitor detect alarm system failure? This seems to be an impossible task [1]. It is also important to consider the impact the job of monitoring has on the operator’s attitude. It can easily seem like a job requiring very little skill but a lot of responsibility. It has been shown that such circumstances are conducive to low job satisfaction, high stress, poor health and can also lead to increased error rates.

Even after being reviewed by Baxter et al. [2] thirty years after first publication, examples of Bainbridge’s ironies [1] were found to still be prevalent and are expected to persist for some time to come.

2.2.2 The hidden roles of the train driver

In a study by Karvonen et al. [9] on the challenges presented in the full automation of the Helsinki Metro, the point was made that there is more to the train driver than basic train control. The case is presented that when the Helsinki Metro operation is considered as a whole, the driver is responsible for operating the train, taking care of passengers, observing events outside the train and acting positively in exceptional situations.

The driver’s position in the train cab provides him with a direct view of the track, stations, platforms and passengers while operating the train. This places him in a unique position to anticipate, observe, interpret and
react to events in that environment. Some of these events may require a speedy reaction such as when an obstacle is observed on the track ahead or when intruders or vandals are detected inside the security fence – observations and reactions that may prove difficult if performed from a remote location [9].

There are also certain tasks that are fairly trivial for a human being to perform but that can be extremely difficult for an automatic system to perform [9]. When considering the design of safety critical systems, it should be remembered that computers excel only at repetitive, basic tasks, and not at complex problem solving. A typical example of this limitation is passenger care. Passengers are independent actors whose actions may be unpredictable. A human train driver, therefore, has a natural interface with human passengers. In the case of emergency, be it a medical condition of a passenger, train accident, or a fire, the presence of a human driver on site to calm other passengers, assist with orderly and speedy evacuation and to coordinate with emergency services is incomparable. In general, the train driver can act as the on-site representative of the railway company for passengers, clients or emergency services when the need arises [9].

Lastly, the train driver also acts as an important link with other actors in the metro system such as the traffic controllers, security guards and maintenance personnel [9]. His actions may include reporting of potential hazards, security risks and technical failures. The driver is also near at hand to fix small technical faults such as train door faults that can bring the whole operation to a stand-still if an unmanned model was pursued [9].

### 2.3 Theoretical Automation Framework

The theoretical automation framework of Theeg & Vlasenko [25] was selected for the study. It is considered preferable because it presents a more linear progression from total manual control to total automatic control while also resisting the impulse for what can be referred to as the “proliferation of gadgets” - the simple and unthoughtful addition of a multitude of buttons, sirens, flashing lights and other countermeasures to the train cab. Such measures often prove more disruptive than helpful to the driver in the execution of his duties. This framework presents a simple and theoretically elegant approach to train driver automation design in general, and is based on discrete steps of increased automation, as discussed below, in reverse order of automation:

#### 2.3.1 Level 4 - Full automation

The train is normally driven automatically with no supervision from a human driver. In some cases a person that is normally charged with other responsibilities like ticket collecting, may be available to take control if needed [25]. At first glance, full automation seems to deliver on all of the perceived advantages of train driver automation: increased safety (driver induced SPADs) [12], increased cost effectiveness (personnel reductions and efficient driving profiles) and operational flexibility [9]. Yet, difficulties are soon revealed when the train control function is considered within the greater context of the railway operation, and operating in the real world. This perspective can be considered as the systems level or system engineer’s view. It may not be that difficult to automate train control, but to automate the train driver may not prove as simple when considering the following:

When the inevitable technical failure does occur, what fall-back modes and recovery mechanisms can be put in place to maintain safety and not bring the whole operation to a stand-still? In such cases a ready and able human train driver is inevitably required to monitor the system for correct operation and take control when needed [1]. Increased automation may also not lead to a reduction in staff as a reduction in train drivers due to automation may only lead to increased requirements in support and supervisory staff and more sophisticated levels of training [9]. Then, there are certain functions that may be quite trivial for a human train driver to perform but almost impossible to automate. These include the ability of a human train driver to observe potential hazards and react to those hazards, passenger care under normal and emergency circumstances, debugging of small technical failures such as door problems and a whole range of interactions with operations and maintenance staff [9]. Automation Level 4 was therefore not considered feasible for this study.

#### 2.3.2 Level 3 - Automatic driving with human supervision

The train is normally driven automatically with the driver observing and intervening in case of danger or technical failure [25]. Automatic driving with human supervision effectively counters most of the defects introduced with full automation but it is confronted by another kind of problem - that of having a fully capable human driver at hand to monitor and intervene when necessary. Bainbridge [1] asserted that, the manual control skills and cognitive skills required for train control will soon deteriorate in a driver if not practiced regularly.

A driver whose responsibility has been relegated to only monitoring the driving performance of a machine whose driving skills are perceived to be superior to his own may not be the right person for the job. He may also not
have enough insight into the decision making process to judge when things are going wrong and require intervention. A driver assigned to monitor an automatic system may very well feel that his job requires little skill, that he has very little insight and control of what is happening, yet is held responsible for the outcomes. These working conditions have shown to lead to high levels of stress and unhappiness and increased error rates. Automation Level 3 was therefore not considered feasible for this study.

2.3.3 Level 2 - Partially automatic operation

Train driving tasks and responsibilities are divided between the train protection system and the driver. The train protection system is fully responsible for some tasks and the driver is fully responsible for the others [25]. Level 2 automation does not seem to counter the criticisms of Level 3 and was therefore not considered feasible for this study.

2.3.4 Level 1 - Manual driving with technical supervision

This involves a train protection system supervising the driver and enforcing safety in case of driver error [25]. Manual driving with technical supervision seems to be the most practical option because the driver is maintained in his traditional role mitigating most of the fundamental criticisms to automatic drivers faced by levels two, three and four.

In addition, the technical supervision system can be scaled to cover only the functions critical to safety and can therefore be much less sophisticated and less expensive than a fully functional automatic driver. Lastly, the technical supervision system can simply be superimposed over the current manual driving model and the implementation will therefore result in minimum disruption to ongoing operations.

2.3.5 Level 0: Manual driving without automation

The driver is fully responsible for driving and there is no train protection systems present [25].

2.3.6 Recommendations

While Level 1 automation (manual driving with technical supervision) is the recommended automation model to be implemented, it should be noted that, to improve the practicability of the new model in the TFR railway environment, the model should be based on the current signalling and operational practices within TFR.

Additionally, the formal countermeasures and informal strategies presented by Naweed et al. [12] align reasonably well with the two elements of probability and criticality that make up the European Committee for Electrotechnical Standardization (CENELEC) concept of risk [4]. The informal strategies and vigilance improvement systems attempt to reduce driver error rates while intervention systems minimise the effects if driver errors were made. Although it is desirable to try and reduce the probability of train driver error, the method seems to be somewhat open-ended as it cannot enforce safety. It does not mean that such methods are ineffective and should not be investigated or implemented or that intervention systems are not subject to failure [6, 23 cited in 12] but it can be argued that vigilance improvement systems do not present a solid foundation for safety control [10, 25]. Reduction in adverse consequences (mitigation) seems to be the most appropriate and accessible approach in this case as it closes the loop in terms of safety enforcement (the result is forced) and is based on technologies that are well established and well understood. These systems (Automatic Train Protection for example) are based on the monitoring of the human driver and the enforcement of safety by applying the brakes if the driver significantly exceeds the required speed restrictions or movement authorities [25]. In many ways such an approach constitutes having all of the advantages of a human train driver, which has been shown to be considerable [1, 9], whilst mitigating the disadvantages. It is therefore recommended that the new model approach be along similar lines to ATP systems.

Finally, it may be worthwhile to consider adding functions that aid the driver in better driving but such functions should not form the basis of safety.

3. RESEARCH METHODOLOGY

The study followed a qualitative approach, utilizing a model development methodology and semi-structured verification interviews with signalling engineers. Qualitative research is interpretative and aims to provide a depth of understanding [5]. Such models provide symbolic, textual or graphic answers to research questions, typically based on logic, theory or verbal descriptions [3]. This study opted for the development of qualitative models, descriptive of the structure and behavior of the system by which train movements are and should be authorized and effected within TFR.
System structure was represented using a simple block diagram scheme, illustrating the different components and role players within the system and how they relate to one another. System behavior was represented using the Enhanced Functional Flow Block Diagram (EFFBD) scheme. Conventional FFBD’s are made of functional blocks, each representing a definite, finite, discrete action to be accomplished. The behavior model is developed using a series of diagrams to show the functional decomposition and to display the functions in their logical, sequential relationship. Diagrams are laid out so that flow direction is generally from left to right. Lines and arrows connecting functions indicate function flow and not lapsed time or intermediate activity. Common logical operations (i.e. concurrency, selection, iteration, repetition and loops) can also be implemented [11].

3.1 Data Collection

3.1.1 Pre-modelling concept development and review

The pre-modelling conceptual framework of South African signalling practices is based on the researcher’s own knowledge and experiences as a signalling engineer. Reference was made to written records and technical literature where possible. To ensure that the framework was accurate, the resulting write-up was submitted to an experienced signalling engineer for review and comment.

3.1.2 Model development interview sample size and selection

The interviewee sample consisted of three railway signalling engineers (designated ENG1, ENG2 and ENG3), the technical discipline specifically responsible for safety in railway movements or the creation of safe railway capacity. They were selected for their extensive experience (30+ years) as signalling engineers within the TFR railway operations, signalling and projects environment.

3.1.3 Model development interview planning, preparation and execution

Interviews were in-depth, semi-structured and consisted of the development and review of the current practice as well as proposed ideal models by expert signalling engineers. Three separate interviews were arranged – one with each engineer. One or two simple modelling examples were discussed to familiarize the interviewees with the modelling language. The background, motivations and recommendations upon which the models were to be based were also explained and discussed with the interviewees. Thereafter the engineers were required to develop proposed models and analyze them to confirm that the models met all the needs set out by the critical research question. The engineers, aided by the interviewer, were free to rework or modify their models until completely satisfied and before signing-off. Any qualifying statements or comments were also recorded in the process. Interviews were not audio recorded and transcribed verbatim. Interview notes, however, took the form of drawings, diagrams, descriptions and qualifying statements.

3.2 Data analysis

Data analysis took the form of the harmonization or consolidation of the interview models into a generic or representative model. This was possible due to the large degree of commonality between the models. Where the models did diverge, the diverging features were highlighted and discussed as possible options or customizations that could be applied on top of the generic model.

3.3 Study validity, reliability and ethics considerations

Various measures were put in place to assure the validity, reliability and ethics of the study. Validity measures included specifically interviewing experienced signalling engineers (experts in the subject of study) and utilizing a graphical modelling language instead of text based descriptions to increase clarity. Reliability measures included following an accepted research method (model development), arranging interviews at convenient times and places as well as interviewee anonymity. Interviewees were properly briefed beforehand and the whole process was accepted by the university ethics committee.

4. RESULTS AND DISCUSSION

4.1 TFR conceptualization

The purpose of this conceptualization was to develop an understanding of how railway movements are effected within TFR. Specific emphasis was given to the roles and functions signalling system actors (e.g. the train driver and Train Control Officer) and signalling system components (e.g. interlocking and field elements) play in those movements. This section presents a brief introduction to the railway signalling practices in TFR while highlighting the implications for SPAD incidents and causes.
4.1.1 Functional Structure: Typical TFR Signalling and Operational Control System

A typical TFR Signalling and Control System can best be visualized in layers stacked on top of each other connecting the Train Control Officer (TCO), who represents railway operational objectives such as the train movement schedule, at the very top to the trains, and signalling field elements at the very bottom. TCO controls are translated to the relevant station via the remote control system, is filtered through a safety interlocking layer after which it affects the desired change to the field elements (e.g. throwing a points set or changing a signal aspect) through field element control units. Field element status information (e.g. lay of a points set or train positions) is reported back to the TCO in similar fashion.

Figure 2 has been adapted from Trinckauf’s [27] Functional structure of the railway control system to be more representative of TFR signalling and control.

4.1.2 Principles of Train Separation

The most common train separation methods include Signalled Fixed Block Operation and Cab Signal Operation of which the Fixed Block is the dominant method on TFR signalled lines. On un-signalled TFR lines, constituting roughly 60% of all TFR lines, operational control is governed by a Track Warrant System (TWS) with movement authorities managed within the in-house developed CS90 remote control and Visual Display Unit (VDU) system.

4.1.3 Signals and Signal Aspects

On TFR signalled lines the dominant practice is that of color-light signalling with fixed block operation. Signals are used to guide a train through a railway network by communicating compulsory movement authorities to the train driver who is then expected to follow them to the letter. These communications include the following:

- Communication of movement authority into a block section including the nature of that authority (e.g. permission to proceed and speed restrictions).
- Inform the train driver as to the upcoming features of the track ahead (e.g. upcoming turnouts, entry into yards and sidings).

As many different possible meanings have to be conveyed to the driver, the signal has been equipped with several different lamps of various colors and arranged in several different configurations. These lamps can then be activated in predetermined combinations to indicate specific meanings called signal aspects. Figure 3 is a...
representation of the physical signal pole of a typical TFR signal that a driver would encounter when approaching a station [8]. The signal pole is populated with a green lamp, red lamp, white lamp, two yellow lamps, a signal identification plate and a shunt lamp-set (two small white lamps arranged diagonally). If all these different meanings or signal aspects, including a “dark” signal (no lamps burning), are summated, a signal with this physical configuration can be used to display up to thirteen different aspects [8].

![Figure 3 Color light signal (physical representation)](image)

The consequences of misreading or even completely missing a signal can vary from the benign to the severe. For example, if a flashing yellow is misread as a solid yellow, the train may apply brakes and slow down too soon, simply resulting in an operational inefficiency. If the reverse happened (i.e. reading a solid yellow as a flashing yellow), the train will not slow down and prepare to stop at the stop signal ahead, possibly resulting in a train collision. The worst case would obviously be to miss a stop signal or to come upon a stop signal unprepared which may result in a train collision while traveling at line speed.

### 4.1.4 Interlocking Principles

TFR interlocking systems typically implement the “Protected route and Overlap” method. TFR interlocked routes can also be manually cancelled by the TCO, but if the train has already entered the route or occupied the approach track to the entry signal, the signal is put back to Danger (stop/red aspect) but the route remains reserved and locked for a predetermined time before normalizing [8]. This prevents endangering the train and allows the driver to bring the train under control and to a safe stop without fear of a collision or derailment due to points sets being thrown under the train.

### 4.1.5 Signalling a Layout (Crossing Station)

One of the simplest illustrative examples of signalled layouts within TFR is that of the crossing station. The purpose of the crossing station is to increase bi-directional traffic density over a single line, albeit at the added cost of additional operational complexity. Figure 4 illustrates a typical signalling layout for a crossing station with functional descriptions for the different types of signals below.

![Figure 4 Signalled Layout (Crossing Station)](image)

The functions of the indicated signals in this layout are as follows [24]:

```markdown
- Starter Signal
- Home Signal
- Intermediate Home Signal
- Warning Signal
- Loop Line
- Main Line
```
Warning Signal: Warns the driver that he is approaching a stop signal. Note this signal does not have a Stop aspect. This signal is sometimes erroneously referred to as a distant signal.
Intermediate Home Signal: First stop signal when approaching the station and acts to protect the overlap of a route setup from the opposite side of the station.
Home Signal: Stop signal before station entry. This signal is to regulate access to the station.
Starter Signal: This signal has a dual purpose – it can either be used as a destination signal for a train entering the station (Danger Aspect) or as a departure signal for a train exiting the station (Proceed Aspect).

### 4.1.6 Dispatching Principles

Centralised Traffic Control (CTC) operation is the predominant model on TFR Signalled lines and is illustrated in Figure 5. In CTC operation, all points and signals inside the controlled area are directly controlled by the CTC TCO. All train movements are governed by signal indications. The local interlockings are remote-controlled without local staff [17].

![Figure 5 Centralized Traffic Control (CTC)](image)

In a TFR Track Warrant System, movement authorities are communicated to train drivers directly via a radio or cellular network (Figure 6).

![Figure 6 Dispatching by Track Warrant](image)

### 4.2 Current Practice and Proposed Automation models (Consolidated)

Due to the high degree of commonality between the Current Practice models and the Proposed Automation models produced by ENG1 and ENG2, the interview format for ENG3 was rather directed towards the confirmation or rejection of those models. The consolidated or generic model was therefore generated and presented to ENG3 for endorsement. All three engineers agreed with the recommendations that flowed from the literature review. Both ENG1 and ENG2 based their automation models on Automatic Train Protection systems that intervene when the driver exceeds the required speed profiles while also promoting efficient driving patterns. These views were also endorsed by ENG3.

The first difference between the models generated by ENG1 and ENG2 was that of the level of detail. ENG2 preferred to define the system on component level where ENG1 preferred to stay on the system level. The consolidation process also preferred the system level as the component level may become too prescriptive about the specific technological implementation and move away from a neutral description of system behavior.

The second difference between the models spoke to the operational environment. ENG2 defined models for both the Signalled and Track Warrant operating environments while ENG1 felt that it was not necessary to consider train driver automation in areas where conventional signalling systems were not considered or warranted in the first place. The two models generated by ENG2 were very similar, only emphasizing the safety integrity ratings of the systems and equipment used in implementation. In this case as well, when consolidating to the system level, the models for the two operating environments merged into one.
The models as well as the consolidation process were discussed with ENG3 and the resulting model was accepted and endorsed by ENG3. The resulting generic model consists of both a structural component (Figure 7) and a behavioural component (Figure 9). As the proposed automation model was based on the current practice, the current practice model elements are shown in grey while the modifications or improvements are indicated in blue - see Figure 9.

It should be noted that the actual models generated in the interview process did not always strictly adhere to the proper notation conventions associated with the EFFBD modelling language. As these models were intended to be primarily descriptive, these deviations were not considered problematic as long as the models were readable, understandable, logical and unambiguous. Per implication, these models may require a measure of reformulation if they are to be ported into software tools for simulation purposes.

![Diagram of generic model - structure](image)

**Figure 7 Generic model - structure**

Interface listing:

a) TCO - Signalling System
   - Computer based control terminal
b) Signalling System - Track
   - Train detection device (axle counter / track circuit)
c) Sig. System - Train Driver
   - Signal lamp
d) Train Driver - Train
   - Driver instrument panel
e) Train - Track
   - Wheel on track

The behavior model was based on the basic train movement on a signalled line - depicted in Figure 8.

![Diagram of train movement](image)

**Figure 8 Train Movement**

A train route was setup and cleared from the departure signal to the destination signal. The Solid Green departure signal is indicating to the driver that the train may proceed at line speed. The follow on signal displays a Solid Yellow aspect, indicating to the driver that the train may proceed but that the driver must be prepared to stop at the next signal (Red / Danger).

The behavior model (Figure 9) can be logically devided into the phases of Movement Setup, Route Traversal and End of Authority.
Figure 9 Generic model - behavior

Ultimately, all the engineers explicitly agreed that the resulting models successfully answered the following questions:
Do you agree with the recommendations from the literature review and were those recommendations faithfully implemented in the proposed automation model?

Would the resulting automation model be effective in mitigating SPADs and would you consider it to be the most appropriate train driver automation method for the TFR environment?

All of the interviewed signalling engineers answered in the affirmative.

5. CONCLUSION

Operator automation is a field that presents enormous potential advantages when it comes to the technological augmentation of human capabilities, yet it comes with significant engineering challenges as well. As has been evident in this study, this statement also holds true when considering the automation of the train driver within the TFR environment. At first glance, the completely automatic control of a train seems to be a simple process to implement, yet when train control is holistically considered within the greater context of railway operation (the systems engineer’s view), there are significant challenges that become apparent.

A thorough review of the literature has shown that human train driver errors and violations significantly contribute as causes of SPADs (a fundamental failure in driving safety) yet it has also been shown that the additional roles and functions fulfilled by a human train driver (i.e. intervention and support under abnormal circumstances) are not as easily automated. The most practical and readily available train driver automation model, mitigating most of the costs imposed by human failure associated with SPAD events yet retaining the value of human flexibility, was demonstrated to be that of retaining the human driver yet with technical supervision. In this arrangement, the human driver would remain in his conventional role of driving the train but with a technical supervision system superimposed that automatically intervenes if a train driver exceeds his movement authority. In addition, such a system could be tailored to also guide the driver towards optimal driving profiles.

The recommendations from the literature as well as the resulting generic model were endorsed by the signalling engineers interviewed, affirming it met the requirements set out by the research question: That of being the most appropriate method of train driver function automation to mitigate SPADs in the TFR railway environment.

5.1 Further study

The financial costs typically attached to safety systems and technologies such as Automatic Train Protection (ATP) can be significant and often prohibitive for large scale implementation and support in third world countries such as South Africa. In many cases (e.g. rural lines that carry predominantly freight traffic) the traffic densities and potential risk levels may not justify the costs associated with equipment carrying the Safety Integrity Level (SIL) ratings of SIL3 or SIL4 [4], typically associated with the high traffic density on metro lines. In such cases, the application of SIL1 or SIL2 systems may be sufficient if combined with soft strategies like the informal driver strategies presented by [12]. The formalization and scientific evaluation of the effects on risk reduction of such strategies and initiatives, may prove a fruitful field for further study.

REFERENCES


