Data redundancy and intelligent verification in the context of signalling and train control

Written on behalf of the ITC by Edward Goddard and Alan Rumsey, with contributions from Yuji Hirao, Wim Coenraad and Rod Muttram

Notwithstanding the benefits of computer-based and communications-based train control (CBTC), there exists in these systems a potential disadvantage that information can be lost, corrupted, or even deliberately altered. In designing train control systems of these kinds, the signal engineer must therefore give specific consideration to the following:

- How do I protect against the train-borne controller failing to determine the train's location, or calculating an incorrect train location?
- How do I protect against a train location report being corrupted during transmission to the wayside/lineside controller, but still being accepted as a valid message?
- What do I do if I fail to receive a train location report?
- How do I protect against a wayside/lineside controller calculating a movement authority update incorrectly?
- How do I protect against an updated movement authority being corrupted during transmission to the train-borne controller, but still being accepted as a valid movement authority?
- What do I do if I fail to receive an updated movement authority?

Fortunately computer- and communications-based systems possess inherent advantages that address these challenges, such as the ability to process information from multiple sources, to communicate information via diverse paths and to apply rigorous logical checks on information received, in order to assure the highest possible levels of safety, availability and performance.

This paper explores to what extent these inherent advantages have been fully exploited in CBTC and European Train Control System (ETCS) system designs, and to what extent train control systems are, or should be, making use of additional information now readily available from traction and braking systems, passenger information systems, and train management systems.

The principles of operation for CBTC systems (as applied to metros) and ETCS Level 3 systems (as proposed for main line railways) are similar in that in both systems:

- Train location is determined by a train-borne controller (independent of track circuits or axle counters) using train-borne sensors (e.g. tachometers) and track-based transponders (or Eurobalise);
- Train location information (and other train status data) is reported to a wayside/lineside controller (zone controller or radio block centre) over a train-to-wayside/lineside data communications link (GSM-R in the case of ETCS);
- The movement authority for each equipped train is determined by the wayside/lineside controller based on train location information and route setting information from interlockings;
- Movement authority information (and other train control data) is then transmitted to the appropriate train over the wayside/lineside-to train data communications link;
- The trainborne controller enforces the movement authority based on its determined train location and speed.

Fundamentals

Many of the following basic principles will appear obvious but not all control systems include each and every one of these features.

Sequence and time stamping

All messages should contain a sequence number and be time stamped. This provides a level of protection against false messages being introduced, and detects delayed messages.

Data consistency

We know that trains travel in a uniform manner within a speed envelope. Any apparently valid message received by a wayside/lineside controller to indicate a train's position, for example, should be viewed with suspicion if it falls outside a reasonable timescale since the last valid message received. Equally, unless train position is critical, a lost message can be tolerated, as we know where the train was and how far it could go in the time within its movement authority.

One train, one place

A simple comparison should ensure that for every train reporting its position, there is only one record.

One place, one train

Only one train can occupy the same location at any one time.

Repeat the message

Vital information that would result in a less restrictive movement authority should be not acted upon unless received in two independent messages.

Diversity

Track versus train

Regular checking for consistency between the information held by the train and that by the wayside/lineside can trap latent errors. One example of this is a consistency check between train location information determined from tachometer sensors and that determined from a detected transponder/balise.

Diverse tachometry

As well as the tried and trusted tachometer and balise, a number of alternative means of determining the position of a train are available. On modern rolling stock these are often already fitted (Doppler radar, inertial guidance and GPS, RFID, etc.). This additional information can be used for enhancing safety and it is also a potential means of overcoming defects and enabling train movement under failure conditions.

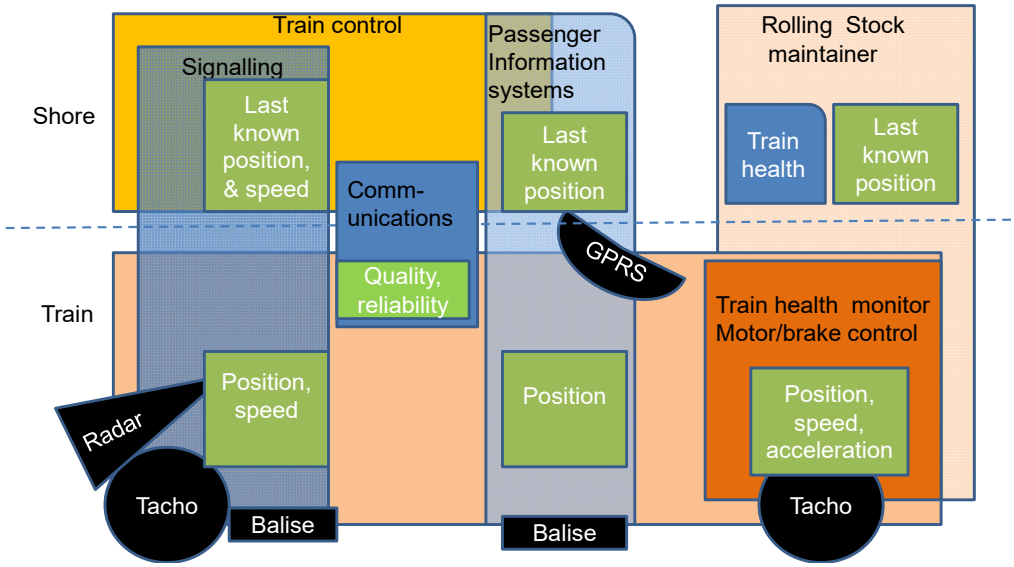

Figure 1 - Are we using all the information available to us?

Safety nets

We need to ask whether we are using all the information from other systems to enhance the overall operation. Figure 1 shows the range of information that can be exploited in this context.

Communication links

Error rate

Communication systems report on the quality of the link. Should high error rates be experienced, not only they should be flagged to the maintainer but also an alert should be given to enable control action to be taken.

Latency

Similarly, an alert should also be given if messages are taking an excessive time to be received or if there is an excessive time between messages being received.

Rolling stock

Modern locos and trains report their status and position regularly. This information is usually contained within the maintenance function of the rolling stock provider. There must be opportunities to provide a comparison with the information held by the signalling.

Information systems

Modern trains have comprehensive passenger information systems that use the train's location to deliver onboard messages to the passengers or to track the movement of freight loads. This information is often confined to the train operating company.

Implementation

To date the experience of operating communications-based train control systems has been largely confined to metro railways. Many different system architectures have been employed and these have each provided an insight into what should be aimed for and what should be avoided. Application to ETCS Level 3 is still at the early stages and this is therefore the right time to consider the potential benefits that can be obtained from the lessons that have been learnt to date.

Train service operation

Application to metro lines varies from main line railways. The management and control of metro trains, rolling stock and stations are frequently exercised from a single, shared control centre. Nevertheless the signalling, maintenance and passenger information systems are usually divided, both in terms of the equipment used and the staff who use them. On main line railways the division between train operating companies, rolling stock leasing companies, and signalling/train manufacturers is even more pronounced. The opportunity exists to provide a framework within which the various operators (signallers, maintainers, and information providers) can exchange information to alert to potential problems, to provide diverse means of moving trains safely under failure conditions, and to alert the police and other bodies involved to any anomalous behaviour detected in the communication links.

Supply chain

Many signalling suppliers are part of larger corporate groupings that embrace both communications and loco and rolling stock supply. When considering the fitting of tachometry to a train, there are considerable advantages to be gained by eliminating duplication and combining information between the signalling and traction/brake control systems. Divergent standards for signalling and rolling stock equipment and differing speed measurement requirements have prevented signalling systems utilising other rolling stock speed sensors in the past. Nevertheless recognition of the benefits of having diverse means of measuring train position and estimating its accuracy should enable us to remove the barriers.

Simplicity versus complexity

Whilst the measures just mentioned will improve the reliability of the system, they also introduce additional functions in the code. This has a counter effect, as it increases the likelihood of coding errors and adds to the testing and verification requirements. Hence a balance is required between seeking a robust system and overcomplicating it with unnecessary features.

A trap that must be avoided is the tendency to increase the complexity of the signalling, particularly in its vital role. By segregating the system into separate vital and non-vital subsystems, the basic safe control loop can be kept as simple as possible. In the vital functions error traps, sense checks and system diversity (duplication) can enable alerts to be given to highlight any emerging issues to the operator. The fallback or non-vital systems can then provide the means of authorising train movements under special rules.

Fail-safe or fault-tolerant?

Signalling has moved on from the basic implementation of fail-safe systems in which 'a stopped train is a safe train'. We recognise the need to bring a train to a place of safety where this is possible and to protect those on and around the train. The

use of data consistency and redundancy can enable trains to be keep moving (e.g. no need to stop the train if a single message is lost or corrupt; a single failed tacho or missed balise should not prevent the signalling staff knowing where the train is).

Where the primary system is unable to authorise a new movement authority, the overall train management system should be capable of assisting the operator by providing a rich picture of the railway derived from the various sources of train information. The design of traffic control centres should reflect these possibilities.

Do what you can, when you can

Whilst the ideal is to have one single universal application that does everything, the reality is that railways grow and evolve. Apart from on the smaller metros, it is inevitable that the total railway control system will have to embrace a variety of systems of different generations. These range from mechanical interlocking to advanced satellite-based train location systems, and from unfitted freight trains to Level 3 equipped trains, each providing its own picture and requiring its own operational controls.

It is no longer possible for the signalling supplier to dictate to a closed world with signalling seen as an end in itself. All the same, the disciplines and technology deployed by signal engineers provide the means of capturing this wider picture and taking a whole-system approach to the introduction of new control centres and train management systems as and when they are introduced.

Enforcing maintenance and operational disciplines

Whilst the above processes will detect potential faults, it is essential that action is taken to determine their root cause and then correct them. This applies equally to operational, maintenance and security personnel, as the tendency is to ignore the alerts when the system 'carries on working OK' or 'always does that'. Consequently strict procedures must be implemented to ensure that latent errors are not left uncorrected.

Conclusions

1. There is much that can still be done to improve the reliability and security of communications-based signalling systems.
   - By checking new data against that currently held and by exploiting the inherent physical characteristics of a railway, it is possible to secure a high degree of protection against data and communications errors, whether these are accidental or deliberately introduced;
   - By comparing the data held by the shore-based systems and that gathered by the rolling stock based systems, a further improvement in reliability and security can be obtained.
2. With the increasing convergence in the technologies used by metros (CBTC) and main line railways (ETCS) the opportunity exists to:
   - Apply many of the system-wide techniques that have evolved in the more enclosed world of metros;
   - Make use of common components to reduce the cost of both CBTC and ETCS.
3. Whilst main line railways are considerably more complex than metros, many of the techniques, technology, and hardware developed for ETCS are already being applied by metro signalling and rolling stock suppliers as well, and vice versa. Care needs to be exercised by standards setters to avoid creating unnecessary restrictions on the acceptability of sensors common to both applications.
4. The use of information from diverse systems to improve service reliability under failure conditions should be encouraged.