COTS – Size Does Matter

George Nikandros
Signal and Operational Systems
QR
GPO Box 1429, Brisbane 4001, Queensland
george.nikandros@qr.com.au

Abstract

Railways, like a lot of industries are becoming increasingly reliant on programmable technology for safety. The development of railway technology is however largely driven through market forces and, given the complexity and cost of developing and certifying safety-related systems, rail industry suppliers tend to accede to the needs of their bigger customers. Consequently the in-built functionality is targeted to specific customer needs, and as these needs can vary considerably between railways, there is often a need for customisation to suit a particular application. However, railway products are constantly evolving largely because of technology obsolescence, but also to enhance through added functionality, whilst sometimes also removing no longer necessary functionality. This paper provides a case study for one such product, namely an axle counter system, which was developed for application on the QR rail network. The first of the systems were brought into service in 1987 and are still in use today. Since then, there have been several evolutions of the product, which progressively saw the removal of functionality and customisation required by QR. The paper describes the application of the axle counter product within QR, the initial development, and what is being done to enable the use of the latest version of the product.

Keywords: railway signalling, axle counter, obsolescence, COTS

1 Introduction

Electrifying a railway introduces a number of hazards that can adversely affect the integrity of a railway signalling system – the system that safeguards the movement of trains on a railway. Electrifying a heavy-haul railway with 25kV, 50Hz exacerbates these hazards due largely to the magnitude of the traction power required. The high traction current and traction system fault current are issues that need to be considered in the design of the railway signalling system.

In the early 1980s, QR embarked on a project to electrify its heavy-haul central Queensland coal railways.

In an electrified railway, at least one of the two rails provides the traction current return path. The use of the rail/s for traction return impacts on the use of track circuits as a means for detecting trains. Track circuits were at the time (and still are) the most common method for proving the absence of a train on a section of track. A track circuit is an electrical circuit that uses the rails as conductors; such that the presence of a train is determined by the track circuit current being shunted between the rail conductors through a train's axle.

Traction current impacts on track circuits by limiting their length because of electrical interference in relation to the track circuit equipment technology and workplace safety (touch potentials for track workers). Also, traction current interferes with line-side power distribution and control cables through electromagnetic induction. Induction from railway traction systems can result in dangerous voltages; dangerous in relation to compromising the integrity of the train control system; and dangerous in relation to electrical workers. To limit the magnitude of the induction, the length of these cables needs to be limited e.g. segmenting cable runs using isolating transformers.

Traction current impacts make the use of track circuits and line-side cabling between train crossing locations that are some distance apart, costly.

Controlling train movements over a bi-directional track between two adjacent train crossing locations requires more than just knowing whether the section of track is occupied or not; it is also necessary to ensure its availability. Once a train is issued with an authority to enter a section of track, it must not be possible for another train to be issued with an authority to enter that same section of track, even though the first train has not yet entered the track section. To do this requires interlocking between the two crossing locations. For track circuit based systems, this is usually achieved by interconnecting the two crossing location interlocking systems via a line-side control cable.

The track circuit at the time was not the only technology available for train detection; the axle counter was emerging as a practical alternative technology, particularly in mainland Europe and South Africa. The axle counter as the name suggests is based on the principle that if you count the number of axles entering and leaving a section of track, and the net result is zero, then the track section can be declared to be free of trains.

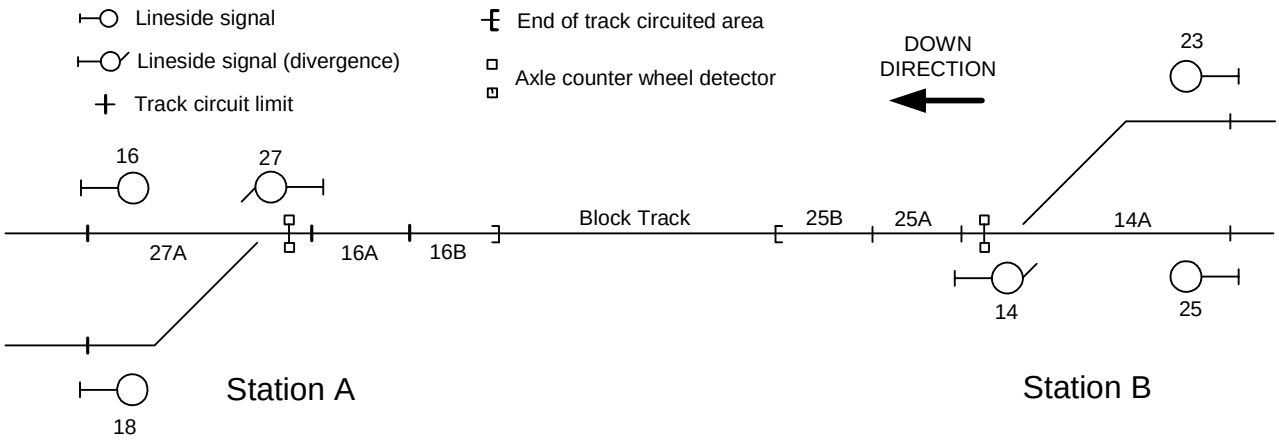

Figure 1: Typical QR Signalling Arrangement for an Axle Counter Application

The axle counter requires a counting processor, commonly known in the rail industry as an Evaluator, and axle detectors (actually wheel flange detectors) located at all extremities of the monitored track section.

This requires the wheel detection points to be connected to the Evaluator and, prior to the mid 1980s, the method used was line-side cabling.

The late 1970's saw the emergence in the use of microprocessor technology and data communications for safety-critical railway signalling applications (Cribbens 1981, Lohmann, and Ziller 1984).

The early 1980's saw railway commercial-of-the-shelf (COTS) products based on processor technology such as signal interlocking systems, axle counters and block data transmission systems becoming available despite the fact that safety-related system concepts and standards were embryonic in relation to today.

Thus, the essential building blocks for an axle counter with a data transmission capability were there.

However the axle counter was only a train detector; it did not ensure the availability of the monitored section.

Section 2 explains the QR application and the functional features of the axle counter system; Section 3 describes the initial systems, their safety-related limitations and how they were overcome; Section 4 discusses the evolution of the product; Section 5 explains how QR is managing to ensure the availability of axle counter technology to sustain their existing applications; Section 6 summarises the key points made.

2 QR Axle Counter Application

Figure 1 schematically depicts the typical signalling arrangement for a bi-directional single line between two adjacent train crossing locations. Track circuits are used at the train crossing locations, with the axle counter monitored section overlapping the track circuited sections.

Signalling principles require that opposing signals must be interlocked. Signal 16 at Station A, for example, must not only be interlocked with Signals 18 and 27, but also interlocked with Signals 23 and 25 at Station B. Therefore before Signal 16 is permitted to display a proceed aspect, the section of track between Signal 16 and Signal 14 must be free of trains (27A, 16A, 16B, Block Track, 25B and 25A all must be unoccupied), the points must be correctly positioned and all opposing signals are displaying a STOP aspect. The term "Block" is commonly used by the rail industry to refer to the section of track between train crossing locations (stations).

QR defines the direction of travel on a line by the terms UP and DOWN. In Figure 1, a train travelling from Station A to Station B would be travelling in the UP direction; conversely a train travelling from Station B to Station A would be travelling in the DOWN direction.

The status of the Station B interlocking in relation to the availability of the section of track between Station A and Station B, is conveyed to Station A via the UP Block function; conversely the status of the Station A interlocking is conveyed to Station B via the DOWN Block function. For an authority to be given for a train to travel from Station A to Station B (e.g. a PROCEED aspect in Signal 16), the UP Block function at Station A must be in the permissive state.

The integrity of the UP Block and DOWN Block functions is fundamental to ensuring safe train operations between Station A and Station B. If either of these functions is erroneously in the permissive state, the circumstances would exist for a train-train collision to occur.

2.1 Inhibit Function

A feature of axle counter systems prior to the mid 1980s, was the Inhibit function.

Trains are not the only vehicles to operate on a railway. Other vehicles such as track inspection and track

maintenance vehicles also operate on track. These on-track vehicles often have the capability to be off-tracked. For example a track inspector may off-track at an at-grade road crossing and travel by road before rejoining the track some distance beyond. Unlike track circuits where track vehicles are continuously detected i.e. if they off-track, the track circuit state would immediately change from the OCCUPIED (restrictive state) to UNOCCUPIED (permissive state), axle counters only detect track vehicles at the extremities of the monitored section. If the track inspection vehicle was "counted in" by an axle counter, the axle counter would remain in the OCCUPIED state if the on-track vehicle was not "counted out".

Such a situation could be addressed by providing a Reset function. However, such a function would also encompass substantial risk, as an inadvertent reset, or an erroneously performed reset could lead to a train-train collision. The nature of track inspections and maintenance is such that the Reset operation would be common-place. A Reset function is effectively an operator system over-ride and whilst necessary to recover from failure situations, which should be relatively rare, using it for normal rail operations would degrade the safety integrity of the axle counter system as the level of safety would be very much dependent on human error rate of the signalling system operator.

The Inhibit function essentially allows the application designer to control when the axle counter is to record (count) axles passing over a wheel detection point. This also has some risk, as the application designer needs to ensure that only those vehicles that are not intended to be detected are in fact not detected. Failure of the axle counter to detect intended axles indicates to the signalling system that the monitored track section is free of trains.

The applications of axle counters in QR very much depend on the use of the Inhibit function. In QR, vehicles that are not controlled by the signalling system are configured to prevent them being detected by a track circuit i.e. their axles are insulated such that they do not provide a shunt path for the track circuit current between the two rails. Thus a track circuit can effectively be used to prevent detection of those track inspection and track maintenance vehicles that are not intended to be detected.

Whilst track circuits are a very effective means for train detection and are designed on fail-safe principles in that a circuit discontinuity results in the track circuit entering the OCCUPIED state, train detection is not always guaranteed. Railhead and wheel tread contamination impacts on the quality of the current shunt that a wheel-axle assembly provides between the rails. Although such unsafe failures are relatively rare events, QR considered it necessary to defend against such an eventuality, as such a failure would result in the monitored track section being declared vacant by the signalling system and available when in fact a train occupied it – a situation that needs to be avoided.

By providing additional functions involving more than one track circuit in each of the station interlocking systems, QR is able to provide a defence against unsafe track circuit failure. The theory being that if it is rare for a train not to be detected by one track circuit, then it is much rarer for two track circuits at the same location to both not detect a train. Locating the axle counter wheel detectors such that there is an overlap of the axle counter monitored section and the track circuit monitored sections, enables the station interlocking to prove that the axle counter has detected at least one axle.

These interlocking functions provided as a defence against the failure of a train being detected by the Inhibit track circuit are outside the scope of this paper, and so a detailed explanation will not be provided here. However it is necessary to comment on the concept to assist understanding. Referring to Figure 1, the wheel detector at Station A is located within track circuit 27A. The Inhibit function at Station A is therefore enabled and disabled on the occupation status of 27A i.e. if 27A is OCCUPIED, then the Inhibit will be disabled, such that passing axles will be detected, assuming that there is no failure of the axle counter Inhibit input.

The interlocking at Station A is configured such that when a train has been given a PROCEED signal to travel to Station B, and for some reason the train is not recorded by the axle counter as entering the monitored track section, 16B will remain in the OCCUPIED state even when the train is completely within the Block Track section. This effectively prevents the signalling system from issuing another authority for a train to enter the track section between Station A and Station B. Similarly, track circuit 25B will remain in the OCCUPIED state for a train travelling from Station B to Station A.

The Inhibit function also has a beneficial effect on the availability of the axle counter system, in that it reduces false counts triggered by electrical transients such as atmospheric disturbances and faults in an electric traction system. False counts force the axle counter to the safe OCCUPIED state, reducing the availability of the signalling system to control the movement of trains, and forcing the use of alternate less intrinsically safe manual procedures.

The system developer did provide a warning in the system documentation regarding the use of the Inhibit function.

2.2 Reset Function

Through practical experience, a facility for the operator of the signalling system to recover the axle counter system in the event of a miscount was, and still is, a necessary feature to maintain high signalling system availability. However the risks associated with such a facility were understood and as such this function is only available (enforced by the system) in the event of a miscount i.e. the number of axles detected leaving the monitored section did not match the axles detected entering. The Reset function is RESET RESTRICTED if the last axle detected was entering the monitored section. A precondition for the signalling system operator to reset the axle counter is that axle counter must not be in the RESET RESTRICTED state.

If the axle counter is RESET RESTRICTED or if it has suffered a system failure, then maintenance intervention is required followed by a Reset by the signalling system operator.

3 Axle Counter System – 1987 Version

Figure 2 depicts the architecture of the axle counter system that QR commissioned into service 1987.

The axle counter system consisted of three key features:

- An axle counter;
- Voice frequency data transmission;
- User defined digital I/O.

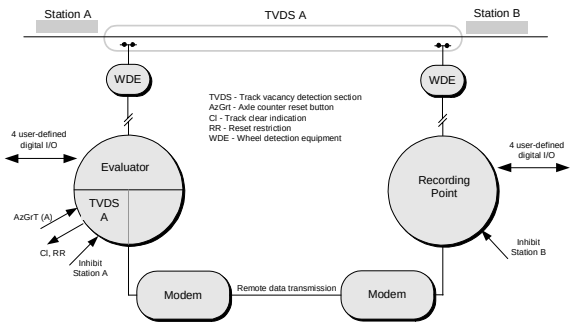

Figure 2: Axle Counter System Architecture (1987)

The basic concept of the axle counter is maintained, in that there is an Evaluator and wheel detectors located at the extremities of the monitored section of track.

The data transmission connection between the two remote wheel detector and the Evaluator necessitated the Recording Point to record axles passing at the remote detection point, process the digital I/O and transmit information to the Evaluator.

Both the Evaluator and Recording Point are implemented using a 2.o.o.2 (two-out-of-two) dual channel configuration.

Each of the two ends of the system is continuously aware of local conditions, such that the system can automatically recover from interruptions in the data transmission system.

3.1 Safety Issues

Conceptually this configuration satisfied the needs of QR. However, when the pre-production system was delivered for evaluation and testing in early 1986, QR identified what they considered to be a serious limitation.

The system was developed in Germany and there had been no QR involvement in the development process prior to delivery of the pre-production system, apart from initially specifying the key features required. The developer was a major railway signalling system and equipment supplier, including axle counters and block data transmission systems, and as such, there was a high degree of confidence in the developer's ability to develop the required system.

The limitation related to the I/O integrity. Figure 3 depicts the I/O arrangement.

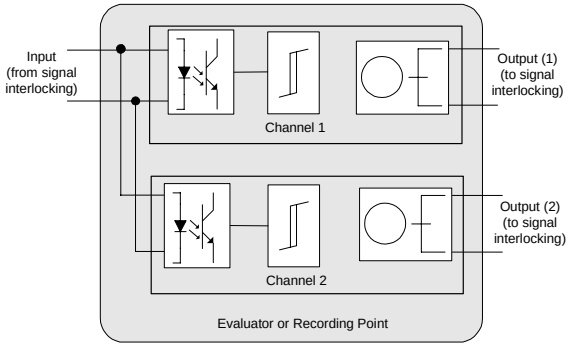

Figure 3: I/O Arrangement (1987)

3.1.1 Input Interface

The input interface from the signal interlocking system consists of opto-isolators. However these opto-isolators were not subject to any system test to verify their operation. Whilst there are two devices, one for each channel, any discrepancy between the devices will only be revealed by comparing the output from each channel. If however the input changes state infrequently, which would be the case on a low trafficked train line, it is possible for both opto-isolators to fail in the same mode, particularly as they are the same type of device and subjected to the same input signal i.e. a potential common mode failure threat.

Given that two of the inputs are the UP Block and DOWN Block i.e. the critical functions which provide the interlocking for the bi-directional single line between train crossing locations, QR did not consider the input interface as being adequate.

3.1.2 Output Interface

The output interface to the signal interlocking system is via voltage free relay contacts. Each output consists of two relays, one for each channel. However the relays used, although of a high quality, are not in any way intrinsically safe i.e. there is no guarantee that the energised contacts open-circuit when the relay coil energy is removed.

3.1.3 Inhibit Interface

The Inhibit input interface from the signal interlocking system has the same opto-isolator arrangement as for the user-defined digital inputs and is also not subjected to any system test to verify the integrity of the input.

The Inhibit is always applied and only removed when a train is to enter the axle counter monitored section of track. For low train trafficked lines, the Inhibit is applied most of the time. There is the potential for the Inhibit to fail in the applied state, and therefore prevent the axle counter from registering the train. If the train is entering the monitored section, and the Inhibit is failed in the applied state, then the axle counter will output that the section of track is not occupied by a train i.e. it is available for another train.

Despite providing a warning in the system documentation on the use of the Inhibit function, there was no warning regarding the failure of the Inhibit input when not used.

3.1.4 Data Transmission

The dual channel architecture configuration applies also to the data transmission function. However this is only in a logical sense as there is only one Voice Frequency (VF) modem at each end of the data link.

There are two data telegrams; Telegram1 for Channel 1 and Telegram2 for Channel 2 in each direction between the Evaluator and Recording Point. Telegram1 and Telegram2 contain identical information. Telegram2 is however the inverse of Telegram1.

Each telegram consists of 4 bytes (32 bits) that includes an 8 bit address and 8 bit parity for error detection. There are separate addresses for each direction i.e. if the address for the Evaluator to Recording Point direction is A_{ER}, the address for the Recording Point to Evaluator is $A_{ER}+1$.

This data transmission approach was considered adequate for the application in QR, as the supporting telecommunications system providing the VF communications channel is a closed QR system and there is no "store and forward" capability i.e. there is no threat due to stale data. However there is some risk, in that VF channels are derived channels on a digital communications network and unlike a physical connection (copper cable), the connection route can vary. This is a threat in that there is a real possibility of an Evaluator being connected to the wrong Recording Point.

3.2 Safety Issues – Resolution

The above safety issues were put to the system developer. The developer did acknowledge QR's concerns that the integrity of the user defined inputs and their corresponding outputs were a significant safety issue for the intended application and that these needed to be addressed.

3.2.1 Input Interface

The solution to the interface was to reconfigure the system inputs. Instead of having four user defined inputs in each direction i.e. a total of eight inputs with corresponding outputs, there were now a total of four inputs, such that each input had an associated 'local' output in addition to the 'remote' output. The 'local' output provides a means to indicate the system's reading of the input and thereby enable a means to prove the correct reading of the input by the Evaluator or Recoding Point. By comparing the state of the input presented to the Evaluator or Recording Point with its 'local' output of that input, it is possible to use an external means to shutdown the particular Evaluator or Recording Point should the input and its 'local' output not correspond.

For the axle counter system, this solution approach could be implemented with a relatively simple system software change without necessitating any hardware change to any of the modules. It did, however, require an external shutdown mechanism to be provided within the station signal interlocking to remove power from the failed Evaluator or Recording Point.

3.2.2 Output Interface

Unlike the input interface, the output interface could be verified externally by the station signal interlocking system. It is feasible to continuously monitor each channel output, and use a shutdown mechanism (the same mechanism as for the inputs) when an out-of-correspondence was detected.

There however remains a threat (due to the fact that there may be long periods of time between changes of state), that both relay output contacts weld in the permissive state, thus preventing detection of the failure. This however is considered a low risk as the switching current involved is small.

3.2.3 Inhibit Interface

Section 2.1 explains the approach taken by QR to ensure that a train was detected by the axle counter system due the Inhibit being enabled. The same control mechanism also addresses any failure of the Inhibit input that causes it to remain in the enabled state when the signal to the Inhibit input is removed.

3.2.4 Data Transmission

To protect against the threat of an Evaluator being connected to the wrong Recording Point, QR adopted the policy of not reusing addresses where the VF channel is a derived channel. This essentially restricted the number of such systems that could be installed to 61 (the address in Telegram2 is the inverse of Telegram1 and there is a separate address for each direction of the data link, and address '0' is not allowed).

4 Product Evolution

Since the 1987 version, there were some initial incremental system changes, followed by a major product change in the later 1990's, which saw the discontinuation of the 1987 version, although support for this version continued to be available until March 2004. 2003 saw yet another major evolution of the product.

4.1 Incremental Changes

Within less than 2 years of QR completing the electrification of its Central Queensland coal railways, there was a need for more of the same type of axle counter system.

During the procurement process, it emerged that there had been some system module changes; the two previous power supply modules had been redesigned as a single module; the wiring interface had been altered; and the system software had been 'improved'. However it was not until testing of the revised product that QR became aware that the input interface proving feature had been removed from the system software, despite there being no compensating change to the input interface configuration.

The removal of this functionality was done to restore the available user-defined inputs to four in each direction (see Section 3.2.1 for background) to make the product more flexible.

This in itself was not a major obstacle for QR, as the 1987 version of the system software was supported by the revised hardware, thus enabling QR to use the same input proving approach previously devised for the 1987 version.

QR continued to replace the system software with the 1987 software version for all axle counter systems of that type that were purchased. The last of these systems was purchased around 1997.

4.2 Current Version

The later 1990's saw the emergence of a new generation of axle counter system technology. Whilst maintaining the underlying axle counter concepts, this new generation allowed for wider range of applications by substantially expanding capacity. It was a merger of axle counter system variations that had come about to meet the specific needs of various customers. Basically this means that an axle counter system can have many wheel detection points, have the capability of monitoring more than one section of track, and support more user defined I/O. Figure 4 depicts the architecture of the current generation needed to provide the "equivalent" functionality as the QR 1987 version.

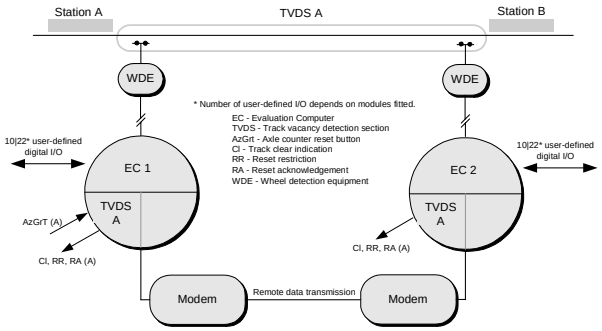

Figure 4: Axle Counter System Architecture (2003)

The architecture is similar to the original QR version; the obvious differences being the two Evaluation Computers, EC 1 and EC 2 instead of the one Evaluator and one Recording Point configuration and the absence of the Inhibit input.

In the Evaluator and Recording Point configuration, only the Evaluator determines the occupation state of the monitored track section, whereas in the two-EC configuration, each EC independently evaluates the occupation status.

4.2.1 Input Interface

Despite a greater I/O capacity, the I/O configuration perpetuates the original concept and is depicted in Figure 5.

As depicted in Figure 5, the 2.o.o.2 configuration of the initial system remains.

There is one minor difference; each input has separate wiring connections for each channel, thus maintaining total independence between Channel 1 and Channel 2 within the axle counter system. This however does not much improve the defence against a common mode input failure (Section 3.1.1) as the input is still driven from the same source in the signal interlocking.

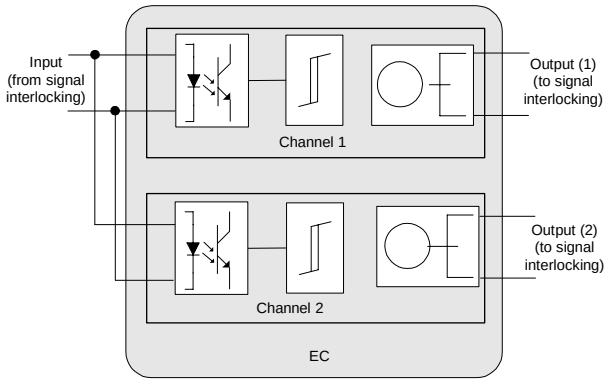

Figure 5: I/O Arrangement (2003)

4.2.2 Inhibit Function

Anecdotal evidence suggests that the German Federal Railways recommended the removal of the Inhibit function feature in new axle counter system products following an investigation of a train collision in Germany in the late 1980s. Apparently, the collision was caused by an axle counter failing to register a train due to a failure of the inhibit function. Consequently the later generation of axle counter products do not have an Inhibit function.

4.2.3 Telegram Structure

The telegram structure is totally new. Each channel processes the same 34 Byte telegram. The addressing range is limited to 6 Bits and a 64-bit Cyclic Redundancy Code protects the data contained in the telegram.

The address is the only mechanism to ensure that the data is received by the correct EC. The 6-bit address limits the number of uniquely addressed systems to 31 (address '0' is not allowed and the are different addresses for each direction i.e. A_{EC1} and A_{EC2}, where $A_{EC2} = A_{EC1}+1$).

4.3 Backward Compatibility

The current system version is totally different from a hardware and system software perspective. It is not possible to use the QR 1987 version software with the current version hardware.

4.4 System Certification

Unlike the 1987 version developed for QR, the current version is subject to formal rail industry safety regulations and standards that have emerged over the last decade.

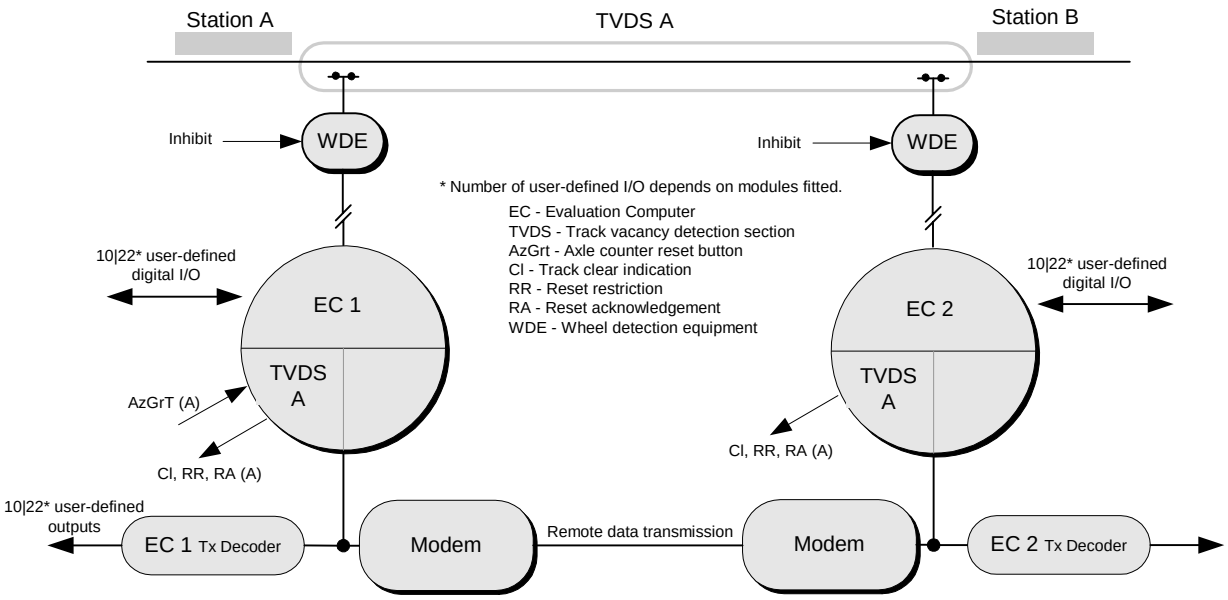

Figure 6: Axle Counter System Architecture (2003) – QR

Eisenbahn Bundesamt (German Federal Railways) has certified (approved) the current version for use according to information available from the supplier. This approval is in accordance with Mü 8004 "Technical Principles for the Approval of Safety Installations", issued by the Federal Railways Office in Germany. Mü 8004 has two levels of approval; 'Protyp Zulassung' (Prototype Approval) and 'Sicherheitsbauform' (Intrinsically Safe Version). Intrinsically Safe Version status requires several years of monitored operation without any safety-related failures.

According to the supplier, approval in accordance with Mü 8004 corresponds to 'CENELEC SIL4' i.e. the product meets current European standards, CENELEC EN50126, EN50128 and EN50129 for a Safety Integrity Level of 4.

The application of axle counters in Germany has historically been different to the QR application described in this paper. The use of the user-defined I/O for the transfer of safety-critical interlocking information has historically not been a feature of the applications in Germany.

The supplier is marketing the current version as a safety certified axle counter COTS product. While they do disclose the approval status in supporting documentation, there are no warnings or caveats on the use of the product in relation to having only 'Prototype Approval' status.

This raises the issue of placing reliance on certifications for COTS products issued by other parties and product acceptance by the industry. However such reliance is necessary as it would be impractical and cost prohibitive, both from the developer's and user's perspectives, in repeatedly having to re-certify the product for each new application. This would effectively defeat the benefit of COTS products.

However the procurer and user of a COTS product have a duty-of-care obligation to be sure as far as reasonably practicable, that the COTS product is appropriately safe for the particular application.

5 How QR is addressing the issue

As the 1987 version is no longer supported and given that QR has some 50 of these systems currently in service and there is continual demand for more such systems, QR is faced with a need to find a like-for-like technology. Whilst the existing systems could be maintained using the maintenance spares stock, this is only a short-term measure and does not address the need for new applications.

For QR's intended application, it is the view of QR that the current COTS product lacks features (no Inhibit function) and is not as safe (no I/O checking) as the now obsolete version currently in service.

Unlike the 1987 version, QR was not a party to the development of the current COTS axle counter system product and consequently has no opportunity to influence the design of the product.

QR has little choice but to use the current axle counter version. However the product needs to be adapted to suit the application needs of QR. The approach taken by QR is to adapt the product without any change to the COTS product hardware or system software, by designing solutions that make use of the available interfaces.

5.1 User-defined inputs

The approach taken by QR to continuous monitor the integrity of the used user-defined inputs is similar in concept to the approach taken for the 1987 QR version. The solution is to provide a means for extracting the input state read-in by the system and compare this read-in state

with the actual input state via an external system shutdown mechanism.

The modem is not part of the axle counter equipment kit. It is therefore possible to access the serial data transmitted from the EC via the serial data communications interface. It is also feasible to develop a module to receive and decode the serial transmitted data and extract the read-in state of the user-defined inputs, assuming one has access to the Telegram Structure specification (the supplier provided this to QR).

QR has prototyped and tested such a module. It so happens, that it is possible to house this module within the EC card frame – there is a slot reserved for diagnosis, and it is very unlikely that this slot will become unavailable in the foreseeable future.

5.2 User-defined outputs

The output configuration is the same as the 1987 QR version, albeit that there are more user-defined outputs available. Each Channel output will be compared using the external system shutdown mechanism.

5.3 Inhibit Function

QR investigated the practicality of designing a module such that when housed in the Wheel Detector Equipment (WDE) it could mask the detection of passing train wheels. The WDE has a card slot reserved for the temporary connection of the WDE Diagnostic Unit – an item of test equipment to enable the correct adjustment of the WDE. Apart from initial set-up and fault finding, this slot is unused.

It so happens that the card slot connector is connected to appropriate points in the WDE to enable an inhibit function to be designed without any other change (the supplier provided the WDE electrical drawings to QR).

QR has prototyped and tested such a module.

The Inhibit function as such has serious safety implications. QR already has a means of mitigating the safety risk associated with the Inhibit function (Section 2.1). However more analysis needs to be done to ensure that the means of mitigating the safety risk contains no new hazard due to the characteristics of the new axle counter product.

5.4 Address Range Limitation

The address range available is not considered sufficient because the data communication channels are derived channels and as such there is no surety that the EC 1 is always linked to the correct EC 2. As it happens, the increased I/O capacity allows the possibility for extending the address range. By reserving two user-defined inputs for this purpose, the number of possible unique systems increases to 127.

5.5 Supplier Consultation

Changes to a COTS product by a customer could blur responsibility in relation to product liability. It is important that any change to the product, even the non-intrusive solutions devised by QR, is done with the consent of the product supplier. QR has discussed and demonstrated their solutions to the supplier.

QR is preparing a report for the supplier describing the approach taken to provide the required functionality for QR applications of the product.

6 Conclusions

The paper gives a rail industry example of managing the introduction of safety-related COTS programmable technology through to its eventual obsolescence.

Being the main customer when a COTS product is first developed gives the customer significant influence in the development of the product. However, further development of the product is very much dependent on the needs of future customers which can, as demonstrated by the example in this paper, lead to a product which is very different to the original.

Also, the bigger the customer, the more influence they have on the evolution of the COTS product, its on-going support and the timing of its obsolescence.

The intrinsic safety of a COTS product is important, but just as important is the safety of the product's application. Claiming a product as CENELEC SIL4 outside an application context could infer that safety is independent of the product's application.

There can also be differences of opinion as to what is an appropriate level of safety for a particular application. QR was concerned about input failures being undetected in relation to the application, whereas the supplier and their subsequent customers were not, as evidenced by the removal of the 'local' output arrangement for verifying the integrity of the user-defined inputs. The removal of the Inhibit function is another example.

Customising a COTS product involves risk; it involves risk in relation to product integrity; product supportability; and product liability should a loss occur. Customisation that is needed should be as least intrusive as possible. This makes it more likely for the customisation to be relevant for future versions of the COTS product.

7 References

Cribbens, A.H. (1981): The Inverness-Wick Radio Signalling Scheme. *Proc. IEE International Conference on Railways in the Electronic Age*, London, UK, 11-13.

Lohmann, H.-J., Ziller, A. (1984): Safety Principle and Fail-Safe-Analysis of Electronic Interlocking Devices and Practical Realisation of Electronic Interlockings. *Proc. IRSE Railway Safety Control and Automation Towards the 21st Century International Conference*, London, UK, 41-48.