Business Continuity in Railway Signalling

ir Wim Coenraad, HonFIRSE, Movares
IRSE International Technical Committee

SUMMARY

In the context of engineering, resilience is the ability to continue operating, perhaps at a reduced performance level, when failures and other events occur, and to recover from such events. This is known as Business Continuity Management.

The application of redundancy, graceful degradation and "spatial diversity", i.e. having multiple routes and the control of track elements allocated to separate "interlocking machines" such that if one fails one or more paths remain available, are typical techniques to achieve this.

This paper presents an international survey of BCM in railway signalling systems and how the digital railway, where communications based signalling systems such as CBTC, ERTMS, ATO over ETCS, C-DAS etc. might experience "systemic failures". Such failures are difficult to predict and determine but consequences can seriously impact on the operational railway. Affordable mitigations need to be developed and tested for effectiveness.

Achieving resilience in day to day railway operation by means of conflict detection and resolution/rescheduling, traffic management systems, control strategies and similar "Operational Technology (OT)" aspects are largely outside the scope of this paper but are referred to if they interact with the "OT" or the System Design and Integration aspects covered in this paper. As with all current complex multi-layered railway control systems, the OT is based on the features and functions provided by the latter. Resilience has to become part the of design process in System Engineering for Railway Control Systems.

1 INTRODUCTION

Modern signalling technology covers systems ranging from simple crossing loops, large interlockings, vital network nodes and control centres containing RBCs, many controlling large sections of a line or network. Whilst system designs usually incorporate redundancy measures (standby systems, backup power supplies, etc) until recently little or no thought was given to the impact of external events, security threats or "acts of god" that could disrupt an entire control centre or similar vital installation.

2 STRATEGIES FOR BUSINESS CONTINUITY

Rail Operators are driving the signalling industry into a more holistic approach to rail operations with solutions that achieve maximised system safety but also high levels of signalling system availability. Signalling must not only exhibit "fail-safe" characteristics but also support some form of operation, albeit degraded, following equipment failures.

Meeting this challenge requires signalling solutions that:

1. Reduce the number and frequency of service-affecting failures in the primary signalling system (chapter 3.1.4);

2. Reduce the time required to recover from service-affecting failures in the primary signalling system;

3. Provide independent means to continue train movements in a degraded mode, pending restoration of the primary signalling system. Such independent means are described as secondary systems and will include 'auxiliary wayside systems', 'fallback systems', 'back-up systems', and 'degraded mode of working' systems.

3 PROVIDING FOR ROBUSTNESS OF SYSTEMS AND PROCESSES

As control of the railway is concentrated in fewer larger centres, the effects of technical failures and operational mistakes have wider ranging and longer lasting consequences.

Operators' priorities are to keep services going, both in normal operations but especially in disturbed situations. Cancelling trains whether due to line capacity reductions owing to adverse weather, technical failures or maintenance possessions, present an operational dilemma. If a whole line is closed, the number of affected passengers can be huge and replacement bus services will not cope, even if they could be ordered and mobilised at short notice. During rush hours, bus operators may not have capacity to spare.

Electronic systems can be designed for redundancy and graceful degradation, but if an important subsystem "goes down" (for example the GSM-R network fails) the consequences can be catastrophic in terms of service reputation. Because incidents happen infrequently, the ability of staff to deal with emergency situations may suffer from "lack of practice".

Scenarios and plans should be developed to handle and limit bthe effects of large scale service affecting failures. Following the Gotthard line power failure (June 22nd, 2005) which stopped train traffic in large parts of Switzerland, the following recommendations emerged:

1. Stabilise the situation
2. Configure installations for optimal availability and containment of knock-on effects
3. Keep a reduced/skeleton service going
    a. Contain the disturbance.
    b. Stabilise still functioning systems.
    c. Rapid ramp-up of additional production capacity.
4. If necessary:
    a. Active reduction of the load via operational management
5. In the crisis, the most important alarms/disturbance messages must be displayed separately.
    a. Prevent overwhelming staff in the flood of information
    b. Focus on the essentials
    c. Keep processes going
6. Analyze risk of unimaginable situations and conceive mitigations

3.1 Provision of emergency operations and recovery strategies

3.1.1 Design operations for robustness

Operational resilience is dependent on "robustness by design" and aligns with "the resilience of signalling systems". A robust timetable design, where train paths are conflict free and platform use is optimised, contributes to a stable and robust service but will require capacity margins to allow recovery from minor disturbances and variations in train running performance in which ATO can significantly help.

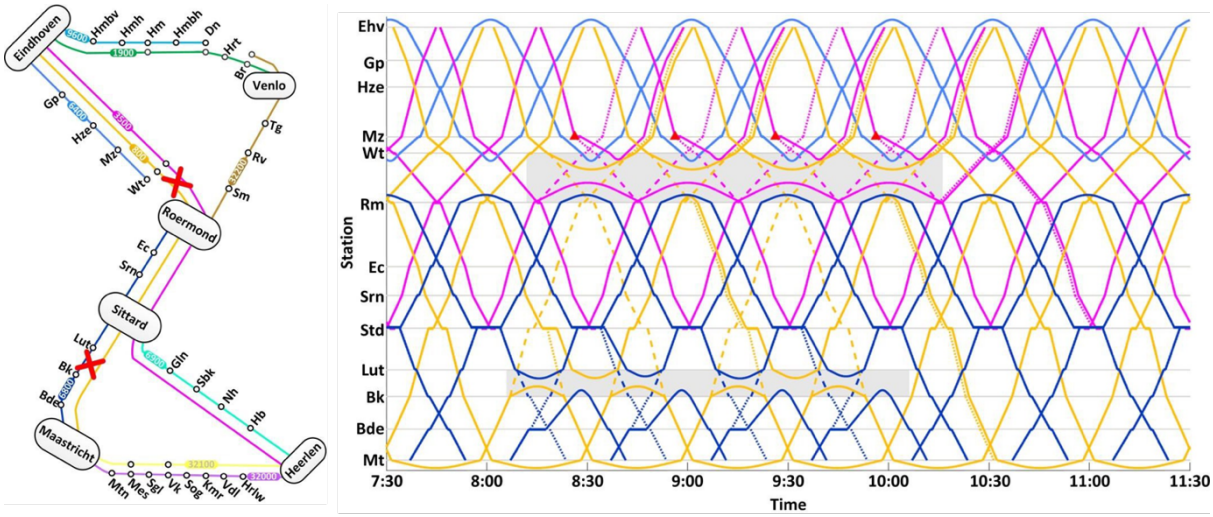
Designing robustness into signalling systems and operational planning, go hand in hand as the latter builds upon the options provided by the former.

Producing a hazard and operational risk analysis is essential to tease out all possible situations and mitigations. Some mitigations may prove unacceptable or unaffordable and these should be documented to show that the risk of severe service disruptions has to be accepted

3.1.2 Graceful degradation of service provision

Disturbances such as blockages of network nodes or level crossing failures may have pre-designed alternative operating arrangements such as cutting services, turning back trains and modifying train and train-crew rosters.

Any analysis should show how to gracefully shutdown services and systems and how to limit the effect of disruptions. This might include turning back trains (figure 1) at stations before blockages, cancelling trains or train services, providing bus services etc. Associated system designs might entail fall back detection systems.[i]



Yongqiu Zhu & Rob Goverde (TRC, ingediend)

Figure 1. Adjusting diagramming for blockages. (Goverde, 2018)

3.1.3 Redundancy and designing systems for high availability

3.1.3.1 Spatial diversity

In the signalling architecture for a layout care should be taken to design in redundancy measures so that partial services can still be run if individual equipment failures occur. Redundant interlocking computers should be configured such that each one is able to handle a complete alternative route in case the other one fails so that service can continue, accepting that connections between the routes may be unusable.

Knowing the system is important as what works for a large urban network may not be appropriate for a self-contained high capacity CBTC metro line. Where possible lines should be kept separate and designs should ensure that failures on line A cannot propagate to line B with interlocking boundaries arranged so that reversing points and loop services can be used during partial failures.

3.1.4 Using Secondary Systems

3.1.4.1 (IRSE ITC, 2018)

3.1.4.2 Primary Signalling System

The “primary” signalling is defined as the fail-safe system designed to deliver the moving of trains safely and reliably from origin to destination. This could be a conventional wayside signal system, a cab-signalling system (providing ATP and possibly ATO functions), a CBTC system, or an ETCS system (at various levels).

A generic signalling system would comprise the following elements:

- Equipment that determines train location (track-based or train-based);

- Equipment that establishes and protects a "safe route" for a train, including interlockings and other wayside signalling equipment in trackside cases, signal equipment rooms, or centralised sites. Some train based systems are now possible;
- Equipment that establishes movement authority limits for individual trains, based on train locations and route status;
- Equipment that provides movement authority enforcement and other safety-related or operations-related functions, either track-based, train-based, or a combination of both;
- Central office equipment providing control and supervision functions;
- Data and radio communications equipment to link the various elements;
- Power supplies for all wayside, train-borne and central office equipment;

3.1.4.3 Secondary Systems

The different terminology used to describe secondary systems can create confusion and misunderstandings arise as to the purpose and intent of these systems. See below the different grades of secondary systems (GoSS)

A. The lowest grade, defined as a ***GoSS 0*** solution, has no secondary system, degraded mode working following a service-affecting failure of the primary signalling system being achieved by compliance with operating procedures. Control centre personnel issue verbal movement authorities, and train operators comply with these authorities. The primary system would typically include facilities to override the "fail-safe" signalling protection in order to move trains (e.g. the 'one shot' train stop override feature in the UK TPWS system).

B. Next, we have the ***GoSS 1*** solution with degraded mode working still managed through strict compliance with operating procedures, but with non-vital secondary systems provided to assist control centre personnel in issuing verbal movement authorities and thus assist the train operator in complying with these. The intent is to reduce the risk of human error and to reduce the operational impact of the primary signalling system failure.

C. Up from this is a ***GoSS 2*** solution, where secondary systems begin to duplicate certain safety functions performed by the primary signalling system but do not provide the same level of safety protection. Specifically, a ***GoSS*** 2 solution would include an independent secondary means of train location determination. The intent is to reduce, but not eliminate, reliance on operating procedures during degraded mode working.

D. The next option is a ***GoSS 3*** solution, where the secondary means of train location determination, is enhanced by a system to provide an independent means for establishing movement authorities (MAs).

E. Finally, there is a ***GoSS 4*** solution, where the secondary systems provide the same level of safety protection as the primary signalling system by independently establishing train location, creating and issuing movement authorities for trains that are not protected by the primary signalling system. These are essentially an alternative signalling system and provide an equivalent level of safety for degraded mode working equivalent to normal operations. A ***GoSS 4*** solution will support "mixed mode" operations i.e. where some trains operating on the line are not protected by the primary signalling system and therefore have to be protected by secondary systems

Clearly, the higher the "GoSS" level, the more complex the signalling solution.

The extent to which secondary systems are required should consider:

a) The frequency and operational consequences of service-affecting failures in the primary signalling system

b) The time required to recover from such failures.

c) The grade of automation (GoA) of the line, i.e. whether or not there is a driver/train operator on board the train

d) The safety and operating performance levels required during degraded mode working.

If the primary signalling rarely fails and the operational impacts are minor with recovery to full service being accomplished rapidly, there would be a limited business case for secondary systems.

3.2 IMPROVING THE AVAILABILITY OF THE PRIMARY SIGNALLING SYSTEM

Minimising the frequency and operational consequences of service-affecting failures in the primary signalling system is key business case requirement, and there are essentially two approaches to achieving high levels of signalling system availability.

Firstly, is to focus on achieving the lowest practical hardware failure rates for individual components and items of equipment that form the specific signalling solution (for example, enhanced reliability in track circuits, point status indications, relays, signals, power supplies, cable connections, etc.). The signalling industry has concentrated on this traditional approach by design improvements, remote condition monitoring of equipment and pro-active predictive maintenance strategies. The advantage is that it retains simple signalling system architectures. However there remains a relatively high number of single points of failure that can be service affecting. In practice, single point failures can be difficult to predict until the failure occurs.

Secondly, is to focus on eliminating or minimizing single points of failure within the signalling system solution, an approach that has become commonplace with the introduction of computer-based and communications-based technologies. The concept is to apply appropriate levels of equipment redundancy and diversity such that the failure of a single component, device, power supply or communications channel will not render the system unavailable or operationally unworkable. Such duplication includes all elements of the system including communication links and power supplies. The advantage should be much higher levels of systems availability but with an increase in system complexity and associated cost.

The ultimate objective is to keep the signalling solution as simple as possible to meet the business case needs and operating/maintenance practices. This includes the system architecture and nowadays the dominant system software.

Redundancy must be designed into the core system design with the complexity being made transparent to the operator. Failed elements should be simple lineside replaceable units and ideally hot swappable.

Whilst modern software-based signalling systems may ultimately exhibit high levels of system availability, the time required to achieve this once commissioned, may justify the need for secondary systems at least in the early part of service. Against this, is that poor system availability during initial operations is a consequence of inadequate/incomplete testing & commissioning plus a lack of operational and maintenance readiness. Consequently, more effort should be expended in these areas before incurring the capital and ongoing maintenance costs of secondary systems.

3.3 REDUCING THE RECOVERY TIME AFTER A SERVICE-AFFECTING FAILURE

Reducing the time required to recover from a service-affecting failure in the primary signalling system requires many considerations including:

- The time required to identify the nature of the failure;
- The travel time to the appropriate site;
- The time at the site to diagnose and identify the failure
- The time to replace the failed component(s)
- The time to test the repaired unit/subsystem.

Measures to reduce the time required for recovery from a service-affecting failure could include real-time condition monitoring, remote and local diagnostic provisions. System access can be improved by minimising track-based equipment and centralising critical systems wherever possible. Sectorised signalling systems whereby sector ‘islands’ yield easy reversing facilities, may offer the best compromise to achieve graceful degradation of service provision (including if necessary bus substitution), whilst facilitating easy access to the failed site .

The effectiveness of maintenance support systems and the training, physical location and availability of maintenance personnel and spare parts will influence the recovery time. Even the best strategy or design fails if trained people are unavailable or there are not enough spares in stock.

3.4 SELECTING THE APPROPRIATE SECONDARY SYSTEMS

Knowing the location of trains is an essential prerequisite for issuing movement authorities, and thus any secondary system must also achieve this. Three specific scenarios are considered:

1) The primary train location determination equipment is track-based (for example, fixed block signalling with track circuits or axle counters to determine train location). In such a scenario, any secondary train location determination system would likely be train-based, with train position information communicated to central control via a train-to-wayside data/radio communications link;
2) If the primary train location determination equipment is train-based (for example, moving block CBTC or ETCS Level 3 systems), then the opposite will apply and the secondary train location determination equipment would likely be track-based (track circuits or axle counters);
3) Thirdly, if movement authorities are established by track-based train location determination equipment, and movement authority enforcement is achieved by train-based train location determination equipment (e.g. "distance-to-go" and ETCS Level 2 signalling systems), then the secondary system should be independent of both.

Discussion on each of the above three scenarios is provided below:

3.4.1.1.1 Scenario #1

Examples of Scenario 1), are ***GoSS 0*** systems with track-based (track circuits or axle counters) train location and traditional fixed-block signalling. Secondary systems are not normally provided, reliance being placed on highly reliable components/equipment to achieve acceptable levels of system availability. Degraded mode of working would typically be strict compliance with operating procedures, utilising communication facilities to override the fail-safe signalling protection (e.g. to allow a train to pass a restrictive signal aspect).

3.4.1.1.2 Scenario #2

Examples of Scenario 2), where train location equipment is train-based, would include the newer generations of moving block signalling technology such as CBTC or ETCS Level 3. To date, the discussion on secondary systems has centred around CBTC deployments on passenger-carrying metros (TRCP, 2017), but would equally apply to ETCS Level 3 deployments for passenger and freight trains on mainline railways.

Since the initial CBTC installations in the 1980's, CBTC technology is now widely deployed around the world, in both "greenfield" (new start) and "brownfield" (re-signalling) applications. The technology is used on light-rail systems, metros, and commuter rail systems, with grades of automation from GoA 1 (ATP only) to GoA 4 (fully automated/unattended). CBTC technology is available from multiple suppliers and is service and safety proven, with substantial operating and system availability experience.

However no "industry standard" CBTC solution exists and CBTC systems have been deployed both with and without secondary systems, the latter having many variants.

A ***GoSS 0*** example is the early "greenfield", inductive loop-based CBTC system on the SkyTrain in Vancouver, Canada, operating at GoA 4, which has no secondary systems. A ***GoSS 4*** example is the first "brownfield", radio-based CBTC system, on the Canarsie Line in New York, USA, operating at GoA 2, which has track-based secondary train detection (track circuits) and secondary train protection (wayside signals and train stops) primarily to support "mixed mode" operations.

Many examples exist of CBTC ***GoSS 2*** and ***GoSS 3*** solutions, using track-based secondary means of train location determination (track circuits or axle counters).

Trends

Every new CBTC application provokes a renewed debate on the requirement for and nature of any secondary systems. Most CBTC systems inherently incorporate features to assist control centre personnel during degraded modes of operation, specifically for the movement of trains in a total failure of train-borne CBTC equipment situation or to work around blocked tracks. Having high-capacity, bi-directional, data communication links between control centre equipment, wayside equipment, and train-based equipment, CBTC systems inherently provide control centre personnel with a high level of information on train and infrastructure status.

Currently, ***GoSS 0*** solutions, with no secondary systems, have been limited to "greenfield" CBTC applications operating at GoA 4, with the emphasis placed on achieving the highest possible levels of availability of the primary signalling system, given the absence of on-board staff to support degraded modes of working. Whilst service-affecting failures can still occur, the frequency of such failures, and the recovery time from such failures, are such that the operational impacts are generally assessed to be acceptable. An analogy can be drawn here to traction power systems which are also designed to include high levels of redundancy with no "secondary" systems. Should a traction power system failure occur, the only option is to suspend service until power can be restored, which is deemed acceptable if the frequency of such failures is sufficiently rare.

Early ETCS Level 3 deployments are likely to be mixed-mode operations. As such, a "Hybrid Level 3" solution is currently being jointly developed by Network Rail in the U.K. and ProRail in the Netherlands where track-based train detection (track circuits or axle counters) would be retained to support both Level 2 and Level 3 compatible trains, such as trains without and with Train Integrity Prooving). This would be a ***GoSS 2*** solution, as there would be no independent equipment to replace the functionality of the Radio Block Centres (RBCs) or train-based ETCS equipment. Any train not equipped for either ETCS Level 2 or 3 operation would not be permitted to run on a Hybrid Level 3-equipped route unless lineside signals were also retained (a ***GoSS 3*** solution). The intent of Hybrid Level 3 is to facilitate Level 3 operation on what essentially is still a Level 2 line.

The primary motive for providing secondary systems on a CBTC line is a ***GoSS 2*** solution to support a more rapid recovery to full service following a failure of the primary CBTC system. A similar motivation should be anticipated for ETCS Level 3 deployments, even when all trains operating on the route are equipped for ETCS Level 3 operation.

Operational risk assessments need to consider the frequency of CBTC system failures, the operational impact of failures, and the time to recover from such failures (using data from existing in-service CBTC systems). Experience would show the highest risk relates to a lack of train location reporting from a single train. While such failures are "fail-safe", recovery requires train location reporting to be re-established, meaning that train movements in a degraded mode have to re-initialise normal train reporting. This can be achieved by strict adherence to operating procedures, utilising features and functions available within the primary CBTC system (***GoSS 0*** solution), or can be supported by independent systems to determine a train's position, typically track circuits or axle counters (***GoSS 2*** solution.

Experience shows that migrating to CBTC is significantly simplified if axle counters are used as the means of secondary train detection as an alternative to track circuits. The ultimate objective is for suppliers to produce systems without single point failure risk, whence secondary detection could be eliminated. However, systems that make claim to this in a RAMS analysis are found to fail in the field in ways not predicted!

3.4.1.1.3 Scenario #3

Examples of Scenario #3, relate to movement authorities established by track-based train location equipment and enforced by train-based train location determination include fixed-block distance-to-go cab-signalling systems and ETCS Level 2 systems.

ETCS Level 2 systems are not usually stand-alone signalling solutions but are deployed as an overlay using existing track-based train detection equipment and existing interlockings for establishing movement authorities, which are then enforced by train-borne ETCS Level 2 equipment. The availability of the complete signalling system solution is therefore constrained by the reliability and failure recovery times of the existing track-based train detection equipment and interlockings. As with scenario #1, these train detection and interlocking subsystems do not include any secondary systems and are thus a ***GoSS 0*** solution, relying on acceptable levels of system availability through highly reliable components/equipment. Any secondary system must be independent of both

track based and train borne elements, an example being the COMPASS DMWS system being trialled by Network Rail

3.5 COMMUNICATIONS

ERTMS equipped railways depend on the availability of the communication between train and Radio Block Centre in ETCS Level 2 and 3 modes and also in ERTMS Regional. This is true also for CBTC systems found on rapid transit systems. Unless some form of distributed communications network is used, such systems can fail quite dramatically. GSM-R as the current standard for main line track to train radio has experienced several embarrassing network failures (in Norway in 2011 and in the Netherlands in May 2014) which led to large scale disruptions to train traffic.

Even distributed coms networks are not immune. CBTC requires fully redundant radio networks and currently most use the industrial, scientific and medical (ISM) radio bands at 2.4/5.8 GHz which can experience interference from passenger mobile devices. Instances have occurred in China where passengers carrying Mi-Fi hot spots have taken out the signalling system. On the Singapore circle line, transmissions from a rogue train affected the signalling system causing trains in the vicinity to randomly fail.

The potential disruption to a high-speed network or busy commuter railway is immense. If the RBC is unable to communicate its movement authorities to the trains under its control, no train would be able to update its location or operational status. Unless some form of degraded mode operation is available, like a Level 1 fall-back or a bespoke national ATP, all traffic would be halted. Also, would all trains be backwards compatible, and thus interoperable, with that system as well? Even when communication is re-established, the re-initialisation process would require all trains to report their locations to a RBC, where a “roll-call” of all trains previously known to be in the system is unlikely to be a speedy procedure. Recourse to running a first train on-sight over the entire line, to prove “line clear” will make service recovery a prolonged process. One possible scenario is to have a secondary communication system using the public mobile networks but this will have design and commercial complications.

3.6 Provision of emergency operations and recovery strategies for Control Centres

3.6.1.1.1 Concentration of Control

Railways nowadays tend to centralise their traffic control functions inside a limited number of “electronic or operational control centres”, which link to interlockings and/or RBCs located along the lines and stations they control by remote control technology. Loss of the control centre itself, or one or more of these remote-control links will mean a line or node being blocked. Maybe some form of local control room capability is retained, but will competent signalmen and traffic controllers be available on site to operate these local controls? Getting to the site may require them to use a car. Murphy’s law predicts they will get stuck in queues on the motorway or some other disruption.

3.6.1.1.2 Emergency Control Facilities

Mission critical large centralised computer facilities should be provided with disaster recovery plans such that if one control centre is rendered unusable as the result of a technical malfunction, fire or terrorist event, the communication links to the interlockings and RBC can be reconfigured and rerouted to an emergency centre. Staff from the “inoperable” control centre must be prepared to move to the emergency one as signallers and traffic controllers require “local” knowledge of the routes they are controlling. The time needed to reconfigure the communications links is not an instantaneous action; Netherlands Railways / ProRail estimate this process will take about four hours. In addition, the configuration data for the evacuated control centre must be loaded into the emergency centre’s systems, as a remote dial in facility is unlikely to still work. Hopefully the interlocking to be controlled from the emergency centre was not co-located in the evacuated building, otherwise it could be inaccessible. Redundancy needs to consider the ‘whole system’ in each of the possible configurations.

Singapore provides back up control centres with full functionality for every line. Transition from main OCC to back-up OCC involves control being passed initially to the Passenger Service Centres at stations whilst operators are moved to the Back-up OCC which then takes control from the PSC. Transition back is the reverse process. Note that the Passenger Service Centres are always manned so transition can be quite quick.

3.6.1.2 Limits to evacuation of Control Centres

3.6.1.2.1 Interlockings

Most electronic or computer based interlocking architectures have an internal bus or communications link between the operator terminals and the "processing units". These allow the operator terminals to be located in an emergency centre, thus fulfilling the evacuation requirement but these links are rarely provided with "open interfaces" using standardised protocols. Networking these connections can therefore be difficult, especially if the operator workstations are subject to SIL 1 or higher safety requirements, as this will require the links to meet the same safety requirements.

Except where trackside object controllers that provide direct connection to points, signals, track circuits, axle counters, level crossing controllers etc., are also networked, the connection between interlocking and field element is usually a fixed, point to point multi-wire link. It is therefore very difficult to locate a backup interlocking in an emergency centre without having a credible way to provide the configuration data from the site, remotely load it into the emergency interlocking and commission it.

Some CBTC suppliers provide the interlocking function and associated movement authorities within the zone controller. If the zone controller fails, the interlocking activates its logic to provide a basic signalling scheme, which relies on the zone controller and the interlocking both being able to control the trackside objects. IP based signalling technology provides this, with some interlockings separating the interlocking core from the object controller for easier management and increased independence.

3.6.1.3 RBC'S

Radio Block Centres are often based upon workstation-like computer systems that can be located "almost anywhere". Connection to the GSM-R system via a network gateway would permit the provision of similar equipment in emergency centres to recover operations if they become compromised, with the same proviso as for control centres in rerouting traffic and loading of configuration data. Unfortunately, the Interlocking-RBC interface is not standardised, each supplier having its own bespoke interface for this safety related link. The result is that ERTMS interlockings and RBCs can currently only be moved as pairs, thus making the provision of an interlocking in an emergency centre more difficult.

3.7 Security

External events such as fires, natural disasters etc. are likely to be service affecting failures and mitigated by the type of IT and OT design strategies prescribed.

Business Continuity Management has been described in terms of System Safety and Reliability Engineering; RAMS for short in the "CENELEC EN50126-50129 standard paradigm". BCM has been analysed from the perspective of increasing complexity of systems, larger areas of control, larger concentrated control centres and increasingly communications-based. This combined with the reduction of "on the ground" equipment, notably track-based train detection, improves the business case and reduces occupational health and safety hazards related to trackside work, i.e. the "danger zone". This process, based on hazard identification and mitigation analyses that are well understood, presumes reasonable and predictable (through training, education etc.) behaviour of humans in a controlled environment. It excludes vandalism, sabotage etc. from the equation but needs to take account of copper theft, persons putting coins across insulated joints in front of trains, irresponsible behaviour at level crossings and suchlike. Such hazards and threats will be present regardless of the technology in use.

3.7.1 Cyber security

Security assumptions are however now required to consider the world where the 'hacking' of systems has evolved and range from young inquisitive minds ("script kiddies") looking to see which systems they can get access to, through to commercial interest groups and nation states employing cyber warfare techniques to disrupt critical infrastructure and / or extort money from operators and owners of such infrastructure.

Cyber security is discussed in other sessions and papers in the Aspect 2019 conference, and this paper will only look at BCM implications.

Cyber threat protection is usually based on the principle of layered defences, diversity in those defences and the ability to "retreat, regroup and recover". Cyber threat specialists and the large signalling suppliers consider that defending against attacks on a nation state level (cyber warfare) is virtually impossible or would require mitigations or preventative measures that would be unacceptable. As such the CENELEC paradigm where a risk with *critical* or *catastrophic* consequences for which the probability of occurrence is likely to be in the region of *unlikely* or *incidental* is classified as *unacceptable* or *must be mitigated to ALARP standards*, would be unachievable. The current hazard log philosophy does not entertain *mitigations too drastic to be contemplated*.

Whilst it will be quite difficult to sabotage a system and e.g. falsify a movement authority, it is quite simple to instigate a denial of service attack that stops the railway. The reality is that someone out there has the knowledge to do just that. Monitoring systems, both from within a Security Operations Centre and radio based, are available to detect intrusions and potential attacks, but one challenge is to separate the immense number of false positives from the real attacks. The Dutch SOC for roads and public infrastructure[ii], which will also monitor the ProRail network, revealed 12 billion logged events in one week, resulted in 260,734 alarms of which 9 were potential cyber-attacks. This high rate of false positives is relevant for ETCS and CBTC systems.

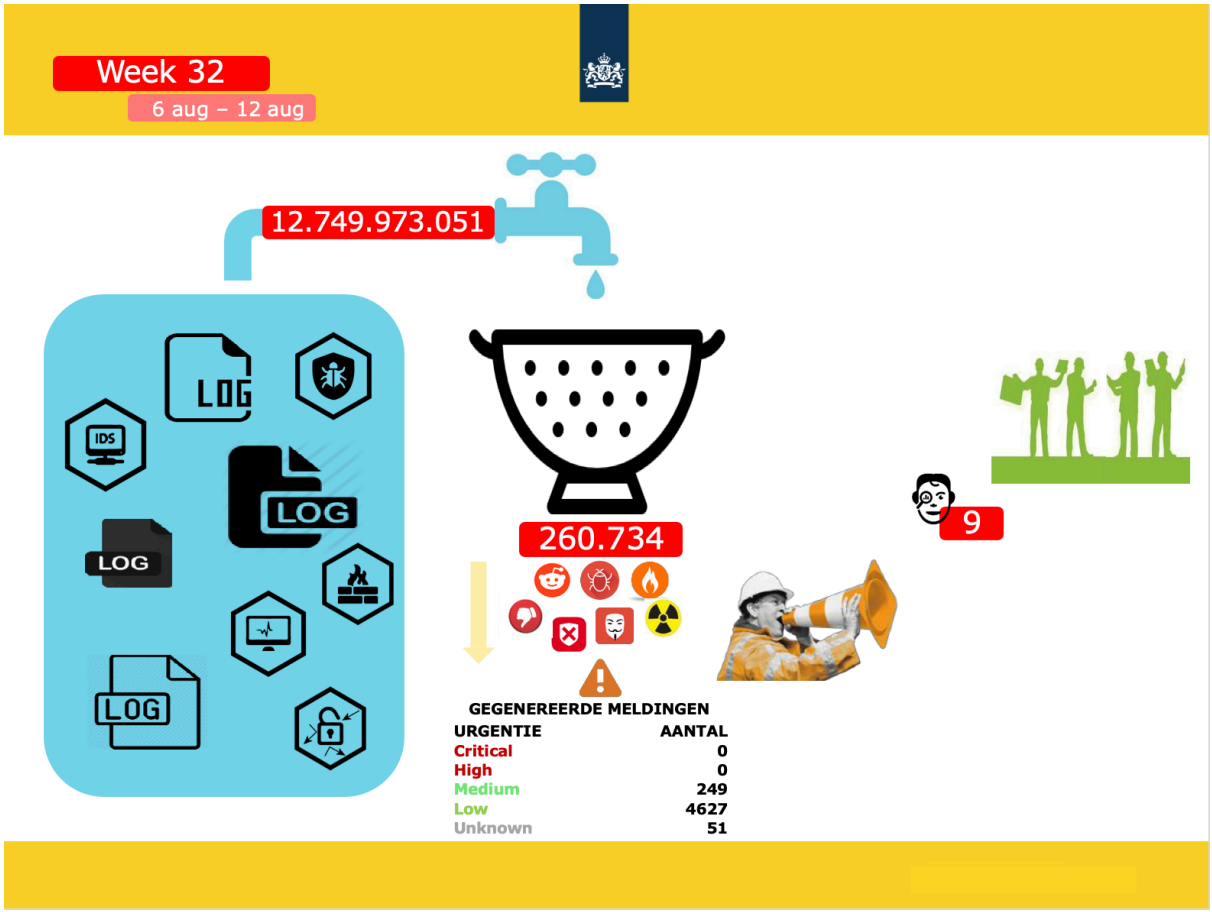


Figure 2. Dutch Highway and Waterway Authority SOC alarm rate (de Coninck, 2019)

Cyber security experts work on the premise of not "if" but "when" a defence will be breached, and once breached the process of "retreat, regroup and recover" involves replacing that line of defence with a better one. This may mean employing more powerful encryption in the comms system. Even when designing systems and interfaces in such a way that "replace and improve" modifications are actually possible, it is likely that the EU safety directive will deem this a "significant change". The risk is that safety cases may need updating, safety and interoperability certificates could become invalid and need renewal and, in the worst case, permission to operate being withdrawn. Advice from the Regulator would appear sensible, but none of this bodes well for Business Continuity!

Lastly, cyber security advice is derived from IT system practices, which hopefully are capable of being applied to modern system architectures such as ERTMS, CBTC and IP based and/or cloud based emerging signalling designs. However, many vital signalling and telecom installations consist of legacy bespoke systems and

architectures which were never designed on those principles. Often described as “operational technology museums” or “signalling zoos”, they may be 10 to 20 years old or more, with expectations of ongoing service for a similar period without support from their original suppliers and manufacturers, if still in existence. Many of such systems are networked and/or remote controlled and the belief that “obscurity” or “obsolescence” is a viable defence against hacking would be misguided, much akin to the fiction of closed networks being impenetrable.

4 CONCLUSION

Business Continuity Protection measures must be based on detailed risk analysis and the possibility of measures such as fall-back systems and the availability of on-board staff to intervene when OT systems fail. There appear to be no simple and “evidence based” recipes to ensure the digital railway, with communications based signalling and control systems, such as CBTC, ERTMS, ATO over ETCS, C-DAS etc. will not expose the operator(s) to “systemic failures”. Such failures, their probability of occurrence and time to recover are difficult to predict and determine. The examples quoted in this paper show that as an industry we are still coming to terms with the inherent complexity of the digital railway. The common theme is that for any fallback strategy, whether only relying on applying rules and regulations or employing supporting systems, knowledge of the number of trains in the system and their location is crucial. This also applies to restarting operations after a major shutdown. Best practice, at least in greenfield applications, tends to focus on achieving reliability levels of the primary systems that are comparable with traction power supplies, rather than complicating design with secondary systems which might add to unavailability themselves, especially when such secondary systems have to be specified to SIL levels 2 or higher. In addition emphasis is placed on designing for degraded mode operations.

5 ABBREVIATIONS

Acronym	Log Form
ATC	Automatic Train Control
ATP	Automatic Train Protection
ATO	Automatic Train Operation
BCM	Business Continuity Management
C-DAS	Connected Driver Advisory System
CBTC	Communications Based Train Control
ETCS	European Train Control System
ERTMS	European Rail Traffic Management System
GoA	Grade of Automation
GoSS	Grade of Secondary System
GSM-R	Global System for Mobile Communications - Railway
IP	Internet Protocol
IRSE	Institution of Railway Signal Engineers
IRSE-ITC	Institution of Railway Signal Engineers - International Technical Committee
ISM	Industrial Scientific and Medical
IT	Information Technology
MiFi	Portable Mobile Data Access Point using WiFi
OCC	Operations Control Centre
OT	Operations Technology (non-user IT)
RAMS	Reliability Availability Manitainability and Safety
RBC	Radio Block Centre
SIL	Safety Integrity Level
TCRP	Transit Cooperative Research Program

6 REFERENCES

1. Goverde, R. (2018). Inaugural Address Prof. RM Goverde, Delft Technical University
2. IRSE ITC. (2018), IRSE ITC Report on Topic 52, Achieveing High Levels of System Availability, IRSE News Issue 247, September 2018
3. de Coninck, S (2019). Rijkswaterstaat, Sandor de Coninck, ASTRIN, Digitale (on)veiligheid, 2019
4. TCRP. (2017). "A Transit Agency Guide to Evaluating Secondary Train Detection/Protection Systems in Communications-Based Train Control Systems, Transit Cooperative Research Program (TCRP) Document 71, April 2017),
5. Wikipedia. ERTMS Regional, https://en.wikipedia.org/wiki/ERTMS_Regional