Avoiding the Butterfly Effect of Failures in Railway Signalling and Telecommunication Systems

How can we design our Railway Control and Command Systems for optimum continuity of operations and business?

Prepared for the IRSE International Technical Committee by ir. Wim Coenraad, Movares, The Netherlands

SUMMARY

In chaos theory, the butterfly effect is the sensitive dependence on initial conditions, in which a small change at one place in a deterministic nonlinear system can result in large differences in a later state. The name of the effect, coined by Edward Lorenz, is derived from the theoretical example of a hurricane's formation being contingent on whether or not a distant butterfly had flapped its wings several weeks earlier.

Although the butterfly effect may appear to be an esoteric and unlikely behaviour, it is exhibited by very simple systems. For example, a ball placed at the crest of a hill may roll into any surrounding valley depending on, among other things, slight differences in initial position.

Modern signalling systems can have spans of control ranging from simple crossing loops to large interlockings controlling vital network nodes and control centres containing Radio Block Centres (RBC) etc. that control large sections of a line. Whilst in most cases the system designs incorporate redundancy measures such as standby systems, backup power supplies etc., little or no thought is given to (catastrophic) external events, security threats or "acts of god" that could take out an entire control centre or similar vital installation. Perhaps a root-cause of the scenarios identified (where a relatively simple failure leads to a more significant system outage) could be that as systems and their associated physical and functional interfaces become more complex, the design of the total system no longer falls totally within the domain of one technical discipline/area or expertise, but rather involves multiple technical disciplines – the signalling engineer, the telecommunications engineer, the vehicle engineer, the power engineer, the fire protection engineer, etc., etc. This really highlights the importance and need for a true multi-discipline Systems Engineering process; a process that is often difficult to embrace within organisations that are rigidly structured around specific technical disciplines with limited coordination between the different engineering departments.

STRATEGIES FOR BUSINESS CONTINUITY

Providing for continuity of service in railway infrastructure systems entails three aspects:

1. Providing for robustness of systems and processes.
2. Graceful degradation of service provision.
3. Provision of emergency operations and recovery strategies.

PROVIDING FOR ROBUSTNESS OF SYSTEMS AND PROCESSES

As the control of the railway is concentrated in fewer larger centres, naturally the effects of technical failures and operational mistakes can have wider ranging and longer lasting consequences. At the same time, since train operations, maintenance etc. have been privatised, contracted out etc., several entities may be competing for scarce resources, such as priority in keeping their service going. Not just during normal operations, but especially in disturbed situations. Consider for example the decision about which train operator's trains are cancelled in case line capacity is reduced due to adverse weather, technical failures or simply maintenance possessions. Who orders the replacement bus services and where does the bill go? In other words, with the dissolving of the integrated railway, the overall system control function also becomes unglued.

Processor based systems can be designed for redundancy and graceful degradation, but at the same time, when the inevitable happens and a vital subsystem goes down, for example the GSM (-R) network fails, the consequences can be catastrophic in terms of service or number of passengers affected, or even damage to reputation. And when the inevitable does happen less frequently, the ability of staff to deal with emergency operations and degraded modes may suffer from lack of practice.

It is for this reason that the Dutch rail sector has voluntarily joined forces and set up the Operational Control Centre Rail (OCCR), which essentially is a nationwide incident room where all actors exchange information and end up agreeing and coordinating their incident response. Ironically, at first this initiative was treated with suspicion by the competition authorities, but since participation is on a voluntary basis and open to all, is indeed now considered a success.

This paper is not about how to design for robustness, but rather sets out to explain why we should.

Provision of Emergency Operations and Recovery Strategies

Graceful Degradation of Service Provision

Despite all our best efforts to make our infrastructure robust and provide degraded modes of operation, one day a system will fail. And given the degree of centralisation and interdependencies of systems, this means a large part of the network will go down. Perhaps because a control centre suffers a power failure, is flooded, catches fire or becomes unreachable because of terrorist activities, or it needs to be evacuated as a result of a leaking tank wagon carrying hazardous materials in a nearby yard.

Recovery may take days or even weeks, so we need an evacuation centre to move our operations into. There are examples of all these types of incidents.

COMMUNICATIONS

ERTMS equipped railways rely heavily on the availability of the communication between train and Radio Block Centre, at least in ERTMS Level 2 (and even more so in Level 3) and also in ERTMS Regional. The same is true for the Communications-Based Train Control systems more commonly found on rapid transit systems. Unless some form of distributed communications network is used, such systems can fail quite dramatically. GSM (and by extension GSM-R) is a case in point. There have been several instances of public mobile phone networks going down for days. Now imagine the disruption to your high-speed network or busy commuter railway, if for example the RBC is unable to communicate its movement authorities to the trains under its control. Unless some form of degraded mode operation is available, like a Level 1 fall-back or the bespoke national Automatic Train Protection system, all traffic would be halted. And even if a fall-back system were available, would all "interoperable trains" be backwards compatible, and thus interoperable, with that system as well?

PROVISION OF EMERGENCY OPERATIONS AND RECOVERY STRATEGIES FOR CONTROL CENTRES

Concentration of Control

A number of railways centralise their traffic control functions inside a limited number of electronic or operational control centres. Using some form of remote control technology these centres interface with interlockings and or RBCs on, or along, the lines and stations they control. Loss of the control centre itself, or one or more of these remote control links means that a line or node can be blocked. Even if some form of local control room capability is retained, it is unlikely that competent signalmen and traffic controllers will be available on site to operate these local control rooms. So they need to travel there to resume local operation. Of course they can't get there by train, so they will need to use a car. And according to Murphy's law they will get stuck in queues on the motorway during the rush hour.

Emergency Control Facilities

As with any mission critical large centralised computer facility, it is necessary and possible to provide emergency facilities. If one control centre is rendered in-operational, e.g. as the result of a technical malfunction, fire or even terrorist event, the communication links to the interlockings and RBC can be reconfigured and rerouted to the emergency centre. Whilst this is being done, the staff from the inoperable control centre moves to the emergency one. Usually this is required because signalmen and traffic controllers require local knowledge of the layout they are controlling. The time needed may be available as reconfiguring the communications links is not a trivial and/or instantaneous action either. E.g. Netherlands Railways / ProRail estimate this process will take about four hours. In addition the configuration data for the control centre that needed to be evacuated must be loaded in the emergency centre's systems, as it is unlikely that a remote dial-in facility would still work. And hopefully the interlocking that must now be remote controlled from the emergency centre was not co-located in the same building that had to be evacuated, rendering the control centre inoperable or inaccessible.

Limits to Evacuation

Interlockings

Whilst most electronic or computer based interlocking architectures have some form of internal bus of communications link between the operator terminals and the processing units allowing the operator terminals to be placed at a distance, even in an emergency centre and thus providing for the evacuation functionality, these links are rarely provided through open interfaces using standardised protocols. Networking these connections is therefore not a trivial exercise, even more so if the operator workstations are subject to SIL 1 or higher safety requirements, as in that case the link between processing unit and operator workstation must meet these safety requirements as well.

Except in systems where the object controllers that provide the input and output functions to the field elements such as points, train detection equipment and signals are also networked, the connection between interlocking and field element is usually a fixed, point to point multi-wire link. And so it is feasible, but very difficult, to provide a backup interlocking in an emergency centre, even if we had a credible way to provide the configuration data off site, remotely load it into the emergency interlocking and somehow commission that.

RBCs

Radio Block Centres tend to be implemented in workstation-like computer systems that can be located almost anywhere. They connect to the GSM-R system through a network gateway and would seem to lend themselves just as well to the provision of similar equipment in emergency centres to recover operations if they, or their locations, become compromised, subject to the same provisions mentioned for control centres in rerouting traffic and loading of configuration data. Unfortunately the Interlocking-RBC interface is not standardised and every supplier has developed its own bespoke interfaces for this safety relevant link. This would suggest that for ERTMS interlockings and RBCs could only be moved as pairs, if the interlocking can be moved to an emergency centre at all.

EXAMPLES OF CATASTROPHIC EVENTS

To illustrate the need for thought about providing emergency recovery and evacuation facilities in our railway we have assembled some examples of the more spectacular outages on the railway.

1 - Utrecht Control Centre Fire, 19 Nov. 2010

As the result of a fire in the room that houses Utrecht Central Station's emergency power supplies and no-break equipment on 19 November, 2010, all train traffic came to a halt. At approximately 16:00, a fire broke out in the equipment room which is located at the first floor of Utrecht Traffic Control Centre. As was discovered later, the fire started in smouldering wires, used in a measurement setup installed by the supplier of the no-break power supply. The OCC building also houses the interlocking and traffic control systems, passenger information equipment etc. The fire brigade ordered the power to be cut. Subsequently, as the fire could not be extinguished using foam, the fire brigade used water to fight the fire. Extensive damage to the equipment resulted. As the power from the control

centre to the field elements was cut and the backup arrangements disabled by the fire, no power to points, signals etc. was available, effectively immobilising Utrecht Central Station, the hub of the Dutch Railway Network and a number of stations on the lines radiating in and out of Utrecht, which are remote controlled from the OCC. The traffic control room and Utrecht Central station were evacuated in a hurry. As a result 30 trains in and around Utrecht could not proceed even though the overhead was still powered and passengers had to wait for hours before their train could be set back to a nearby station or they could be evacuated walking along the tracks.

Once the staff was allowed back on the control floor and maintenance teams were allowed in the equipment rooms, emergency power supplies were installed. As during the hasty evacuation and due to the power being cut, the computer systems were not shut down in a controlled fashion, all systems had to be restarted and tested after emergency power supplies had been installed by early Saturday morning. Around 15:00 on Saturday, traffic around Utrecht was slowly resumed. By early Sunday morning a temporary backup power supply had been installed in a container, and power was restored to point and signals in Utrecht CS, allowing traffic to be resumed there as well.

This fire was instrumental in triggering ProRail's strategy to provide an emergency evacuation OCC co-located with the Operational Control Centre Rail some distance from Utrecht CS. Tests have demonstrated that control of a large OCC can be switched to the evacuation centre in a mater of 4-5 hours. During this time, which is required to reroute all communications, control centre staff can travel to the evacuation centre.

2 - SBB Power Failure, 22 June 2005

An unprecedented power failure shut down the entire rail network of Switzerland. SBB operated its own power grid at 15 kV 16.6 Hz and has a number of power plants. The north and the south of the network are connected by two High Voltage power lines. Furthermore the SBB power grid is linked to the DB grid at two locations.

An SBB "post mortem" management presentation explains what happened:

At 17:08 a short overload on the high voltage power line across the Gotthard during the rush hour caused the maximum current protection devices to trip, separating the north of the SBB power grid from the south, at a time when the second High Voltage power supply line route was out of service for planned works.

11 seconds later three power generating plants in the south were tripped as well, at 17:17 a further generating plant tripped and attempts to switch the alternative High Voltage route back in, after completing of the building work, failed. In the ensuing confusion and information overload for the staff in the power network control centre the fact that the links tot the DB power grid were overloaded were missed and the situation deteriorated further.

The resulting network wide power failure left thousands of tourists and commuters across the country stranded and the rail authority scrambling to fix the problem.

The first trains began to run again shortly after 20:00, but much of the system remained out of operation.

Post mortem analysis shows that the risk of allowing the work on the High Voltage line was erroneously considered manageable, alarms and information in the control centre allowed no separating wheat from chaff and operational staff "could have been better prepared to deal with emergency situations".

(Source: stromausfall medienkonferenz)

3 - Network Switch Brings Down Traffic in Zurich Area

Wrong maintenance activity on a network switch caused the breakdown of the entire train describer and remote control system in the Zurich area (around 80 km diameter) and the loss of information on train location information of several hundred trains; duration about one day.

4 - Collapse of SBB ERTMS Level 2 Operations in 2009

In 2009 a software bug in a Message Switching Centre brought down the Swiss GSM-R network and caused the entire ETCS Level 2 traffic in Switzerland to come to a stop for several hours. Trains on the Mattstetten–Rothrist line and in the Lötschberg Base Tunnel were brought to a stop, making evacuations in the Lötschberg Base Tunnel necessary on three occasions.

5 - Software Update Gone Wrong Closes Tunnel Operation

On Monday 16 May 2011 at 14.00, train traffic through the Lötschberg base tunnel was interrupted due to problems caused by a software update causing problems in the transmission network for the control of the tunnel.

This is network, among other things, controls the ventilation and lighting in the tunnel.

Closure of the tunnel was necessary because the monitoring of the tunnels safety systems was no longer possible.

Utrecht Operational Control Centre Rail

7 - Disruption Caused by a Fire in an Air Conditioner

A Signal box fire triggered peak-hour commuter chaos across Sydney as trains stopped for 30 minutes.

Disruption caused by a fire in an air conditioner at the Strathfield control centre that controls about 25% of the network last March. Passengers were stranded on platforms from the Blue Mountains to the Central Coast after a fire alarm went off at the Strathfield Signalling Centre. Lines on the CityRail network affected included Bankstown, Inner West, Airport and East Hills, South, North Shore, Western, Northern, Blue Mountains and Newcastle and Central Coast.

Source: ***http://www.news.com.au/national-news/nsw-act/chaos-across-rail-network-after-fire-alarm/story-fndo4bst-1226577462712#ixzz2dMFqlZMg***

8 - GSM-R Problems, Norway

1: Fire caused a power outage causing link failure at a Base Station Controller site in Oslo central station in 2007;

2: A power overload and shutdown in Trondheim 2010, all trains stopped for 3 hours due to missing functional numbers.

9 - DB GSM-R Shutdown, 13 August 2009

The DB GSM-R network in Duisburg, which controls all rail traffic in Nordrhein Westfalen, shut down as the result of a nightly lightning strike. Restart of the systems and restoration of the train radio service took until approximately 15:00 the next day, causing delays to traffic all day.

EXAMPLE OF MITIGATIONS

Prorail Evacuation Centre

As a result of the 2010 fire in the Utrecht OCC, ProRail has set up a emergency evacuation centre on the top floors of its Operational Control Centre Rail.

In case of an emergency anywhere in the network, such as a fire or a leaking tanker necessitating the evacuation of one of its OCCs, operations can be diverted to the emergency evacuation centre. It takes about four hours to reroute all communications systems to the evacuation centre and load the configuration data for the centre from which operations have to be diverted. In this time the evacuated staff can make its way to Utrecht to resume operations from there, also ensuring knowledge of the layout of the controlled area is available.

In January 2013 the facility was successfully tested in a simulated emergency during which the Amsterdam Control Centre was evacuated and operations diverted to Utrecht.

Webvideo: ***http://www.youtube.com/watch?v=DZiAwNFFSLI*** (Dutch language commentary)

WORKS CITED

- ***http://en.wikipedia.org/wiki/Butterfly_effect***
- SBB stromausfall medienkonferenz
- ***http://www.teltarif.de/netzausfall-gsm-r-deutsche-bahn-verspaetungen/news/35327.html***
- ***http://www.youtube.com/watch?v=DZiAwNFFSLI*** (Dutch language commentary)
- ***http://www.news.com.au/national-news/nsw-act/chaos-across-rail-network-after-fire-alarm/story-fndo4bst-1226577462712#ixzz2dMFqlZMg***