The Role of IP Communications in the Latest Generation Trackside Communications Systems
Presented by Ray Lock | Network Technical Director | Westermo
1.0 Introduction

Clearly there are many ways data communications on the trackside can be used to enhance and improve the operation and sustainability of the railway infrastructure. The idea of intelligent infrastructure or remote asset monitoring is a good example of how systems and processes are changing in the rail industry. The rail network needs to work more efficiently; that trains need to run closer together and power needs to be managed and delivered more effectively are just two examples. To facilitate this change, a technology refresh of the communication infrastructure is required. The trend in recent years has been to replace the old style telecoms infrastructure with one based on IP (Internet protocol). This trend has been driven by events in the wider telecoms industry; virtually every major developed country now uses IP based backbone communications to carry voice and data. Despite this the transition from the legacy telecoms systems towards IP is not without issues:

- The selection of equipment is crucial to operation and reliability.
- How to reuse existing infrastructure
- Transition management
- Network resilience and maintainability
- Network security or Cyber Security
- Critical and non-critical data on the same network

This white paper will focus on how the change can be managed and how data can be sent in a timely, secure and sustainable way in the challenging environment of the trackside.
2.0 Equipment Selection

The core IP infrastructure will be largely supplied by the giants of the routers industry and will be based on the latest router technology. The core infrastructure components will be sited some distance from the trackside or in locations where measures have been taken to protect the equipment. The direct trackside environment must be more specialised and can be either a flat Layer 2 switched network or a hybrid of Layer 2 and Layer 3. The challenge at the trackside is to have all the advantages of IP communications within robust, resilient and sustainable equipment that is designed to deal with the rigours of the environment.

The railway environment is not a friendly place for electronics; temperature swings, electrical interference and mechanical stress can all take their toll. Devices designed for the enterprise environment are not best suited to the trackside and will experience a much shorter operational life.

At a device level we need to be looking at certain criteria that will give us confidence equipment will match the operational life requirements of the system. A good indicator of the reliability of a product in the railway environment is the product MTBF (Mean Time Between Failure), calculated using a reliable method such as MIL-HDBK-217. Electromagnetic fields as well as transient and surge pulses can be extreme; the EN50121-4 standard is a good indicator of equipment’s ability to operate in these conditions. Other factors such as tri-galvanic isolation can also help to mitigate or limit the effects during fault or high noise conditions. The product temperature specification is also important. Devices designed for the 0-50 °C environment won’t last that long when run in a continuous ambient of 45-50°C, the MTBF will be reduced drastically. Inline or blister pack power supplies are often overlooked as the focus is on the main product. Claims of operating from -40 to +85°C should be treated with some scepticism. Evidence should be sought, to prove that the devices will COLD start at -40 and will operate continuously at an ambient of the claimed temperature rating and not for a short dry heat test or inside case temperature measurement.

3.0 Re-use of existing assets

Going forward new projects will normally expect to utilise fibre optic cable as the interconnecting media to form the network infrastructure. However this does not always have to be the case. It should not be forgotten that there is an existing copper
infrastructure covering practically every location on the trackside. The technology exists to re-use this existing trackside copper asset and integrate it into the new IP infrastructure. One of the most commonly used and, above all, reliable technologies used is SHDSL. A member of the xDSL family of protocols, SHDSL can take an existing copper link previously used with, for instance, FSK modems (V.23) at 1200 bps and transmit data at up to 15.3 mbps, a 12750 times increase in the bandwidth over the same piece of cable. Unlike domestic or commercial asymmetric ADSL (broadband) SHDSL is symmetrical i.e. the data rates in the upstream and downstream directions are equal. Furthermore the communications over the cable will be 1000 times more reliable than the old V.23 modulation due to the inherent error correction and retry mechanisms built into the SHDSL protocol.

Notable examples where this technology has been used:

- Banverket (Swedish rail):- ERTMS
- London underground:- SCADA control
- Network Rail (UK):- Voice recorders, HADB, Axial counters, station PA
- Poland:- Centralana Magistrala Kolejowa Signalling and level crossing control

### 4.0 Transition Management

The transition from the legacy systems to IP can be a daunting prospect. The perception is that when the infrastructure is moved from legacy to IP the dependant systems will also have to change at the same time - this is not necessarily the case. Networking devices supporting legacy serial and Ethernet have be specifically designed for the industrial and rail environments. Supporting both interfaces means that the existing serial device can be left in place and can continue to operate over the IP infrastructure while the legacy telecoms system is being decommissioned. The legacy serial device will benefit from the improved communications reliability while new services or the devices ultimate replacement can be run in parallel making for a more controlled and phased installation process. A good example would be how the Microlok II interlocking protocol can be migrated onto a new IP infrastructure without any loss in system integrity.
5.0 Network resilience and topology

IP communications on the track side breaks down largely into 2 categories; Layer 2(L2) switched networks and Layer 3(L3) routed networks. The choice of L2 or L3 will be driven by the overall system requirements i.e. size of the network, speed of access, latency, protocols used, level of resilience and speed of topology re-convergence.

The advantage of a L2 network is that all links will be operating at full wire speed i.e. the speed between points on the network are the same as the physical layer bit rate. A number of IP protocols can only be used on a L2 switched network, these protocols tend to require low latency or use a broadcast messaging structure to communicate with the rest of the peers in the control group. A number of signalling systems use Multicast data to communicate between peers. However it is not always a good idea to have a L2 only approach as this provides no boundaries to data and restricts access to the network.

The implementation of L3 allows larger physical networks to be broken down into more manageable physical or virtual sections. The use of L3 increases the flexibility to link the trackside networks to the core infrastructure or other WAN (Wide Area Networks) to provide trunk or backup links between sections of the network. The L3 links are not restricted to the fibre or copper media. Other media e.g. cellular, satellite or microwave can be brought into the mix to ensure that the network is not caught in a media or vendor trap.

The topologies that can be created using IP networking equipment can range from simple linear radial topologies to full mesh. There is a danger of over complicated topologies that assume that the network is increasing its resilience with each new connection! In reality there is a point where the ability of the network to quickly detect and re-configure starts to degrade due to the number of interconnections and rerouting required. The maintainability is also overlooked at the design stage, at some point equipment or media failure, if the system is only understood by a few people it may not be possible to return the system to full operation for some time.

6.0 Cyber security

The increase in IP connectivity does have a downside. The vulnerability of the network to cyber-attack is considerably increased, due to the sheer number of access point on the
network. Cyber-attacks come in many forms and are ever more sophisticated. There is a vast amount of information available offering some sound advice when it comes to securing a network from cyber-attack. Experience has shown that the best way to approach this issue is to create a multi layered security system.

As with all security measures there is a balance to be struck. If a network is rigidly locked down and no variations are tolerated the network will quickly fall into disuse and the expenditure on the asset totally wasted. This often leads to a culture where a new communications network will be installed alongside the current underutilised network, just because it’s too difficult to get permission to use it. A good model to secure the network is to push the security of the network right out to the trackside. This approach does not necessarily mean that additional equipment is required. There are already a number of devices that include L2/3 routing functionality combined with Firewall, DMZ, 802.1x and VLAN technology. This approach should not be instead of the high availability central firewalls but in addition to it.

7.0 Critical and non-critical data on the same network

Attitudes have changed and IP is being more readily accepted for safety critical applications in the rail environment. The most obvious is signalling and points control. The flexibility of IP, the levels of resilience and cost benefit have all helped to convince the most sceptical opponents that IP communications is safe and reliable. The new argument is whether safety and non-safety related traffic can co-exist on the same network. This was not seen as an issue on the legacy telecoms systems, as services were assigned bandwidth whether it was used or not. Bandwidth on an IP network is assigned on a demand basis, so potential conflicts could arise. To manage the conflicts and ensure critical traffic always arrives at its destination the IP traffic can be prioritised through the network. The details of how the prioritisation works at a packet or network level is outside the scope of this white paper, at this point it is sufficient to say that safety and non-safety related traffic can co-exist on the same network infrastructure in much the same way as they did on legacy telecoms systems with no loss in safety or functionality.

8.0 Conclusion

IP based communications are here to stay in the railways. The universal ability to carry data from multiple vendors and applications lends itself to the modernisation and extension of
the services run across the whole rail network. The railways will benefit from new developments within the IT enterprise sector which can be integrated into the core and trackside installations as they are required. Using equipment correctly selected to suit the environment at the edge network will lead to lower whole life cost and a high level of reliability. Using a hybrid of new fibre and existing copper within the IP network means the intelligent infrastructure concept will become reality and provide the railways with the tools it needs to manage a sustainable railway for the future. Existing assets can be integrated into the new IP infrastructure without the need for modification or replacement. Using IP in the railway infrastructure can be used to deliver high levels of resilience from simple ring to complex mesh topologies. Far from increasing the vulnerability to cyber-attack, selecting the correct device at the edge of the network can enhance the security of the network. Through use of prioritisation and resilient network topologies critical and non-critical traffic can share the same infrastructure. With the correct equipment selected the IP based network will provide the rail industry with flexible and most importantly sustainable communications infrastructure into the future.