Driving evolution towards Internet Protocol (IP) in signalling telecomms

Prepared on behalf of the IRSE International Technical Committee by Christian Sevestre with contributions from Frans Heijnen, Clive Kessel and Rod Muttram

Introduction

Earlier generations of non-IP based transmission systems are becoming more and more difficult to procure. A lot of them are no longer supported by their original manufacturers. Their obsolescence is planned and unavoidable.

The need for increased transmission capacity pushes us to use more efficient transmission systems.

Copper cables are being replaced gradually by optical fibres that offer higher transmission capacity and are intrinsically unaffected by EMI (electromagnetic interference).

The management of IP networks is centralised by design. They are easily supervised from a central location on a 24/7 basis, which was impossible with copper cables and dedicated circuits.

The result of all these developments is the progressive replacement of the entire existing copper cable network by up-to-date telecom systems based on IP technology. Only connections from lineside termination points to local equipment (such as point machines and level crossing barriers) will remain as copper cables in the foreseeable future.

This technological evolution is imposed on the railway networks. The question is not whether to accept or reject this evolution but when and how to make this evolution financially and technically acceptable.

As signalling engineers, we have to convince the operators and the maintainers that there is no other choice and that we know how to obtain high availability levels.

This transition creates a lot of new challenges to be solved in the areas of:

- Design process;
- Outsourcing of the transmission systems and facilities;
- Cybersecurity issues;
- Safety issues;
- Availability issues;
- Deployment issues;
- Maintenance and operating issues.

This article offers some examples of existing IP networks being used operationally in different countries, describing the differences between the IP networks and existing solutions, explaining the new challenges we are facing and giving some recommendations on how to deploy IP networks successfully.

The article also mentions cybersecurity issues but these are not its main focus. For an in-depth review on these see Peter Gibbons' paper 'Cyber Security – An Infrastructure Manager's View' in the February 2015 issue of IRSE NEWS (Number 208). This article focuses on the new challenges mentioned above that are not universally recognised and correctly handled.

Existing IP networks

All modern signalling control command systems use IP networks.

Many manufacturers propose this kind of network and know how to design, build and maintain them.

The Eulynx project is a good example of an IP-based network with distributed intelligence. This is a European initiative by several Infrastructure Manager organisations to standardise parts of the signalling systems.

Many railway networks (including Network Rail, PRORAIL, SBB, DB, Finland, SNCF, Sweden, Queensland Railways and/or Aurizon in Australia) are already using or are deploying IP networks dedicated to critical applications in terms of safety or reliability (signalling, telecom and power distribution (SCADA))

This type of network is used for various applications: communication between interlockings and object controllers, communication between interlockings and Radio Block Centres (RBCs), communication between adjacent interlockings, communication between interlockings and Regional Operational Centres etc. etc..

They cover all safety levels, up to SIL4 (Safety Integrity Level 4 as defined by the IEC61508 standard).

Design process:

The design process must take into account the following issues:

- Functional safety must be ensured by the applications and not by the network, moreover it must be independent of the internal protection mechanisms of the network;
- Any constraints affecting the applications (response time, predictability of the redundancy mechanisms, transmission delay, switching time from the normal routing to the backup transmission, etc.) must be specified clearly and carefully without excessive margins.

These constraints are usually expressed initially by signalling engineers who do not necessarily have a good knowledge of telecom technology and are thus tempted to protect themselves with extra margins.

A constructive dialogue between signalling and telecom engineers is absolutely necessary to converge towards the optimal solution.

Essentially, the signalling engineer buys a service and must specify the service that is needed, not a technical solution.

The safety of this type of technology must be type-approved by the product safety acceptance process. This avoids having to prove the safety of this type of solution for every project individually.

Outsourcing of transmission facilities

The provision of transmission links is increasingly dependent on third-party telecom organisations not under the direct control of the railway signal engineer. This may be from a separate department within the Infrastructure Manager organisation (as in the case of the UK with Network Rail Telecom) or more likely by acquiring digital capacity from a public telecom supplier.

Having multiple links (either by a transmission ring or discrete diversely-routed circuits) for the purposes of delivering critical messages that change the state of the signalling will provide greater resilience and availability. Providing the link(s) are not in themselves safety-critical but merely a means of delivering data, then this is acceptable and many observers view it to be inevitable.

The same parameters will apply to the control systems needed, for example, by the emergency services and the military. Providing the IP address structure is suitably controlled and safeguarded, then the risks are acceptably small.

Cybersecurity issues

Modern transmission networks cannot be totally closed.

Modern IP networks used by control command systems allow new applications that require links with the public Internet.

Control command systems must exchange information in both directions with other systems and therefore must include firewalls within the connections that naturally have security limitations.

Malicious attacks (e.g. hacking) are not the only risk in the short-term period.

In this transition period, a large number of problems may occur after using non-secure flash drive devices (such as USB keys) or reinitialising existing systems with new software releases.

This risk can be mitigated by procedures, operator information and training, but the best way is to design control command systems in such a way that infected software or data will be detected automatically by the system.

The nature of malicious attacks is constantly changing. We need to identify all attacks continuously and carefully, and must find protective measures in a very proactive way.

Risks must be identified and the protective measures to be taken have to be formulated and implemented. A security protection policy must be defined and applied.

The common technique is to protect the networks with firewalls. There are many examples where this type of solution has been compromised, with the network suffering intrusion. We are moving towards the protection of each individual transmission by encryption on an 'open' network instead of trying to protect the whole network. This is the principle used by the KISA system developed by DB, which uses separate components for establishing system security and system safety (the latter being provided by the signalling system itself). Due to the nature and speed of changes in the security field, the concept relies on COTS (Commercial Off the Shelf) solutions also used in the defence industry, allowing an easy and rapid upgrade of the system security without affecting the system safety case.

The senior managers of all railway companies need to be made fully aware of these risks.

Railway companies must create internal cybersecurity authorities dedicated to control command systems.

Cybersecurity measures applicable to ticketing systems or financial transmissions are not directly applicable to real-time applications with safety-critical impact and specific constraints on continuity of service.

The types of attack are changing every day.

Control command systems and IP networks must be monitored continuously to detect all the attacks that could threaten them.

Mitigating solutions must be adapted constantly to new types of attacks.

A separate security layer needs to be established.

Some have stated their intention to insert a security layer into the safety layer — INESS with Euroradio+. INESS is the Integrated European Signalling System, a project to define and develop specifications for a new generation of interlocking systems, and Euroradio+ is a safety protocol used by ERTMS for vital communications. However, that is really not good enough. The German Deutsche Bahn (DB) with its KISA (Kommunikations-Infrastruktur für sicherheitsgerichtete Anwendungen or Communications Infrastructure for Safety-related Applications) security approach is on its way to prove a viable concept.

Any system is fully closed until the moment a cable is plugged into the wrong socket. Hence security encryption is needed around the perimeter of all housings of signalling systems.

Safety issues

Safety assurance (IEC 62880, EN 50159) must be challenged. There is a strong interaction between safety issues and security issues, which is a new problem area by comparison with previous control command systems.

The general recommendation is to treat safety and security issues separately.

Availability issues

A virus attack or an intrusion by 'hackers' may create major disturbances on the quality of service without direct safety consequences.

The transmission service may be lost for a long period. This scenario must be taken into account in the system risk analysis. The appropriate backup procedures and technical solutions must be defined and implemented.

One extreme solution may be to accept this risk, but the customer or the user must be made aware of this and required to sign formal acceptance of this.

It must be clearly understood that the question is not whether or not this problem will occur but when.

When it occurs, all means and mechanisms needed to revert to the normal situation must be made available as rapidly as possible. An emergency organisation must be already in place and financed, and it must have regular training and exercises.

In order to keep trains moving, an alternative degraded means of control may be necessary if a cyber attack has caused loss of communications. In the UK the COMPASS (Combined Positioning Alternative Signalling System) development is aimed at just such a contingency.

Deployment issues

The migration process from the existing situation to the ultimate one must be addressed from the very beginning of the deployment of the IP network.

There will be a long period during which the legacy, non-IP based transmission system and the new IP transmission system must both be operational.

Experience shows that this is a very critical period. Not all the redundant mechanisms are necessarily in place or fully effective; for instance the central supervisory system may not have a vision of all the routers or have only a partial vision of the interfaces between the existing and the new networks.

The deployment of an IP network is not only an engineering project but is a major sociological and organisational change. This change has to be organised and monitored. The telecom and signalling maintenance staff have to develop an 'IP culture' (should cultural training be given?). This culture has then to be maintained.

Maintenance and operating issues

- An IP network requires a highly centralised maintenance organisation. It is a major change for telecom people; probably a larger one than for signalling people, who are used to being very independent and to maintaining highly decentralised equipment.
- An IP network changes the technical and organisational interfaces between the signalling and telecomms maintainers, and this must be addressed very carefully.
- An IP network evolves permanently, which is a rather novel issue (geographical, new version of routers, compatibility with the different applications such as interlockings, power supply SCADA and railway voice communications) that are evolving independently and with which compatibility has to be proven after each and every slight change.
- An IP network imposes a need to manage its evolution — and the associated safety and security — for three decades during which everything around and inside is changing.

Summary

The deployment of IP networks on railways is unavoidable.

The IP networks pose new challenges in different areas:

- *Design Process, Safety and Availability issues.* Functional safety is implemented by the applications and not by the network itself. The high degree of centralisation imposes specific mechanisms to obtain the high level of reliability required.
- *Outsourcing of transmission* facilities is feasible but only under some conditions.

These networks create cybersecurity issues that are usually underestimated and must be addressed seriously from the very beginning of the design.

- The protections available for public or administrative data networks are not applicable to these networks and must be adapted/extended.
- It is an illusion to think that these networks can be totally closed. It appears to be more efficient to protect every individual transmission than to try to protect a whole network.

The deployment of such networks takes time. There are specific *availability issues* when the whole network is not complete (redundant paths, recovery mechanisms or operating centre not totally operational). *Maintenance and operating issues* must also be taken into consideration. These networks are dynamic. They are in constant evolution: changes in their topology occur; new routers are added with new software releases. The compatibility between networks built upon IP technology and that of the applications using it, is not easy to test or simulate. Specific checks and tests must be carried out on the real system before any commissioning or modification of an IP-based network.