



Rail Safety & Standards Board

Published by

**Rail Safety and Standards Board
Evergreen House
160 Euston Road
London NW1 2DX**

**© Copyright 2008
Rail Safety and Standards Board Limited**

GN

GEGN8579
Guidance on Digital Wireless Technology for Train Operators
Issue One, June 2008
Railway Group Guidance Note



Documents

Document Sharing Hub

Guidance on Digital Wireless Technology for Train Operators

Issue record

Issue	Date	Comments
One	June 2008	Original document

Superseded documents

This Railway Group Guidance Note does not supersede any other Railway Group documents.

Supply

The authoritative version of this document is available at www.rgsonline.co.uk. Uncontrolled copies of this document can be obtained from Communications, Rail Safety and Standards Board, Evergreen House, 160 Euston Road, London NW1 2DX, telephone 020 7904 7518 or e-mail enquiries@rssb.co.uk. Railway Group Standards and associated documents can also be viewed at www.rgsonline.co.uk.

Guidance on Digital Wireless Technology for Train Operators

Contents

Section	Description	Page
Part 1	Introduction	6
1.1	The growth of communications	6
1.2	Objectives	6
1.3	Purpose of this document	6
1.4	Copyright	7
1.5	Approval and authorisation of this document	7
Part 2	Background	8
2.1	Scope	8
2.2	Structure of this document	8
2.3	Related documents	9
2.4	Next steps	10
2.5	Technology background	10
2.6	Digital wireless technologies	10
Part 3	Guidance on deploying digital wireless technologies	13
3.1	The needs addressed by wireless technology	13
3.2	The deployment of data communications	13
3.3	The interface with position reporting	16
Part 4	Guidance on classes of service	18
4.1	Objective of classes of service	18
4.2	The classification scheme for applications	18
4.3	The classification scheme for networks	19
4.4	Guidance on basic communication classes	19
4.5	Capacity – grades of service	21
4.6	Data transfer priority	22
4.7	Resource reservation	23
4.8	Communications security	23
Part 5	Guidance on system arrangements for service provision	25
5.1	Services in the operational communication domain	25
5.2	Arrangements for the public communication domain	29
5.3	Arrangements for the administrative communication domain	32
Part 6	Guidance on system architectures	34
6.1	The communications management unit (CMU)	34
6.2	Antennae	38
6.3	The train operator's secure communications gateway	39
Part 7	Guidance on hardware and software selection	42
7.1	The communications management unit (CMU)	42
7.2	The train operator's secure gateway	42
Part 8	Environmental and installation considerations	43
8.1	Power supply and EMC	43
8.2	System approval	44

Guidance on Digital Wireless Technology for Train Operators

Definitions		46
Acronyms and abbreviations		48
References		92
Appendix A	Technology overview	50
A.1	Working towards a UK railways internet	50
A.2	Communication technologies	51
A.3	IPv4 versus IPv6	53
A.4	WiFi	55
A.5	WiMAX	59
A.6	Communications priority	61
A.7	Communications security	62
A.8	IPsec	64
Appendix B	Using the communication classes of service	71
B.1	A simple matching of applications to network	71
B.2	Analysing the capacity requirement	71
B.3	Network independent security	72
B.4	Use of more than one train-to-shore network	72
Appendix C	Proposed addressing plan	74
C.1	Overall approach	74
C.2	IPv4 addresses	74
C.3	IPv6 addresses	77
C.4	Multicast IP addresses	78
C.5	Autonomous system numbers	78
Appendix D	Proposed public key infrastructure (PKI)	79
D.1	Objectives	79
D.2	Implementation	79
Appendix E	Example application classification	82
E.1	List of application classifications	82
E.2	Descriptions	82
Appendix F	Illustrative examples (test cases)	85
F.1	Introduction	85
F.2	Position feed for an energy monitor	85
F.3	OTMR download	86
F.4	Closed circuit television	88
F.5	Entertainment system upload	90
Tables		
Table 4-1	Basic grades of service	21
Table 4-2	Network capacity classes of service	22
Table 4-3	Classes of service for secure communications	24
Table 8-1	Typical locations available for installation of equipment	44
Table 8-2	Railway Group Standards relevant to system approval	45
Table E-1	List of GNSS / DBWT applications	82

Guidance on Digital Wireless Technology for Train Operators

Figures

Figure 2-1	Applications of different communications technologies	12
Figure 3-1	The physical objective for on-train communications	14
Figure 3-2	Example of use of communications technology with position information	16
Figure 5-1	Operational comms – on-train components	26
Figure 5-2	Public communications gateway	31
Figure 6-1	Communication management unit (CMU)	34
Figure 6-2	Positioning of the secure communications gateway	40
Figure A-1	Example of UK railway internet topology, showing use of IPsec tunnels	50
Figure A-2	On-train WiFi network	56
Figure A-3	IPsec communications model	69
Figure A-4	Tunnelling example	70
Figure C-1	Non-unique IP address ranges	74
Figure C-2	Public communication domain on-train allocation	75
Figure C-3	Example of IP address allocation for trains	75
Figure C-4	Example of allocation for duty holders	76
Figure C-5	Mobile and fixed network allocation	76
Figure F-1	Energy monitoring systems	86
Figure F-2	Addition of OTMR to basic energy monitor	87
Figure F-3	Adding CCTV	89
Figure F-4	Addition of public communications	90

Guidance on Digital Wireless Technology for Train Operators

Part 1 Introduction

1.1 The growth of communications

Effective communications have always been essential for railway operation. In the nineteenth century, the railways were a driver of the electric telegraph, and semaphore signalling was developed to provide a robust and efficient means of communication between the signaller and the train driver. In the twentieth century, the telephone replaced the telegraph, and coloured lights replaced semaphore signalling, and general improvements in communications allowed the replacement of individual signal boxes with centralised facilities. The twenty-first century has already seen the introduction of GSM-R, enabling direct voice communications between the signaller and the driver, and this is only the beginning of what can be achieved with modern technology.

The ultimate goal is to be able to replace the trackside signalling infrastructure with a communications infrastructure that offers at least the same level of safety as trackside signals, while offering many more capabilities. Trackside signals are a low bandwidth data communications mechanism for shore-to-train uni-directional communications. They are expensive to maintain and constrain train control to fixed block operations. A high-speed data communications infrastructure has the potential to be cheaper to maintain, while allowing for more efficient train control using moving block operations, including the giving of speed advisories to drivers and the feedback of real-time train position and speed information to signallers.

On the other hand, a data communications infrastructure can also support many non-safety applications, and applications with only limited safety implications. Such applications can improve operational efficiency and give a direct and quantifiable benefit, while also helping to gain confidence in the data communications infrastructure. They can also be deployed now.

1.2 Objectives

This document provides guidance on achieving inter-operability at the IP (internet protocol) level. Although within a single private implementation the standards and features employed do not impinge on other applications, it is the nature of IP that common transmission and equipment provide a service to many users. This guidance applies principally to those facilities to be shared; private applications would also benefit from the guidance, but particular requirements could make it less relevant. The guidance also considers 'future proofing' of applications, but in a sector as dynamic as internet communication this cannot be assured. This document will be reviewed as experience indicates and identifies useful revisions and additions.

A second objective of this guidance note is to ensure a common industry approach to data communications deployment. The aim is to both minimise costs through common procurement, and to ensure that data communications deployments have long-term value.

1.3 Purpose of this document

This document sets out good practice on the specification, purchase, implementation and installation of data communications technology in support of broadband applications on the UK railways. Deployment of high-speed data communications and its use on the railways is the main focus of this guidance note. The guidance provided is for the use of train operators, infrastructure providers, train builders and communications service providers. The RSSB takes no position regarding the validity or scope of any intellectual property rights or other rights that might be claimed to pertain to the implementation or use of the technology set out in this document or the extent to which any licence under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights.

Guidance on Digital Wireless Technology for Train Operators

1.4 Copyright

Copyright in the Railway Group documents is owned by Rail Safety and Standards Board Limited. All rights are hereby reserved. No Railway Group document (in whole or in part) may be reproduced, stored in a retrieval system, or transmitted, in any form or means, without the prior written permission of Rail Safety and Standards Board Limited, or as expressly permitted by law.

Rail Safety and Standards Board (RSSB) members are granted copyright licence in accordance with the Constitution Agreement relating to Rail Safety and Standards Board Limited.

In circumstances where Rail Safety and Standards Board Limited has granted a particular person or organisation permission to copy extracts from Railway Group documents, Rail Safety and Standards Board Limited accepts no responsibility for, and excludes all liability in connection with, the use of such extracts, or any claims arising therefrom. This disclaimer applies to all forms of media in which extracts from Railway Group Standards may be reproduced.

1.5 Approval and authorisation of this document

The content of this document will be approved by:

Control Command and Signalling (CCS) Standards Committee on 12 June 2008

This document was authorised by RSSB on 27 June 2008

Guidance on Digital Wireless Technology for Train Operators

Part 2 Background

2.1 Scope

- 2.1.1 The scope of this document is the on-train arrangements that support digital communication technologies. It includes the on-train and train-to-shore communications, and those aspects of fixed communication networks necessary to support communication with trains.
- 2.1.2 Communications and positioning technologies are expected to be key enablers for the modernisation of the railway system in the UK. Applications include precise vehicle positioning, vehicle position monitoring, customer information, customer services, internet and entertainment services. Digital technologies (which include SATCOM and WiFi/WiMAX) are increasingly available for transferring large volumes of data between track and train systems.
- 2.1.3 This document sets out guidance to duty holders, so that a level of system performance commensurate with user needs is achieved. It sets out the foundation for duty holders to establish best practice that should enable data communications systems to meet the needs of the rail market more effectively.
- 2.1.4 The successful integration of commercially available data communications technologies should provide greater cost benefit for the railway. The methodology and standardisation presented in this document for their fitment and use within the railway environment supports this goal.
- 2.1.5 This document does not mandate or recommend any particular arrangement for the provision of communications services for operating or administrative purposes, nor for their provision to passengers by train operating companies. Train operators are free to offer commercially attractive services to their passengers as long as there is no conflict with operational objectives or safety.
- 2.1.6 To facilitate installation on rolling-stock, the guidance provides for:
 - a) One aerial shared between as many applications as is reasonably practicable
 - b) One data communications unit, accommodating the requirements for as many applications as is reasonably practicable. This provides for upgrading by straightforward replacement.

This approach limits the proliferation of multiple equipments providing similar functions, with the potential to compromise one another's performance.
- 2.1.7 Guidance on the use of satellite positioning technology is set out in GE/GN8578: Guidance on the Use of Satellite Navigation.
- 2.1.8 The installation of these systems is subject to the requirements of Railway Group Standards.

2.2 Structure of this document

- 2.2.1 The structure of this document is top-down. The earlier parts address the wider issues concerning the implementation of digital technology, and the later parts set out guidance on the equipment used. It is comprised of seven major sections and six appendices.
- 2.2.2 The main document comprises:
 - a) Part 2, which sets out the background and context to this document and introduces digital communication technologies

Guidance on Digital Wireless Technology for Train Operators

- b) Part 3, which sets out the deployment of digital technologies and identifies the subjects requiring guidance
- c) Part 4, which sets out guidance on classification schemes for communication networks and the performance of the services that are provided to the applications. Concepts such as communications priority and security are also explained
- d) Part 5, which sets out guidance on the system arrangements required for service provision to the passenger, operational and administrative domains. Key concepts are introduced as regards the functional elements that provide data communications services with the provision of network independent security
- e) Part 6, which sets out guidance on the system architectures
- f) Part 7, which sets out guidance to procurers on hardware and software subjects
- g) Part 8, which sets out guidance on environmental and installation considerations.

2.2.3 The appendices comprise:

- a) Appendix A, which sets out a technology overview and includes discussion of internets, WiFi, WiMax and concepts such as communications priority and security
- b) Appendix B, which sets out the interpretation and use of the classes of service presented in Part 3
- c) Appendix C, which proposes an internet protocol (IP) addressing plan for the UK railways. The purpose of such a plan is identified in Part 4, and Appendix C is a candidate solution to this requirement
- d) Appendix D, which proposes a public key infrastructure (PKI) for the UK railways. The purpose of a PKI for both network independent security and for the protection of WiFi communications is set out in Part 4
- e) Appendix E, which sets out an example application classification applying the classification scheme described in Part 3. The purpose of this appendix is to stimulate ideas about what could be achieved, and captures some of the results of the workshops held during the preparation of this document
- f) Appendix F, which illustrates how the communications services presented in Part 4, and the components presented in Part 5, can be used to implement the requirements of some example railway applications.

2.3 Related documents

- a) RSSB research report T351 Future Rail Communications. This document develops this work further
- b) GE/GN8577: Guidance on the Application of Selective Door Operation Systems, for which digital communication and positioning technologies are suitable
- c) GE/GN8578: Guidance on the Use of Satellite Navigation. Some of these applications are independent of data communications, but to obtain the most benefit from satellite positioning requires access to data communications services, for example to report position or to gain access to up-to-date map information.

Guidance on Digital Wireless Technology for Train Operators

2.4 Next steps

- 2.4.1 Following publication of this guidance note, the co-ordination of applications of broadband technology and the sharing of experience will support its future development.

2.5 Technology background

- 2.5.1 Modern communication technologies develop at a rapid pace. To take advantage of this, the rigorous safety and security arrangements required for railway applications, the harsh environment and the relatively long life of the dominant assets of a railway, need to be recognised.
- 2.5.2 The availability of cheaper and more integrated digital communication systems offers operational and commercial opportunities to the railway industry, as elsewhere. Early applications have been disparate systems. A more unified approach should improve commercial viability for the industry's duty holders.
- 2.5.3 This document includes the conclusions of two workshops, which addressed the themes of industry consultation and research.

2.6 Digital wireless technologies

- 2.6.1 This document does not prescribe any specific technology. Rather, it sets out information for railway operators, that promotes a stable technology platform, facilitating controlled evolution, as commercial communication technologies go through their life cycle.
- 2.6.2 When considering coverage, it is necessary to appreciate that wireless systems cannot provide a permanence of connection equivalent to that of a wired connection. There are several reasons for this:
- The wireless spectrum is open to interference, and the absence of interference, accidental or deliberate, cannot be guaranteed absolutely
 - Even where 100% coverage is planned and designed for, the influence of extreme atmospheric conditions, extreme climatic conditions and extreme tropospheric and ionospheric conditions can interfere with the quality of the communication and can cause interruptions
 - In conditions of high demand, most systems may find it necessary to delay or deny some of the traffic. A period of high traffic is unlikely to be noticed by a voice application.
- 2.6.3 Appendix A sets out a summary of the technologies that are available and that should continue to form the basis of commercial equipment into the medium term. The technologies are:
- GSM / GPRS
 - GSM-R
 - HSDPA / UMTS
 - WiFi
 - WiMAX
 - SATCOM
 - Other wireless communications.
- 2.6.4 Wider communication industry practice is now to use internet technology to support all end-to-end data communications. It is increasingly the basis of

Guidance on Digital Wireless Technology for Train Operators

commercial off-the-shelf (COTS) products. It is being used in high demand and safety-critical applications. This document recognises that internet engineering practice plays an increasing role in railway communications.

- 2.6.5 Figure 2-1 illustrates how the above technologies support each other and can be used together. In different contexts, SATCOM, WiMAX and HSDPA / UMTS (3G) can all be used to support train-to-shore communications, while GSM-R can provide operational railway communications, and GSM provides passenger voice communications. Multiple public service GSM providers are also available, illustrated here by the use of different colours.
- 2.6.6 WiFi has become the de facto standard for mobile computer internet access, and it is a reasonable assumption that provision of passenger internet access on trains will continue to require the use of WiFi.
- 2.6.7 The leading open issue is the choice of technology for 'train-to-shore' communications. Experience is indicating that WiMAX is a suitable candidate; however, more experience is needed before a stronger statement can be made on this subject. In particular, where railways are concerned, the issue of base station deployment in rural areas should be pursued.
- 2.6.8 This document recognises the use of GSM-R for operational voice communications; however, because of its limitations it is unlikely to be available for more general data communications. Indeed, there is a potential safety benefit from having at least two independent means of communications to a train. GSM-R voice is able to be one of these with support from broadband technologies.

Guidance on Digital Wireless Technology for Train Operators

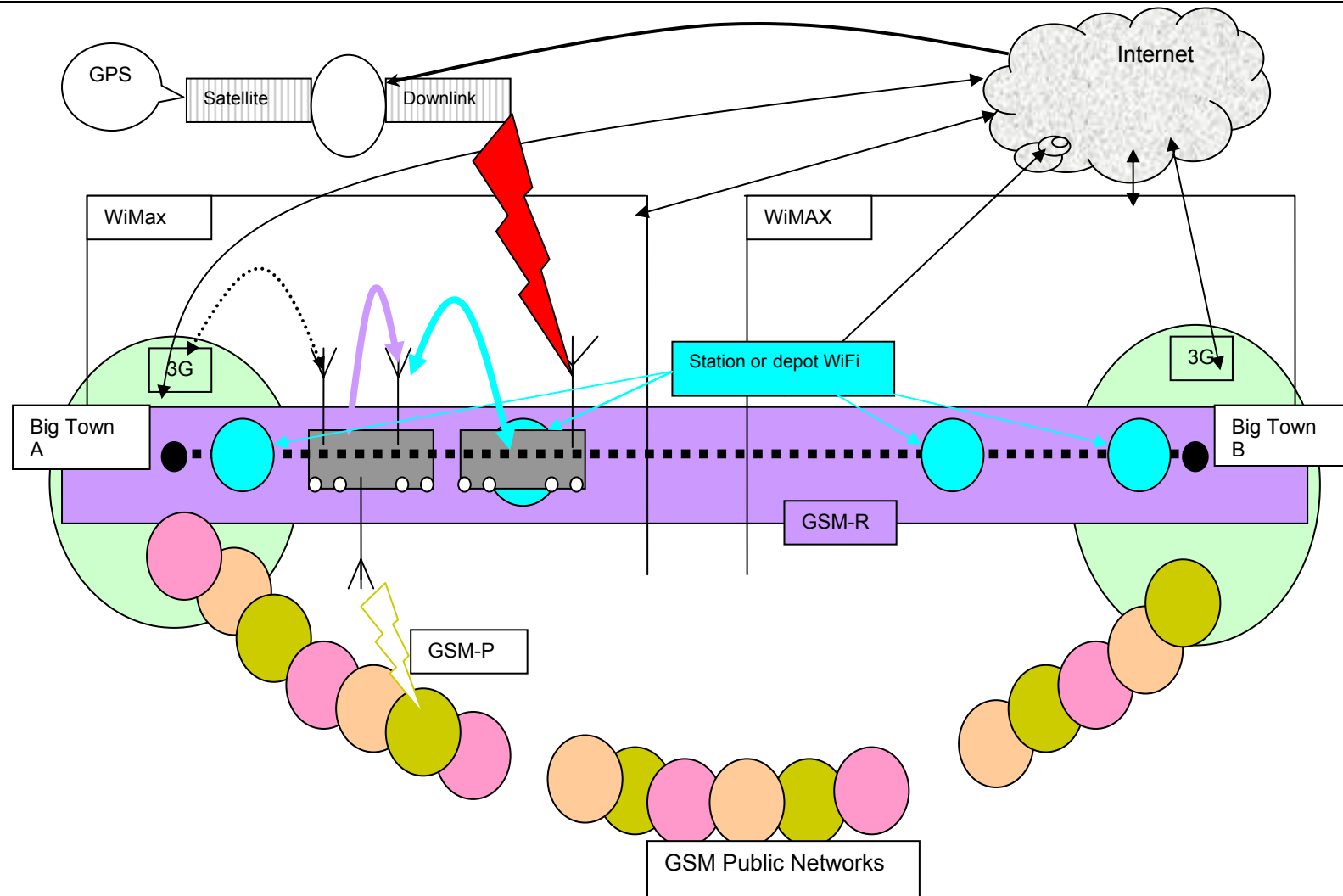


Figure 2-1 Applications of different communications technologies

Guidance on Digital Wireless Technology for Train Operators

Part 3 **Guidance on deploying digital wireless technologies**

3.1 **The needs addressed by wireless technology**

- 3.1.1 Duty holders are responsible for providing digital communications to passengers and for operational applications.
- 3.1.2 This document sets out communications best practice within which diversity and shared experience creates success in implementation.
- 3.1.3 The approach to digital communications supports the development of more applications, with the associated benefits. It enables the sharing of communications practices and services, so permitting an application to be justified on its marginal costs rather than the application having to bear the full costs of its own infrastructure. Train operators are then free to focus on the applications themselves.

3.2 **The deployment of data communications**

3.2.2 **The physical objective**

- 3.2.2.1 The commercial pressure is to develop communication facilities on board trains that can, by strategic upgrading, follow the evolution of the communication technologies, giving the following benefits:
 - a) It eases the interfacing to the dependent applications and minimises performance difficulties
 - b) It enables the use of COTS products with a minimum of modification
 - c) It enables commercial services to meet the expectations of the passengers.
- 3.2.2.2 To the extent possible, a minimum of communication facilities should provide an acceptable service to the maximum of dependent applications.
- 3.2.2.3 Deployments should be scaleable. An initial implementation could be limited by the equipment available, but subsequent products should have increasingly improved performance. Therefore, a clear migration and evolution path to benefit from the higher performance without imposing a radical redesign of the train fitment is indicated. Yet, trains with different levels of equipage should also be compatible.
- 3.2.2.4 Figure 3-1 illustrates this physical objective by the use of one 'Communications Box' for the train applications, and one antenna.
- 3.2.2.5 The communications box is known as the 'Communications Management Unit' or CMU. The CMU is the gateway between the on-train environment and the train-to-shore environment. It provides secure communications between a train and the trackside. For the on-train environment, the CMU can allocate IP addresses to the dependent systems, when needed. Appendix C provides a proposed IP Addressing Plan.
- 3.2.2.6 Although in practice no single antenna is yet sufficient to support the different communication needs, a common antenna housing supporting different combinations of standard antennae should be sufficient. It may not always be possible, due to the limitations of height restrictions and good clearance, to achieve reception from low-level antenna, for example WiMax base stations at trackside.
- 3.2.2.7 The strategy is chosen so that building a CMU is a system integration task and does not require significant original development.

Guidance on Digital Wireless Technology for Train Operators

- 3.2.2.8 The CMU implementation on the railway should take place within a co-ordinated framework.
- 3.2.2.9 Guidance on the CMU functions is set out in section 6.1, and guidance on the equipment is set out in section 7.1.

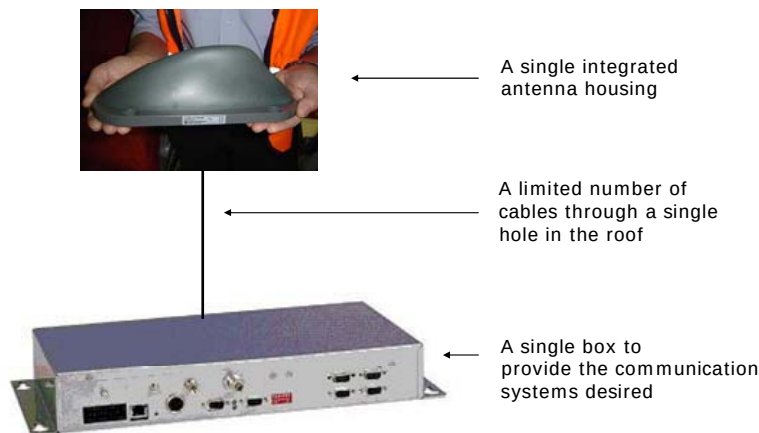


Figure 3-1 The physical objective for on-train communications

3.2.3 Guidance on the communications management unit

- 3.2.3.1 The on-train environment should be either wired ethernet or wireless WiFi.
- 3.2.3.2 The CMU is a gateway between the on-train environment and the off-train environment. This box could support some applications directly, but it is more usual for on-train applications to be connected to it via the train's data bus arrangement.
- 3.2.3.3 One of the key advantages of a common communications architecture is that once the CMU has been installed, the cost of adding an additional application that requires train-to-shore communications would be marginal.
- 3.2.3.4 Each application has an impact on the train-to-shore network capacity. In order to support more applications, the CMU can be adapted to support additional networks, such as WiFi for data upload and download in the depot, or to use a high-capacity network, such as WiMAX instead of GPRS. Use of internet technology ensures that the only impact of the application from a change of network is on the performance attained.
- 3.2.3.5 The train-to-shore communications environment is a rapidly evolving area. There are different competing technologies, each with its own merits. Some are offered as private dedicated railway networks, while others can be shared public access networks. The CMU hides this diversity from the applications that use its services.
- 3.2.3.6 The CMU should be the bridge between the existing 'legacy' environment and the development of a railway internet. The CMU implementation could require interfaces to be established on train networks, for example the IEC train bus. It provides an evolutionary approach from the current environment to developments depending upon IP, and accommodates train management systems (TMS).
- 3.2.3.7 The train systems should treat the CMU as a default router on the train's local area network (LAN). They are provided with an IP service that hides any

Guidance on Digital Wireless Technology for Train Operators

complexity as regards train-to-shore communications. The service provided means that the on-train LAN appears to have little functional difference from any office LAN. Issues of mobility management are hidden from the systems on the on-train LAN.

- 3.2.3.8 Detailed guidance on the CMU is set out in section 6.1 (guidance on system architecture) and section 7.1 (guidance on hardware and software).

3.2.4 Guidance on train-to-shore security

- 3.2.4.1 The inescapable need for communications security is a major driver of how the CMU manages the train-to-shore environment. Where identified, the duty of care extends to protecting operational applications from anyone that wants to disrupt railway operations. In providing protection, a pragmatic approach should be adopted in order to ensure that the application performance requirements can be obtained.

- 3.2.4.2 The protection of data communications is to:

- a) Identify and authenticate trains to gateways to train operator's or Network Rail's virtual private network (VPN)
- b) Validate the train's authorisation to use its assigned IP Address ranges
- c) Protect train-to-shore communications from masquerade, modification and replay threats
- d) Optionally, protect train-to-shore communications from confidentiality threats
- e) Permit trains to move from one communication network to another without risk of denial of service attacks
- f) Provide a minimum level of security to all applications.

- 3.2.4.3 Guidance is provided on a public key infrastructure to support the protection of data communications.

3.2.5 Protection of broadband communications

- 3.2.5.1 This guidance references two security techniques:

- a) WPA2 Enterprise, which protects WiFi communications
- b) IPsec, which provides security to communication between a train and a secure gateway, and maintains security as a train moves between gateways and networks.

- 3.2.5.2 The industry standard IPsec security framework sets out this pragmatic approach in the train-to-shore environment. This is capable of providing current communication security requirements between a train and the train operator. The focus is firstly on authentication of the train to the operator and the operator to the train. Secondly, any data exchanged is protected from modification and replay. Optionally, data can also be encrypted. As set out in Appendix A.1, this approach can be extended to support direct communications between the train and another organisation (for example, Network Rail).

- 3.2.5.3 IPsec is a network independent security mechanism, which allows a wide variety of public and private networks to be used in the support of operational railway communications. The effect is to create a VPN comprising all trains operated by a given train operator. If required, train operator VPNs could be further combined into a single UK railways VPN.

Guidance on Digital Wireless Technology for Train Operators

3.2.5.4 IPsec supports separation of the networks used to support train-to-shore communications and the routing of data between a train and the train operator. This property can be exploited to provide a strategy for managing movement through one train-to-shore network to another, so allowing trains to make use of more than one train-to-shore networks.

3.2.5.5 Guidance on IPsec is set out in Appendix A, section A.8.

3.2.5.6 Other main references to IPsec are:

Section 5.1.8 – Network independent security

Section 5.1.9 – The communications management unit

Section 5.1.10 – The train operator's secure communications gateway

Section 6.1.8 – IPsec functionality for the CMU

Section 6.1.9 – Multiple train-to-shore networks for back-up and opportunity connections.

3.2.6 The common antennae housing

3.2.6.1 It should be considered necessary to co-ordinate the deployment of communications antennae on trains. The roof space available for antennae is limited, and holes in the roof are subject to structural and cabling limitations. A common antenna housing to accommodate a range of antennae, and a common cabling duct, aids the design.

3.2.6.2 Guidance for antennae is set out in section 6.2.

3.3 The interface with position reporting

3.3.1 Where an application requiring position reporting is used with a CMU, then Figure 3-2 illustrates the on-train architecture.

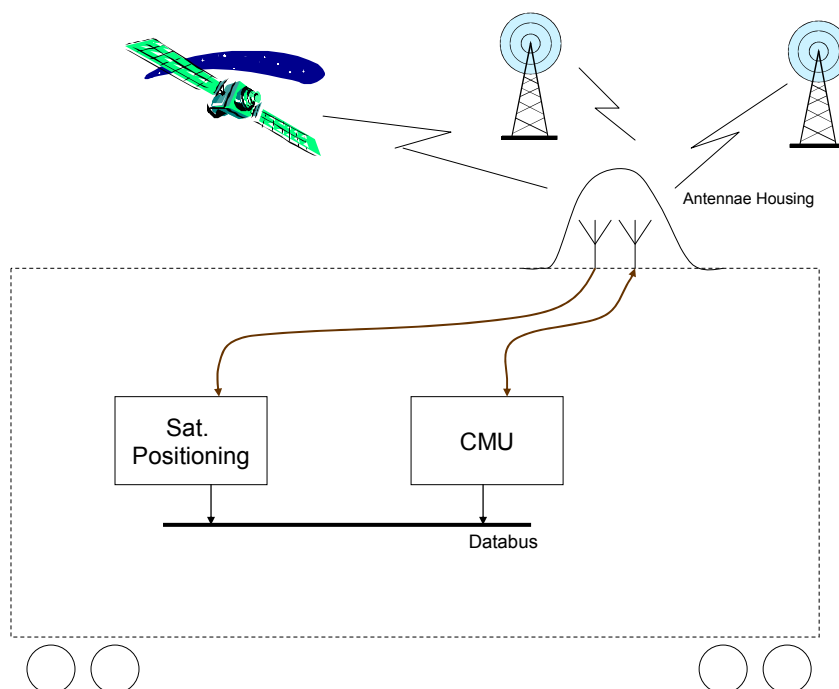


Figure 3-2 Example of use of communications technology with position information

Guidance on Digital Wireless Technology for Train Operators

- 3.3.2 In this architecture, a common antennae housing contains an antenna for receiving location information from a satellite constellation, such as that used for GPS, and an antenna tuned for terrestrial communications, such as GPRS or WiMAX.
- 3.3.3 These antennae are connected to separate physical systems. One is responsible for interpretation of the location information received from the satellite constellation and through correlation with the network map and other information sources, such as odometry, determining an accurate position for the train. The other physical system is a communications management unit (CMU) that provides the gateway between on-train and off-train communications.
- 3.3.4 The position data can be used by other on-train systems (for example selective door opening). It can also be reported to the train operator and/or Network Rail. For this purpose, the satellite positioning system is connected to the CMU via a wired ethernet, and the CMU supports train-to-shore communications via a suitable communications network.
- 3.3.5 Communication can be two-way, and the train operator can, as an example, use the communications path maintained by the CMU to instruct the satellite positioning system as to the reporting interval required. The train operator and/or Network Rail can then be sent regular position reports which can be used to determine the rate of travel, expected arrival times, etc. This information is available to be copied to other applications and duty holders.
- 3.3.6 Where positioning is supported by a form of network map, the CMU communications path should be used for updating it.

Guidance on Digital Wireless Technology for Train Operators

Part 4 Guidance on classes of service

Classes of service are defined that can be used to describe the applications and the service to be provided by communication networks. Each class of service is defined in terms of a set of quality of service metrics, including availability, reliability, continuity and integrity, and capabilities such as data prioritisation and security. The definitions of quality of service, priority and security metrics are set out in Appendix B.

4.1 Objective of classes of service

- 4.1.1 The objective is to provide a straightforward means to identify application requirements and network capabilities, so that network providers and other suppliers have clear guidance on the performance expected, and train operators have a clear means of judging whether a given network meets the requirements of the applications they decide to deploy.
- 4.1.2 Guidance on a classification scheme is therefore provided for both applications and networks. This classification scheme uses the same terminology for both, so that straightforward comparisons can be made.
- 4.1.3 However, it is not possible to construct a simple linear classification scheme for communications. This is a multi-dimensional problem and, for example, high availability, low capacity high-security communications services are potentially just as useful as low availability, high-capacity high-security communications services.
- 4.1.4 This document sets out guidance on separate classification schemes for availability / reliability, capacity (that is to say, the achievable bit rate) and security, so that users and providers can describe a service or application in each of the relevant dimensions.

4.2 The classification scheme for applications

- 4.2.1 The availability, reliability, continuity and integrity requirements of an application translate directly onto network requirements. The same classification scheme as used for networks should therefore be used for applications in respect of these metrics.
- 4.2.2 An application has a data throughput requirement that varies independently of the above metrics and should be stated separately.
- 4.2.3 Applications do not have a requirement for prioritised data transfer as such. A network manager may assign a given application a relative priority, but only in context and when prioritised data transfer is needed to ration network capacity under a 'best efforts' data transfer regime. When applications have minimum data transfer rate and / or maximum delay (jitter) requirements, then these should be stated explicitly.
- 4.2.4 Each application should have a security requirement that is determined from a threat and vulnerability analysis specific to the application. However, taking into account known capabilities of both networks and end-to-end security mechanisms, it is possible to group together security mechanisms into a simple hierarchy that should be used to classify application requirements. Such a classification scheme should start with 'no security required', moving up to a 'low security' environment using shared secret keys to protect data, before moving to a high-security environment requiring a public key infrastructure (PKI). The high-security environment should be further distinguished by 'with or without confidentiality' through data encryption.
- 4.2.5 Applications do not have a denial of service requirement that is separate from the overall availability and reliability requirement.

Guidance on Digital Wireless Technology for Train Operators

4.3 The classification scheme for networks

- 4.3.1 Availability, reliability, continuity and integrity are basic properties of a network, and are related, for example, in the sense that a high availability network is unlikely to offer low reliability and there is little value in offering high reliability if the data integrity is low.
- 4.3.2 Network capacity is a separate metric. It is perfectly reasonable to have high availability and low capacity networks, or low availability high-capacity networks, and many other combinations. An application that requires a high available network is supported by a high availability network service, but its throughput requirement would be aggregated with the other applications that use the network and, by considering all on-trains applications together, the required network capacity can be determined. It therefore makes sense for capacity to be a separate network classification.
- 4.3.3 Network capacity is limited, and communications priority is a means of managing capacity under a 'best efforts' data transfer service. Appendix A.6 sets out communication priority as a separate attribute of a network service.
- 4.3.4 Some networks may also offer resource reservation schemes that allow them to offer data transfer rate and / or maximum transfer delay guarantees.
- 4.3.5 Security is an essential network capability. Although communications security mechanisms can be provided by a network, it could be better implemented end-to-end independently of the network. Security does not need to discriminate between different networks, and the security provided by a given network could have no more impact than deciding what additional security should be provided end-to-end – which impacts on costs.
- 4.3.6 However, security in terms of preventing denial of service is network dependent, but can be mitigated through having alternative and independent networks available.

4.4 Guidance on basic communication classes

- 4.4.1 The basic communication classes apply to both networks and applications, and bring together availability, reliability, continuity and integrity into a single classification scheme. Classes A, B, C and D are defined, with D as the lowest. These are set out in Table 4-1.
- 4.4.2 The classification scheme is based on a view of what it is reasonable to require from the network infrastructure, taking into account the likely cost of deployment and which applications are anticipated. The classifications are not based on a rigorous analysis of application requirements. Such data is not yet available.
- 4.4.3 The classifications given here should be reviewed against the requirements of a specific project and should be modified when this can be justified. The classification scheme, as presented, does not cover safety related applications, although it is able to be extended to cover such applications in the future.
- 4.4.4 Users of this document should distinguish between the requirements for voice communication and the requirements for data communication. The effects of circuit (physical or logical) interruption on these two types of application can be expected to be different.

Guidance on Digital Wireless Technology for Train Operators

Basic comms classes	Interpretation
A	Very high: Availability: better than 99.99% Reliability: response received within 30 seconds to a 1K byte message for 99.9% of message exchanges Continuity: no outage longer than 15 seconds Integrity: better than 1 in 10^4 messages. Train-to-shore networks in this class are expected to cover the whole railway network, including 'difficult' areas such as tunnels, cuttings and stations. Dual and sometimes triple coverage from base stations is anticipated, together with a suitable fixed infrastructure that avoids single points of failure. Applications in this class should be provided with continuous communications service availability and have their effectiveness severely compromised whenever communication services are not available.
B	High: Availability: better than 99.9% Reliability: response received within two minutes to a 1K byte message for 99% of message exchanges Continuity: no outage longer than 90 seconds Integrity: better than 1 in 10^4 messages. Train-to-shore networks in this class are expected to cover the whole railway network, including 'difficult' areas such as tunnels, cuttings and stations. However, dual coverage from more than one base station is not anticipated. Applications in this class should be provided with continuous communications service availability and have their effectiveness compromised whenever communication services are not available.
C	Medium: Availability: better than 95% Reliability: response received within 10 minutes to a 1K byte message for 90% of message exchanges Continuity: no outage longer than six minutes Integrity: better than 1 in 10^3 messages. Networks in this class aim to provide coverage over most of the railway network but keep their costs down by avoiding more difficult areas (for example tunnels). A SATCOM network is expected to come into this class. Applications that require this class of service can tolerate occasional loss of communications and automatically resume use of the service after any outage.

Guidance on Digital Wireless Technology for Train Operators

D	Low: No guarantees are provided nor are they required for availability, reliability, continuity or integrity purposes. This is a 'best efforts' service used when it is available. Depot WiFi and other 'hot-spot' network services fall into this class, together with the applications that use them. These are low-cost services used opportunistically by applications.
---	---

Table 4-1 Basic grades of service

- 4.4.5 When network providers claim to provide a Class A or Class B service, the availability, reliability and continuity of service figures should take into account the risk of a denial of service attack and the steps that the network provider takes to limit the effect of such attacks.

4.5 Capacity – grades of service

- 4.5.1 In order to provide a simple means for declaring the 'headline' capacity of a given network and application requirement, guidance on a classification scheme for networks and applications is set out in Table 4-2. This is a technology driven classification that takes account of what existing networks can deliver. It is intended to be used to indicate the performance band of a network service in a simple manner. It should not be used for a procurement requirement or in a service level agreement.
- 4.5.2 Network providers are expected to state the actual capacity of their network in terms of the mean sustainable throughput (bits per second) that each user can achieve and the minimum they can expect. For train-to-shore networks, the user is a 'train' as a whole. The term 'capacity' is preferred here, as more commonly used terms such as 'bit rate' often refer to theoretical maxima, and their interpretation depends on the network technology and the use of statistical theory. 'Capacity' is a network independent measure that allows for genuine comparison between different technologies.
- 4.5.3 Some networks may offer asymmetric data transfer rates. For example, a 3.5G High-Speed Downlink Packet Access (HSDPA) network may offer 7.2 Mb/s downlink, but only 384 kbit/s uplink; only when High-Speed Uplink Packet Access (HSUPA) is also offered, is a higher uplink speed achievable. Network providers offering asymmetric services are expected to state separate capacity classes and detailed performance figures for each direction of service.
- 4.5.4 Application designers should state the actual throughput requirements of their application in terms of 'bits per second', both mean and peak.
- 4.5.5 The assumptions under which the stated network capacity is calculated should also be given. It should be noted that wireless communications services use shared channels, and the actual service that a user receives therefore depends on the use that others are making of the same communications channel. Fixed services often express this as the 'contention ratio' recognising the number of users that compete for the available bandwidth.

Capacity classes	Interpretation
1	~ 9.6 kbits/s A GSM circuit switched communications service fits into this class of service. This is a low bandwidth class of service and can be provided by public operators or through GSM-R.

Guidance on Digital Wireless Technology for Train Operators

Capacity classes	Interpretation
2	~ 20 kbits/s This class of service has been developed for GPRS services that improve the throughput of standard GSM.
3	~ 1.2 Mbits/s This is a medium speed service targeted on the lowest rate UMTS/HSDPA service. These services are provided by public operators and are anticipated to be available over part of the railway network.
4	~ 3.6 Mbits/s for example, Intermediate rate UMTS/HSDPA
5	~ 7.2 Mbits/s for example, higher rate UMTS/HSDPA
6	~ 14.4 Mbits/s This is a high-speed (broadband) service targeted on the highest rate current UMTS/HSDPA services or IEEE 802.11b WiFi services, and lower speed WiMAX services.
7	> 14.4 Mbits/s This is a high-speed broadband service and includes higher speed WiMAX services and IEEE 802.11a and 802.11g WiFi.

Table 4-2 Network capacity classes of service

4.6 Data transfer priority

- 4.6.1 Support of data communications priority is a network capability rather than an application requirement. Network administrators may choose to prioritise traffic under a 'best efforts' delivery guarantee, on the basis of some characteristic of the data (for example, destination port number) or by an explicit indication of relative priority added to every packet by the sending application.
- 4.6.2 While an application can indicate its relative priority, the network administrator decides how this is interpreted. Unless the same administrator is also responsible for the application, there may only be limited trust in the priority level signalled by the application.
- 4.6.3 At least three relative priority levels of data transfer should be supported before this capability is considered effective. In practice, three levels are probably sufficient for most needs. Not all communications networks support prioritised data transfer.
- 4.6.4 Even when priority is supported, during a failure mode, there may not be enough resources for the safety related applications to meet their performance targets. Safety related applications, therefore, still have to be designed to ensure that safe operations are maintained during periods when network resources are below the required level for adequate performance.
- 4.6.5 Priority is discussed further in Appendix A.6.

Guidance on Digital Wireless Technology for Train Operators

4.7 Resource reservation

- 4.7.1 Resource reservation is another capability that may be offered by a network, and is useful when, for example, real-time delivery guarantees or throughput guarantees are required. Resources can be reserved for an application either statically by a network administrator or by using a resource reservation protocol such as RSVP (RFC 2205).
- 4.7.2 IP packets are traditionally delivered on a 'best efforts' basis, where transit delay and throughput is dependent on the current network load. Resource reservation is appropriate when data transfer is 'rate sensitive' or 'delay sensitive', that is to say, when a minimum delivery rate should be maintained, or when the transmission delay should be kept within well-known bounds.
- 4.7.3 Application communications requirements should identify any rate or delay sensitivity dependencies.
- 4.7.4 Care should be taken to distinguish resource reservation from priority. When a user refers to their application as 'high priority', they usually mean that the application is rate or delay sensitive rather than requiring a means of arbitrating between different user's demands on a 'best efforts' delivery guarantee.

4.8 Communications security

- 4.8.1 Providers of communications networks are expected to identify the security mechanisms available, including physical security. Similarly, application designers are expected to carry out a threat analysis, in order to determine the communications security requirements for their application.
- 4.8.2 However, it is possible to develop a classification scheme based on existing communications security technologies. Network providers can use this to indicate their security mechanisms, and application designers can use it as a simple way of presenting the results of a threat analysis in a way that aligns with implementation.
- 4.8.3 It is possible to protect data using network independent mechanisms, to avoid dependencies on the network provider.
- 4.8.4 Guidance on a classification of service for secure communications is set out in Table 4-3.

Security classes	Interpretation
U	Unclassified. This covers networks that provide no protection from communications threats and applications that have no security requirements.
W	Password based access controls. Basic authentication is required to use the application using a password based mechanism. Subclass W1: password sent in clear Subclass W2: password encrypted or used to compute a hash; password never sent in clear.

Guidance on Digital Wireless Technology for Train Operators

Security classes	Interpretation
Y	Enterprise grade cryptographic security (data sent in clear) A PKI is deployed and used to authentic users and service providers alike. The PKI is also used to establish a cryptographic context for the secure exchange of data (protection from modification and replay only).
Z	Enterprise grade cryptographic security with data encryption As for Class Z, but data is also encrypted while being transferred end-to-end using the cryptographic context established when the users are authenticated.

Table 4-3 Classes of service for secure communications

Guidance on Digital Wireless Technology for Train Operators

Part 5 **Guidance on system arrangements for service provision**

Service provision is discussed in three domains:

- a) Operational
- b) Passenger and commercial
- c) Administrative.

5.1 Services in the operational communication domain

5.1.1 Service principles

- 5.1.1.1 This document promotes an industry solution to on-train application requirements for train-to-shore digital communications.
- 5.1.1.2 This solution is based upon a communications box termed the communications management unit (CMU). This provides a standard communications gateway between operational applications on a train and train-to-shore communications with the train operator, and extendable to support direct communications with other parties, such as Network Rail.
- 5.1.1.3 Physically separate implementations can be used for the operational communication systems and the public communication systems. Guidance on the criteria to apply to this decision is set out in section 6.1.14.1.

5.1.2 Service details

- 5.1.2.1 The basic requirement is to provide an internet communications service between the train and the train operator that includes the industry standard IPv4. This service would be extendable to support communications between the train and duty holders.
- 5.1.2.2 Provision is made in this guidance for operational applications to include a secure communications service to a minimum of Class Z (see Table 4-3). Where deployments make use of the same train-to-shore networks as those deployed for passenger internet access, the availability of security performance should be verified. A network independent security solution can be provided as an alternative. Provision should be made to include network independent security for operational applications as a matter of routine.

5.1.3 System elements

- 5.1.3.1 Train-to-shore communications for operational applications, as illustrated in Figure 5-1, consist of:
 - a) An on-train network that can deliver internet communications to on-board systems supporting operational applications
 - b) One or more wireless train-to-shore networks providing communication with the train operator. These can be dedicated private networks or public networks providing communications with the train operator via the public internet
 - c) The CMU: a gateway between the on-train and train-to-shore networks, and which can also manage the on-train network.
- 5.1.3.2 The on-train network can be implemented as a single network for the whole train supported by a single gateway to a train-to-shore network. Alternatively, each carriage can be a separate network with its own gateway to the train-to-shore network. Other combinations are also possible with several carriages sharing the same gateway, with several such gateways per train. Not all carriages need to

Guidance on Digital Wireless Technology for Train Operators

be equipped. (Appendix A, section A.4.2 sets out guidance for the on-train architecture.)

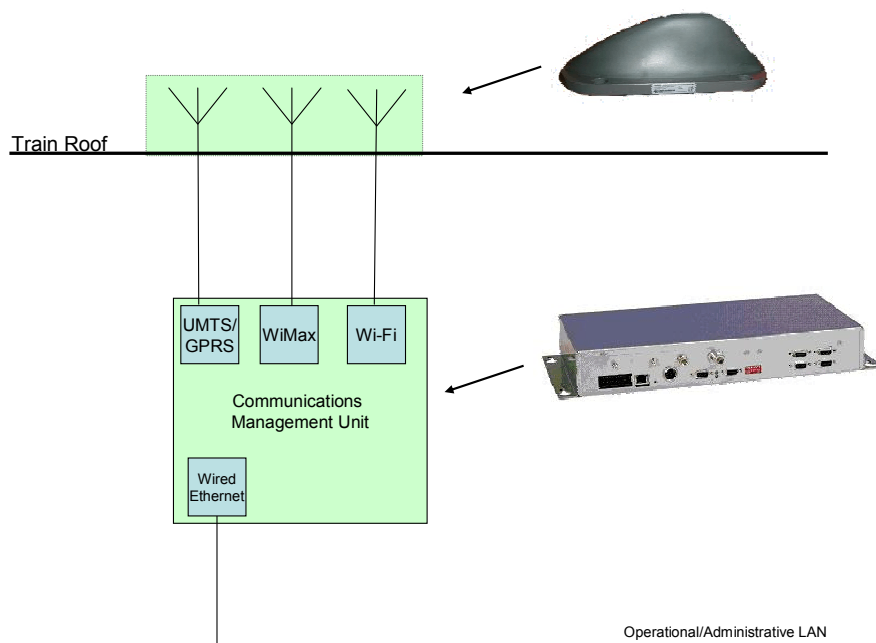


Figure 5-1 Operational comms – on-train components

5.1.3.3 The on-train operational network should be logically separate from any on-train network used to support public communications, and can be physically separate as well.

5.1.4 The on-train network

5.1.4.1 The on-train network should be either a wired ethernet or a WiFi network, or a combination of the two. Section 5.1.5 sets out guidance on the ethernet and section 5.1.6 sets out guidance on WiFi. These are industry standards for the provision of high bandwidth communications in a limited area. Wired ethernet is currently preferred for fixed equipment installations. However, WiFi is appropriate for installations that are spread out over the train (for example, closed circuit television (CCTV) cameras).

5.1.4.2 Both wired ethernet and WiFi networks are usually extended between carriages. When this is required, the guidance given for public communications set out in section 5.2.5 applies.

5.1.4.3 Guidance on the use of WiFi channels is set out in Appendix A, section A.4.5.

5.1.5 Fixed ethernet on trains and security

5.1.5.1 Wired ethernet on trains is suitable for use within a single carriage or locomotive, or in multiple unit rolling stock where the carriages are only rarely decoupled from each other. A wireless technology is more appropriate for vehicle-to-vehicle communication where the vehicles are only coupled together for a short time (for example a single journey). Wired ethernet should provide more reliable and predictable performance than wireless communications. If used, it should be for the interconnection of a limited number of operational systems in a controlled and secure manner.

Guidance on Digital Wireless Technology for Train Operators

- 5.1.5.2 Initial installations of wired ethernet on trains should be compliant to IEEE 802.3u for 100 MBits/s or IEEE 802.3ab for 1000 MBits/s operations.
- 5.1.5.3 Use of screened twisted pair (ScTP) cable Cat 5e 100Ω cable with ruggedized RJ45 connectors should be used for a wired ethernet. This recommendation is intended to minimise the likelihood of electromagnetic interference (EMI) through use of ScTP cable, and that of mechanical vibration through use of ruggedized RJ45 connectors, or M12 connectors. Cables should have a minimum of two twisted pairs (suitable for M12 or RJ45 connectors), which is sufficient for 100 MBit/s ethernet, but four pair cable is preferred to permit later upgrade to Gigabit ethernet (RJ45 connectors only). Standard Railcat (two pairs) can be terminated with M12, not RJ45. Railcat is needed for compliance with BS6853, and is also needed for robustness and durability in the inter-vehicle jumpers.
- 5.1.5.4 Fibre optic versions of wired ethernet may be applicable to areas of very high EMI or where differential voltages over the length of the cable may be an issue.
- 5.1.5.5 Wired ethernet used for operational communications are potentially vulnerable to vandalism and can therefore be used for unauthorised access to the network. For such reasons, wired ethernet should not be present in an area accessible to passengers.

5.1.6 WiFi and security

- 5.1.6.1 Where WiFi is used to support operational communications within a train or carriage, the implementation should be compliant with industry standards, specifically at the date of publication IEEE 802.11b (11 Mbps) and IEEE 802.11g (54 Mbps) operating in the 2.4 GHz band. Other standards can be expected to be adopted over time.
- 5.1.6.2 A WiFi network for operational use should always be encrypted, in order to avoid unauthorised use. The insecure wired equivalent privacy (WEP) standards should not be used in this context. The more recent WiFi protected access (WPA) and IEEE 802.11i (WPA2) encryption standards should be used, using public key encryption and a suitable PKI.
- 5.1.6.3 WiFi networks used for operational communications within the same train set should use the same Service Set Identifier (SSID) and encryption key, and different from those used by any other train set. SSID broadcast suppression is also recommended in order to avoid such networks being visible to passengers.
- 5.1.6.4 Recent WiFi equipment is capable of supporting multiple logical WiFi networks. This enables an operational WiFi network to use the same physical access points as those used for passenger internet access, subject to the criteria set out in section 6.1.11.

5.1.7 Train-to-shore communications

- 5.1.7.1 The train-to-shore networks used to support operational applications can be either dedicated private networks or public access networks. Operational communications are able to share a public access network, provided the required class of service is available and has sufficient capacity to provide both operational and passenger services.
- 5.1.7.2 Figure 5-1 illustrates an example with a CMU supporting WiFi, WiMAX and UMTS for train-to-shore communications. Other support combinations are viable, and the actual set of train-to-shore communication services supported by a given train depends upon the chosen implementation and on the routes that it operates.
- 5.1.7.3 The antenna mounting and the potential for contention for roof space should be addressed. Wherever possible, train operators should combine antennae together into a single housing, typically roof-top mounted. The minimum practical

Guidance on Digital Wireless Technology for Train Operators

number of cables should be used to access the antennae through a single hole in the train roof.

- 5.1.7.4 Where separate networks are used for passenger and operational services, their antennae should be combined in a single housing.

5.1.8 Network independent security

- 5.1.8.1 Network independent security is consequent on the assumption that train-to-shore communications have to be pragmatic and make use of any available network with sufficient capacity and quality of service. As these networks usually have other users and offer public access services, they cannot be relied upon to protect operational communications from external threats. A network independent communications security solution should therefore be considered.
- 5.1.8.2 An IPsec security framework should be used to provide network independent security between a train and the train operator. Guidance on IPsec is set out in Appendix A, section A.8.
- 5.1.8.3 The need for encryption depends upon the application requirements, but operational data should always be protected from modification and replay.

5.1.9 The communications management unit (CMU)

- 5.1.9.1 The CMU fulfils the role of the communications gateway between the on-train environment and train-to-shore communications. It provides a common service to all operational on-train applications. It avoids those applications and their supporting systems from having to manage train-to-shore communication. It therefore facilitates the development of communications applications on the railways by allowing application designers and implementers to concentrate on the application without having to worry about the mechanics of data communications between the train and the train operator.
- 5.1.9.2 The CMU has an interface to all train-to-shore networks used for operational communications and an interface to the on-train network. It should support:
- a) The routing of IPv4 (RFC 791) packets between the on-train network and the train operator via a train-to-shore network. It should also be capable of routing IPv6 (RFC 2460) packets between the on-train network and the train operator via a train-to-shore network
 - b) Network independent security and the IPsec protocols. It is the CMU's responsibility to establish and maintain IPsec security associations with the train operator and to route IPv4 (or IPv6) packets to the train operator via the IPsec tunnel
 - c) Other network management functionality, including the allocation of IP addresses to operational systems using Dynamic Host Configuration Protocol (DHCP) and providing access to the Domain Name Server (DNS). This should include the monitoring of the quality of service provided by the train-to-shore communications networks.
- 5.1.9.3 The CMU also plays a role in the migration from existing on-train 'legacy' communications to the shared environment set out in this document. The CMU deployments should be capable of including application level gateways to existing and often non-standard applications and on-train networks, and thereby enable the migration to the shared approach.

5.1.10 The train operator's secure communications gateway

- 5.1.10.1 A consequence of the use of IPsec for the protection of digital communications between a train and a train operator is that a secure communications gateway should be implemented by the train operator.

Guidance on Digital Wireless Technology for Train Operators

5.1.10.2 This provides the 'other end' to the IPsec security association and tunnel. It is a secure gateway between the train operator's internal networks and the access networks to the train-to-shore network(s) used to communicate with the train.

5.1.11 IP addressing plan

5.1.11.1 Appendix C sets out a draft IP addressing plan. A shared IP addressing plan should be applied to all operational communications. This plan applies to:

- a) The on-train network
- b) Railway private train-to-shore networks
- c) The train operator's own networks.

5.1.11.2 Together with the deployment of IPsec, the implementation of this addressing plan allows the unambiguous routing of packets between a train operator and each of its trains over any train-to-shore network. It also supports the exchange of packets between a train and other train operators and Network Rail. This is achievable either via the train's own train operator or, in more advanced deployments, through IPsec tunnels established directly with another train operator or with Network Rail.

5.2 Arrangements for the public communication domain

5.2.1 Objectives

5.2.1.1 It is not the intention of this document to mandate or recommend any particular approach for the provision of communications services to passengers by train operators. Train operators should be free to offer commercially attractive services to their passengers as long as there is no conflict with operational objectives or safety.

5.2.1.2 This document sets out the matters that train operators should take into account when offering communications services to passengers and specifically passenger internet access.

5.2.2 The service provided

5.2.2.1 Guidance is limited to providing passenger internet access to the public internet. This addresses the provision of an industry standard IPv4 internet service to the passenger seat.

5.2.3 System elements

5.2.3.1 Passenger internet access offers:

- a) An on-train network that can deliver internet communications to the passenger
- b) One or more wireless train-to-shore networks providing access to the public internet via an internet service provider (ISP)
- c) A gateway between the on-train and train-to-shore networks, which can also control passenger access to the service and manage the on-train network.

5.2.3.2 While the provision of dedicated consoles is not ruled out, it is assumed that most train operators will limit their investment to providing internet access to passengers who use their own laptops, and the provision of a link to them.

5.2.4 The on-train network

5.2.4.1 The technology used for the on-train network is limited to wired ethernet and WiFi. Either can be used, but WiFi appears to be the most popular choice at present.