



Joint Chairs Group

The UK's National Technical Framework
for Intelligent Transport Systems

Communications networks

NTFI01-1.0

May 2011

The National Framework for ITS is supported by:



Executive Summary

The Guideline aims to provide an overarching framework for transport-related communications networks, aimed principally at the UK context. It is consistent with, and can be seen as underlying, all of the main current frameworks.

This Guideline is a high level document, and further detail may be available for specific technical and functional contexts. The JCG is happy to offer guidance on where to look for more detailed specifications.

The key recommendations in this Guideline are as follows:

Principles

NTFI-Comms-1: Transport systems should be based on mainstream digital communications technologies wherever possible.

Planning and managing communications

NTFI-Comms-2: All organisations should document their communications network: the location of points served, and the links/technologies serving them.

NTFI-Comms-3: All organisations should have a named person responsible for managing their transport communications network.

NTFI-Comms-4: Communications network managers should ensure that a security policy and framework is built into their networks.

NTFI-Comms-5: Make sure your network is designed to provide a suitable quality of service for each of the services it supports.

NTFI-Comms-6: Use service level agreements where appropriate, but don't rely on them.

NTFI-Comms-7: Emergency situations need some communications more than others: make use of robust fallback services, but don't over-engineer them.

Linking to other systems

- NTFI-Comms-8:** Users should carefully consider the facilities to be provided via external connections, and communications channels will need to reflect these.
- NTFI-Comms-9:** Users should consider the potential challenges and benefits of setting up communications collaboratively with others.
- NTFI-Comms-10:** Where specialist communications are necessary, it may be less costly and less risky to outsource delivery.

Communications technologies

- NTFI-Comms-11:** The core of any transport communications network should be based on IP.
- NTFI-Comms-12:** Transport communications networks should be free to use any suitable bearer.
- NTFI-Comms-13:** Non-IP links can and should be used where there is good functional reason; in these cases managers should clearly identify whether and how the information is ported into the main IP network.
- NTFI-Comms-14:** Use licensed spectrum for operational long haul radio links.
- NTFI-Comms-15:** Local non-IP networks should be gatewayed into the main IP network by default.
- NTFI-Comms-16:** Voice and video networks should be considered separately, but there may be scope for integrating them with the data network.

Introduction

About the National Framework for ITS

“Intelligent Transport Systems” (ITS) means the use of information and communications technology in the transport context. It covers many different systems, from motorists’ satnav to traffic lights, from automated train announcements to web journey planners, from airline check-in kiosks to pollution monitors.

The ITS industry is highly complex and constantly innovating. This poses a challenge for organisations who need to use many different ITS in their business – for instance, fleet managers, public transport operators and road/rail network authorities.

The Joint Chairs Group (JCG) brings together a wide range of stakeholders involved in setting UK ITS standards and specifications. In 2009, we initiated a long term process to build on the historical work of our member groups, with a view to creating a coherent *de facto* National Framework for ITS in the UK.

The aim is that, by having a common framework adopted across the range of stakeholders, the implementation and integration of systems will be easier, cheaper and less risky for everyone. We therefore encourage all stakeholders to build this framework into their technology strategy.

JCG benefits from representations from Department for Transport, Highways Agency, innovITS and ITS(UK), whose support for this project we welcome and acknowledge. We are also delighted to acknowledge the support of PTEG and ADEPT for the National Framework project.

About this Guideline

The Guideline aims to provide an overarching framework for transport-related communications networks, aimed principally at the UK context. It is consistent with, and can be seen as underlying, all of the main current frameworks (including of course those of the JCG’s member groups: ITSO, RTIG and UTMC/TIH).

This Guideline is applicable in principle to any stakeholder. It is likely to be of special relevance to local authorities, which have many different transport interests, and need cost-effective, easily managed networks to support them.

This Guideline is necessarily a high level document, and further detail may be available for specific technical and functional contexts. The JCG is happy to offer guidance on where to look for more detailed specifications.

There are a number of places in the document where specific recommendations are identified. Many of these are likely to be familiar, but are felt to merit repetition. These specific recommendations are identified by reference numbers to aid citation, in the form NTFI-Comms-XXX.

Authority of this Guideline

This Guideline is issued under the authority of the Joint Chairs Group. It has no statutory or other force, and is rather built on emerging good practice.

Principles

In transport, communications networks have four principal roles:

- to link devices into management centres, for monitoring and control (manual or automated)
- to support people making tactical decisions, by bring information together from diverse sources
- to publish information to external users, both individual travellers and other service providers
- to support transactions between users, sometimes but not always monetary

The options for technology to support these roles are many and varied.

Communications is vast and hugely diverse industry: a trillion-dollar global community with many individual specialisms. Its commercial drivers are diverse and demanding – military, banking, medicine, nuclear power, etc.

In the transport sector our demands, while real, are not of the same order, and cost-effectiveness is much more significant. As a principle, therefore, we should adopt mainstream systems and technologies as far as possible. “Novel” communications may be considered by innovating product developers (eg terahertz radio or advanced PCB buses for specialist sensor systems), but strictly for use within their product: mainstream interfaces should still be provided.

Many, though not all, communications may most efficiently be done digitally. Digital information is the basis for current mainstream computing, and information can only sensibly be brought together in this form. Where analogue communication is necessitated for specific reasons, the data will need to be rendered into digital form if there is any desire to manage it.

NTFI-Comms-1: Transport systems should be based on mainstream digital communications technologies wherever possible.

Planning and managing communications

Determining requirements

Communications may be one-to-one or one-to-many; they may be along a direct link, or may pass through numerous different systems on the way. In designing a network the specific content of the communication is rarely important, but the following generic features are crucial:

- how much: the rate of communications, in bits per second (bandwidth) or message size (bits)
- how fast: the maximum time to complete the communication (end to end latency)
- how reliable: the acceptable proportion of communications which may be lost, corrupted or not completed (availability)
- how secure: the importance of preventing unauthorised access to the data (confidentiality), the acceptable risk of the data being altered in transit (integrity)

Requirements should cover not just normal operations, but also disrupted conditions. Some communications will increase dramatically under these circumstances. It will not be possible to meet all conceivable demands, and a trade-off will need to be made between cost of provision and likelihood of occurrence. See also the section on Planning for service disruption, below.

Design principles

Recognising that the skills of communications technologists and the skills of the business users are different, almost all communications adopts the principle of “layering”. Under this principle, the “network layer” is built to provide the requirements of size, speed, reliability and security between a given network of points, which the business (“application layer”) is then free to use.

The speed and reliability of communications obviously depends on the underlying technology of wireless or wired “bearers”, and how they are connected together as a network. However security, and to an extent other requirements, also depend on the protocols used to manage data flow around the network. It can even be possible to use “workarounds”: if your network is (cheap but) unreliable, then it may be useful to have an application intelligent enough to provide an alert when it expects data but fails to receive it.

Some points are fixed (eg street equipment or desk PCs), while some are mobile (eg vehicle equipment or laptops). Some links are open-ended (eg external internet connections) or generic (eg smartcards). There is an art in effective and intelligent network design.

On this principle, an organisation will “own” a (known) network of communications, possibly based on links using many technologies. The data flowing across this network may be its own data, or those of third parties.

To ensure that the network is fulfilling its role on size, speed, reliability and security, it needs to be managed more or less actively. As necessary the network may need to be extended/expanded, or technologies swapped out; equally, underused network elements may be removed or downsized, bearing in mind the need to maintain adequate “headroom”.

NTFI-Comms-2: All organisations should document their communications network: the location of points served, and the links/technologies serving them.

NTFI-Comms-3: All organisations should have a named person responsible for managing their transport communications network.

These tasks require time and skill. The more complex the context, the more worthwhile it will be to ensure that professional support is used.

Managed networks

The blocks out of which networks are constructed are not always simple wires or radio channels. In many cases an organisation will build its transport network by incorporating a pre-built network, either through a commercial telecoms provider or through an in-house system (eg a corporate network provided by a multi-service IT department).

This is of course perfectly acceptable and may be very cost-effective. It also reduces the need to maintain technical design skills in-house.

A managed solution can be particularly effective for a multi-agency environment where communication patterns are similar, and/or intercommunication is essential – for instance, a group of neighbouring local authorities.

Having a managed network does not absolve the need for the owner to understand and manage it:

- it may have additional business requirements, not shared by the managed network (eg on network availability)
- it may have additional device requirements (eg on environmental robustness of communications equipment)
- it may have additional coverage requirements

Each of these may require the transport comms network to negotiate different terms, add fallback channels, provide additional facilities etc.

Security

As a rule, the more integrated a network is, the greater the security challenges. The nature of these depends strongly on both the functions deployed, and the technology used to deploy them, but may include the potential to compromise safety, financial transactions, personal privacy, operational efficiency, etc.

In particular, while wireless systems can be indispensable in many places, they are by nature more open to attack than wireline systems: it is much easier to “listen in”, to spoof, or to jam if you can do so from your own hidden location than if you need access to a data cable. Wireless protocols do normally include security protocols, but these need active management and the possibility of electrical jamming in particular can never be discounted. Conversely, of course, they are not vulnerable to cable damage, which can be difficult and expensive to find and repair.

Communications security is a specialist discipline, and there is a considerable amount of specific guidance on what is appropriate for specific contexts.

NTFI-Comms-4: Communications network managers should ensure that a security policy and framework is built into their networks.

NB Privacy raises a whole set of issues of its own, and a separate Guideline on this subject is currently being considered.

Quality of service

A communications facility is only useful when it is operational. End-to-end communications reliability depends on many factors including network architecture, protocol choices, and the robustness of specific products/services.

Networks can evolve as requirements change, but each supported application should carefully review the offer provided to it. There may be one or two applications which “pace” the network: video is likely to dominate bandwidth requirements, enforcement likely to have the most stringent security, and control systems the most demanding timeliness. In some cases it may be more cost effective *not* to integrate communications for applications with very different their quality of service needs.

For any given technology, not all commercial offers will provide equivalent quality of service. The well-known example is: “you are too expensive – I could buy a PC in the high street for £300”, overlooking the need for the PC in question to operate in a noisy, hot and wet outdoor environment. The same caveat applies to communications services, as well as to items of equipment.

NTFI-Comms-5: Make sure your network is designed to provide a suitable quality of service for each of the services it supports.

Specifying quality of service is important for all communications solutions, whether provided as wires and radios or as a managed network service..

Service level agreements

In buying a product or service, it may be beneficial to pay a premium for a specific service level. The Service Level Agreement (SLA) may promise guaranteed uptime, time to fix, spares holdings, etc; it is likely to incorporate financial incentives and/or penalties.

However an SLA does not absolve the communications manager of responsibility for communications faults and failures. If a traffic signal link fails and there is an accident, the telco may be penalised but the authority is not exonerated.

NTFI-Comms-6: Use service level agreements where appropriate, but don't rely on them.

Planning for service disruption

Managing transport has been compared to keeping a dozen plates spinning while blindfolded: the day job is hard enough, hence the need to consider helpful technologies. Every so often, though, there is a significant disruption and “business as usual” changes to “crisis mode”.

Crises tend to operate very differently. Both information and people are often at a premium. Most stakeholders will have undertaken contingency planning (aka: business continuity planning) and will, therefore, have a special set of communications requirements for these circumstances.

In designing for these, bear in mind that you may not be the only affected party. A flood management plan, say, needs to consider which comms systems and services will be available in a flood situation. The same applies to major events, riots, terrorist attacks, gas leaks, and other types of “crisis”. To meet these needs, much may be gained by talking to local resilience teams, the emergency services etc – not only about how to design your network, but who needs to be talking to whom, and why.

Some communications systems have useful built-in facilities. Examples include dual routing to protect against network breaks, circuits that generate an alarm message when power is cut, and mobile services which give priority to specially configured SIMs. All of these come at a price though, which can be quite high.

NTFI-Comms-7: Emergency situations need some communications more than others: make use of robust fallback services, but don't over-engineer them.

Linking to other systems

External connections

Information shared between transport management systems may also be of use to others:

- different local departments (children's services for school transport, the air quality team for emissions data, etc)
- neighbouring transport authorities (traffic flows along a connecting road/rail line, for instance)
- construction and utilities (for information related to roadworks)
- major transport users (public transport operators, logistics fleets)
- individual travellers

Information may be exchanged directly or via third party information services.

In each case, a connection outside the network is required. It will usually be appropriate to achieve this through a point on the IP network and to use Internet Protocols to achieve: normally web access for individual travellers, possibly something more structured like an XML exchange for "business-to-business" use.

Many ITS frameworks include a component on the provision of external links. In some cases (for instance, links with the emergency services), there may be separate frameworks applying to each "side", or specialist requirements may emerge; these will need to be resolved by local discussion.

NTFI-Comms-8: Transport information networks should carefully consider the facilities to be provided via external connections, and communications channels will need to reflect these.

Working with other organisations

Working with other organisations may require communications at many levels from simple telephone and email contact, through the routine exchange of data files, to real-time collaborative control. A lot of this can be achieved through normal business communications, but the more critical levels of engagement may need special implementation.

There are often multiple ways to do business, which have different technical implications. Shared control centres reduce the need for data links (although of course they raise other operational issues).

There are important commercial aspects of communications between organisations. Some impose challenges (eg who is responsible in the case of a communications failure?) but others are definitely opportunities (eg collective bulk-buy contracts).

NTFI-Comms-9: Users should consider the potential challenges and benefits of setting up communications collaboratively with others.

Connecting to vehicles and travellers

One of the biggest developments in recent years has been in the ability of organisations to communicate with many individuals on a one-to-one basis. There is now a wide and diverse set of opportunities here.

Old-style, telephony based solutions (for example call centres) are still valuable for some purposes and some users. They can be expensive, though, and automated solutions (websites, SMS services etc) can help reduce the need for these.

More challenging is the direct communication to vehicle devices, in the so-called “cooperative systems”. The challenge is how and why a link should be established. This is only really widespread at present in two circumstances:

- public transport operators (road, rail, and air), whose vehicles can be equipped with devices to “talk” to infrastructure managers on agreed protocols and for agreed purposes
- charging and tolling systems in which “in vehicle units” are offered (and sometimes required) to allow automatic collection

This is, however, an area of considerable research.

Organisationally, it may be useful to consider outsourcing these public facing systems. For example local radio and motoring organisations provide broadcast travel information (and web and mobile service providers have somewhat similar functions); similarly, specialist companies who undertake vehicle monitoring, tracking or tolling can handle the more “difficult” communication links on behalf of a local authority or transport operator.

NTFI-Comms-10: Where specialist communications are necessary, it may be less costly and less risky to outsource delivery.

Communications technologies

Introduction

The framework and guidance presented above is generally applicable. The actual technologies used in an ITS system, however, will change over time. What is presented below is therefore a snapshot of key technologies at the date of publication.

That said, there is a tendency to worry too much about “upcoming” versus “outdated” technologies. There is seldom a need to use leading edge systems; “proven” is usually a less risky, and often less costly, choice. Moreover, the market lifetime of “old” technologies is determined more by whether people still find them useful than whether there is something better. Telephone landlines are built to standards many decades old, and show no real sign of abandonment.

Using the Internet Protocol

The single most pervasive communications network technology, by far, is the Internet Protocol (IP). It provides a clear and simple description of how to identify and address any specific device, application or system within a network. On the principles we have established, this is clearly the most important protocol.

NTFI-Comms-11: The core of any transport communications network should be based on IP.

IP addresses may be allocated manually (“static”) or automatically by a server (“dynamic”). Each approach has pros and cons; the two approaches can be mixed.

There are many different ways of implementing IP on specific bearers, and there is an extensive set of related protocols within the IP suite to help achieve this. Advice should be sought from a network engineer, as similar products/services may not all operate in the same way.

On top of IP, there are a small number of communications protocols that help to improve the management and reliability of the network. Specifically, the Transmission Control Protocol (TCP) acknowledges receipt and should be used wherever bandwidth is not seriously constrained; elsewhere the User Datagram Protocol (UDP) may be used, though applications may need to take account of the lower level of assurance.

Specialised transport/network layer technologies such as the Resource Reservation Protocol (RSVP) may be useful in some circumstances, but are likely to be over-complex for most transport comms networks.

Each of these approaches is able to support a rich mix of applications such as web (HTTP), file transfer (FTP), email (SMTP/POP), device control (SNMP), instant messaging (XMPP) etc, and also supports a base of application services such as synchronising network time, managing network addresses, etc.

Current mainstream IP is IPv4. For some while now there has been a steady introduction of a radically new network protocol, IPv6. However the two versions are not naturally compatible and care should be taken in designing or managing any network which uses both protocols.

Bearer technology – wide area

Many wide area bearers are suitable for IP networks, including:

- Fixed wireline links – leased lines, at speeds from 64kbps upwards
- DSL – usually much cheaper than leased lines, though not quite so reliable as they share a core network among multiple users
- Own wireline systems, including fibre and coaxial – expensive to install but highly resilient and very high capacity
- Dial-up telephony – occasionally still useful though the low cost now rarely outweighs the capacity limitations, slow operation and modem problems
- Commercial radiocomms – notably GPRS and the more expensive, but more capacious, 3G
- Some fixed wireless links, for instance microwave systems – though these are likely to provide an optimal solution in very few circumstances
- Own wireless systems – the established analogue Private Mobile Radio (PMR) will struggle, the newer Digital Mobile Radio (DMR) is narrowband, while systems based on TETRA are effective but considerably more expensive
- Mesh network based on shorter-range protocols such as IEEE802.11 “WiFi” – now reasonably well established in the urban context, and with the benefit of a natural direct connection into IEEE802.11-based consumer devices

The communications industry is constantly developing and new protocols are constantly emerging, or moving from innovative to mainstream. Current “new” technologies include DMR, IEEE802.16 “WiMAX”, LTE (the “Long Term Evolution” of commercial radiocomms beyond 3G), and the transport-sector-specific framework CALM (Communications Access for Land Mobiles). Only time will tell which, if any, of these will be cost-effective for ITS users.

Routers will be necessary to connect these various network components into an integrated IP network.

NTFI-Comms-12: Transport communications networks should be free to use any suitable bearer.

Of the current mainstream wide-area bearer options, those not advised for IP networking are dial-up telephony and PMR. These are narrowband analogue systems, optimised for voice, and while they can be adapted to a digital role it is seldom worthwhile.

Bearer technology – short range

Short-range communications in transport tend to be used for much more specialist purposes than wide-area networks, which often carry a wide range of different communications streams between distant points. As a result the choice of short-range bearers is likely to be much more dependent on the specific functions being supported. Nevertheless, it is often necessary to connect them into the overall network:

- Applications communicating over a LAN may need to share data obtained from vehicles and the street
- Devices communicating within a vehicle may exchange information which is passed onward to a control centre

As with wide-area technology, there are a number short-range bearers that directly support IP networks, including particularly those standardised in the IEEE802 series:

- Wired and wireless local area networks, such as IEEE802.3 “Ethernet” and IEEE802.11 “WiFi”
- Short range direct links such as IEEE802.15.1 “Bluetooth”, IEEE802.15.4 “Zigbee” and similar systems

However there are also many specialised short-range protocols that are designed around radio physics and not directly optimised for IP, such as:

- Digital Short Range Communications (DSRC) at 5.9GHz
- ISO 14443, the international standard for “Identification cards – Contactless integrated circuit cards – Proximity cards” – a short range (<10cm) protocol operating at 13.56MHz, used by ITSO, Oyster, the “NFC” of some mobile phones and the “EMV” of next-gen bank cards
- Radio Activated Key Entry (RAKE) – a low power protocol (MPT 1340) operating at 433MHz, widely used for car key fobs etc and operating in unlicensed (=free to use but not protected) spectrum
- RTIG’s short-range protocol at 180MHz, designed for bus-to-streetside use

NTFI-Comms-13: Non-IP links can and should be used where there is good functional reason; in these cases managers should clearly identify whether and how the information is ported into the main IP network.

Local “hubs” and routers may be useful, to connect nearby devices using short-range protocols into wide-area systems. This communications function may be:

- built into an existing device – for instance a bus may use NFC for smart ticket readers, but transmit this back to base using GPRS, with translation provided in the ticket machine
- through a standalone hub with a purely comms function – for instance, at a road junction where there are many nearby devices such as traffic signals and detector loops

Spectrum usage

Generally transport users will want to use licensed spectrum for operational purposes. Unlicensed spectrum is often appropriate for short-range links, and may be suitable for research or trial purposes.

NTFI-Comms-14: Use licensed spectrum for operational long haul radio links.

Analogue radio systems

Analogue radio systems are not designed for IP networking but, owing to their relatively low ongoing cost, remain popular with public sector transport stakeholders. They also benefit from high robustness and low latency. While there are increasingly realistic alternatives for both economic and technical aspects, it is likely that PMR will continue to provide valuable service for some while.

Analogue networks may be used in two ways:

- as a “black box” subnetwork within an IP network: modems transform IP datagrams to a form suitable for transmitting across the analogue network, which are then unpacked at the receiver modem
- as an end-network: end devices communicate over analogue, and a gateway translates the data from native to a format suitable for storing on main (IP based) information network

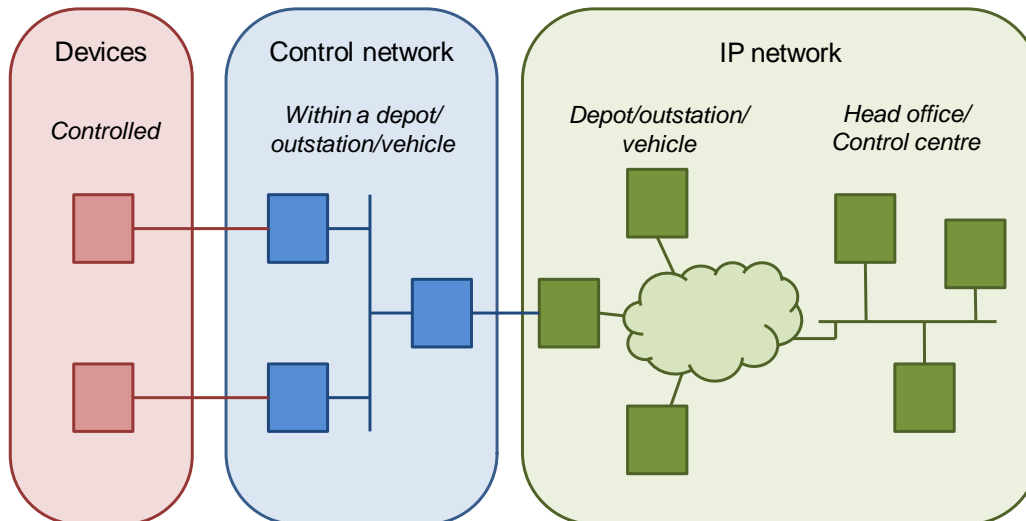
The second approach enables the use of legacy systems but should be avoided for future implementations, as the translation function is much more complex.

Control networks

Some local systems may be integrated using non-IP technology. This may be true in harsh environments where the information passed is highly specific, and not complex in terms of volume or structure. For instance, a meteorological sensor is of this type, as is a vehicle detector.

Where the information is of purely localised interest the communication will normally be provided by the product supplier and there is nothing further for system managers to do. However where the information needs to be brought back to a complex management system a suitable mechanism needs to be found. For instance engine temperature may be monitored as part of a maintenance regime, or loop occupancy as part of an automated traffic control system.

In some cases the device controller will be able to port directly to the IP network. In other cases this will not be practical and an intermediate network will be needed. In these cases, a suitable robust set of standards is required. Suitable standards might include CANbus at networking level, or RS485 at the electrical level; specific advice is required on each systems context.



So, the red links enable local, proprietary communications to a specific device. The blue network enables information exchange where IP is inappropriate; a gateway is provided into the main (green) IP network, enabling the devices to be monitored or controlled.

In choosing a control network protocol, the ability to provide an IP gateway is, in this architecture, essential.

NTFI-Comms-15: Local non-IP networks should be gatewayed into the main IP network by default.

Voice and video

Voice and video, as continuous rather than file-based communications, traditionally use different protocols from data. Voice over IP (VoIP) and video over IP are now well established technologies and should be considered as part of an integrated network approach.

However, it will not always be cost effective to achieve this, and will not always be necessary. Separate channels – such as plain old telephony for voice, and in the mobile world GSM – may be simpler to operate and provide all the required functionality.

There may even be reasons to have separate networks – say a standard telephony solution for normal “office” voice services, a separate (possibly IP based) voice network for operational communications.

NTFI-Comms-16: Voice and video networks should be considered separately, but there may be scope for integrating them with the data network.

Abbreviations

Communications is a technical subject and has its fair share of abbreviations. The following list represents some of the more common, as referenced in this Guideline, but is far from complete.

3G	Third Generation (mobile) – a technology which allows broadband services over mobile devices such as smartphones
CALM	Communications Access for Land Mobiles – an emerging framework of standards designed for surface (mainly road) transport
CANbus	Control Area Networking – originally aimed at factory automation, this is now widely used in vehicles to interconnect automotive components
DMR	Digital Mobile Radio – a newer, digital version of PMR
DSL	Digital Subscriber Line – a means of getting digital broadband over normal phone lines (widely used for both household and business internet connections)
DSRC	Dedicated Short Range Communications – a set of transport domain standards designed for short range links between roadside and vehicle
EMV	“Europay, MasterCard and VISA” – a global interoperability standard developed by the banking industry for payment cards and card readers, now being considered for transport smartcards
GPRS	General Packet Radio Service – an adaptation of cellphone technology based on GSM to enable it to carry data in IP format
GSM	Global System for Mobiles – the technology standard for mobile phone voice calls, in UK and over much of the world
HTML/XML	Standards (“languages”) which are used to structure data to be sent over IP networks. HTML (Hypertext Markup Language) is for words-and-pictures web pages, while XML (eXtensible Markup Language) is aimed at data exchanged between computer systems.
HTTP etc	Standards (“protocols”) for sending data of various kinds over IP networks. HTTP (Hypertext Transfer Protocol), primarily for web pages, is one of the most widely used but there are numerous others

IEEE	Institute of Electrical and Electronics Engineers – a US-based professional body which develops the world’s most widely used data network standards
IP	Internet Protocol – the underlying technology for all internet communications, capable of sending any kind of data between any two devices with an “IP address”
LTE	Long Term Evolution – an emerging commercial upgrade for 3G
NFC	Near Field Communication – a short-range protocol based on international standard ISO14443 used to enable mobile phones to act as smartcards
PMR	Private Mobile Radio – any radio comms system using own equipment (as opposed to services bought in from a telecoms operator)
RAKE	Radio Activated Key Entry – a low power, short range radio protocol widely used in keyfobs etc
SLA	Service Level Agreement – a contractual condition with a provider to promise a specific quality of service, with penalties for failure
TCP/UDP	Two different ways of sending data over IP networks. With TCP the receiver acknowledges receipt; with UDP it doesn’t, which is more efficient but less reliable
TETRA	Trans European Trunked Radio – a digital standard for PMR
VoIP	Voice over IP – a way of converting voice analogue signals into digital form, suitable for use over IP networks
WiFi	Wireless Fidelity – name given to a popular set of radio networking standards suitable for local areas, developed by IEEE as IEEE802.11

About the JCG

The Joint Chairs Group, and its component groups, use their communities to build specifications and provide guidance on a market neutral basis. The notes below summarise in brief the scope of specifications available through each group and which, collectively, form part of the UK's *de facto* technical framework for ITS.



RTIG-INFORM provides a strategy and architecture for public transport technology, on and off the vehicle. Its interface specifications cover on-vehicle, vehicle-to-centre, and centre to centre data exchange, linked to European standards where available. Guidance is provided on areas as diverse as DDA compliance, use of CCTV and data sharing.



UTMC provides a Technical Specification for road network management, in two parts. The first part (the Framework) defines a general architecture and protocols, while the second (the Objects Register) is an evolving library of modules for different UTMC functions, ranging from ANPR to car parks and air quality to incidents.



TIH provides a common practice approach to the exchange of travel information. It also provides the UK focus for issues relating to the European DATEX II project.

In April 2011, the TIH Executive was merged into the UTMC Development Group.



ITSO provides a platform and tool-box for the implementation of interoperable contactless smart customer media, public transport ticketing and related services. Specifications cover consumer media, media readers and back end facilities; in addition ITSO provides the national security management system.

Feedback on this Guideline

The JCG welcomes feedback from the marketplace, whether from systems developers or users, on areas where our recommendations could be improved. Feedback should normally be provided through UTMC as the lead group – please contact secretariat@utmc.uk.com.