



UTMC

Urban Traffic Management and Control

TS003:2005

Framework Technical Specification

May 2005

Cover + 48 pages

© Crown Copyright 2005

Foreword

This document, UTMC Technical Specification 003 (TS003:2005), was prepared by UTMC Programme Management and is published under the authority of the Department for Transport (DfT). It forms part of the range of UTMC specifications and supersedes previous versions of the Technical Specification, TS001:1997 and TS002:2001.

TS003:2005 takes into account feedback from the consultation process and ongoing international initiatives in this field. It presents the core technical standards recommended for use by UK traffic managers in their systems. Non-normative annexes provide guidance on how to use the specification.

This document should be used in conjunction with the other main repository of UTMC technical recommendations, namely the Data Objects Registry, TS004. TS004 is under continuous review and update, while TS003 is not likely to be updated for 2-3 years.

Copies of all UTMC documentation, together with background material and other information, can be found on the UTMC website at: <http://www.utmc.gov.uk>.

Please note: (1) Compliance with this specification does not of itself confer immunity from or compliance with any statutory or legal obligations. (2) Whilst DfT strongly supports the adoption of UTMC standards, such standards are not mandatory.

List of contents

Foreword	1
1 Introduction	4
1.1 General	4
1.2 Document approach and structure	4
1.3 Definitions	5
2 UTMC compliance	10
2.1 Interface compliance	10
2.2 UTMC compliance of Products and Systems	10
2.3 Statutory and legislative compliance	10
2.4 System Certification	10
2.5 Compliance and procurement decisions	10
3 Architecture	11
3.1 Introduction	11
3.2 Logical Reference Model	11
3.3 Functional Reference Model	12
4 Human-Machine Interface	14
4.1 User Interface	14
4.2 System Management Services	14
5 Information level standards	15
5.1 General	15
5.2 Types of Data Object	15
6 Application level standards	16
6.1 General data exchange	16
6.2 UTMC specific data exchange	16
6.3 Common Database and Data Services: Applications Interface	16
6.4 Applications Service Interfaces	17
7 Transport level standards	18
7.1 Communication protocols	18
7.2 UDP and IP usage: the 'typical implementation'	18
8 Subnetwork and plant level standards	21
8.1 General	21
8.2 Use of wireless technology	21
9 Safety and security	22
9.1 Operational safety	22
9.2 Security and availability	22
A References (Normative)	23
B Management authority for this document (Informative)	24
B.1 Formal authority	24
B.2 Day to day management	24

C	Examples of UTMC architectures (Informative)	25
C.1	Architecture choices: FEPs and adapters	25
C.2	York UTMC demonstrator	25
C.3	Preston UTMC demonstrator	26
C.4	The impact of being 'UTMC compliant'	27
D	Data objects & applications layer communications (Informative)	28
D.1	General	28
D.2	Target profiles	28
D.3	The SNMP/MIB approach	29
D.4	UK UTC using SNMP	30
D.5	The Common Database and the Logical Data Model	32
D.6	The CORBA approach	33
D.7	The XML approach	34
E	Communications: networks and bearers (Informative)	36
E.1	General	36
E.2	Basis profile: wide area IP	37
E.3	Central office profile: SUPS	38
E.4	Application of wireless technologies in UTMC networks	39
E.5	Deployment issues with wireless communications	40
E.6	Design: efficiency, bandwidth and cost	40
F	Guidelines on safety in UTMC systems (Informative)	42
F.1	Context	42
F.2	Conclusions of demonstrators	42
G	Information security (Informative)	44
G.1	Introduction	44
G.2	UTMC security requirements	44
G.3	Structural security	44

1 Introduction

1.1 General

- 1.1.1 TS003 specifies a framework of applicable standards for Urban Traffic Management and Control (UTMC) systems, which will provide a cost effective and flexible means to manage transport in urban areas to support a wide range of transport policy objectives. The UTMC framework facilitates integration of transport systems, and enables information to be provided to system for traffic management and as a means of influencing traveller behaviour.
- 1.1.2 TS003 has been developed to promote open systems and interoperability of components within UTMC systems. As far as possible, it utilises readily available open standards and makes maximum use of relevant international initiatives.
- 1.1.3 This document specifies, in the form of a framework, requirements for UTMC systems which will provide a cost effective and flexible means to manage transport in urban areas to support a wide range of transport policy objectives. It will facilitate integration of transport systems and make available information as a management tool and as a means of influencing traveller behaviour.

1.2 Document approach and structure

- 1.2.1 TS003 is composed of numbered clauses and subclauses, which form the normative elements of the specification. The titles of each clause are listed in the contents list. This document incorporates, by reference, provisions from specific editions of other publications (Normative references) and other publications that provide information or guidance (Informative references). These references are cited at the appropriate points in the text.
- 1.2.2 The following annexes are included. With the exception of Annex A, these annexes are informative and not intended to constrain those developing or deploying UTMC systems; they merely provide guidance on how the normative aspects of this document could be used.

Annex A: Normative Reference Documents: a list of all normative documents referenced in this document.

Annex B: Management authority for this document: a statement of how this document is maintained and where questions relating to its provisions or updates should be addressed.

Annex C: Examples of UTMC architectures: an outline of some of the ways in which Local Authorities have used the UTMC specification in deploying their Traffic Management Systems

Annex D: Data objects & applications layer communications: guidance on how the applications layer protocols can be used in conjunction with the UTMC Data Objects of TS004.

Annex E: Communications: networks and bearers: guidance on the use of different types of bearer, and multiple bearer types, to deliver a UTMC network.

Annex F: Guidelines on safety in UTMC systems: an overview of the outcome of trialling a formal approach to UTMC safety, acting as guidance to future implementers.

Annex G: Information security: an overview of good practice guidance on information security in UTMC systems.

1.3 Definitions

1.3.1 The following definitions apply to this document:

Application: Software hosted on UTMC components and infrastructure to implement UTMC functions.

Application message: messages used to transfer data between applications within UTMC systems and between UTMC systems and external systems.

Authority: local or central government or other body responsible for a UTMC system.

AVL: Automatic Vehicle Location.

BER: Basic Encoding Rules.

CCTV: Closed-Circuit Television

CDR: Common Data Representation.

CEN: Comité Européen de Normalisation, the European Standards body. CEN functions via a series of Technical Committees (TC), with TC278 being responsible for transport telematics.

Communication protocol: A set of rules or procedures governing the transfer of data from one point to another.

Component: Any equipment connected to the UTMC infrastructure. Components can be either instation or outstation components. Components in a UTMC system may be supplied by more than one manufacturer.

CORBA: Common Object Request Broker Architecture, a technical framework for object-oriented programming suited to the open interconnection of systems.

Data Object: A specific coherent structure of data, registered for public use at the UTMC Data Objects Registry. Data Objects may be defined to several different standards for use by different technology systems.

DATEX: A task force under the European Road Transport Telematics Implementation and Coordination Organisation to set standards for data exchange between fixed installations. This has included setting up the DATEX data dictionary.

DSRC: Digital Short Radio Communications.

ETSI: European Telecommunication Standards Institute.

External system: Systems that are not formally part of an individual UTMC system, but may exchange information with the UTMC system. An external system has no direct contact with UTMC outstations.

FEP: Front End Processor.

FTP: File Transfer Protocol – an internet protocol for the transfer of files across a network.

Functionality: The nature of what an application or component does within itself (cf interface).

Functions: Defined transport related activities performed by a UTMC system. Functions are implemented by single or multiple Applications hosted in single or multiple Components on the UTMC infrastructure.

GIOP: General Inter-ORB Protocol (GIOP).

GPRS: General Packet Radio Service.

GSM: Global System for Mobile communications.

HTTP: Hyper Text Transfer Protocol – the transport layer for exchange of XML files over TCP/IP networks.

ICMP: Internet Control Message Protocol is a messaging and service management protocol for IP.

IDL: Interface Definition Language.

IETF: Internet Engineering Task Force.

IHL: Internet Header Length.

IIOp: Internet Inter-ORB Protocol.

Information: Processed data to meet the needs of authorities or travellers.

Interface: The technical means by which one application, component or element of a UTMC infrastructure connects to others, through communications and information exchange.

Instation: Collection of UTMC components and applications based in an indoor environment. Instations will typically be regularly manned.

IP: Internet Protocol is the basis for addressing within TCP/IP networks that provides a connectionless-oriented network layer protocol.

ISO: International Standards Organisation.

ITS: Intelligent Traffic Systems.

ITU: International Telecommunications Union, the world telecommunications standards body.

LAN: Local Area Network.

Message: Package of information created for the purposes of communications between components or between applications.

MIB: Management Information Base.

MIB-II: Managed objects for the internet suite of protocols as defined by RFC1213.

Module: A group of components, applications or elements of a UTMC infrastructure subject to separate procurement, against specifications for functionality and interfaces.

MPT: Ministry of Post and Telecommunications.

NTCIP: National Transportation Communications for Intelligent Transport Systems (ITS) Protocol as prepared by the NTCIP Joint Standards Committee and referred to the ISO.

OASIS: Organisation for the Advancement of Structured Information Standards, open industry-led body responsible for development of standards such as UDDI and development of XML-based services

Ofcom: The Office of Communications, the UK's regulatory body for telecommunications service providers.

OID: Object Identity.

OMG: Object Management Group, an international grouping of systems developers that maintains CORBA.

Open standards: Standards in the public domain. Two kinds of 'standards' are distinguished: de jure (created in a formal legal manner by standardisation body, eg ISO, CEN, or BSI), and de facto (specifications that gain near-universal adoption, eg Microsoft Windows). Some standards are administered to be open by a user group or committee rather than a legal standards body – see under IETF, W3C, and OMG.

ORB: Object Request Broker.

OTU: Outstation Transmission Unit, field-based equipment that communicates with the transport controller within a UTC network.

Outstation: UTMC components and applications based in the field. Outstations will not normally be manned.

PDU: Protocol Data Unit.

Physical interface: Physical and electrical interface types - connectors, signal levels, device addressing schemes etc.

PMR: Private Mobile Radio.

PPP: Point-to-Point Protocol links two permanent points enabling IP transport of data.

Product: A package of components, applications or elements, with or without associated services, offered for sale to potential implementers of UTMC systems, and possessing specifications for functionality and interfaces.

PSTN: Public Switched Telephone Network.

RFC: Request For Comment (used as the description of internet 'standards').

RTA: Road Traffic Advisor.

RTTE: Radio & Telecommunications Terminal Equipment.

SCOOT: Split Cycle Offset Optimisation Technique is a real time adaptive control system for linked signal junctions.

SOAP: Simple Object Access Protocol – an XML language used to make requests for service and receive the response

SLIP: Serial Line Internet Protocol is an access protocol primarily designed to allow PCs to access the internet using a modem although this technology has now been surpassed by PPP.

SNMP: Simple Network Management Protocol is an email application that defines the sending and receiving of emails.

SQL: Structured Query Language is employed for accessing databases.

STMF: Simple Transport Management Framework.

STMP: Simple Transport Management Protocol.

SUPS: Simple UTC Protocol System.

SVD: Selective Vehicle Detection.

TCP: Transmission Control Protocol is a connection-oriented protocol.

TETRA: Terrestrial Trunked Radio.

TOS: Type of Service.

Traffic and Travel Data Dictionary: The data dictionary prepared by the DATEX Task Force and referred to CEN.

Traffic Management System: Any collection of components and applications deployed for the purposes of managing and controlling road traffic in a specific area, whether or not it complies with the UTMC Technical Specification.

TTL: Time To Live.

UDDI: Universal Description, Discovery and Integration – an XML language used to catalogue Web Service providers.

UDP: User Datagram Protocol is a connectionless transport protocol.

UHF: Ultra High Frequency.

UTC: Urban Traffic Control.

UTMC Data Objects Registry: The repository of Data Objects managed on behalf of the UTMC community, and recorded in TS004.

UTMC infrastructure: Basic UTMC system services that support components and applications, such as communication services, database management systems, operator interfaces etc.

UTMC system: an integrated Traffic Management System (qv) that conforms to the requirements of the UTMC Technical Specification.

UTMC Technical Specification: TS003 as supplemented by TS004.

VHF: Very High Frequency.

VMS: Variable Message Sign.

W3C: The World Wide Web Consortium, an open organisation of developers responsible for developing and maintaining web applications standards including XML, WSDL and SOAP

WAN: Wide Area Network.

Web Services: a set of industry standards, using XML, which allow applications to share functionality and data with other applications connected by a network.

WSDL: Web Services Description Language – an XML language used to describe services that are available.

XML: eXtensible Markup Language – a language for describing data in a simple ASCII Text document.

XML schema: Used to define an XML Language in terms of tag names, data types and formats. The schema is itself an XML document.

2 UTMC compliance

2.1 Interface compliance

2.1.1 The primary intention of UTMC Technical Specification is to facilitate the interoperability of modules in a Traffic Management System, and between such systems and external parties. In this regard:

- a) A specific interface in a Traffic Management System may claim to be a “UTMC compliant interface” if all communications across it are conducted using the technical standards of TS003:2005 sections 4-8, conveying only registered UTMC data objects as listed in TS004.
- b) An interface may claim to be an “extended UTMC compliant interface” if it uses the technical standards of TS003, and the data it conveys are in the structure of registered UTMC data objects wherever they are available.

2.2 UTMC compliance of Products and Systems

2.2.1 Products may have a number of interfaces, and a Traffic Management System may be constructed from a number of Products configured in a particular way. It will not always be necessary or efficient for all of these interfaces to be UTMC compliant interfaces, in order to meet the primary goals of facilitating interoperability. Thus, the “UTMC compliance” of a Product or System is not a simple yes-or-no property.

2.2.2 Nevertheless, it is recognised that suppliers and traffic managers would value the ability for Products and Systems to be assessed against the UTMC Specifications and, if appropriate, their compliance recognised. To this end, the Department for Transport is currently working towards the establishment of a suitable monitoring and assessment regime for Products and Systems.

2.3 Statutory and legislative compliance

2.3.1 All UTMC systems, their components and applications shall conform to all relevant UK and EU statutory or legislative requirements.

2.4 System Certification

2.4.1 UTMC systems shall conform to the requirements of the System Certification Procedure, as defined in MCH 1813.

2.5 Compliance and procurement decisions

2.5.1 The UTMC Specifications are guidelines only, which document a consensus technical approach to modular Traffic Management Systems. Procurement decisions must continue to be made in accordance with procurement regulations.

3 Architecture

3.1 Introduction

3.1.1 A UTMC system shall have a documented architecture which includes:

- a) A system diagram based on and similar to the Logical Reference Model of section 3.2, indicating the physical components and connectivity between them.
- b) A functional diagram based on and similar to the Functional Reference Model of section 3.3, indicating the applications and interfaces between them.

3.2 Logical Reference Model

3.2.1 The Logical Reference Model describes a UTMC system as a series of interconnected nodes (see figure 3-1).

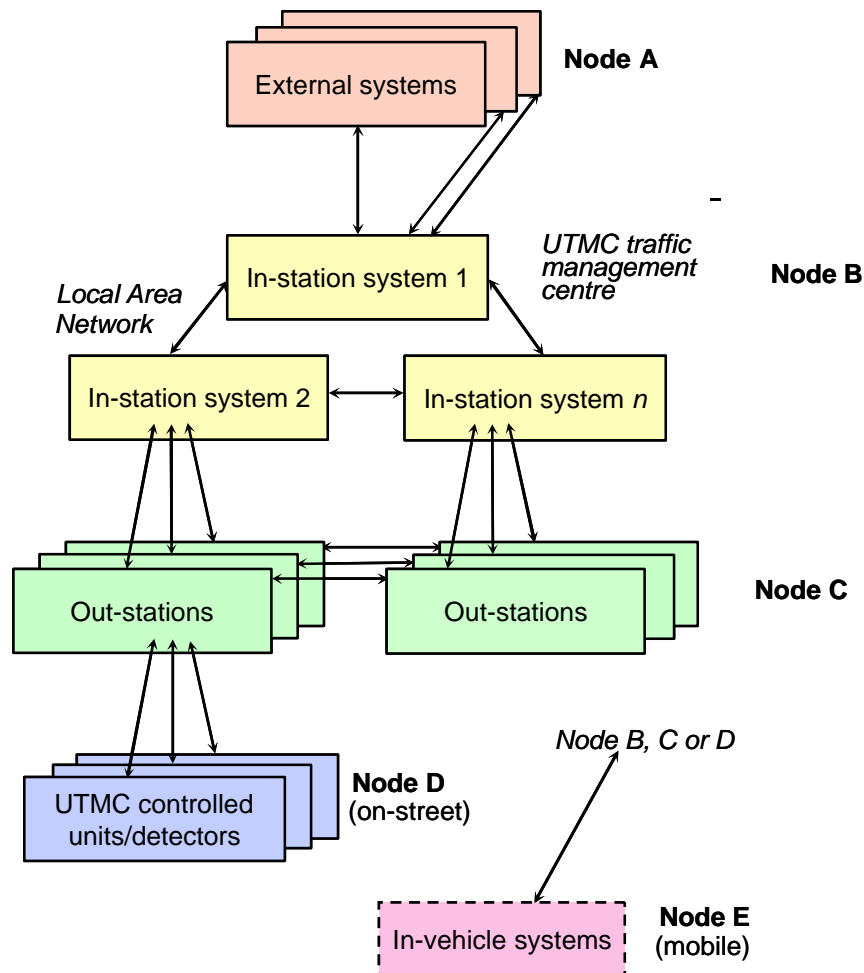


Figure 3-1: The Logical Reference Model for a UTMC system

3.2.2 UTMC nodes are defined as:

- a) Node A: fixed gateways to external systems including other UTMC systems;
- b) Node B: UTMC management centres;
- c) Node C: UTMC outstations;
- d) Node D: UTMC controlled units; and
- e) Node E: mobile units.

3.2.3 The following restrictions on configuration shall apply:

- a) there may be zero or more Nodes A;
- b) there shall be one and only one Node B;
- c) there may be zero or more Nodes C;
- d) there may be zero or more Nodes D;
- e) there may be zero or more Nodes E; and
- f) there shall be at least one Node D or Node E in a UTMC system.

3.2.4 Node B may be physically distributed in several locations, but shall act as a single logical node. Node B will typically host a range of components and applications, including databases.

3.2.5 Nodes C may be capable of acting autonomously taking higher level control decisions. Nodes C may be permanent or temporary installations.

3.2.6 Nodes D cannot act autonomously. Nodes D may be permanent or temporary installations.

3.2.7 Nodes E may range from simple units to sophisticated units with local processing power.

3.2.8 There may be links between the following:

- a) Nodes A and Node B;
- b) Node B and Nodes C;
- c) Node B and Nodes D;
- d) Node B and Nodes E;
- e) Nodes C and Nodes C;
- f) Nodes C and Nodes D;
- g) Nodes C and Nodes E; and
- h) Nodes D and Nodes E.

3.2.9 Links may be one-way or two-way.

3.2.10 There may be single or multiple logical channels per single physical channel.

3.3 Functional Reference Model

3.3.1 The elements of the Functional Reference Model are:

- a) User interface;
- b) Applications;
- c) System management services;
- d) Communication services.

3.3.2 Applications shall use the system infrastructure as its operating environment. Applications may have local, private databases or data caches associated with them.

3.3.3 Communications services are based on a stack architecture of five levels (see figure 3-2):

- a) *Information Level* – Standards for the data elements, objects, and messages to be transmitted. These are specified in section 5 of this document.
- b) *Application Level* – Standards for the process and structure of information exchange, and of session management. These are specified in section 6.
- c) *Transport Level* – Standards for data packet subdivision, packet re-assembly, packet error detection and retransmission, and routing. These are specified in section 7.
- d) *Sub-network Level* – This level provides standards for the physical interface and the data packet transmission method). These are specified in section 8.
- e) *Plant Level* – Standards for the physical transmission media. These are also specified in section 8.

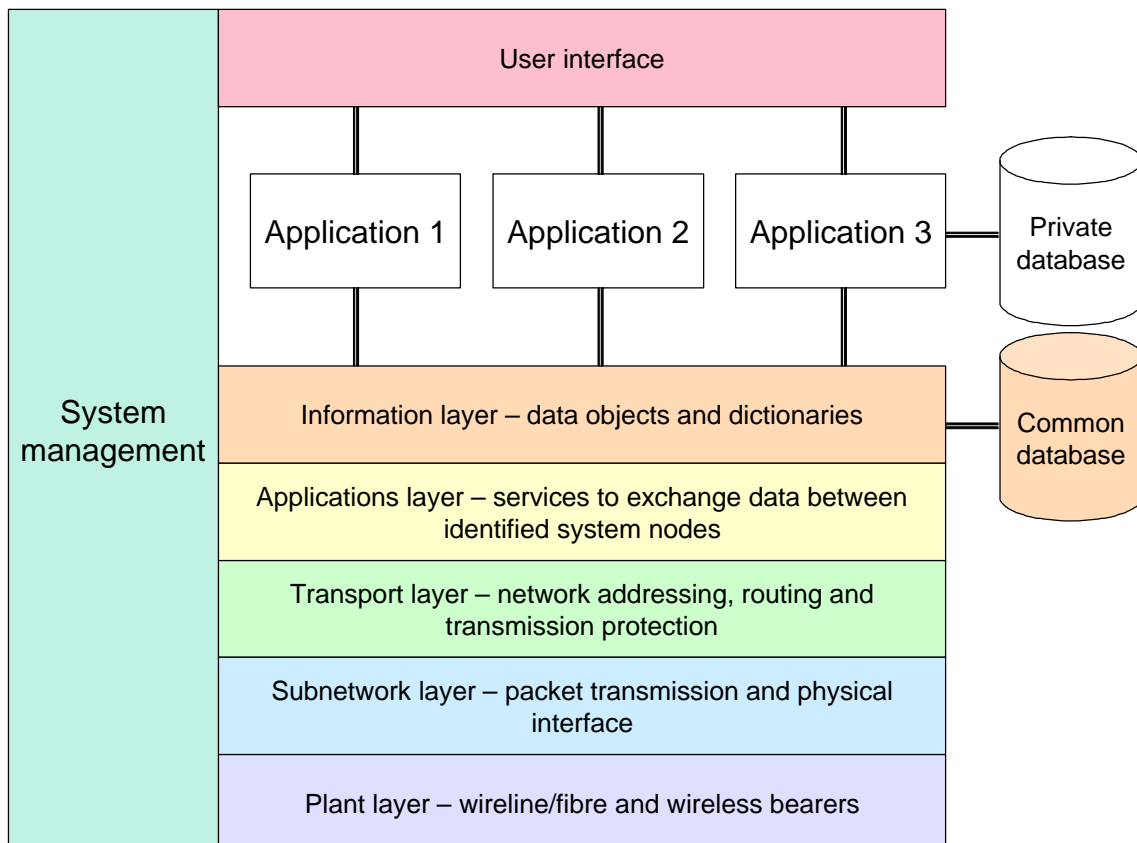


Figure 3-2 – Functional Reference model for a UTM C system

4 Human-Machine Interface

4.1 User Interface

- 4.1.1 A UTMC system shall have a consistent user interface to configure and control applications at Node B. A user interface may also be available at Nodes C.
- 4.1.2 The user interface for every application should be available from all operator terminals, where applicable.
- 4.1.3 The user interface for every application shall provide user authentication and access control for security purposes.
- 4.1.4 The UTMC user interface to applications shall support a common and suitably open operating system interface. This may be one of the following:
 - a) Browser interfaces based on HTML and extensions;
 - b) Microsoft™ Windows™, Win 32 API;
 - c) X/Open standards, X/Window and X/Terminal.
- 4.1.5 Non-UTMC applications software, such as systems management services and off line data analysis tools, may use the user interface of the underlying network operating system as appropriate.

4.2 System Management Services

- 4.2.1 The following system management facilities shall be provided as a minimum:
 - a) Management/monitoring to ensure the operational status of components and communication links; and
 - b) Facilities to configure components and communication links.
- 4.2.2 System management facilities shall be provided as part of the Node B network operating system. Where components of a UTMC system require to be managed centrally, a suitable standard device management protocol shall be used. The preferred standard is SNMP.
- 4.2.3 System management facilities for the configuration of remote networking components and communication links shall comply with SNMP version 1 as specified in RFC 1157.

5 Information level standards

5.1 General

- 5.1.1 Data standardisation within a UTMC system shall make reference to a system architecture, based on the UTMC logical, functional and combined reference models which clearly indicate the scope and interfaces of the modules of that system. In this context a module is defined as “a group of components, applications or elements of a UTMC infrastructure subject to separate procurement, against specifications for functionality and interfaces”.
- 5.1.2 Data communicated across an interface between modules of a UTMC system, or between a UTMC system and an external system, is subject to specification. For UTMC compliance all such data shall be constructed as registered Data Objects. Data communicated within a module of a UTMC system is not required to follow this Technical Specification.

5.2 Types of Data Object

- 5.2.1 A Data Object shall be of one of the following types:
- Database Objects, developed for use within the Common Database.
 - Internet objects, developed for passing over web-browsing services (ie HTTP).
 - MIB Objects, developed for transport using a Management Information Base (MIB) over SNMP.
- 5.2.2 Data Object definitions should address the following aspects:
- object structure and ‘packaging’ information;
 - units and coding standards for parameter values;
 - source and destination;
 - data quality measures.
- 5.2.3 Data Objects should be developed to be compatible, as far as possible, with relevant international standards.
- 5.2.4 Data Objects, and their exchange processes, shall be specified in a suitable standard specification language. Acceptable languages include:
- XML (particularly for Internet objects);
 - IDL (for additional CORBA services);
 - Entity-relationship diagrams (particularly for Database Objects);
 - Abstract Syntax Notation 1 ASN.1 (particularly for MIBs);
 - UML.
- 5.2.5 A UTMC Data Objects Registry, TS004, has been established as a companion to this document. This Registry will maintain an open list of approved Data Objects of all types, and will be subject to continuous review. The procedure for registering and using Data Objects, and the current list and definitions of registered Data Objects, may be obtained from the contact points in annex B.

6 Application level standards

6.1 General data exchange

6.1.1 General data exchange includes:

- a) user messaging;
- b) file transfer; and
- c) web-based information access.

6.1.2 User messaging should not normally be provided in UTMC systems. If necessary it should be provided through Simple Mail Transport Protocol (SMTP) as specified in RFC821 and associated documents.

6.1.3 File transfer should be provided through File Transfer Protocol (FTP) as specified in RFC959 and associated documents.

6.1.4 Web-based information access should be provided through Hypertext Transfer Protocol (HTTP) as specified in RFC1945 and associated documents.

6.2 UTMC specific data exchange

6.2.1 UTMC specific data exchange comprises the exchange of UTMC Data Objects.

6.2.2 A CORBA-compliant object brokerage service used to exchange UTMC Data Objects shall use:

- a) the General Inter-ORB Protocol (GIOP) message formats and Common Data Representation (CDR).
- b) the Internet Inter-ORB Protocol (IIOP) for use over TCP/IP.

6.2.3 MIB Objects shall be exchanged using the Simple Network Management Protocol (SNMP) as specified in RFC1157 and associated documents.

6.2.4 Any Data Objects may be exchanged using a suitable XML schema over HTTP.

6.2.5 In the case that it necessary to use a null or proprietary applications layer communication protocol (for example, because of limitations in the capacity of a communications bearer), the communications link shall be regarded as embedded in a component. In this case, an interface shall be provided as near to one end of the communications link as practical which utilises a suitable open applications layer protocol.

6.3 Common Database and Data Services: Applications Interface

6.3.1 A UTMC Common Database may be implemented using a middle tier Applications Server between UTMC applications and the database server. A UTMC Common Database Applications Server shall be based on either CORBA or XML/HTTP or both.

6.3.2 A UTMC Common Database Applications Server shall offer query and subscription services. The interfaces offered by the UTMC Common Database Application Server shall be based on suitable approved Interface Definition Language (IDL) scripts and/or XML schemas, as appropriate.

- 6.3.3 All user visible names (tables, columns etc) must be as given in the logical data model. Names which are normally hidden from the user (constraints, indices etc) may follow any rational scheme.
- 6.3.4 All datatypes should be SQL92 compliant equivalents of the generic types expressed in the logical data model.
- 6.3.5 A Common Database will normally be based on a relational database management system. Integrity constraints (or triggers) should be used to enforce referential integrity of the expressed relationships. Good practice in database design (for instance, regarding the use of indices) and operation (for instance, regarding account management and database administration) shall be followed.

6.4 Applications Service Interfaces

- 6.4.1 The interface between Applications, or between an Application and a Common Database, shall use agreed written specifications for relevant service features. These specifications may include aspects such as:
 - a) Whether 'push' or 'pull' delivery (or both) is to be adopted.
 - b) 'Granularity' of the blocks in which data may be requested or provided.
 - c) Applications-level triggers and handshaking protocols for data exchange.
 - d) Application-to-application authentication.
 - e) Directory services.
 - f) An assessment of likely data exchange volumes.
 - g) Conditions on acceptable delivery, for instance on timeliness.
- 6.4.2 The documentation provided from time to time by the Travel Information Highway (TIH) initiative is recommended as an additional source of good-practice guidelines.

7 Transport level standards

7.1 Communication protocols

- 7.1.1 For communications between nodes, UTMC systems shall utilise the Internet Protocol (IP) as specified in RFC791 and associated documents.
- 7.1.2 The preferred transport level standard is the User Datagram Protocol (UDP) as specified in RFC768 and associated documents. Transport control (that is, ensuring that packets have been delivered and resending if necessary) should be achieved end-to-end, at the application level.
- 7.1.3 It is also acceptable to use the Transmission Control Protocol (TCP) as specified in RFC793 and associated documents.

7.2 UDP and IP usage: the 'typical implementation'

- 7.2.1 This section presents the preferred build of a UDP/IP implementation for UTMC systems (a 'typical implementation'). Other build are permissible where local economic or technical constraints indicate them.
- 7.2.2 A typical implementation of UDP shall support the following capabilities:
 - a) data transfer as specified in RFC 768, page 2 and RFC 1122, Section 4.1.1.
 - b) port addressing as specified in RFC 768, pages 1 and 2 and RFC 1122, Sections 4.1.1, 4.1.3.1, 4.1.3.5, and 4.1.3.6.
 - c) checksum as specified in RFC 768, page 2 and RFC 1122, Sections 4.1.1 and 4.1.3.4.
 - d) MIB-II UDP group as specified in RFC 1213, Sections 3.10 and 6.9.
- 7.2.3 A typical implementation shall support the following fields as described in RFC 768:
 - a) source port;
 - b) destination port;
 - c) length;
 - d) checksum.
- 7.2.4 General Interface requirements are as specified in RFC 768. A typical implementation shall:
 - a) act upon all ICMP messages as stated in RFC 1122, Section 4.1.3.3.
 - b) support the UDP to Application Layer Interface requirements as defined in RFC 1122, Section 4.1.4.
 - c) pass IP options as described in RFC 1122, Section 4.1.3.2. A user-defined IP option is described for use with multiple addressing. This transport profile defines this option.
 - d) implement and use the checksum as described in RFC 1122, Section 4.1.3.4.
 - e) provide for UDP Multihoming as described in RFC 1122, Section 4.1.3.5.
 - f) support the MIB-II UDP group object definitions as defined in RFC 1213, Sections 3.10 and 6.9.
- 7.2.5 A typical implementation shall support the following capabilities:
 - a) data transfer as specified in RFC 791, Sections 1.1 and 2.3.
 - b) addressing as specified in RFC 791, Sections 1.4, 2.3, 3.1, and 3.2 and RFC 1122, Section 3.2.1.3.

- c) fragmentation/reassembly as specified in RFC 791, Section 1.4, 2.3, 3.1, 3.2 and RFC 1122, Section 3.3.2, 3.3.3, and 3.2.1.4.
- d) header checksum as specified in RFC 791, Section 1.4, 3.1 (page 14), and RFC 1122, Section 3.2.1.2.
- e) Type of Service (TOS) field as specified in RFC 791, Section 1.4, 3.1, 3.2 and RFC 1122, Section 3.2.1.6.
- f) time-to-live as described in RFC 1122, Section 3.2.1.7
- g) additional options as described in RFC 1122, Section 3.2.1.8, as further modified by this standard.
- h) MIB-II IP group as specified in RFC 1213, Section 3.7 and 6.6.

7.2.6 A typical implementation shall support the following fields as described in RFC 791, Section 3.1 and 3.2:

- a) version number, also as specified in RFC 1122, Section 3.2.1.1;
- b) Internet Header Length (IHL);
- c) type of service (TOS), also as specified in RFC 1122, Section 3.2.1.6;
- d) total length of datagram;
- e) segment identification, also as specified in RFC 1122, Section 3.2.1.5;
- f) control flags;
- g) fragment offset, also as specified in RFC 791, Section 3.2 and RFC 1122, Sections 3.2.1.4 and 3.2.1.5;
- h) time-to-live (TTL), also as specified in RFC 1122, Section 3.2.1.7;
- i) protocol;
- j) header checksum, also as specified in RFC 1122, Section 3.2.1.2;
- k) source address, also as specified in RFC 1122, Section 3.2.1.3;
- l) destination address, also as specified in RFC 1122, Section 3.2.1.3;
- m) IP options, also as specified in RFC 1122, Section 3.2.1.8;
- n) padding;
- o) data.

7.2.7 The procedure calls described in RFC 791, Section 3.3 and RFC 1122, Section 3.1, 3.3.4, and 3.4 shall constitute the Internet/Transport Interface.

7.2.8 A typical implementation shall structure its addresses as a class A, B, C, or D addresses and follow the procedures described in RFC 1122, Section 3.2.1.3 or, optionally, use the Classless Inter-Domain Routing address structure and the procedures described in RFC 1517 through RFC 1520. For use within a transportation system, an IP Address may be allocated from the Private Address Space as described in RFC 1918, Section 3.

7.2.9 A typical implementation providing gateway functionality shall support the functions described in RFC 1122, Section 3.3.1.

7.2.10 A typical implementation shall provide for the requirements as described in RFC 791, Sections 3.1, 3.2, and RFC 1122, Sections 3.2.1.4, 3.2.1.5, 3.2.3, 3.3.1-3.3.7.

7.2.11 For use within the transportation environment, IP shall support a datagram size of at least 576 bytes per RFC 1122, Section 3.3.3.

7.2.12 A typical implementation shall provide:

- a) the TOS field as specified in RFC 791, Sections 1.4, 3.1, 3.2, and RFC 1122, Section 3.2.1.6.
- b) the TTL field as specified in RFC 791, Sections 3.1 , 3.2, and RFC 1122, Section 3.2.1.7. This field shall be used as a 'hop counter' as described in RFC 1122.
- c) the MIB-II IP group object definitions as defined in RFC 1213, Sections 3.7 and 6.6.

7.2.13 Systems using ASN.1 should use Basic Encoding Rules (BER) for transmitting data in accordance with ISO 8825 and CCITT's X.209.

8 Subnetwork and plant level standards

8.1 General

- 8.1.1 The key areas for UTMC standardisation are in the information, application and transport levels. Lower levels will generally be free to adopt appropriate open-source communications technology.
- 8.1.2 A UTMC system shall utilise appropriate wireline or wireless bearers to meet performance requirements.
- 8.1.3 The following service and bearer types are recommended, provided they have been properly assessed to meet system-specific performance requirements:
- a) Established retail offerings from any UK public telecommunications operator.
 - b) Managed network services which are capable of delivering IP networking, provided either by a UK retail operator or under a contracted service level agreement.
 - c) IEEE802 standards including Ethernet (including high-speed variants) and wireless networking protocols, for local area networking.
 - d) Digital Short Range Communications (DSRC).
- 8.1.4 Where none of these options is feasible or cost effective, other services and bearers may be considered.
- 8.1.5 The physical interfaces of a UTMC component shall conform to suitable open standards. No specific standards are mandated.

8.2 Use of wireless technology

- 8.2.1 Wireless links shall, wherever reasonably practical, support full duplex communications. A wireless bearer which is not full duplex shall be permitted provided that a pseudo full duplex service is maintained which is transparent to IP traffic.
- 8.2.2 Equipment providing a half-duplex air interface but presenting a full-duplex data interface to the user shall provide a 'transmit' buffer of suitable capacity and latency. The buffer shall provide an alert if it is close to full.
- 8.2.3 All wireless communications equipment deployed within a UTMC system shall either meet the type approval requirements of Ofcom, or be in accordance with the appropriate EuroNorm (EN) specifications for the class of equipment.
- 8.2.4 Good design practice should be used to ensure that antenna mounting, power emissions and other features provide an end-to-end bit error rate of better than $1:10^4$ under all operating conditions likely to be experienced at each installation site.

9 Safety and security

9.1 Operational safety

- 9.1.1 All UTMC projects should prepare a safety plan. The extent of safety analysis should be decided by each project individually. The safety analysis should be reviewed periodically throughout the service life of the system and on each and every system/communication network change.
- 9.1.2 Where the safety plan indicates that the specific project constitutes a “safety critical system” in the sense that a system failure will lead to a direct and immediate safety problem, the detailed technical approach of the international standard IEC 61508 shall be adopted.
- 9.1.3 In the event of system functional failure, the UTMC system shall degrade safely, following a defined hierarchy of failure modes. A hierarchy of failure modes shall be provided with the system design documentation.
- 9.1.4 UTMC system failures shall be logged, in a non volatile format, and displayed to system operators. UTMC systems shall conform, as a minimum, to both the operational and failure log requirements of MCE 0360C. Details of the method used to display failure logs, and initiate system alarms shall be defined in the system design documentation.
- 9.1.5 System alarms shall be initiated in the event of system functional failure. System failure alarms shall be graded in accord with the severity of the failure. Details of the grading of alarms shall be defined in the system design documentation.

9.2 Security and availability

- 9.2.1 All UTMC projects should prepare a security policy, based on BS7799. The detail of the security policy should be decided by each project individually.
- 9.2.2 UTMC system design should take care to ensure the security and availability of the information they contain. A UTMC system security policy shall be prepared which describes the approach to be taken, if any, to security in the following areas as a minimum:
 - a) Access control processes for user access to applications.
 - b) Access control processes for application access to each other and to common data.
 - c) Operation using trusted staff.
 - d) System design to ensure that capacity, timeliness etc are not exceeded.
 - e) Use where appropriate of technical solutions such as encryption, mirrored servers, and non-volatile records.
- 9.2.3 The security policy should be reviewed periodically throughout the service life of the system and on each and every system/communication network change.
- 9.2.4 The system security shall be validated against the system security policy.
- 9.2.5 All interfaces to the Internet shall be protected by appropriate security measures, including the implementation of a suitable managed firewall.
- 9.2.6 UTMC systems should include a suitable range of security audit tools.
- 9.2.7 Additional information is provided in Annex G (Informative).

A References (Normative)

A.1 The following is a list of documents to which normative reference is made in the main text of this document in such a way as to make them indispensable for the application of the standard.

- a) MCH 1813 : Highways Agency
- b) MCE 360C : Highways Agency
- c) ISO 8571 : International Standards Organisation
- d) ISO 8572 : International Standards Organisation
- e) ISO/IEC 8824:1990: Specification of ASN.1
- f) ISO/IEC 8824-1/2/3/4:1998 Various enhancements to ASN.1 specification
- g) ISO/IEC 8825:1990 Specification of Basic Encoding Rules for ASN.1
- h) ISO/IEC 8825-1:1998 Specification of Basic Encoding Rules (BER) Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER). Informative references
- i) I.410 : International Telecommunications Union.
- j) V.24/V.28 : International Telecommunications Union
- k) V.35 : International Telecommunications Union
- l) X.21 : International Telecommunications Union
- m) X.21 bis : International Telecommunications Union
- n) RFC 768: Internet Engineering Task Force
- o) RFC 791 : Internet Engineering Task Force
- p) RFC 793: Internet Engineering Task Force
- q) RFC 821 : Internet Engineering Task Force
- r) RFC 854 : Internet Engineering Task Force
- s) RFC 959 : Internet Engineering Task Force
- t) RFC 1155: Internet Engineering Task Force
- u) RFC 1157 : Internet Engineering Task Force
- v) RFC 1212: Internet Engineering Task Force
- w) RFC 1945: Internet Engineering Task Force
- x) CORBA: OMG
- y) SOAP: W3C
- z) XML: W3C (see also OASIS)
- aa) UDDI: OASIS

A.2 Further information may be found on the following websites:

- a) UTMC: www.utmc.gov.uk
- b) DfT: www.dft.gov.uk
- c) Highways Agency: www.highways.gov.uk
- d) ITU: www.itu.int
- e) ISO: www.iso.ch
- f) CEN: www.cenorm.be
- g) IETF: www.ietf.org
- h) OMG: www.omg.org
- i) OASIS: www.oasis-open.org
- j) W3C: www.w3.org
- k) e-GIF: www.e-Envoy.gov.uk
- l) TIH: www.tih.org.uk
- m) RTIG: www.rtig.org.uk
- n) TPEG: www.ebu.ch/en/technical/projects/b_tpeg.php

B Management authority for this document (Informative)

B.1 Formal authority

B.1.1 The UK Department for Transport is the management authority for the UTMC Technical Specification.

B.1.2 The contact address for formal matters is:

Traffic Management Division
Department for Transport
Great Minster House
76 Marsham Street
London
SW1P 4DR
UK

B.2 Day to day management

B.2.1 DfT has delegated the task of managing the Technical Specification to the UTMC Development Group (UDG), a cooperative grouping of local authorities and system suppliers. The UDG is currently the “relevant body” for matters relating to UTMC compliance (see section 2).

B.2.2 The UDG Specifications and Standards Group manages the documentation and procedures on a day to day basis. The UDG secretariat is the point of contact from which up to date copies of the Technical Specification can be obtained.

B.2.3 The contact address for day to day matters is currently:

UDG Technical Secretariat
c/o Centaur Consulting Limited
Surrey Technology Centre
Surrey Research Park
Guildford
Surrey GU2 7YG
UK

Tel: +44 (0) 1483 688270
Fax: +44 (0) 1483 688271
E-mail: utmc@centaurconsulting.co.uk

B.2.4 Any changes to this will be published on the UTMC website.

C Examples of UTMC architectures (Informative)

C.1 Architecture choices: FEPs and adapters

- C.1.1 The UTMC architecture envisages that several different applications at, or linked to, a control centre can access the same outstations connected to field devices. To achieve this, a 'gateway' Front End Processor (FEP) is used, with multiple computer connections on one port, probably via a Local Area Network (LAN), and multiple lines radiating from another port or ports to the outstations (see figure C-1). In theory the lines radiating to the outstations could utilise different media types though in practice it is more likely to be economical to have a different FEP for each transmission medium – analogue leased lines, dial-up links, packet switched media, etc.
- C.1.2 Within a Node B, it may also be appropriate or efficient to have one or more 'gateways'. These would take the form of adapters which enable one application to talk to other applications in ways convenient to the system operator. A specific kind of adapter is the adapter used for 'wrapping' a legacy application to present a UTMC compliant interface.

The FEP: router and priority manager

- C.1.3 A three-tier communications architecture allows multiple applications to share a common IP bearer network while enabling the specific requirements of individual applications to be met. Where one of the applications is SCOOT UTC, this necessitates:
- a fast short message delivery service;
 - a less time critical, but relatively high capacity, 'conversational channel'.
- C.1.4 The fast short message delivery service is needed for second by second control of traffic signal controllers. In an ideal design the data transmission will be capable of sending a minimal message if there is no significant data to send, eg same data as last second. This maximises the remaining bandwidth for the conversational channel.
- C.1.5 The conversational channel uses 'spare capacity' for background communications with, for instance, VMS or environmental detectors. This channel must be reliable and able to cope with breaks when the fast channel seizes the link for its urgent needs.
- C.1.6 It is a matter for network design to ensure that the communications loading allowed for each service does not exceed the available capacity, given the communications requirements of each data exchange requirement.

C.2 York UTMC demonstrator

- C.2.1 Figure C-1 illustrates a model deployment, based on the UTMC29 York demonstrator, of a UTMC compliant system, based on:
- applications that obtain all the data they require from the CDB and control UTMC compliant field equipment via the CDB/adapters; and
 - SNMP/CORBA adapters (a special type of application) to manage the interface between the CDB and equipment in the field, with one adapter for each equipment type (VMS, air quality monitor).

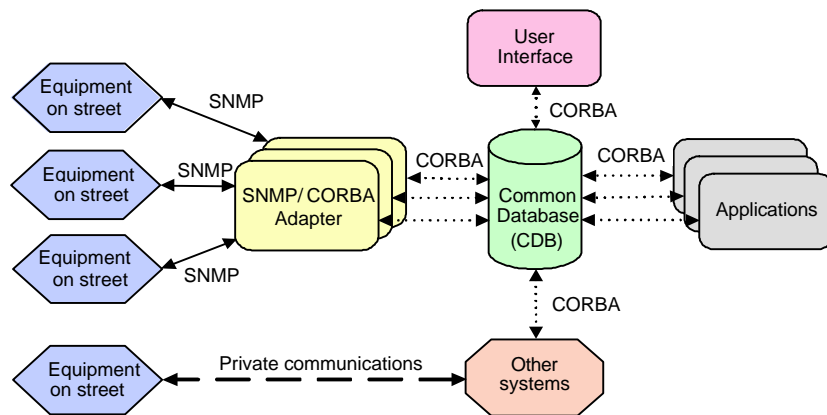


Figure C-1 UTMC model deployment

C.2.2 Also shown in Figure C-1 is a CORBA interface to other systems that use non-compliant interfaces. This CORBA interface:

- a) supports exchange of data with legacy systems;
- b) provides a possible migration path from non-compliant systems with evolving UTMC systems, as individual elements may be 'cut over' one at a time.

C.3 Preston UTMC demonstrator

C.3.1 An alternative arrangement is shown in Figure C-2, based on the UTMC29 Preston demonstrator. In this case applications interfacing with street equipment (eg UTC) have their own data store and are fitted with a CORBA adapter to enable them to share common data with other applications.

C.3.2 Equipment on street is a mixture of new units from different suppliers using SNMP and a common MIB, and legacy equipment still using proprietary communications. The User Interface is an integral part of the common database and takes the form of a Common Database Viewer. This is available locally and remotely.

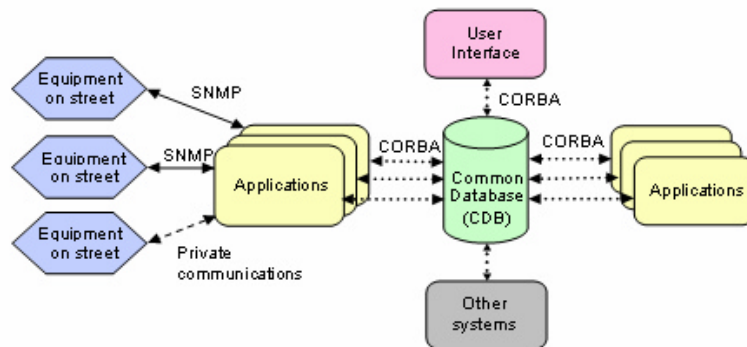


Figure C-2: UTMC model deployment

C.4 The impact of being 'UTMC compliant'

- C.4.1 UTMC compliance, as defined here, is a pragmatic approach rather than a 'purist' approach. It does not provide a guarantee of interoperability between connecting systems. It does, however, make it easier to achieve interoperability or interchangeability.
- C.4.2 A 'purist' approach to compliance would require a complete detailed technical specification which would be extremely time consuming to prepare and maintain, and would almost certainly stifle innovation. It would probably also result in significantly higher equipment costs than the present, lightweight approach. This approach has therefore not been adopted.
- C.4.3 The impact is that LAs and developers/suppliers alike will have work to do in order to converge on truly interoperable solutions. LAs or their system integrators will also need to adapt their skills base, to be able to configure different devices onto a UTMC 'framework'.

D Data objects & applications layer communications (Informative)

D.1 General

- D.1.1 A typical UTMC implementation will use three core approaches to data exchange: the SNMP/MIB approach, the CORBA approach and the XML approach. Additional data exchange mechanisms may emerge in the future and will be considered for future revisions to TS003.
- D.1.2 SNMP is likely to be used from centre to devices, and CORBA and XML for centre-to-centre communication or for application-to-application communication within the instation. In future XML may also be considered for some centre-to-device communications.
- D.1.3 CORBA provides a much richer environment for data exchange, while XML provides a simpler and more basic approach (especially for making information available through the internet). The balance between these should be determined by the implementer's local strategy and requirements.

What is normative?

- D.1.4 The UTMC Technical Specification specifies quite tightly the protocols that may be used at the Information, Application and Transport Levels.
- D.1.5 The Information Level uses the UTMC Data Objects Registry (TS004), while the Applications Level uses a variety of mainstream data exchange standards. Complexities arise in the way that different Applications Level profiles can be efficiently used to exchange these Data Objects.

D.2 Target profiles

Centre to field

- D.2.1 For communications between Instation and field devices, the preferred model is for SNMP at the Application Layer and the defined Data Objects (normally MIBs) at the Information Layer.
- D.2.2 The specification for the Transport Layer requires UDP/IP for time critical applications but TCP/IP may be used for non time-critical applications.

Centre to centre

- D.2.3 Centre-to-centre communications are expected to use the CORBA or XML approach, and should exploit the technical guidance provided by the Travel Information Highway where appropriate.
- D.2.4 The General Inter-ORB Protocol (GIOP) specifies a set of message formats and Common Data Representation (CDR). The CDR (and BER) takes care of inter-platform issues such as byte ordering and memory alignment, etc.
- D.2.5 The Internet Inter-ORB Protocol (IIOP) specifies how GIOP messages are exchanged over a TCP/IP network.

At the instation

- D.2.6 The Instation will normally be divided into two subnetworks, one that 'talks to' field devices (in which the stack is based on SNMP exchanging MIB objects) and one that 'talks to' the outside world (in which the stack is based on CORBA/XML exchanging a wider range of data objects).
- D.2.7 The SNMP/MIB approach is designed for relatively 'formal' data exchange over relatively narrowband comms links, with managed devices; the instation network has plenty of bandwidth and a much more fluid set of information exchange requirements. It is therefore expected that the SNMP/MIB model would not be used to any great extent in the instation network.
- D.2.8 A consequence is that a router in a UTMC system may be required to be more intelligent than the typical product. It will have to know what the type of message is. This could have the consequence of it being effectively an additional node in the communications architecture.

D.3 The SNMP/MIB approach

Role of the MIB

- D.3.1 One of the key reasons for the initial choice of SNMP as the management protocol, beyond its proven capabilities, is the existence of the associated data definition known as the MIB, or Management Information Base.
- D.3.2 SNMP uses an industry-standard get/set model to read and write data in a database. The database groups related objects into a 'management information base' which is known as a MIB. The entity that manages the database within a device is known as the agent. The management application sends messages to the agent to fetch or modify values of objects stored in the MIB. Changes in values of objects in the MIB will result in the device responding in the defined way determined by the device's programming.
- D.3.3 MIB objects are related by device type (for example traffic signal controller MIB or variable message sign MIB). The use of standard MIBs ensures practical interoperability, but new functions require additional variables and therefore new versions of MIBs can be created. By using the standard protocol rules, proprietary or experimental MIBs are not excluded from use.

SNMP message structure

- D.3.4 Each element of an SNMP message is defined using the Tag-Length-Value representation method defined in ISO 8825.
- D.3.5 All objects can be expressed as Tag (or Type) of SEQUENCE, INTEGER, OCTET STRING, or OBJECT IDENTIFIER. The Tag indicates the meaning of the Value component. It indicates that it may be number, string (or text), or an identifier. It can also indicate that what follows is a series of data elements, each expressed as a Tag-Length-Value.
- D.3.6 An SNMP message consists of two predefined fields and a Protocol Data Unit (PDU), all defined as a Sequence. Within the PDU is a Request ID, Error Status and Error Index followed by the actual content of the message. The message can consist of one or several objects.
- D.3.7 SNMP adds a considerable overhead to the data transmitted. As a rule of thumb, the SNMP message structure adds 23 bytes per object plus an additional 26 bytes per message. The UDP

header adds 8 bytes to the message, and the IP header adds 20 bytes to the message. There will be a lower level protocol, which may add some additional limited information. For example a PMPP HDLC frame would add an additional 6 bytes, whereas an Ethernet frame would add 26 bytes.

Content of SNMP messages

- D.3.8 The Data Objects Registry TS004 maintains and publishes a list of all Data Objects, together with their status. These will be used to form the basis of any UTMC SNNMP messages.

D.4 UK UTC using SNMP

- D.4.1 The existing UTC communications in the UK are based on the MCE0360 Area Traffic Control Specification. The key features of this specification are:

- a) A control message is sent from instation to outstation every second;
- b) A reply message is sent from outstation to instation every second;
- c) If a traffic controller does not receive a message for more than 3 seconds it reverts to local control;
- d) Control messages are three bytes long, consisting of Address Byte, Control Byte 1 and Control Byte 2;
- e) Control Bytes 1 and 2 have a parity bit;
- f) Reply messages are seven bytes long, consisting of Address Byte, Reply Byte1, Reply Byte 2 and four SCOOT detector bytes if it is a SCOOT outstation.
- g) Reply bytes have no parity.

- D.4.2 The specification also defines the messages in terms of what the control and replay message can consist of. The main control messages are:

- a) Common UTC Demand Bits: Active common demand setting shall cause the simulation of detector inputs to the controller from detectors for vehicle or pedestrian activated stages.'
- b) Demand UTC Stage Bit: Active demand bit for a stage shall simulate the operation of a detector by simulating the demands and extensions on selected phase(s) associated with the stage.
- c) Hold Vehicle (PV) – Stand-alone pedestrian facility: Active condition shall prevent the appearance of the pedestrian stage by the imposition of a 'hold' condition on the vehicle stage.
- d) Pedestrian Demand (PX) – Stand-alone pedestrian facility: Active condition shall simulate a pedestrian push button operation or kerb side detector for puffin facility.
- e) Solar Switch Override (SO): Active condition shall switch the traffic signals to the non-dimmed condition overriding the solar switch.

D Data objects & applications layer communications (Informative)

- f) CLF Group Timer Synchronisation Signal (SG): This object is used to set the CLF group timer to a value of 0 to 255. A value of 0 shall set the relevant plan cycle timing from the start of the first group
- g) Lamps On/Off (LO): Active condition for a minimum of ten seconds shall cause the signals to switch on in accordance with the Start Up Sequence. A non-active condition for a minimum of ten seconds shall cause the signals to switch off.
- h) Local Linking Inhibit (LL): Active condition shall inhibit local linking between parallel stage streams or other local links.
- i) Fall Back Mode Selection (FM): Active condition whilst the controller is NOT in UTC mode, shall inhibit CLF and cause the controller to fall back to the next lowest priority control method.
- j) Take Over (TO): The facility shall change control to be accepted from a remote source.
- k) Hurry Call Inhibit (HI): Active condition shall inhibit hurry call requests.
- l) Transmission Confirm (TC): A condition of indicates that the OTU has received a valid control message. A non-active condition indicates that the OTU is inactive and that the controller shall ignore messages from the OTU.
- m) Close Car Park (CP): Active condition shall close the car park.

D.4.3 Within this specification, the two UTC manufacturers in the UK have produced systems that use different and incompatible protocols for communications. This is an effective illustration of how important it is to clearly define standards with sufficient detail to ensure compliant systems are compatible.

D.4.4 All the information that can be communicated between the instation and the outstation is contained within the control and reply bytes and the detector bytes. This is best explained using an example in which a 7 stage junction with stages 5 and 7 demand dependent, as the example field device the communication is required to:

- a) Synchronise the time and date in all field devices (TS).
- b) Control the operation of 7 Stage Intersection (Fn).
- c) Stage 5 and 7 demand dependent on detectors (Dn)
- d) Common demand to over-ride any stage dependency (DX)
- e) May be operated in part time mode (LO)
- f) Solar Override mode (SO)
- g) Give priority to Emergency vehicles (HI)

D.4.5 All this information can be contained within one message to the controller, within the two bytes of the control message. This same message format will be sent to the controller every second.

The content of the message will depend on whether a particular bit is set or not. It can be seen that this message format is extremely compact and efficient.

D.4.6 SNMP utilises the concept of objects for communication, using the Get/Set model to read or set the state of an object. Using the traffic control draft MIB developed for the UK by UTMC09, the following objects would be required in this example (the associated OIDs are drawn from the draft UTC MIB):

- a) For control:
 - i) solarswitchOverride – OID of module is 1.3.6.1.4.1.2380.3.1.1.16.10
 - ii) lampSwitch – OID of module is 1.3.6.1.4.1.2380.3.1.1.16.12
 - iii) hurryCallInhibit – OID of module is 1.3.6.1.4.1.2380.3.1.1.16.16
 - iv) forcebitEntry – OID of module is 1.3.6.1.4.1.2380.3.1.1.16.5

- b) For reply:
 - i) StageConfirmbitEntry – OID of module is 1.3.6.1.4.1.2380.3.1.1.16.5
 - ii) solarswitchOverrideConfirm – OID of module is 1.3.6.1.4.1.2380.3.1.1.16.10
 - iii) lampSwitchConfirm – OID of module is 1.3.6.1.4.1.2380.3.1.1.16.12
 - iv) hurryCallInhibitConfirm – OID of module is 1.3.6.1.4.1.2380.3.1.1.16.16

D.5 The Common Database and the Logical Data Model

D.5.1 UTMC adopts a 'logical' or 'conceptual' data model for the Common Database. It is recognised that different database systems may implement the required functionality in different ways, but none of the requirements should be unduly onerous for a modern database management system which supports the SQL92 standard. Use of vendor proprietary 'extensions' is acceptable between the application server and the database server but it must be assumed that UTMC applications will not be required to use them.

D.5.2 The logical data model specifies the required structure for a set of tables which implement Data Objects. These will emerge over time. The data model provided here is therefore a framework rather than a complete specification.

D.5.3 No data gets into or out of the database except as in the action of a recognised UTMC function. The agents which carry out these functions are known in the Common Database model as Implementations, and normally they would represent individual UTMC compliant application programs.

D.5.4 The logical data model includes descriptions of data quality. Suppliers of data should specify the quality with appropriate metrics, and consumers should specify the quality required. The common database will assist in matching supplier output to consumer needs.

D.5.5 Some data will not naturally fit into a traditional CDB format (eg a relational database) – specifically, CCTV input. At present it appears that the simplest solution is to 'stringify' the relevant data (in the case of CCTV, an image) and place in the database as part of the Data Object (large field). This approach may need to be reconsidered if there is more demand for 'non-standard' data types.

D.6 The CORBA approach

About CORBA

- D.6.1 The CORBA model is an internationally accepted open standard for distributed object oriented programming. It enables otherwise heterogeneous applications to co-operate in a single distributed application, potentially worldwide.
- D.6.2 Each application must have an ORB, which may be regarded as an adapter onto the CORBA bus, or as a member of the federation of co-operating applications. The interfaces between remote applications are defined in Interface Definition Language (IDL). Developers choose an ORB that supports the program language of their choice (C++, Java, COBOL...) and develop an implementation of the interface.
- D.6.3 With its ORB, an application can access remote objects as if they were local; UTMC client applications can invoke methods on objects hosted on other UTMC systems (eg a car park management system can invoke methods on data objects on a UTC host). They do not need to be set up as native clients of the database server itself because the application server is able to manage this aspect, and provides all the required application components to receive queries and deliver results.
- D.6.4 Any application server product may be used, provided it is associated with an ORB which is CORBA-compliant and that its components implement the specified interfaces. In the UTMC 10 trials Sybase Enterprise Application Server was chosen as the natural partner for the Sybase database server, but many other systems are available.

Architecture

- D.6.5 A Common Database using CORBA should be implemented using a middle tier application server between UTMC applications and the database server. This brings several advantages:
- a) It implements a 'pushed data' service so that client applications can subscribe for data they need and receive automatic delivery of data which meet their requirements. Clients no longer need to repeatedly 'poll' the database to check for new data.
 - b) It supports the (future) provision of common ITS application services, as well as data from the database, e.g. predictive services or management of video-streaming.
 - c) It preserves database independent access. Whatever database management system is chosen to implement the Common Database, access to it is provided by the Application Server using a constant interface defined in Interface Definition Language (IDL).
- D.6.6 In this architecture, UTMC applications may undertake queries. The Common Database will forward the results from such queries on request.
- D.6.7 Applications may also partake in a subscription service. The Common Database will forward new results which become available. Two forms of delivery service are available:
- a) 'Blocked pull' notification - client invokes a pull method which blocks until data is available, then returns it inside a DataNotification object.

- b) 'Callback push' notification - client provides a reference to its own implementation of a NotificationTarget object, Common Database invokes its notificationReceived method when new data becomes available, passing the DataNotification as an argument.

Developing a compliant application

- D.6.8 Application developers will need to develop interfaces for their existing systems to exchange data with the Common Database.
- D.6.9 The supply of data to the Common Database will be driven by the requirements of the applications which need to consume it. Thus development of new UTMC applications is a cooperative activity: suppliers of data need to know what items are required and consumers of data need to know what items are available. An exception to this is when a QualityTemplate completely specifies the data requirements.
- D.6.10 In program development, developers need to install a suitable CORBA ORB which supports a binding for their preferred program language (C++, Java, COBOL...) and generate 'proxy' code for the UTMC interfaces. Then they can use these proxy objects to become part of a distributed application with the UTMC Application Server.
- D.6.11 In order to gain access to the Common Database applications must be authorised by the Manager.createSession method. Obtaining the original reference to the Manager object is a bootstrap issue, and the means is not currently specified. Use of the standard CORBA Naming Service is encouraged.

D.7 The XML approach

About XML

- D.7.1 XML stands for eXtensible Markup Language. It provides a language for describing data in a simple ASCII Text document. XML was designed to store, carry, and exchange data. XML was not designed to display data.
- D.7.2 The Government's "e-Government Interoperability Framework" (e-GIF), which aims to achieve "interoperability and system coherence across the public sector", adopts XML as the core standard for data integration, a policy that is mandatory for all local authorities. Also, XML has also been widely adopted amongst the Public Transport systems community, for example:
 - a) The TransXChange protocol for the exchange of bus timetables;
 - b) The ATOC Real Time Train Information (RTTI) portal;
 - c) The Real Time Information Group (RTIG) server-to-server protocol for Real Time Passenger Information (RTPI);
 - d) Journey Web – XML standard for interconnecting Regional Journey Planners.
- D.7.3 An XML document is both machine readable and human readable; an XML document can be created by a human operator using a simple text editor, though a wide range of software tools are now available to generate XML documents automatically from existing data sets.

- D.7.4 The use of tags and the structure of XML documents is defined in an XML Schema. XML with a Schema is designed to be self-descriptive. XML Schemas are extensible: data items can be added to the structure without affecting any existing clients.
- D.7.5 A Schema is a definition of the syntax of an XML-based 'language'. It provides a formal definition of the syntax of a set of XML documents in a precise but human-readable form. It can be used to:
- a) Formalise and agree data formats for exchange;
 - b) Validate documents;
 - c) Create classes to hold data from XML documents within an application.
- D.7.6 TIH Principles currently recommend the use of a simple HTTP GET command for the exchange of XML-structured data.

About Web Services

- D.7.7 Web Services is a suite of industry standards, using XML, which allow applications to share functionality and data with other applications connected by a network. As well as XML and HTTP this suite includes:
- a) WSDL: Web Services Description Language, to describe services that are available. It provides a similar function to IDL in CORBA implementations.
 - b) UDDI: Universal Description, Discovery and Integration, to catalogue Web Service providers.
 - c) SOAP: Simple Object Access Protocol, to make requests for a service and receive the response.
- D.7.8 Instead of getting requests from browsers and returning web pages in response, a Web Service receives a request formatted in XML from an application, performs a task, and returns an XML-formatted response. For example, a personnel system could use a Web Service on a Finance System to calculate an employee's take-home pay, given different parameters. In this example the personnel system is not just 'looking up' the salary in a remote database, it is getting the remote system to carry out the calculation using parameters passed in real time. The personnel department can do 'what if' calculations using a service provided by the finance department, which can use specialist resources within its own domain.
- D.7.9 There is currently no standard WSDL for the UTMC context, and the development of a UDDI-based approach to UTMC information is unlikely to be of great importance until there is much more activity in the exchange of transport information generally.

E Communications: networks and bearers (Informative)

E.1 General

- E.1.1 The data transmission philosophy adopted in UTMC is intended to be adaptable to technological advances that will be made in data transmission techniques and media over the next 10-15 years. Since this approach involves many unknowns the engineering approach must be system-oriented rather than device-oriented. It must also recognize that change on a large scale can only take place slowly and that current systems will have to co-exist with new systems for considerable periods of time.
- E.1.2 The standard framework followed by UTMC is aligned closely with the US NTCIP framework, while keeping in step with other initiatives. Through a combination of existing communications standards and a few new standards developed specifically for ITS, it provides a family of communications protocols that serve most of the common needs in ITS.
- E.1.3 The application level is the primary focus. Although some existing standards are useful here, ITS has special requirements that have necessitated the extension of existing standards, or development of entirely new protocols for specific applications within ITS. Some of the special communications requirements of ITS are:
- a) Continuous, automated, secure, real-time exchange of large volumes of small data packets in a many-to-many multiple-authority network.
 - b) Continuous high volumes of real-time data sent to and from embedded processors in roadside or on-vehicle equipment sharing the same, often low-speed, data channel and requiring low latency.
- E.1.4 A study is currently underway to provide more detailed guidance on the use of different communications technologies within a UTMC system. The output from this, when available, will be published on the UTMC website.

What is normative?

- E.1.5 The UTMC Technical Specification specifies quite tightly the protocols that may be used at the Information, Application and Transport Levels. The current position is that it is not necessary to specify tightly the Subnetwork and Plant levels in order to achieve interoperability and interchangeability.
- E.1.6 The Transport Level uses IP. As IP is so pervasive, there are standard ways of using the great majority of bearer technologies to carry IP packets, and the UTMC initiative is following the market in this respect. In the few areas where this has not yet been achieved in a standardised way (eg Band III PMR systems), there will be a need for users to work with industry to achieve a seamless network.
- E.1.7 There are various off-the-shelf products available (bridges, gateways etc) that enable communications to be linked across different physical media. While this approach is viable, it is necessary to ensure that inclusion of such off-the-shelf devices does not introduce time delays through the network that might compromise system performance.
- E.1.8 Within this framework, each individual application interface within a UTMC system will use a 'profile' of different acceptable protocols. The remainder of this annex suggests how this can be done.

E.2 Basis profile: wide area IP

Current systems as pre-UTMC stacks

- E.2.1 System designers and implementers are likely to need to move to UTMC communications in an evolutionary way. The first step is therefore to understand how legacy systems fit into the UTMC framework.
- E.2.2 In a typical existing UTC system, Ethernet is used as the connection bus between the instation and one or more FEPs. The FEP lies physically between the Host and the OTUs, and acts as a transparent routing device; that is, it does not modify the data passed between the Host and the OTU. Typically the FEP and the OTU drive the modem at 1200bps in half- or full-duplex mode. Communication over the Ethernet is via the standard IEEE 802.3 Protocol.
- E.2.3 Thus the legacy UTC data transmission system comprises two separate stacks, the UTC host to FEP stack and the FEP to Outstation stack. In a similar way the UTMC data transmission needs two separate stacks and the UTC host to FEP stack must be compatible with the legacy equivalent.
- E.2.4 In the terms of TS003, implementations of the legacy centre-to-field protocol stack MCE361 typically have the following characteristics:
- a) Information level: Proprietary.
 - b) Application level: Null.
 - c) Transport level: Null.
 - d) Sub-network level: MCE361.
 - e) Plant level: Analogue leased line.
- E.2.5 The instation stack is similar but with Ethernet at the plant level. Although the lower levels are based on open published standards, this stack is not fully open, and therefore not UTMC-compliant. However it enables Authorities to determine how and where change may be introduced a step at a time.
- E.2.6 Non-UTC applications have similar, though less demanding, issues.

UTMC stacks

- E.2.7 Where there is no requirement for second by second data, the Gateways can be simple standard IP routers with data channels appropriate to the required media. Under these conditions the standard UTMC Application Protocol will be NTCIP AP-STMF throughout the system.
- E.2.8 Where second by second data is required there is a need to devise special protocols and gateways. For this purpose the Front End Processor (FEP) provides a protocol translation function. Under these conditions the standard UTMC Application Protocol will be NTCIP AP-STMF from the FEP to the outstation.
- E.2.9 The approach adopted by London's TCAM protocol is that UDP packets must always have priority in the internal queuing structure. All UDP packets are scheduled or shuffled to the top of the queue in either direction.

E.2.10 It is also important that the choice of a maximum packet size, the MTU, for the secondary channel must ensure a balance between achieving maximum throughput without compromising the priority channel message timing constraints. The size will need to be derived empirically and fine-tuned by the network administrator after run-time analysis of communication traffic. This will be simplified if devices are SNMP compliant.

E.2.11 In either case SNMP is used as the device management protocol, ie to enable a remote user to set certain characteristics of a field device or to query data collected at the device. An example usage might be to 'upload' data monitored and stored by a device such as a pollution monitor.

E.3 Central office profile: SUPS

E.3.1 To deal with the particular needs of UK legacy UTC systems a special protocol, the Simple UTC Protocol System (SUPS), has been devised. SUPS defines an interface between a UTC computer and a data transmission FEP, enabling the old proprietary transmission systems to co-exist with the new UTMC versions. All the UK industry UTC system suppliers have produced software to implement this protocol.

E.3.2 The protocols specified by SUPS at each of the various communications stack levels are as follows:

- a) Information Level - The SUPS Information Level profile is defined by the UTMC document "SUPS Communications Profile", Version 1.0. This document specifies not only the Object definitions, also information concerning timing and other constraints.
- b) Application level - The SUPS Application Level Profile is defined by the NTCIP document 2301, "AP-Simple Transport Management Framework" (AP-STMF). This document is available from the NTCIP bookshop (see www.ntcip.org). It is not anticipated that the optional features of STMP will be implemented, although this option is retained by SUPS.
- c) Transport Level - The SUPS Transport Profile is defined by the NTCIP document 2202, "NTCIP TP-Internet (TCP/IP and UDP/IP)" (TP-Internet). All mandatory features are required, with the exception of mandatory features exclusively associated with TCP/IP.
- d) Sub-Network Level – The SUPS Sub-Network Profile is defined by the NTCIP document 2104 "NTCIP SP-Ethernet" (SP-Ethernet). All mandatory features associated with this subset are required. Other LAN interfaces are not supported.
- e) Plant Level - The SUPS Plant Level Profile is Ethernet, in any of its many guises (10base2, 10baseT, etc.). This choice is based on the extensive acceptance of the medium within industry and the consequent widespread support.

E.3.3 SUPS is defined fully in the relevant specification document, available from the contact points in annex B.

E.3.4 SUPS transfers UTC messages in block format between the UTC computer and the FEP. This minimises the loading on the Instation computer network. The FEP must convert the block format either to individual messages for forwarding to the appropriate field devices or to a small subset message format for forwarding to a parallel or serial multiplexer. Similarly it must package individual reply messages into block messages for transmission back to Applications.

E.4 Application of wireless technologies in UTMC networks

E.4.1 UTMC applications protocols likely to be used over wireless links include SNMP and FTP. Running these on UDP or TCP over wireless bearers, for applications such as VMS, is established and should cause no difficulty.

E.4.2 What is not yet clear is whether these applications can be universally extended to Node E – moving vehicles. The feasibility of using protocols such as SNMP to the vehicle is dependent upon the wireless bearer type terminating in Node E. For example, GPRS, 3G, Wi-Fi and other services are explicitly designed to support TCP/IP. However, DSRC is not and it is unlikely that anything other than simple (non-standardised) messaging using UDP/IP transport would be possible using this type of bearer.

Scenario 1 - probe vehicles

E.4.3 Probe vehicles may be used to obtain accurate and timely information about road networks that are managed by UTMC systems. In order to recover timely information from the probe vehicles, the use of wireless link into the UTMC systems is a necessity.

E.4.4 The key issue in determining lifetime cost is how frequently data is to be uploaded from the probe vehicle. Consideration should also be given to how existing infrastructure could be leveraged to reduce cost, for example, by integrating probe vehicle communications into an existing bus AVL system.

Scenario 2 - urban road user charging

E.4.5 The functional requirements for urban road user charging include vehicle detection at specific locations and returning transaction information to a central point. However, these functional requirements are heavily dependent upon detection and enforcement methods adopted for particular systems. The choice of a pre-pay or post-pay tolling solution also affects the infrastructure needed to support the application.

E.4.6 Note that Communications from ground-based tolling outstations to management centres have not been included in the scope of this scenario. In this case, it would be expected that the volume of transactions would be such that they would predicate the use of wire-line communications.

Scenario 3 - selective vehicle detection and fleet manager applications

E.4.7 In this scenario Selective Vehicle Detection (SVD) is combined with new fleet management tools. As well as vehicle presence and identification this could include vehicle status information as well.

E.4.8 Short range protocols for bus SVD purposes have been considered by RTIG and advice should be sought from them. DSRC has not been widely adopted, and is increasingly seen as difficult to justify economically.

Scenario 4 – communications cost reduction

- E.4.9 The decision to deploy wireless instead of wire-line communication technologies will generally be driven exclusively by the cost of meeting specific performance targets. The key issue is the cost over life and as yet no information is available on tariffs for these services.

E.5 Deployment issues with wireless communications

Vehicle based equipment

- E.5.1 A number of standards are emerging for vehicle based telematics equipment, which may need to be integrated with UTMC systems.
- E.5.2 These are all based on open mainstream communications protocols, and integration within a UTMC system should not be problematic. However, there is little experience of this as yet and it is unclear what requirements might emerge.

Grade of service issues

- E.5.3 It is generally preferable for UTMC system procurers not to attempt to specify any particular wireless technology to provide the solution, but simply express the requirement in functional and performance terms. This does not preclude an invitation to contractors to also offer lower performance for a demonstrated cost benefit.

Other regulatory issues

- E.5.4 All equipment fitted within vehicles shall not interfere with the vehicle electrics in accordance with relevant European Union directives. Functional testing and certification is a requirement for new vehicles and is recommended for retrofitting. Reference should also be made to MPT Specification 1362 for guidelines on the installation of radio equipment.
- E.5.5 All equipment installed in a UTMC system must comply with the relevant EMC directives. The individual manufacturer or system integrator should be asked to provide evidence of compliance and to include a clear statement of the relevant standards applied.
- E.5.6 All wireless telecommunications equipment installed in a UTMC system must comply with the requirements of the Radio & Telecommunications Terminal Equipment (RTTE) Directive. The operator must ensure that the equipment used is compliant with the appropriate requirements and European (ETSI) equipment standards. The certification documents should be checked to ensure that it includes a clear statement of the standards applied.

E.6 Design: efficiency, bandwidth and cost

Communications efficiency

- E.6.1 One impact of the adoption of open standards is that there are more communications overheads, thus requiring more bandwidth for the same exchange of information. For example, to send a control message of 3 bytes and receive a subsequent reply message of 7 bytes on a 1200 baud system the following impact is seen:

- a) Using MCE361 over IP, the system can handle up to 9 such interrogations per second when operating full-duplex and 7 half-duplex.
 - b) STMP can operate in theory at 3-5 interrogations per second.
- E.6.2 SNMP, operating half-duplex, can handle only one such interrogation per second. In practice there are factors which limit this further:
- E.6.3 Whenever the client (UTC) sends a 'SetRequest' command, the agent (OTU/FEP) responds with a 'GetResponse' message by way of acknowledgement. To get the reply message collected by the FEP, the UTC client must also send a 'GetRequest' command in order for the agent FEP to respond with a 'GetResponse' message containing the data.
- E.6.4 The STMF application profile defined by the NTCIP tries to overcome this verbosity by reducing the overhead in the STMP protocol associated with a pair of messages. They achieved this by reducing the overhead by embedding in the format whether a response is sent from the agent, for example on a 'SetRequest' command.
- E.6.5 The question needs to be addressed of reducing the overhead further in case of the reply message, as there is again a pair of messages generated between UTC and FEP. The question is: should the client using a GetRequest for the reply data make a request or should a 'Trap' be generated in the course of accepting a 'SetRequest' command by the agent? The use of the 'Trap' mechanism then makes the half-truth into a whole truth for the STMP protocol. However, the 'Trap' mechanism should be used for unforeseen or special situations; and furthermore it is non-deterministic. Therefore, the usage is not recommended.

Implication for procurement and costs

- E.6.6 The implication of the foregoing is that communications bearers currently deployed by LAs will need significant enhancement. In the long term, this is not likely to increase costs. Nonetheless, there may be a substantial cost of changeover.
- E.6.7 The challenge will be how to define an architecture that yields a cost advantage as soon as possible. It will help to use the following rules of thumb:
- a) Where communications costs dominate, it may be advantageous to carry as many lines of communication as possible over a single bearer. Where device costs dominate, it may be better to separate communications (UTC, video, other) so that off-the-shelf communications devices can be used.
 - b) Where it is possible to use owned lines, then the serial approach may be used. Anything from a simple RS485 to a Fibre optic link will reduce operational costs and give a very reliable private network.
- E.6.8 Newer digital circuits provided may be utilised. xDSL over analogue lines may be useful (for video as well as other data), as this is a fast and inexpensive kilobit stream.

F Guidelines on safety in UTMC systems (Informative)

F.1 Context

- F.1.1 Urban traffic managers are called upon to deliver a wide range of policies: reducing congestion, sustaining air quality, providing priority for public transport, etc. An increasing range of Intelligent Transport Systems (ITS) can help them achieve this. To assist local authorities gain the most from ITS, the UK Department for Transport initiated the Urban Traffic Management and Control (UTMC) programme in 1997.
- F.1.2 The UTMC approach permits a much greater level of modularity and systems integration among ITS than has been the case historically. An “open systems” approach makes for a responsive and evolvable traffic management framework. However, integrated systems can exhibit ‘emergent properties’ that are not present in the individual items of equipment, and one concern was that this might raise new types of safety issue that must be addressed.
- F.1.3 The programme therefore commissioned, early on, a review of good practice in systems safety (project UTMC22). This project, conducted by MIRA and the University of Leeds, produced its final report in July 1999 (*Framework for the Development and Assessment of Safety-Related UTMC Systems*, release version 1.0). This report is available on the UTMC website, and provides a thorough review of possible approaches to safety assessment in a UTMC context.
- F.1.4 The UTMC demonstrator projects commissioned in 2000 were asked to evaluate the alternative approaches identified in the review, and to report on their relevance and practicality. By far the most thorough investigation was undertaken in the Preston demonstrator, and this appendix uses their perspective to provide interim advice on safety matters to LAs implementing, or considering implementing, UTMC systems.

F.2 Conclusions of demonstrators

- F.2.1 The Preston demonstrator considered that:
- a) the UTMC22 separation of safety planning into “system safety analysis”, “traffic safety analysis” and “HMI analysis” was appropriate and covered the various safety aspects of the project effectively. The usefulness of each of these types of analysis will vary from project to project.
 - b) preparation of the safety plan was useful to develop safety requirements and identify how they would be addressed in the project. Ideally this should be updated to reflect the actual analysis process and results.
 - c) The system safety analysis was a relatively expensive exercise whose value it is difficult at this stage to assess.
 - d) The traffic safety analysis is an essential part of any traffic management project, although UTMC is unlikely to pose any additional safety challenges over and above those relating to each individual system.
 - e) The HMI analysis proved the usefulness of early involvement of the operations staff in the design.
- F.2.2 The experience from the project is that to be most effective the analyses should be carried out by the project team, whose staff should have the necessary expertise to do so. Reliance on

external specialists does not lead to the full integration of safety within the design and development process and means that the project team may not have full confidence in the process or the results.

F.2.3 The demonstrators considered that the UTMC Programme should:

- a) Be very cautious on whether UTMC systems are 'safety-critical' and thereby merit the analysis requirements of IEC 61508 (Safety Integrity Levels, etc).
- b) Produce guidelines for the preparation of the safety plan and the undertaking of safety analyses in a stand-alone document for use by individual projects. Such guidelines should be based on the basic concepts of the safety plan, system safety analysis, traffic safety analysis and HMI analysis as outlined in UTMC22; should allow projects wide discretion to determine their own approach within the basic framework; and should clearly separate background material from the main text.

G Information security (Informative)

G.1 Introduction

- G.1.1 Security is a complex mix of the way systems are built and the way in which their users/managers understand and operate them.
- G.1.2 Security needs to be addressed at a system level, by means of appropriate (process and technical) measures. This annex outlines the general security framework for UTMC and provides assistance in how this applies to communications.
- G.1.3 Implementing security in any system leads to an increase in both capital and operating expenditure costs. This should be seen as the costs of an 'insurance policy' against failures of particular types.

G.2 UTMC security requirements

- G.2.1 UTMC networks must be engineered to avoid 'flooding' attacks, through appropriate network topology, instation router sizing and attack detection/rejection.
- G.2.2 Appropriate provision should be made for system sizing, software quality testing, and system resilience/redundancy.
- G.2.3 Commercial use of UTMC networks and systems needs to include end-to-end protection of transactions. This includes design of in-vehicle units, communications protocols, applications, transaction control and commitment, transaction auditing facilities etc.
- G.2.4 UTMC systems managers must ensure that the communications services they provide to financial systems, commercial services etc enable the latter to operate securely.
- G.2.5 Systems which identify and track individual vehicles need to have the highest level of security provision. This includes the need for well-protected special access for law enforcement agencies – not just the Police but other Government agencies as well.
- G.2.6 Enforcement devices will continue to be type-approved to Home Office/ACPO requirements.
- G.2.7 Communications links with vehicles should not be susceptible to tapping or jamming.
- G.2.8 Partners should be given limited and managed access only to their information, unless there are good reasons to the contrary (eg the trustworthiness and legal requirements surrounding police activity).

G.3 Structural security

Architecture principles

- G.3.1 Security should focus on the following boundaries within the UTMC architecture:
- G.3.2 From the Logical Reference Model:
 - a) interceptable or interruptible wide area communications links (achieved by protocol handshaking, encryption and/or link redundancy);

- b) the interface from Node B (instation) to communications links (achieved by firewalls);
- c) Node C, D and E (street and in-vehicle device) hardware (achieved by physical means);

G.3.3 From the Functional Reference Model:

- a) the user interface (achieved by physical protection and authentication);
- b) the applications to data service (common database) interface (achieved by authentication and redundancy);
- c) the interface with management applications and services (achieved by audit logs).

G.3.4 Figure G-1 indicates the points at which particular security measures apply to the UTMC Logical Reference Model. Figure G-2 does the same for the UTMC Functional Reference Model.

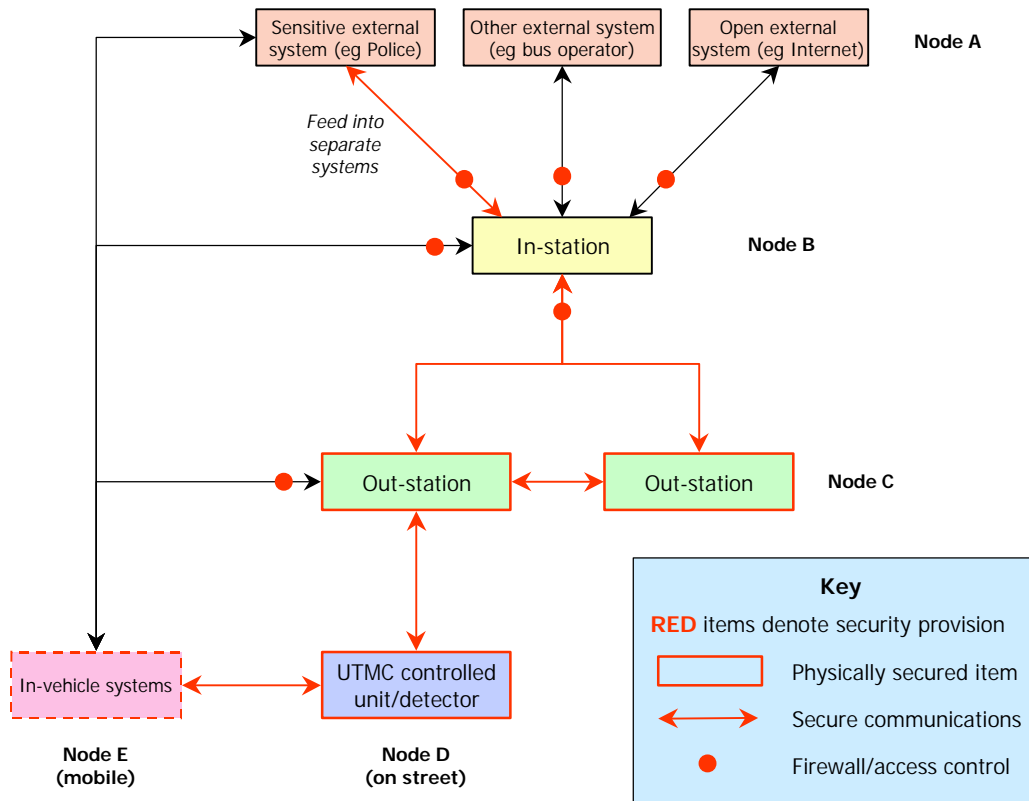


Figure G-1: Diagram indicating security points on UTMC Logical Reference Model

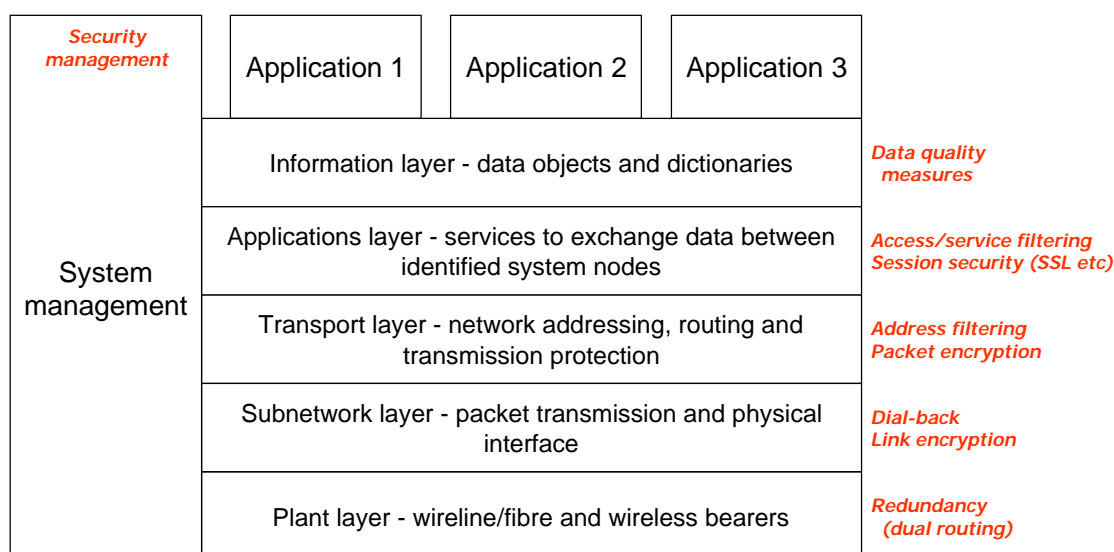


Figure G-2: Diagram indicating security options on UTMC Functional Reference Model

- G.3.5 There is a primary security barrier at the external boundary of the instation, of the 'firewall' kind. This needs to prevent unauthorised entry into the main system from roadside and from partners. This needs to incorporate access control, audit log, and virus protection in addition to the standard firewall functions (address filtering etc).
- G.3.6 There is a similar primary security barrier at the instation desktops, particularly for applications host machines carrying sensitive information (traffic control, enforcement or financial). This also needs to incorporate access control, audit log, and virus protection.
- G.3.7 There are various secure options for access control by users to applications and data. Specifically:
- a) Direct dial-in may be appropriate for own staff conducting external maintenance on the UTMC system, or occasionally access to systems contractors for support and maintenance; while proxy access is technically preferable for business partners, police access, etc.
 - b) For internal users, either an applications-specific access control or a 'single sign-on' approach could be taken. As a UTMC system gains more separately-controlled applications, it may be worth considering a single sign-on architecture.

Technology: security layers

- G.3.8 The general focus of security-conscious industries – on access control/authentication as the primary means of assurance at the user level, supported by encryption at the data level and connectivity at the system level – should be adopted by UTMC.
- G.3.9 Common database implementations may consider use of CORBA security tools, though control at the network layer (though address filtering etc) may be sufficient.

- G.3.10 UTMC Data Objects should include parameters, where relevant, to cover security needs.
- G.3.11 Address filtering and user filtering (through commercial firewalls) will provide protection at specific points (eg external interfaces), and should be a mainstay of all UTMC networks with external connectivity. SSL should be considered for all non-public Web-enabled access.
- G.3.12 Electronic financial exchange (eg using the SET standard) is unlikely to be an internal UTMC matter.
- G.3.13 There are a number of low-level Internet protocol standards that are applicable to UTMC. Many off-the-shelf products incorporate these and no specific standards need normally be called up.
- G.3.14 The choice of IP, as the communications network protocol for UTMC, is a good one from the security point of view. Because of the (justified) public concerns about internet security, there is a great deal of development on security devices, add-ons and plug-ins for IP that should make communications security for UTMC entirely sound, at the three main points (Node B to Node A, within Node B, and Node B to Nodes C/D/E).
- G.3.15 Encryption and segregated networks will provide bearer-level security. For the immediate future, private networks will still need to be used for any link that requires reliable high-timeliness communications.

Operations

- G.3.16 Security needs to be tailored to local commercial, legal and institutional requirements. UTMC security should not be solely at the request of commercial third parties (eg travel information services), although clearly this is an important aspect of it.
- G.3.17 As UTMC systems become more complex, all systems-level concerns will become more significant. As with safety, type approval will feed into this but will not by itself be sufficient, because of all the architecture issues discussed.
- G.3.18 The British Standard Code of Practice BS7799 is fully relevant to UTMC systems, and it would be entirely sensible for local authorities to adopt it as a framework standard (for all systems, and not just for their ITS). It addresses the management issues associated with access control of all sorts.
- G.3.19 Security needs to be maintained through the implementation and migration processes, which means ensuring that:
 - a) partially-implemented systems do not have unacceptable functional security 'holes' (eg communications access to traffic signals before they are linked to the UTMC centre);
 - b) maintenance and repair do not expose security flaws (eg opportunity for access into network from a 'down' device);
 - c) the process of integration with legacy systems does not expose sensitive data to unacceptable risk;
 - d) security management procedures are in place and tested before the system goes live.

G.3.20 Tools are widely available to support the security management of networks and systems, and these should be considered in any UTMC system. Some aspects of this (eg privilege management) are naturally implied by the needs for access control.