ETSI TR 102 653 V3.1.1 (2007-08)

Technical Report

Project MESA;
Technical Specification Group - System;
System and Network Architecture

Reference

DTR/MESA-SYS0070015V311

Keywords

air interface, architecture, broadband, digital, emergency, radio, safety, SAR, satellite, security

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services:
http://portal.etsi.org/chaircor/ETSI_support.asp

Copyright Notification

Contents

Intellectual Property Rights

Project MESA is a collaborative activity who's Organizational Partners (OPs) as of the date of this document are the European Telecommunications Standards Institute (ETSI) and the Telecommunications Industry Association (TIA). It is not a legal entity.

MESA's Technical Working Procedures ("Procedures") provide that Individual Members of MESA are bound by the IPR Policy of their respective OPs. The Procedures further provide that Individual Members should declare at the earliest opportunity any IPRs that they believe to be essential or potentially essential to any work ongoing within MESA.

Under the Procedures, the MESA Secretariat is required to maintain a register of IPR declarations relative to MESA, received by the OPs.

Information concerning declarations of IPR relative to MESA which have been received from OPs and which have been communicated to the MESA Secretariat are available and can be found as follows:

1. as to the MESA Secretariat: www.projectmesa.org or mesa@projectmesa.org;
2. as to ETSI: http://webapp.etsi.org/IPR/;
3. as to TIA: ipr@tiaonline.org.

The use or practice of the contents of this document may involve the use of IPRs including, but not limited to, pending or issued patents, or copyrights. Pursuant to their respective policies, none of ETSI, TIA or MESA makes any search or investigation for IPRs of any nature. ETSI, TIA and MESA, and each of them, takes no position with reference to, and disclaims any obligation to investigate or inquire into, the scope or validity of any claims of IPR which are contained in declarations or otherwise communicated to them, or any of them.

The ETSI IPR Policy is available on the ETSI web server (http://www.etsi.org/legal/) and the TIA IPR Policy is available on the TIA web server (http://www.tiaonline.org) as part of the TIA Engineering Manual.

Foreword

This Technical Report (TR) has been produced by Public Safety Partnership Project (MESA).

The contents of the present document are subject to continuing work within the Specification Group (SG) and may change. Should the SG modify the contents of the present document, it will be re-released by the SG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

x the first digit:

1 presented to SG for information;

2 presented to SG for approval;

3 or greater indicates SG approved document under change control.

y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.

1 Scope

The present document defines a network and system architecture for public safety networks that is capable of meeting the requirements of next-generation public service and public safety agencies. The present document elaborates an architecture consistent with the Project MESA Systems Overview and requirements that are specified in the Project MESA Statement of Requirements and defines other elements needed to develop detailed technical requirements for MESA systems, applications and interfaces. The interfaces specified in the present document are described at a high level, in a generic fashion, to allow for detailed proposals that will provide all the specific details needed to support interoperability. These interfaces are described in separate MESA specification documents.

2 References

For the purposes of this MESA Technical Report (TR), the following references apply:

NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long term validity.

[1] MESA 70.012: "Project MESA; Technical Specification Group - System; System Overview".

[2] MESA 70.001: "Project MESA; Service Specification Group - Services and Applications; Statement of Requirements".

[3] MESA 70.002: "Project MESA; Service Specification Group - Services and Applications; Definitions, symbols and abbreviations".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

connection: entity formed when two devices communicate

NOTE: A connection between two devices includes the interfaces used and the link that is formed between them. A connection can also describe the upper layer elements within the context of overall connectivity to a mission's application needs.

device: type of communication component differentiated from other components by its stand-alone accessibility and functionality

NOTE: It is physically interactive, such that an input results in an action taking place within the device, as opposed to a component which may only be accessible through the network. Devices are generally more portable than other components and may possess capabilities to access or communicate with other devices and/or networks.

interface: physical or logical link between two entities

NOTE: In the present document it is used to refer to the physical interface that network components use to communicate with each other. This interface may be either wired, wireless or utilize other emerging techniques. All software interfaces will be specifically referred to as software interfaces.

When two or more interfaces communicate they form a **link**. This link may be wired, wireless or utilize other techniques, depending on the interfaces forming the link. The interfaces forming the link also determine the protocol of the link. Note that components or devices (i.e. NGN, converged) may be enabled to utilize and access multiple interface and link possibilities.

network component or simply a **componen**t**:** represents a physical piece of the network

NOTE: This component may serve in creating the network, facilitating the network or to access the network.

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in MESA 70.002 [2] and the following apply:

AAA	Authentication, Authorization and Accounting
AWN	Ancillary Wireless Network
EAN	Extended Area Network
FMC	Fixed/Mobile Convergence
IAN	Incident Area Network
ITS	Intelligent Transportation System / Intelligent Transport System
JAN	Jurisdiction Area Network
JSNCP	JAN Service and network Control Point
LMR	Land Mobile Radio
MESA	Mobility for Emergency & Safety Applications
NGN	Next-Generation Network (relates to convergence and FMC; packet-data)
OAN	Over the Air Networking
PAN	Personal Area Network
PSCD	Public Safety Communication Device
QoS	Quality of Service
SaR	Search and Rescue
SENTRY	Federal Bureau of Prisons' "SENTRY" database (US)
SOA	Service Level agreements
SoR	Statement of Requirements

4 Overview

The Project MESA Network and System Reference Architecture describes the communication components that will either be incorporated into a Project MESA system, or with which a Project MESA system will interact. The present document describes a general public safety and emergency services sector communication architecture or structure, and the common components in that architecture. The MESA Architecture is designed to meet the rigorous requirements of the Public Safety and Emergency Services community. Actual implementations may differ, as long as the user community requirements are met, but the overall hierarchy and architecture should be similar even if all the components are not included, thus allowing for maximum flexibility and discretion of system owners, operators and users. The flexibility of the architecture allows for a communication system that addresses many different scenarios and specialized agency or user needs.

5 Architecture

5.1 Overview

The overall public safety communication system architecture provides a description of the identified systems' components, including the components' structure and the connections formed among them. The high-level architecture also explains the design principles behind the components and their connections. The chart below also implies a potential access or architectural relationship (interoperability, accessibility) between network types and or components.

5.2 Networks

The MESA network hierarchy consists of Personal Area Networks (PAN), Incident Area Networks (IAN), Jurisdictional Are Networks (JAN) and Extended Area Networks (EAN). These networks are defined to meet primarily the needs of the Public Safety user community. These networks may be interconnected with Ancillary Wireless Networks (AWN) to provide additional and/or backup coverage. The AWN is a network whose primary design is for public commercial or other non-public safety services, but whose ubiquity makes availability of its services desirable for the public safety user community. The service characteristics that the public safety user receives from these networks will depend on Service Level Agreements (SOA) that may exist between a particular Public Safety Agency and the AWN network operator.

The role of a MESA Network in the hierarchy is determined by its characteristics in multiple dimensions. These dimensions may include technology, service, regulatory, legal and deployment considerations. Thus on a technology front it may be possible to either have heterogeneous technologies for a single network type or a single technology across multiple network types. The MESA high level architecture is described in a manner that is flexible to allow for multiple deployment and regulatory environments without imposing any artificial constraints.

Type	Scope	Capabilities	Bandwidth Required
Personal Area Network (PAN)	Single subject or object.	Limited applications and location.	Only enough for pre-designated and localized applications.
Incident Area Network (IAN)	An incident or specific event. Examples include a MESA-capable ad-hoc "hot-spot" or other temporary network.	Application varied and flexible network establishment, but location limited. **An IAN may or may not contain any infrastructure elements or links to external networking functions. In such a case, PSCDs communicate amongst themselves constrained by their individual propagation characteristics.**	Enough to support the incident or specific mission, including ad-hoc capabilities across environmentally challenging scenarios.
Jurisdiction Area Network (JAN)	An entire jurisdiction. A **JAN might be implemented for a given governmental entity. A JAN may be implemented to provide services for a number of governmental entities, covering well beyond the jurisdictional area of responsibility for any given entity. A JAN may be shared also be shared among government and non government users, under the management of a government entity, a non-government entity, or shared government/ non-government control.**	Varied applications and locations, robust, well managed. Further requirements can be found in [2].	Able to provide high bandwidth throughout the coverage area; extensive planning and engineering. Further requirements can be found in [2].
Extended Area Network (EAN)	Unlimited, as technically feasible.	Mainly a core network designed to interconnect and aggregate JANs to cover larger geographical areas and provide inter-JAN connectivity. Varied applications and locations as technically feasible; could include national or territorial services and database access, enhanced access capabilities and alternate communication channels.	Unlimited, as technically feasible. Dimensioning to be determined by the expected transit and terminating traffic between interconnected JANs.

Type	Scope	Capabilities	Bandwidth Required
Ancillary Wireless Network (AWN)	Unlimited, typically this may be a commercial services network that can be accessed by public safety personal.	Full commercial service capabilities and potentially supporting pre-emptive capabilities for Public service emergencies.	Bandwidth will be determined bases on the network dimensioning done by the service provider. If public-service pre-emption is supported minimum public-service bandwidth requirements can be supported.

5.2.1 Physical and virtual networks

Ultimately, in order to offer a communication service a physical network is used to transmit the user information. The physical network may consist of wireline and/or wireless facilities, which may be interconnected by switches and routers. It is possible to construct dedicated physical networks to serve specific user requirements and communities or specific traffic types. The advantages to the deployment of dedicated networks is that these networks can be optimized to carry the traffic type for which they are designed, security of the network is more easily maintained and usage of the network including priority access is more easily managed. The obvious disadvantages to dedicated networks are the redundant deployment of facilities for each service provider, increased cost of management and operational complexity.

An alternative to dedicated and separate physical networks is the employment of a common network infrastructure with software defined virtual networks providing the appearance of dedicated networks to the individual user communities. The common network infrastructure may be an infrastructure shared among various entities all engaged in providing public safety and emergency services or may even involve sharing of infrastructure with commercial services. When virtual networks are used to satisfy various user communities efficiencies are achieved in facilities and operational costs but the virtual network provides the requisite quality of service and security by means of networking and security applications and appropriate design of network protocols. The assurance of service availability to the public safety and emergency personnel is especially critical when the infrastructure is shared with commercial applications that may need to be pre-empted to accommodate public safety and emergency traffic.

An alternate attractive option is the possibility of providing dedicated access networks that access a shared common core network that is virtualized for each user community.

Public safety services may be provided by:

i) networks that are special purpose constructed and are separate physical networks;

ii) instantiated as a virtual network on top of shared common physical networks; or

iii) a combination of physical and virtual networks;

vi) a combination of public safety networks, shared public safety networks, and shared public safety and public networks.

5.2.1.1 IAN

A major interest in IANs, is in response to disasters or in response to special events where the existing physical infrastructure is either non-existent or inadequate to serve the communications needs of the situation. In these circumstances the IAN will be a separate physical network with or without infrastructure. In some cases there will be an interface to a JAN. In those cases where the incident area is large, the dedicated infrastructure may use parts of the JAN or EAN to extend the range of the IAN. Potentially IANs could also tunnel through VPNs provided by commercial networks.

IANs may also be instantiated as a virtual network on top of facilities that are deployed as a JAN or EAN. This may be desirable where the traffic generated for the incident can be satisfactorily carried by existing JAN/EAN infrastructure but specific security and performance requirements need to be met for all staff involved in responding to the incident. In these cases, conceptually, the IAN can be created as a virtualization on top of the IAN/JAN facilities.

5.2.1.2 JAN

Jurisdictional area networks can be dedicated to a particular jurisdiction using both a dedicated core network and dedicated access networks. This gives the jurisdiction great flexibility in managing its own communications resources. As an alternative the JAN may use dedicated access networks but the core network may be a virtual network defined on top of a commercial network or on top of an EAN. Synergies can be gained if multiple jurisdictions in the same geographic area, share a common physical network.

5.2.1.3 EAN

The EAN provides no direct user access capability but provides connectivity between individual JANs and may provide additional service capabilities to the aggregate public safety user community.

5.2.1.4 AWN

The AWN provides public safety staff with additional or alternative wide area and local communications capability. The AWN may be a commercial services network or purpose built network for the public safety community. The AWN may also provide additional capabilities to the MESA core networks.

5.2.2 Network types

5.2.2.1 Incident Area Networks (IAN)

The Incident Area Network (IAN) is generally dedicated to a single incident or event. A key public safety requirement is the ability for peer-to-peer and peer-to-multiple peers in the lack of any supporting infrastructure. The IAN can be pre-deployed for a planned event, such as a sporting or "nationally significant" event, or it could be dynamically deployed for an unplanned event or incident (all-hazards). Possible unplanned events range from a local law enforcement situation to relief efforts in a natural disaster area. Depending on the affected situational area and agencies engaged, interoperability, inter-connection and resource management become more critical. Note that an unplanned incident can involve fluid and challenging geographic and infrastructure scenarios that can affect initial staging operations and overall communication capabilities (i.e. terrorist attack or major hurricane/tsunami). The IAN can be deployed, for example, in situations where existing private and/or public communication infrastructure is diminished or non-existent. The IAN can involve MESA-capable or other components.

5.2.2.2 Jurisdictional Area Networks (JAN)

The Jurisdiction Area Network (JAN) is designed to provide specific agency or shared access coverage over a wide area that may include such geographic boundaries as a city, county or country. The design and deployed placement of JAN infrastructure elements are well planned to ensure complete coverage and sufficient bandwidth, a high QoS level and reliability factor that corresponds to the nature of this mission-critical user group. The JAN's infrastructure utilizes powerful communication towers and other two-way broadcast infrastructure elements to provide for the capabilities mentioned above and the communications coverage required to meet public safety and public protections service agency needs. These towers or communication link points can vary in both shape and size, depending on planning and coverage needs. Some are designed for placement on hill tops while others are much smaller and are designed for use inside buildings and tunnels. This clause mainly relates to more traditional JANs, however, a MESA System of Systems [JAN] deployment can also be considered a form of temporary or dynamically deployed JAN that connects and manages multiple IANs, PANs, etc.

Although a JAN is normally a static or predominantly pre-configured network, it allows for some dynamic reconfiguration. This may especially be the case with emerging or next-generation capabilities. If a particular jurisdiction needs supplementary resources, it may be possible to allocate additional network resources to the affected area. For example, it is possible to augment the network with mobile transmission towers that can be repositioned in areas requiring additional or augmented resources, assuming the local backbone network has adequate capacity to accommodate the additional load. Additionally, it is possible to augment network resources and or enhance user capabilities through other available or Ad-Hoc infrastructure components; realizing that "mission-critical" quality levels expected in a planned JAN may be transformed while accessing such augmented resources. Even with these abilities the JAN is not as dynamic as an IAN. The JAN is dedicated to providing complete and consistent coverage over a specified jurisdiction as may be defined by the first responder in cooperation with the JAN provider. Therefore, though allowing some dynamic reconfiguration of bandwidth, an established multi-use JAN cannot radically shift resources as demands change because the JAN still needs to provide consistent availability across the entire coverage area.

JANs include traditional Land Mobile Radio (LMR) networks, with the infrastructure of the JAN providing network access and coordination over a large area. Such a JAN uses a topology were devices normally communicate through towers instead of talking directly to each other. Fixed infrastructures such as towers enable the JAN to provide a predetermined level of coverage for a specified area. The fixed topology of the JAN makes it possible to guarantee minimum performance and coverage levels. In some case this may allow the JAN to provide a higher level of coverage and mission-critical reliability than the IAN. Devices should be able to reliably connect to the JAN anywhere within the area of coverage. Connectivity handoff, with regard to device or terminal mobility, between the different JAN communication towers and associated infrastructure, should be seamless and invisible to the user. Additionally, the ability for peer-to-peer communications, to augment user capabilities, is recognized and desirable for next-generation designs. Next-generation capabilities may also include other flexibility options that are not tied only to the network.

5.2.2.3 Extended Area Networks (EAN)

The Extended Area Network (EAN) is mainly a network designed to provide connectivity between various JANs it can also include traditional backend networks used to access various databases and information sources. The EAN can be designed to provide overlay services or access coverage over a very wide area and can be responsible for tying together various JANs. Note that JANs are frequently connected at the physical level and may also need to sustain or be required to provide end-to end security/authorization across such systems. The EAN can also provide for a bridging that allows for mobility and some form of access between JAN or other network access, and thus can provide for continuous basic access or seamless communication when travelling across or between jurisdictional boundaries or authorized networks. This also implies, for example, that a connection formed while in one IAN could be able to be carried over to another IAN or MESA JAN, via an EAN link, and that this authorized migration should happen automatically and with minimal user intervention.

The JAN Service and Network Control Point (JSNCP) for each JAN should also manage the connection between that JAN and other JANs, through the EAN or other facilitating means. The JSNCP already serves as a central coordination point for the JAN's entire communication infrastructure and also manages the communication within the JAN. This makes the JSNCP a natural point from which to coordinate a connection to other JANs. Each JANs' JSNCP should coordinate with each other to ensure that communication can migrate seamlessly between JANs.

While the EAN plays an important role in the system of systems concept, it is not the focus of the present document. This is largely because the EAN is mainly a fixed resource and the interface between networks should be standardized by applicable standards bodies. Attention should be paid to the access and security procedures for the EAN to ensure compatibility across different implementations; however this is outside the scope of the present document.

5.2.2.4 Ancillary Wireless Networks (AWN)

An Ancillary Wireless Network (AWN) is a network that is (primarily) designed and operated to accommodate commercial services, but is accessible by and available to public safety users for both general purpose and public safety communications needs. The service provider may include specific support functions, such as pre-emption and priority, in the AWN in order to meet specific requirements of the public safety sector. It is assumed that service level agreements between a given carrier and a user organization will specify the specific functionalities that will available during heavy loading situations to assure public safety priority to the network.

5.3 Components

5.3.1 Public safety sensor and networked devices

The PAN is comprised of special purpose devices or components of limited scope and transmission radius. There is a great variety of devices that may be deployed in the PAN as a PAN can provide the basis for a distributed implementation of a terminal device as well as serve as a "concentrator" network. In many cases, devices on the PAN are sensors and these sensors are referred to as Public Safety Sensors. These sensors are generally limited to communicating with other devices on the PAN. An example can involve heart rate and ambient temperature monitors worn by first responders. Such a configuration involves three devices, including the two sensor devices and one device which aggregates the data and transmits it to the radio or terminal device utilized by the first responder or other public service/safety user. Data could also be transmitted from the third device to a command monitoring point. The first responder radio referred to is called the Public Safety Communication Device (PSCD) and explained in detail later. The third device's data-logger functionality is also capable of recognizing preset events, such as a spike in temperature, and pushing an alert to the associated PSCD. In addition the PSCD can poll the data-logger device for updated monitoring information.

It is important to emphasize that this is an envisioned configuration to illustrate the general architecture. It is plausible that different devices or terminal types are utilized, or that devices are focused on another subject type, such as a building. The PAN and the devices connected to it are specialized for a defined subject, such as a building, person or vehicle, and encompass a limited functional radius. Interconnection with other PANs or networks allows for increased communication reach, coordination and information flow.

5.3.2 Communication devices

The Public Safety Communication Device (PSCD) and the Mobile Terminal are both general types of communication devices. The major differences between the device types relate to their design specifications, portability and capability levels. A PSCD is generally a handheld or mobile device and may not include as many capabilities in the interest of conserving power and weight. They may be built to different design specifications with regard to adjacent channel interference, power output, and receiver sensitivity, inter-modulation, and co-channel interference rejection. In many cases, the expected duty cycle, coupled with the increased power requirements, dictates lager batteries. A Mobile Terminal is usually vehicle based, allowing it a more dependable power supply, improved antenna placement or reach and improved transmit/receive functionality due to increased power levels. Note that the term "Mobile", in this specific context, does not translate to other uses of the term or the term mobility, as "Mobile" in this Public Safety context usually involves vehicles or other similar situations. The term "mobility" utilized in standards activities has more relation to a PSCD than a Mobile Terminal. These units on occasion may be required to meet even tighter operating specifications.

Both device types may be capable of communicating over an established compliant and compatible IAN or a JAN. A PSCD may be in the range of both an IAN and a JAN, the PSCD should support dynamic configuration of which network will be used to provide the primary access. If an IAN is not reachable or one has not been established, communication will go through the JAN, as able or authorized. Depending on individualized structure, the communication devices are also capable of connecting to PANs, EANs or other networks, as capable and authorized. A PSCD or Mobile Terminal can also serve as the aggregate point for a PAN and monitor the values of connected devices and may be capable of forwarding information from the PAN onto the IAN or JAN if necessary. The devices on a PAN that a PSCD would connect to, for example, might include heart rate monitors, geo-location sensors, motion sensors and many more. A Mobile Terminal, for example, might connect to the existing JAN and to a PAN, including functionalities that could include the vehicles light bar and the various sensors, video units and other elements incorporated into the vehicle.

An IAN is dynamically formed between the enabled communication components or devices in given area. The most capable devices are responsible for determining the structure of the network (i.e. accessing and linking to a Master Node) and providing the network, as appropriate, a linkage to a MESA-type JAN or provide resources such as a bridge to external networks. The coordination of communication between all of the devices in an IAN could be handled by a specific or master device on the IAN or through a MESA-type JAN (i.e. System of Systems). In many cases, the vehicle-based Mobile Terminals could assume this role as they may offer a stable point from which to build a network around. A Mobile Terminal can also allow for a more stable connection due to better antenna location and length, increased signal strength dynamics and a dedicated power source. However, there are many cases when a Mobile Terminal is not practical or desired, and as such, an IAN could be formed by two or more mobile (untethered) PSCDs. The method used to form MESA IANs should be adaptable enough to handle a wide variety of communication device deployments and also can involve variant architectures and networks. Other network types utilize communication devices and terminals as appropriate for their architecture and needs. MESA devices should also be inclined to self-heal and re-establish connections.

5.4 Overall network architecture

The present document generally defines interfaces relating to the overall communication architecture and as found in a MESA-capable system. Presently the Network Architecture is defined with the goal of allowing the identification of network interfaces required for network connectivity and does not address the architecture of application services and the operations support infrastructure. For a fully functional MESA network application servers and operations support capabilities are required to allow dynamic management of Quality of Service, security and overall network operations. Appendix A of the present document is a first attempt at beginning to characterize an overall end to end architecture that also addresses services and applications.

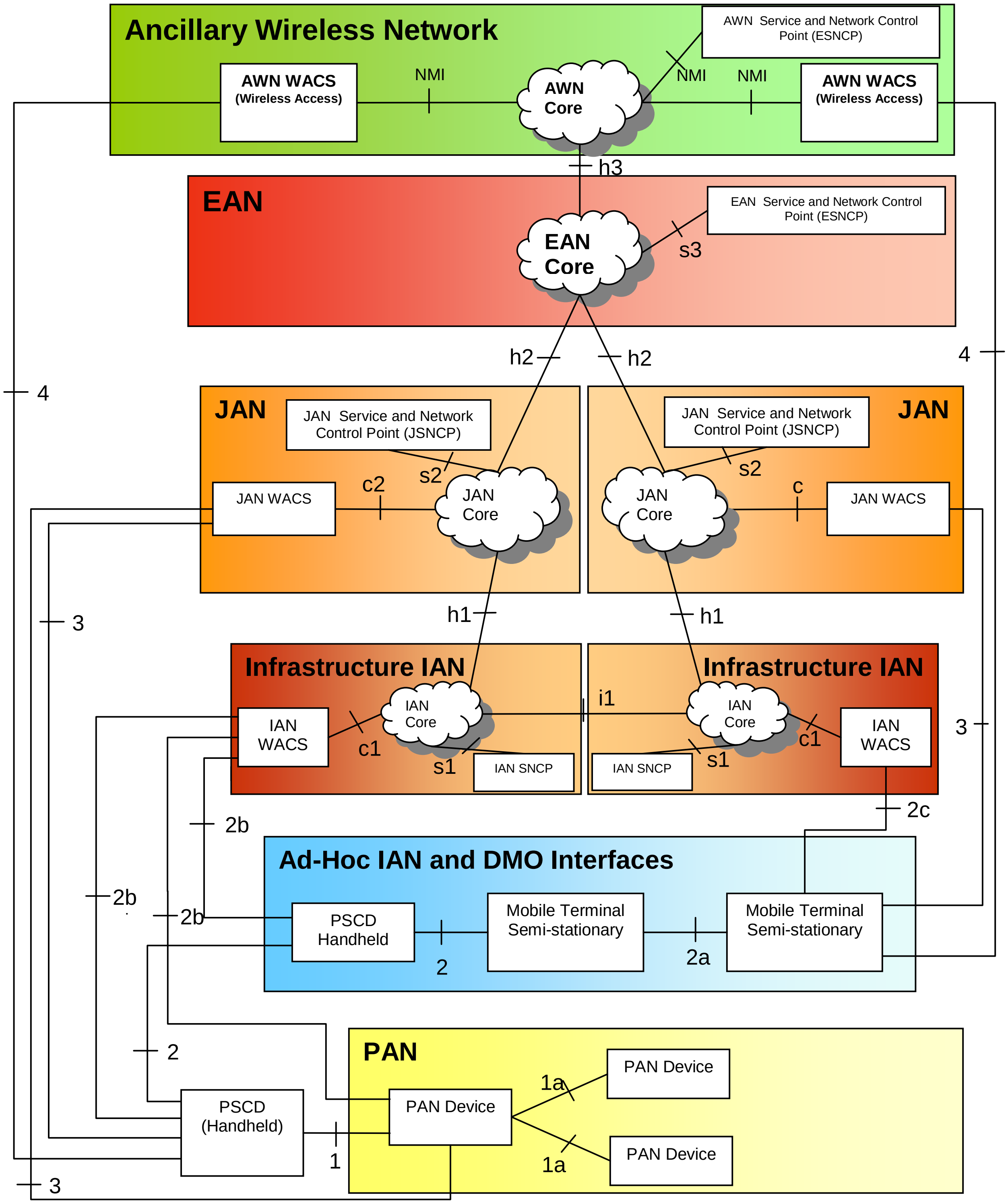

Ancillary Wireless Network
AWN Service and Network Control Point (ESNCP)
AWN WACS (Wireless Access)
NMI
AWN Core
NMI
NMI
AWN WACS (Wireless Access)
h3
EAN
EAN Service and Network Control Point (ESNCP)
EAN Core
s3
h2
h2
4
4
JAN
JAN Service and Network Control Point (JSNCP)
JAN Service and Network Control Point (JSNCP)
JAN
JAN WACS
c2
s2
JAN Core
JAN Core
s2
c
JAN WACS
3
h1
h1
Infrastructure IAN
Infrastructure IAN
IAN WACS
c1
IAN Core
s1
IAN SNCP
i1
IAN SNCP
s1
IAN Core
c1
IAN WACS
3
2b
2c
Ad-Hoc IAN and DMO Interfaces
2b
2b
PSCD Handheld
2
Mobile Terminal Semi-stationary
2a
Mobile Terminal Semi-stationary
2
PAN
PAN Device
1a
PAN Device
PSCD (Handheld)
1
1a
PAN Device
3

Figure 1: Interface Architecture

Interface designators

The present document employees an interface classification scheme as described below:

- Numerical interface designators without an alphabetic prefix are access interfaces.
- Core network interfaces are identified by the alphabetic prefix "c".
- Internetwork interfaces are identified by the alphabetic prefix "i".
- Interfaces going up the network hierarchy are identified with the alphabetic prefix "h".

- Interfaces to services and control platforms are identified with the alphabetic prefix "s".

5.4.1 Interface 1

Interface 1 is an interface between a PAN Device (e.g. a Public Safety Sensor or a PAN device concentrator) and a PSCD. The distance of this link is generally short. Bandwidth requirements may be dependent on the type of PAN devices connected, with relatively low bandwidths being satisfactory for sensors but UWB connections possible needed where video information may need to be deployed. The interfaces utilized are generally wireless, but may be wired in some instances.

NOTE: PAN devices may connect to Vehicular mobile terminals not just handheld PSCDs.

5.4.2 Interface 1a

Interface 1a is an interface between various devices on a PAN, this interface may be identical to Interface 1 but potentially may exist in a variety of different capabilities to accommodate the great variety of PAN devices that may be deployed, e.g. low bit rate sensors, high bandwidth video feeds.

5.4.3 Interface 2

Interface 2 is an interface between PSCDs and between a PSCD and Mobile Terminal Semi Stationary. This interface supports communications from one PSCD to one or more PSCDs or Mobile terminals, in the absence of any fixed or transportable infrastructure.

5.4.4 Interface 2a

Interface 2a is an interface between Semi-stationary Mobile terminals (such as parked first responder vehicles or transportable base-stations). These mobile terminals can provide an ad-hoc or infrastructure type network for the IAN. A key distinguishing feature between interface 2 and 2a is that due to the nature of the operating environment of interface 2a different link-budget assumptions are appropriate for this interface. Interface 2a can also be used for purely vehicle to vehicle communication.

5.4.5 Interface 2b

Interface 2b is an interface between the PSCD and the Infrastructure IAN wireless access system or between a PAN device (with an IAN interface) and the Infrastructure IAN wireless access system. This interface and the associated protocols and mode of operation may be different than that used for ad-hoc or direct mode operation between PSCDs.

5.4.6 Interface 3

Interface 3 is an interface between a Communication Device or PAN device (with a JAN interface) and the JAN wireless access system This interface provides direct connectivity to the JAN.

5.4.7 Interface 4

Interface 4 is an interface between a Communication Device and the AWN Wireless Access.

5.4.8 Interface s1

Interface s1 is an interface between the IAN core network and the IAN Services and Network Control Point.

5.4.9 Interface s2

Interface s2 is an interface between the JAN core network and the JAN Services and Network Control Point (JSNCP). The JSNCP contains the dispatch office for the jurisdiction. In addition the JSNCP handles interfacing between an established EAN and the JAN.

5.4.10 Interface s3

Interface s3 is an interface between the EAN core network and the EAN Services and Network Control Point. The ESNCP supplements functionality provided the individual JNSCPs and may provide cross-jurisdictional capabilities.

5.4.11 Interface i1

Interface i1 is an interface between the core networks in two different IANs. It allows direct interworking between two IANs. Note that communication between two IANs is also possible via a JAN interconnection.

5.4.12 Interface h1

Interface h1 is the interface between the IAN and JAN core networks it allows communication between IANs even in the absence of direct interconnection and provides access to remote databases and services.

5.4.13 Interface h2

Interface h2 is the interface between the JAN and EAN core networks it allows communication between JANs and provides access to remote databases and services.

5.4.14 Interface h3

Interface h3is the interface between the EAN and AWN core networks it provides access to remote databases and commercial services.

5.4.15 Interface c1

Interface c1 is the interface between the IAN access wireless system and the IAN core network.

5.4.16 Interface c2

Interface c1 is the interface between the JAN access wireless system and the JAN core network.

6 Communications device architecture

6.1 Common communication device

MESA-capable wireless communication devices that will be utilized to provide next-generation public service and safety communications can be viewed as consisting of two types of functional blocks (see figure 2); the Mobile Radio Termination Function and the Terminal Equipment Function.

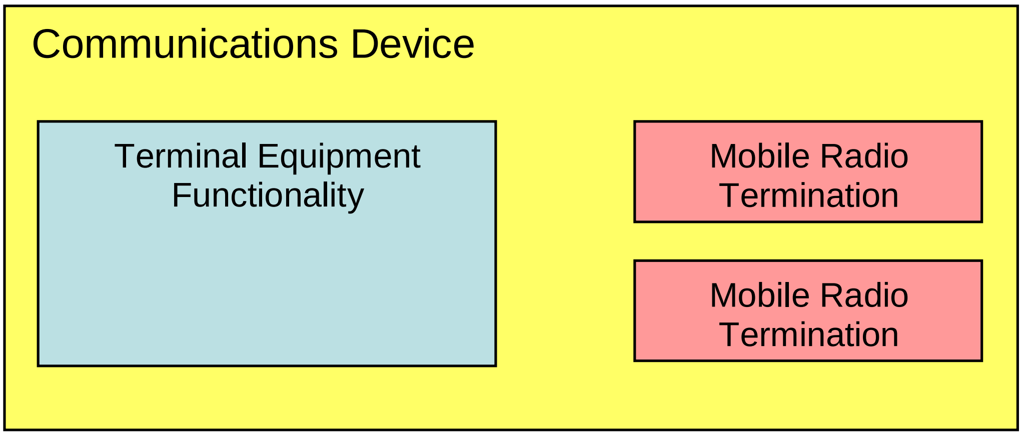


Figure 2

The Terminal Equipment Functionality provides specific capabilities to the end user such as the user interface, information display, data input, environmental sensing, etc. The Mobile Radio Termination Function provides the support for the radio interface and mobility support. A Communication Device may have more than one Mobile Radio Termination (MRT) function. When multiple MRTs are provided these may be present in order to allow the device to operate on multiple radio interfaces (i.e. a multi-mode device) or the device may serve as a relay/router, forwarding information from one MRT to the other MRT. A uniform API by which the TE can access the services of the MRT will facilitate evolution of new communication device features and capabilities.

This high level device architecture allows for the modelling of both handheld and vehicular terminals.

6.2 Communications device interfaces

This clause provides an overview of the interfaces provided by the communications devices associated with MESA networks. The interfaces discussed below go beyond those shown in the overall architecture diagram.

6.2.1 PSCD interfaces

A PSCD device's primary function is to provide the public safety staff with all their communications capabilities. As such a PSCD has a number of interfaces that access the MESA networks hierarchy. In addition the PSCD supports the distribution of functionality around a personal area network and relaying that information to other devices and networks. To support the latter capability the PSCD has a south-bound interface supporting PAN devices (see clause 6.2.2).

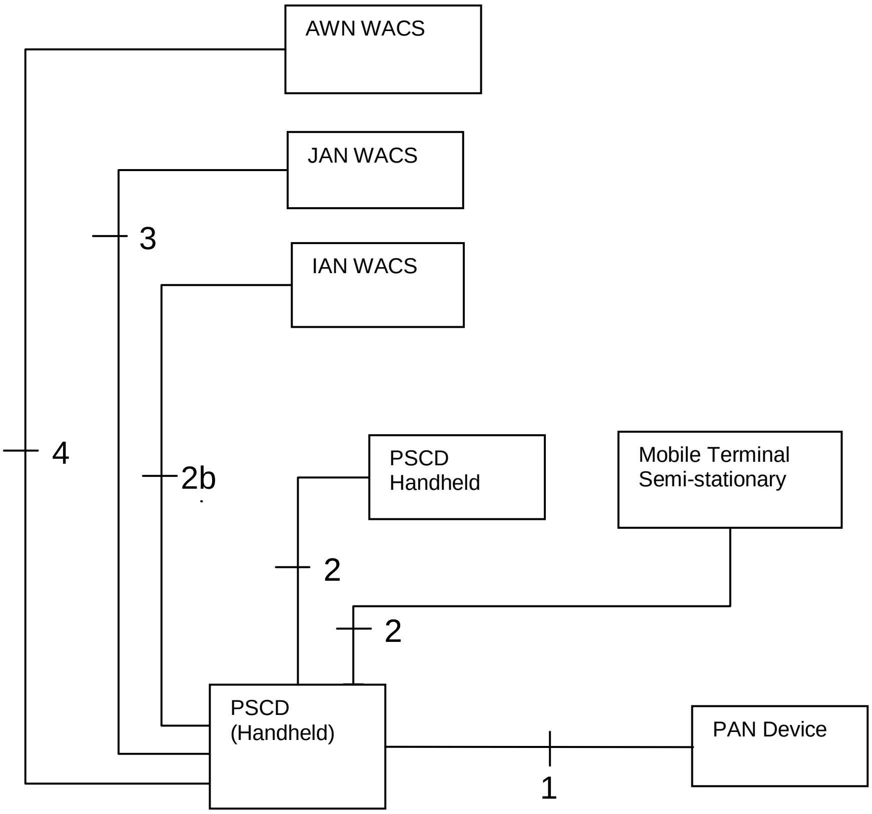


Figure 3

6.2.1.1 Interface 1

This is the primary interface between a PSCD and the PAN. Over this interface the PSCD communicates with the PAN and the PSCD can then act as concentrators/relay device to the MESA network hierarchy. The PSCD may also serve as controller for the PAN devices and the protocols need to accommodate that functionality.

6.2.1.2 Interface 2

This interface is used in support of networking between PSCDs and Mobile Terminals. The interface also supports peer-to-peer communications between PSCDs. The range of the physical layers of these protocols needs to be able to accommodate considerations that the communicating entities may both be battery powered and therefore have a limited link budget.

6.2.1.3 Interface 2b

This interface supports communication between a PSCD and an IAN Wireless Access Point. The range of this interface may be greater than for interface 2 and a richer service environment may available to the PSCD.

6.2.1.4 Interface 3

Interface 3 provides the PSCD direct access to the JAN. This may, but need not, use lower layer protocols similar to interface 2b but at the upper layers will need to address issues of service availability to PSCDs from foreign jurisdictions accessing the local JAN.

6.2.1.5 Interface 4

This interface provides the PSCD with direct access to the AWN. This network may, but need not,   use lower layer protocols similar to interface 2b and 3. Since the AWN is generally a network that is open to the public upper layer support will need to accommodate the needs to preserve privacy and service integrity when this network is used for public safety communications. Additionally, public safety agencies may require minimum SLAs before making such connections available to their personnel for secure communications.

6.2.2 PAN device interfaces

PAN devices may provide some stand alone functionality (e.g. environmental sensors) or may be the result of functional dis-aggregation of a terminal (e.g. a wireless earpiece). The architecture also supports the ability of one of the PAN devices acting as a concentrating relay to interconnect other PAN devices to the PSCD or the MESA network hierarchy. PAN devices may be simply reporting devices (inferring one-way communication), or be capable of also being interrogated or communicated with (inferring two-way communications capability).

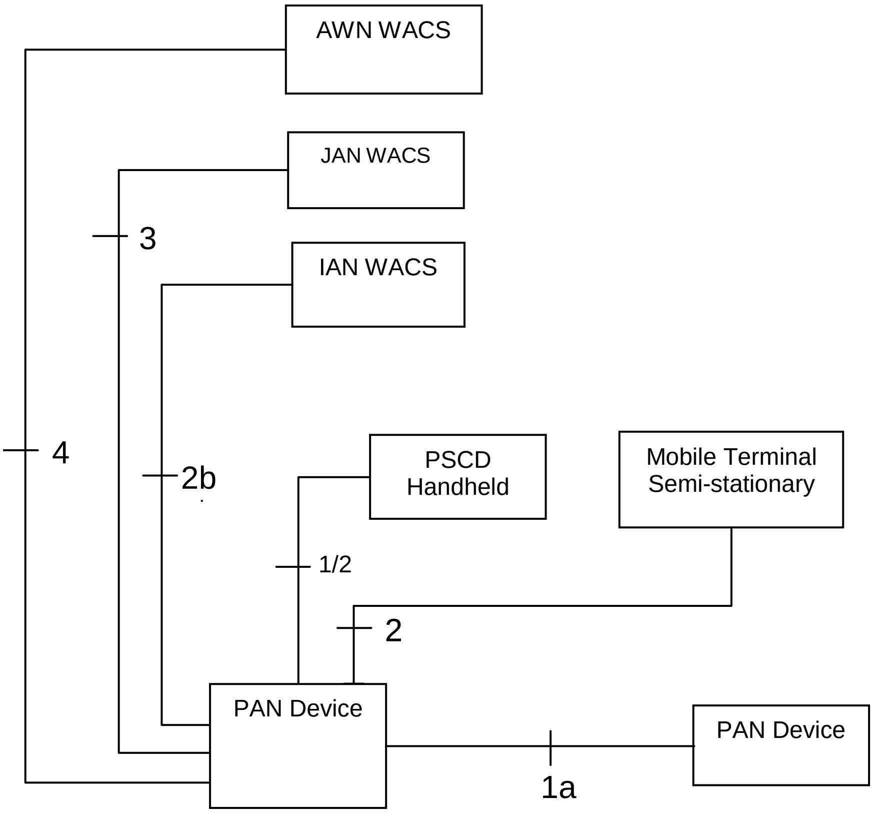


Figure 4

6.2.2.1 Interface 1

The functionality provided is similar to that for a PSCD, but allows a PAN device to act as concentrator/relay to the MESA networks.

6.2.2.2 Interface 1a

This interface allows devices on a PAN to communicate with each other. Various protocol are likely to be required in order to support the full gamut of devices and components that may be connected via the PAN, as interconnected components may vary from low bit-rate sensors to ultra-wideband video devices.

6.2.2.3 Interface 2

The wide-area interfaces (2, 2b, 3 and 4) may be supported by OAN devices to provide direct connectivity to a MESA network without requiring the presence of a PSCD to transfer the information out of the PAN area. This functionality is useful, for instance, when a set of environmental sensors is left in an incident area and the monitoring is done in some jurisdictional centre.

6.2.2.4 Interface 2b

The functionality provided is similar to that for a PSCD, but allows a PAN device to act as concentrator/relay to the MESA IAN.

6.2.2.5 Interface 3

The functionality provided is similar to that for a PSCD, but allows a PAN device to act as concentrator/relay to the MESA JAN.

The functionality provided is similar to that for a PSCD, but allows a PAN device to act as concentrator/relay to the AWN.

Annex A: Public service services and core network architecture

A.1 Overview

Figure A.1 shows a generic core network and services architecture for MESA Public Services networks. This architecture is appropriate for JANs and EANs. Many of the identified characteristics are also appropriate for IANs that can be pre-planned. In the case of ad-hoc IAN scenarios this functionality may still be required but may be distributed among the communication devices; this will be especially true if the IAN is limited in its access to external networks.

NOTE: Figure A.1 is an attempt at defining an architecture that is somewhat technology independent and is proposed as a basis for further work.

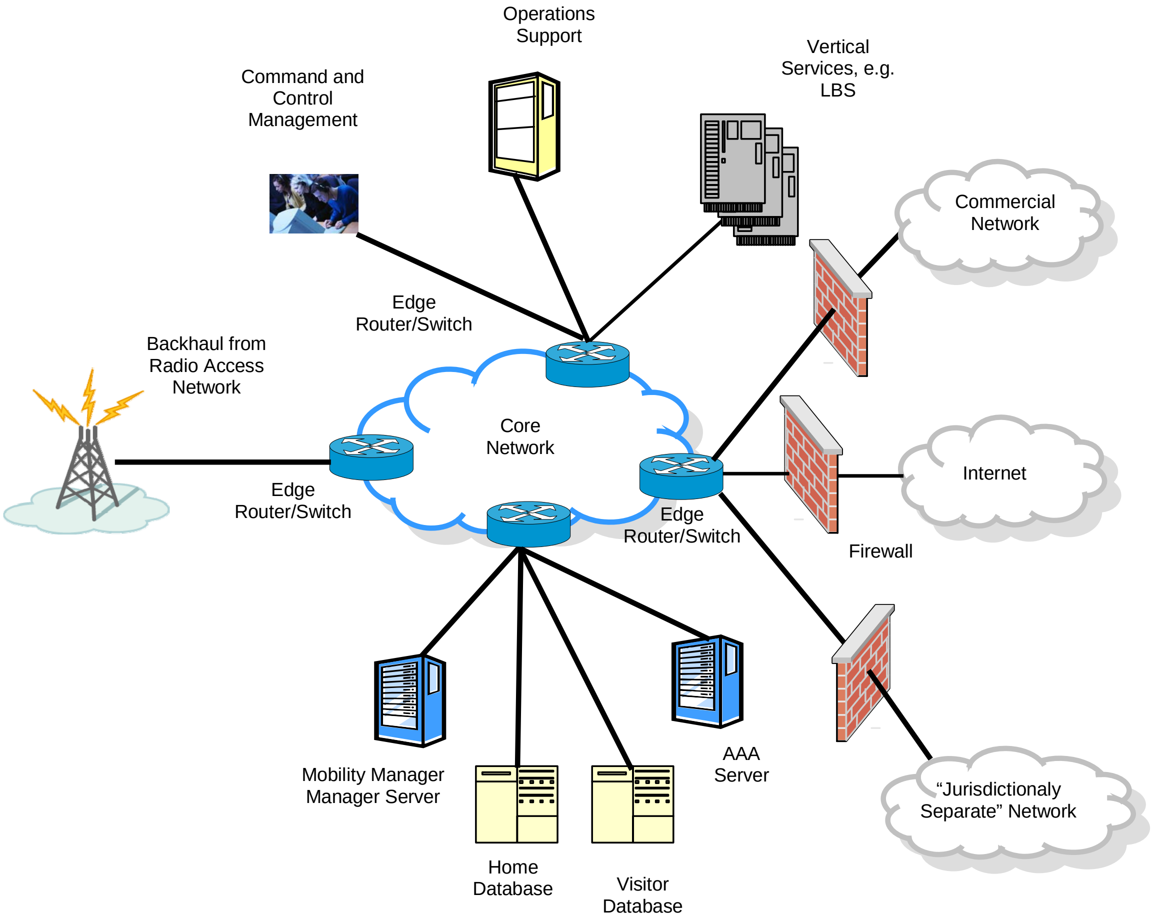


Figure A.1: Generic public service services architecture

A.2 Functional component descriptions

A.2.1 Home database

The Home Database contains the information concerning the users that are directly associated with the administration responsible for operating that network. The information contained includes security information, service capabilities of the user's terminal, service priority levels associated with the user and information about the user's roles and responsibility in the jurisdiction. This latter information may need to be accessed in real time from an external database.

In a case of an IAN the Home DB function may be absent and only a Visitor Database populated with information from the individual jurisdiction responding to the incident may be present.

A.2.2 Visitor database

The Visitor Database contains information concerning users that are temporarily located in the zone being served by that particular network. The information is obtained from the Home DB of that user.

A.2.3 Mobility manager

The Mobility Manager contains the functionality to allow users to move between cells and networks. It assures that context is transferred in order to facilitate seamless handoff.

A.2.4 AAA server

The AAA Server's responsibility in the public safety networking area is mostly associated with authorization and authentication of service access. However, if accounting support is required, e.g. for usage monitoring or cost allocation to departments, this would be provided by the AAA server.

A.2.5 Operations support systems

The operations and support infrastructure provides the functionally to provision the network and services as well as to monitor and maintain networks services and facilities.

A.2.6 Vertical service systems

Vertical Service systems provide services above the network layer. Examples may be, location based services, e-mail, etc.

A.2.7 Command and control systems

Command and control systems allow human operators to interact with the network and field personnel in order to determine whether any special situations arise that require intervention.

Annex B: Public service services and system architecture views

NOTE: Further elaboration is required on the content.

B.1 Overview

Figure B.1 depicts an end to end system that encompasses end users and use cases to the physical system implementation that meets the end user needs with various "Architecture Views" into the system. For complex systems, it is often desirable to segment the system into manageable parts, and having multiple architectural views allows for the system to be separated into manageable parts for requirements analysis and architectural design, while maintaining the integrity of the overall system, such that the dependencies and system impacts of decisions and changes within view components can be easily communicated and shared.

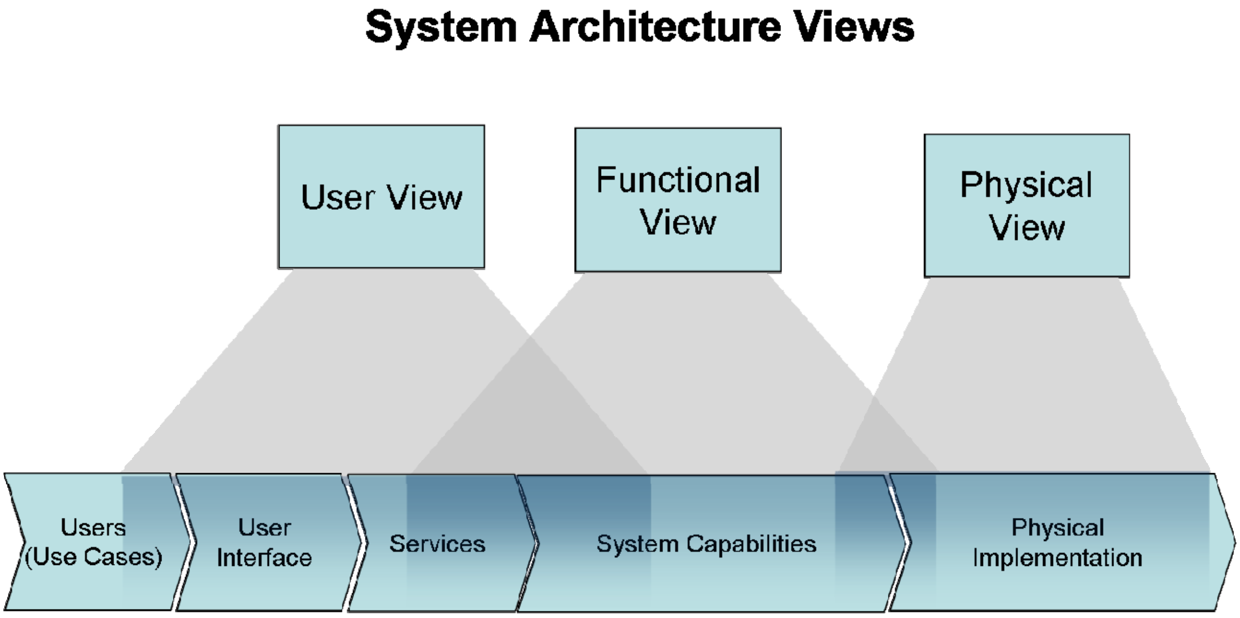


Figure B.1: System architecture views

In MESA, High level user requirements and use cases have been provided (need to cite SoR), the architecture to support those requirements and use cases is under development and is the purpose of the present document.

B.2 User architectural view

The purpose of the User Architectural View is to treat the entire system as a "black box" and focus on the user needs and system interaction. This is accomplished by breaking the system down into a set of "Services" that meet some specified need of the user, and "Interfaces" that provide the mechanism for the user to use those Services. This view is most useful as the mechanism to ensure that the users of the communication system and the designers of the communication system are aligned. Figure B.2 functionally diagrams the users, interfaces and services of a proposed Mesa Communication System.

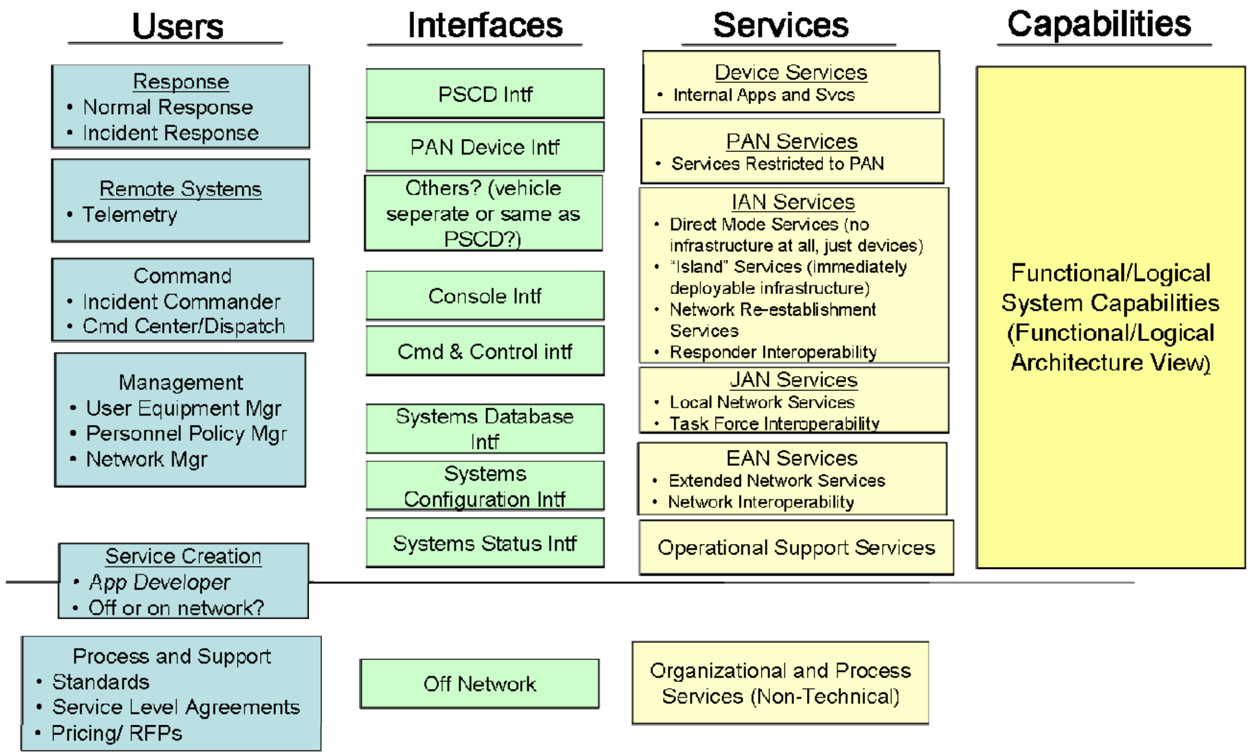

Users
Interfaces
Services
Capabilities
Response
• Normal Response
• Incident Response
Remote Systems
• Telemetry
Command
• Incident Commander
• Cmd Center/Dispatch
Management
• User Equipment Mgr
• Personnel Policy Mgr
• Network Mgr
Service Creation
• App Developer
• Off or on network?
Process and Support
• Standards
• Service Level Agreements
• Pricing/ RFPs
PSCD Intf
PAN Device Intf
Others? (vehicle seperate or same as PSCD?)
Console Intf
Cmd & Control intf
Systems Database Intf
Systems Configuration Intf
Systems Status Intf
Off Network
Device Services
• Internal Apps and Svcs
PAN Services
• Services Restricted to PAN
IAN Services
• Direct Mode Services (no infrastructure at all, just devices)
• "Island" Services (immediately deployable infrastructure)
• Network Re-establishment Services
• Responder Interoperability
JAN Services
• Local Network Services
• Task Force Interoperability
EAN Services
• Extended Network Services
• Network Interoperability
Operational Support Services
Organizational and Process Services (Non-Technical)
Functional/Logical System Capabilities (Functional/Logical Architecture View)

Figure B.2

NOTE: Figure B.2 is not yet a complete architecture. A complete architecture will provide the mapping between users, interfaces and services, as highlighted in the example below. To date, the focus has been on a single type of users (the responder), and the interface that responder uses. Figure B.3 is an initial mapping that needs vetting. If using this approach proves useful, then work can be done to define the details of the interfaces.

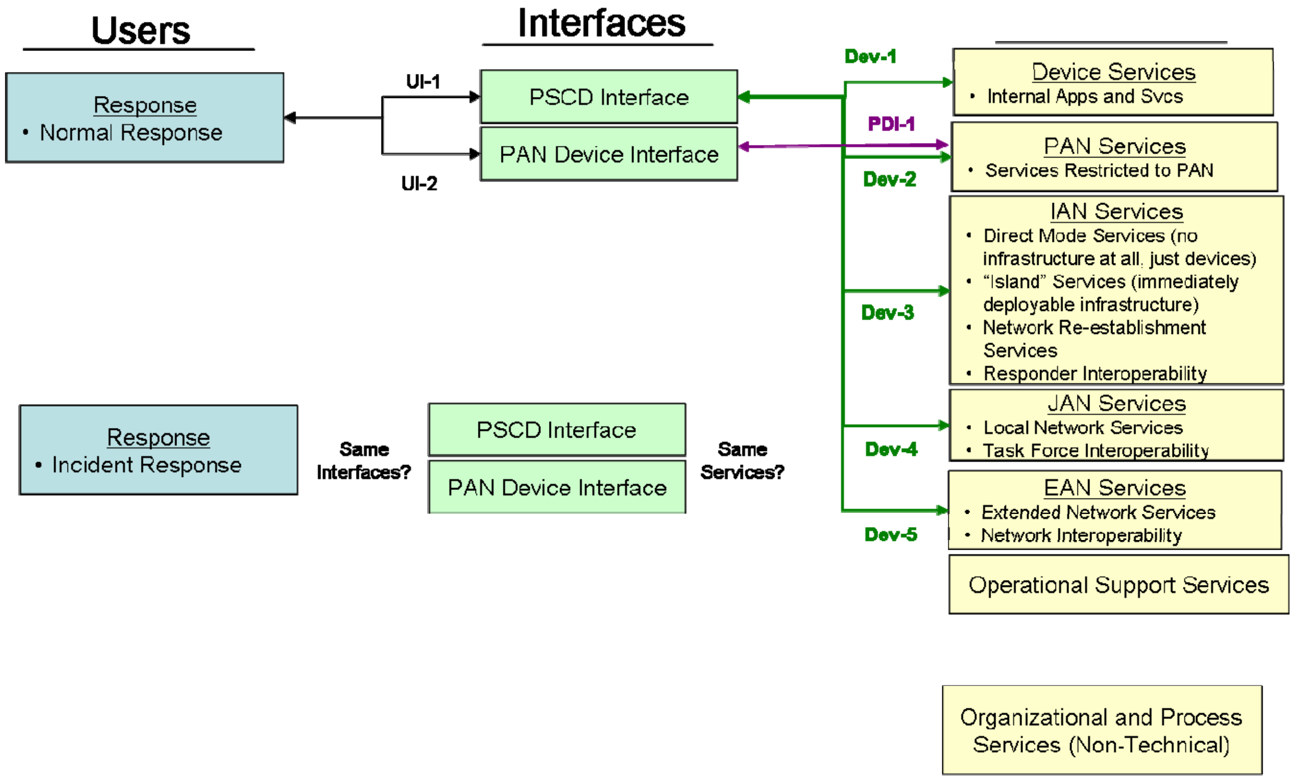

Users
Interfaces
Response
• Normal Response
UI-1
UI-2
PSCD Interface
PAN Device Interface
Dev-1
PDI-1
Dev-2
Dev-3
Dev-4
Dev-5
Device Services
• Internal Apps and Svcs
PAN Services
• Services Restricted to PAN
IAN Services
• Direct Mode Services (no infrastructure at all, just devices)
• "Island" Services (immediately deployable infrastructure)
• Network Re-establishment Services
• Responder Interoperability
JAN Services
• Local Network Services
• Task Force Interoperability
EAN Services
• Extended Network Services
• Network Interoperability
Operational Support Services
Response
• Incident Response
Same Interfaces?
PSCD Interface
PAN Device Interface
Same Services?
Organizational and Process Services (Non-Technical)

Figure B.3

B.3 Functional architectural view

Figure B.4 is a high level view of the Functional Architecture. The system is broken down into those functions that support user services (Logical Service Functions), functions that support the communication network (Logical System Functions), and functions of the Physical implementation of the communication system (Physical Functions).

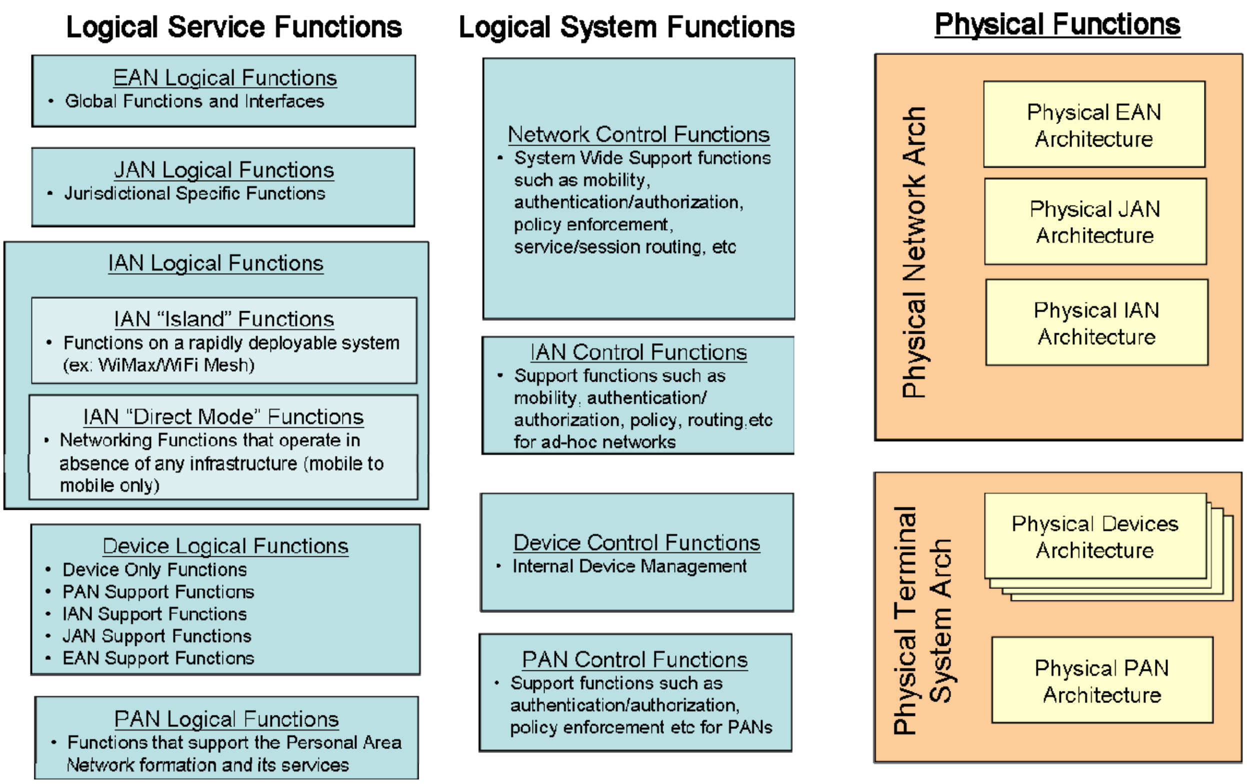

Logical Service Functions
EAN Logical Functions
• Global Functions and Interfaces
JAN Logical Functions
• Jurisdictional Specific Functions
IAN Logical Functions
IAN "Island" Functions
• Functions on a rapidly deployable system (ex: WiMax/WiFi Mesh)
IAN "Direct Mode" Functions
• Networking Functions that operate in absence of any infrastructure (mobile to mobile only)
Device Logical Functions
• Device Only Functions
• PAN Support Functions
• IAN Support Functions
• JAN Support Functions
• EAN Support Functions
PAN Logical Functions
• Functions that support the Personal Area Network formation and its services
Logical System Functions
Network Control Functions
• System Wide Support functions such as mobility, authentication/authorization, policy enforcement, service/session routing, etc
IAN Control Functions
• Support functions such as mobility, authentication/ authorization, policy, routing,etc for ad-hoc networks
Device Control Functions
• Internal Device Management
PAN Control Functions
• Support functions such as authentication/authorization, policy enforcement etc for PANs
Physical Functions
Physical Network Arch
Physical EAN Architecture
Physical JAN Architecture
Physical IAN Architecture
Physical Terminal System Arch
Physical Devices Architecture
Physical PAN Architecture

Figure B.4

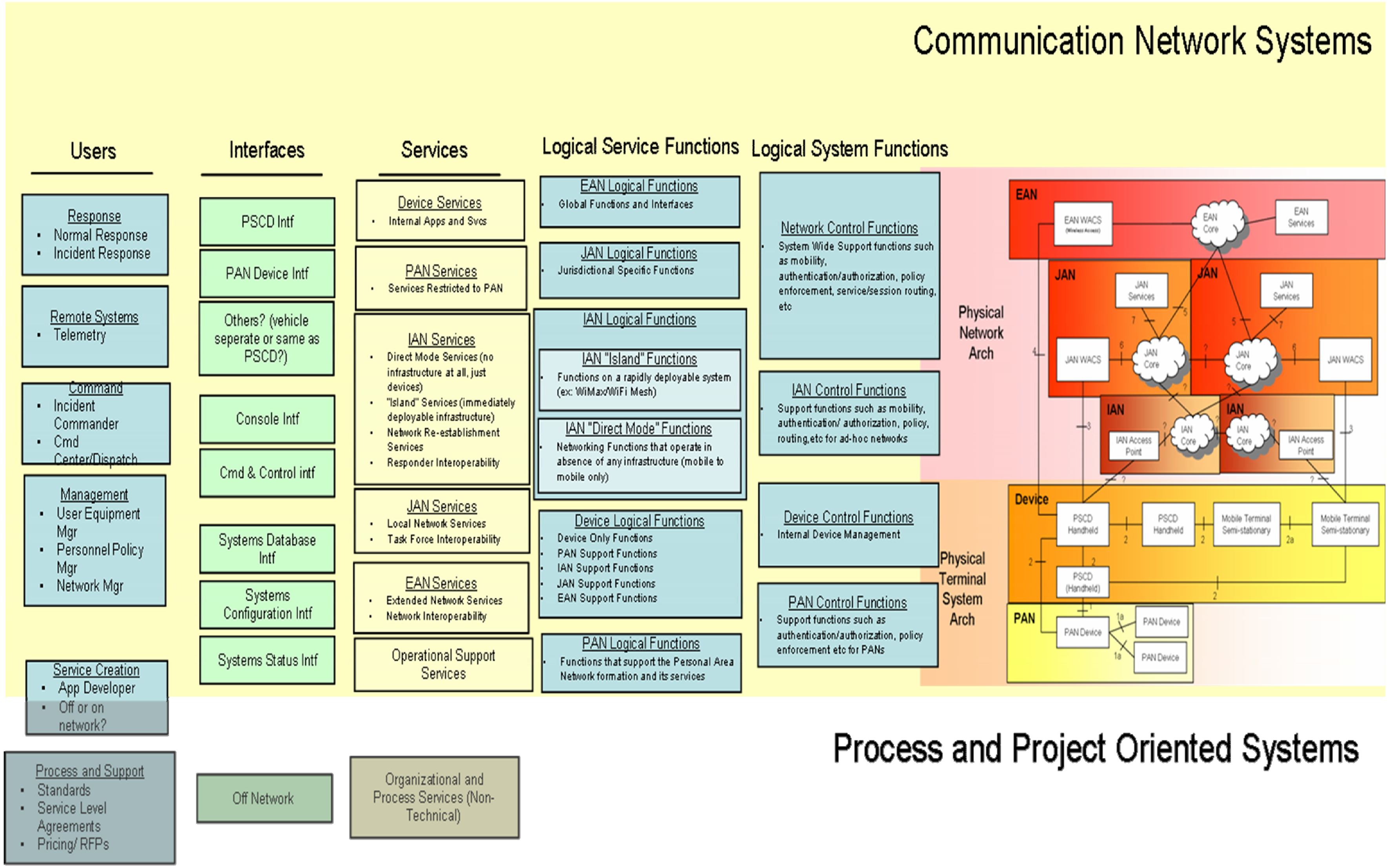
NOTE: The diagram above is not yet a complete architecture. A complete architecture will include the interfaces between functions.

B.4 Physical architectural view

The physical architecture is described in the main portion of the present document.

B.5 Complete architectural view

Figure B.5 provides an illustrative example, at a high level, of how each of the architectural views relate to each other and flow together to form a complete picture of the communication system.



Communication Network Systems

Users

Response
- Normal Response
- Incident Response

Remote Systems
- Telemetry

Command
- Incident Commander
- Cmd Center/Dispatch

Management
- User Equipment Mgr
- Personnel Policy Mgr
- Network Mgr

Service Creation
- App Developer
- Off or on network?

Interfaces

PSCD Intf

PAN Device Intf

Others? (vehicle seperate or same as PSCD?)

Console Intf

Cmd & Control intf

Systems Database Intf

Systems Configuration Intf

Systems Status Intf

Services

Device Services
- Internal Apps and Svcs

PAN Services
- Services Restricted to PAN

IAN Services
- Direct Mode Services (no infrastructure at all, just devices)
- "Island" Services (immediately deployable infrastructure)
- Network Re-establishment Services
- Responder Interoperability

JAN Services
- Local Network Services
- Task Force Interoperability

EAN Services
- Extended Network Services
- Network Interoperability

Operational Support Services

Logical Service Functions

EAN Logical Functions
- Global Functions and Interfaces

JAN Logical Functions
- Jurisdictional Specific Functions

IAN Logical Functions

IAN "Island" Functions
- Functions on a rapidly deployable system (ex: WiMax/WiFi Mesh)

IAN "Direct Mode" Functions
- Networking Functions that operate in absence of any infrastructure (mobile to mobile only)

Device Logical Functions
- Device Only Functions
- PAN Support Functions
- IAN Support Functions
- JAN Support Functions
- EAN Support Functions

PAN Logical Functions
- Functions that support the Personal Area Network formation and its services

Logical System Functions

Network Control Functions
- System Wide Support functions such as mobility, authentication/authorization, policy enforcement, service/session routing, etc

IAN Control Functions
Support functions such as mobility, authentication/ authorization, policy, routing,etc for ad-hoc networks

Device Control Functions
Internal Device Management

PAN Control Functions
- Support functions such as authentication/authorization, policy enforcement etc for PANs

Process and Project Oriented Systems

Process and Support
- Standards
- Service Level Agreements
- Pricing/ RFPs

Off Network

Organizational and Process Services (Non-Technical)

Figure B.5

History

Document history		
V3.1.1	August 2007	Publication