



MODURBAN

FP6 Project: TIP4 – 2005 – 516380

EC Contract n°: 516380

MODCOMM SUBPROJECT

– DELIVERABLE REPORT –

Deliverable ID:	D41
Deliverable Title:	DATA COMMUNICATION SYSTEM ARCHITECTURE
Responsible partner:	THALES
Contributors:	WP9 Partners

PROPRIETARY RIGHTS STATEMENT

This document contains information, which is proprietary to the MODURBAN Consortium. Neither this document nor the information contained herein shall be used, duplicated or communicated by any means to any third party, in whole or in parts, except with prior written consent of the MODURBAN consortium.



Document Information

Document Name: DATA COMMUNICATION SYSTEM ARCHITECTURE
Document ID: D41
Revision: V10
Revision Date: 2009/03/31
Author: WP9 Partners
Security: PUBLIC

Approvals

	Name	Company	Date	Visa
<i>Technical Management Committee</i>	B. VON WULLERSTORFF G. POITRASSON-RIVIERE D. DIMMER G. LEGOFF L. LINDQVIST A.PRICE / U. HENNING M. NOCK JP RICHARD / D. COINEAU Y. AMSLER C. GOUTORBE	UNIFE ALSTOM THALES ANSALDO STS BOMBARDIER SIEMENS KNORR BREMSE RATP UITP ALMA	31/03/2009	OK
<i>Coordinator</i>	B. VON WULLERSTORFF	UNIFE	31/03/2009	OK
<i>Subproject Coordinator</i>	D. DIMMER	THALES	31/03/2009	OK
<i>Quality Manager</i>	B. VON WULLERSTORFF C. GOUTORBE	UNIFE ALMA	31/03/2009	OK

Documents history

Revision	Date	Modification	Author
V0	060208	Table of content proposed by Alcatel	Alcatel
V1A	060213	Updated table of content proposed by WP9 partners	WP9 Partners
V2A	060310	First draft proposed by WP9 partners	WP9 Partners
V3A	060413	Second draft proposed by WP9 partners	WP9 Partners
V3B	060426	Third draft proposed by WP9 partners	WP9 Partners
V4A	060831	Fourth draft proposed by WP9 partners	WP9 Partners
V5A	061003	Fifth draft proposed by WP9 partners	WP9 Partners
V6A	061127	Sixth draft proposed by WP9 partners	WP9 Partners
V7A	061220	Seventh draft proposed by WP9 partners	WP9 Partners
V7B	070104	Version 7B with accepted revision and drawing of section 3.4 modified for editorial purpose	WP9 Partners
V8A	070119	Ninth draft proposed by WP9 partners	WP9 Partners
V9	090227	Glossary updated	RATP
V10	090331	Replaced PXSS with PDIU; removed reference to non-existent D40 coupling value	Thales



SECTION I – DELIVERABLE SUMMARY

DATA COMMUNICATION SYSTEM ARCHITECTURE

Deliverable ID , associated WP & Subproject	<i>D41 MODCOMM / WP9</i>
Type of Deliverable	<i>Reference document</i>
Input / Starting stage	
Output / Final stage	

Lead partner(s)	
Achievement to date (%)	<i>100 %</i>
Expected date of achievement	<i>Month 25</i>
Type of exploitation	<i>input for other MODURBAN WPs</i>
Exploitation potential	
Protection	<i>Not relevant</i>
Protection date	<i>Not relevant</i>

IP's	Partners, (type, identification, date)
Pre-existing Know-How	<i>Not relevant</i>
Exploitation Rights	<i>Not relevant</i>

Associated Risk analysis	Type, solution envisaged, action, actors	Actual Reduction
Before start		
During task implementation		



DATA COMMUNICATION SYSTEM ARCHITECTURE

Deliverable Abstract

The D41 deliverable defines the architecture of the urban transit Data Communication System such that a single communication system can be used in place of the multiple communication systems that are often used in transit systems today.

The architecture emphasis is on fault tolerance in order to ensure an increase in the reliability of communication.

The definition of the DCS architecture take into account the functional, performance, reliability and maintainability requirements specified in earlier tasks.

In the WP9, the D41 document is the end document of the Work Package. It complements the D39 (Data Communication System Functional Requirements) and the D40 (Performance, reliability and maintenance requirements of the urban transit Data Communication System) .

Associated Milestone (if relevant):

Contribution to MODURBAN Objectives as mentioned in the Description of Work		
<i>Objective Definition</i>	<i>Comments</i>	<i>Quantification</i>
Objective 1 -		
Objective 2 –		
Objective 3 ...		
Objective 4 ...		



TABLE OF CONTENT

DOCUMENT INFORMATION 2

APPROVALS 2

DOCUMENTS HISTORY 2

SECTION I – DELIVERABLE SUMMARY 3

SECTION 2 – DELIVERABLE DETAILED DESCRIPTION 6

1. S0 – INTRODUCTION 6

 1.1 Preamble 6

 1.2 Objectives 6

 1.3 References 7

 1.4 Bibliography 7

 1.5 Acronyms 8

 1.6 Definitions 9

2. DCS REFERENCE MODEL 10

 2.1 Introduction 10

 2.2 Reference on-Board configuration 10

 2.3 Reference Guideway configuration 10

 2.4 Reference on-Board application configuration 10

 2.5 Reference wayside application configuration 11

 2.6 Reference DCS application architecture 11

3. DCS DESIGN CONSTRAINTS 14

 3.1 Redundancy constraints 14

 3.1.1 Interface Constraints 14

 3.1.2 Wayside DCS constraints 14

 3.1.3 On-Board DCS constraints 14

 3.2 Train-coupling constraints 15

 3.3 Radio propagation constraints 15

 3.4 Security constraints 16

 3.5 Performance constraints 18

 3.6 Other constraints 18

 3.6.1 Power saving mode 18

 3.6.2 Prioritisation 18

 3.6.3 Level 1 Maintenance 19

4. ARCHITECTURE AND PRINCIPLES 20

 4.1 DCS Architecture 20

 4.1.1 Overall 21

 4.1.2 Wayside or Station to Control Centre 24

 4.1.3 Station Equipment 25

 4.1.4 On-board Equipment 26

 4.1.5 Control Centre Equipment 27

 4.2 Architecture principles 28

5. OPEN POINTS DESCRIPTION 29



SECTION 2 – DELIVERABLE DETAILED DESCRIPTION

1. S0 – INTRODUCTION

1.1 Preamble

This section addresses the objectives of the document, the reference documents, the bibliography, the abbreviations and useful definitions.

1.2 Objectives

According to the description of WP9, this D41 document (« Data Communication System Architecture») has to:

- Define the architecture of the Communication System
- Emphasize fault tolerance
- Take into account the functional, performance, reliability and maintainability requirements specified in earlier tasks

The D41 deliverable defines the architecture of the urban transit Data Communication System such that a single communication system can be used in place of the multiple communication systems that are often used in transit systems today.

The architecture emphasis is on fault tolerance in order to ensure an increase in the reliability of communication.

This document take into account the functional, performance, reliability and maintainability requirements as defined in earlier deliverables of WP9:

- D39. Data Communication System Functional Requirements
- D40. Data Communication System Performance, Reliability and Maintainability Requirements

In the WP9, the D41 document is the end document of the Work Package.

1.3 References

This document is built upon :

- [DOW] Annex I - "Description of Work" DOW-MODURBAN-516380-final.pdf
- [D39] D39 Data Communication System Functional Requirements
- [D40] D40. Data Communication System Performance, Reliability and Maintainability Requirements
- [D77] D77 Common Definition of MODURBAN Train Protection System
MODSYSTEM_WP21_D77_Deliverable report.pdf
- [D81] First MODURBAN prescriptions: overall architecture and allocation of vital functions
- [D9 UGTMS] UGTMS functions and architecture. D9_v1.9 04-06-04.pdf
- [EN 50159-2] Railway applications – Communication, signalling and processing system
Part 2: Safety-related communication in open transmission system
(CEI 62280-2)
- [GL] MODURBAN Glossary. GL-0050_RATP_WP20
- [ISO 7498] Basic reference model for Open System Interconnection (OSI) and its two addenda
about OSI Management & Security

1.4 Bibliography

- [ESCORT, 01] "State of the Art Report" ESCORT - Deliverable D2011- project IST March 2001,
Dr. M. Berbineau & ESCORT WP2 partners
- [CERTU 113, 01] "Communication avec les mobiles: application au trafic et aux transports routiers"
Collections du Certu n° 113, Mars 2001, Y. David, Y. Robin-Jouan, M. Heddebaut
- [ETSI] www.etsi.org - Web site of the European Telecommunication Standards Institute
- [ANFR] www.anfr.fr - Web site of ANFR (Agence Nationale des Fréquences)



1.5 Acronyms

AP	Radio Access Point
ATC	Automatic Train Control
BITE	Built-In Test Equipment
CC	Car borne Controller
COMSEC	COMmunication SECurity: Security at network level (OSI layer 3)
DCS	Data Communications System
DSU	Data Storage Unit
HMI	Human Machine Interface
I	I(nformative)
IL	Interlocking
IPSec	Internet Protocol Security
LAN	Local Area Network
LRU	Line Replaceable Unit
MMS	Maintenance Management System
MR	Mobile Radio
NMS	Network Management System
NWK	Network
OCC	Operations Control Centre
OIS	On-Board passenger Information System
OTAR	Over The Air Rekeying
PDIU	Platform Door Interface Unit
PSTN	Public Switched Telephone Network
R	Requirement (of a function)
RADIUS	Remote Authentication Dial-in User Service
SCADA	Supervision, Control And Data Acquisition
SG	Security Gateway
TRANSEC	TRANsmission SECurity: Security at transmission level (OSI layer 2)
WIS	Wayside passenger Information System
WR	Wayside Radio
ZC	Zone Controller



1.6 Definitions

DCS user	DCS user includes mobile users and fixed users.
Fixed user	User of the DCS wired to the wayside network. The user can be a human through a device or just a device.
Line Replaceable Unit	The Line Replaceable Unit is the units of each sub-system which are replaced for the Maintenance Level 1
Mobile user	User of the DCS linked to the wayside network through a wireless link. The user can be a human through a device or just a device. He can be part of a mobile network (Indirect Mobile User such as a device connected to the train network) or be directly wireless linked to the DCS (Direct Mobile User).
Nominal	Intended value about which there may be statistical variation.
Quality of Service of communication (QoS)	The quality of the communication service provided in terms of guaranteed throughput, jitter, latency and packet loss.
Scalability	Scalability is the possibility to expand a line by adding equipment of the kind already in use
Security Gateway	From a DCS user point of view, SG is a secure router at layer 3 even if some kind of standard or specific high layer protocols is embedded into SG to enforce end-to-end security
Train set	The minimum part of a train that can be operated separately.

2. DCS REFERENCE MODEL

2.1 Introduction

This section describes the reference model used to define the architecture of the DCS and especially the reference DCS application architecture. This reference model also includes a synthesis of the parameters applicable to the DCS and related to its urban transit environment.

2.2 Reference on-Board configuration

This section summarizes the main on-board configuration parameters which can impact the architecture of the DCS.

- Train set configuration
 - a) single train set
 - b) 2 coupled train sets
 - c) more than 2 coupled train sets

It implies some constraints on the on-board radio.

2.3 Reference Guideway configuration

This section summarizes the main guideway configuration parameters which can impact the architecture of the DCS.

- Single or double tunnel may impact the choice of APs
- Aerial or tunnel has an impact on the DCS architecture as the propagation differ.
- Number of stations has a dimensioning impact on the DCS architecture.
- Length of inter stations has an impact on the number and the localisation of AP. Operators rather have easily accessible AP for maintenance purposes.
- Junction between lines. Some interference could occur.
- Guideway train Density is dimensioning in terms of throughput and number of APs as their capacity can be limited to a certain number of subscribers.
- Number of trains per parking areas. It is dimensioning in terms of throughput and number of APs as their capacity can be limited to a certain number of subscribers.

2.4 Reference on-Board application configuration

This section summarizes the on-board application configuration parameters which can impact the architecture of the DCS.

- Driver or driverless. It impacts the DCS architecture as long as some applications become vital.
- On-Board video devices. It is dimensioning for the DCS architecture in terms of throughput and number of connections.
- On-Board audio devices. It is dimensioning for the DCS architecture in terms of throughput and number of connections.

2.5 Reference wayside application configuration

This section summarizes the wayside application configuration parameters which can impact the architecture of the DCS.

- Wayside video devices. It is dimensioning for the DCS architecture in terms of throughput and number of connections.
- Wayside audio devices. It is dimensioning for the DCS architecture in terms of throughput and number of connections.

2.6 Reference DCS application architecture

This section describes the architecture of the DCS environment and more specifically the architecture of the non-ATC equipment such as video and audio which is not described in other high level MODURBAN documents.

This reference application architecture is used only as the basis to define the DCS architecture. In practice, the real physical location of equipment is likely to differ from one operator to the other, and the final design of the DCS will have to be adapted accordingly.

A) General DCS application reference architecture

The figure below for the General DCS application reference architecture is the most complete architecture which includes ZC, IL and PDIU in every station and coupled train consists.

It shows a possible split between applications which will have mainly local communications (inside OCC or inside station for example) or mainly external communications (from station to OCC for example). If necessary, the DCS design can use this kind of split to separate the local communications from the external ones and therefore to decrease the maximum necessary throughput in each sub-network, but local and external sub-networks remain interconnected.

The OCC box in the figure includes the Clock, the SCADA and the elements of the WIS and the OIS which are located in the Control Centre.

In a real system, ZC, IL and PDIU will be included only in those stations where the signalling system requires it.

The Station Control Centre is the local HMI for equipment in station.

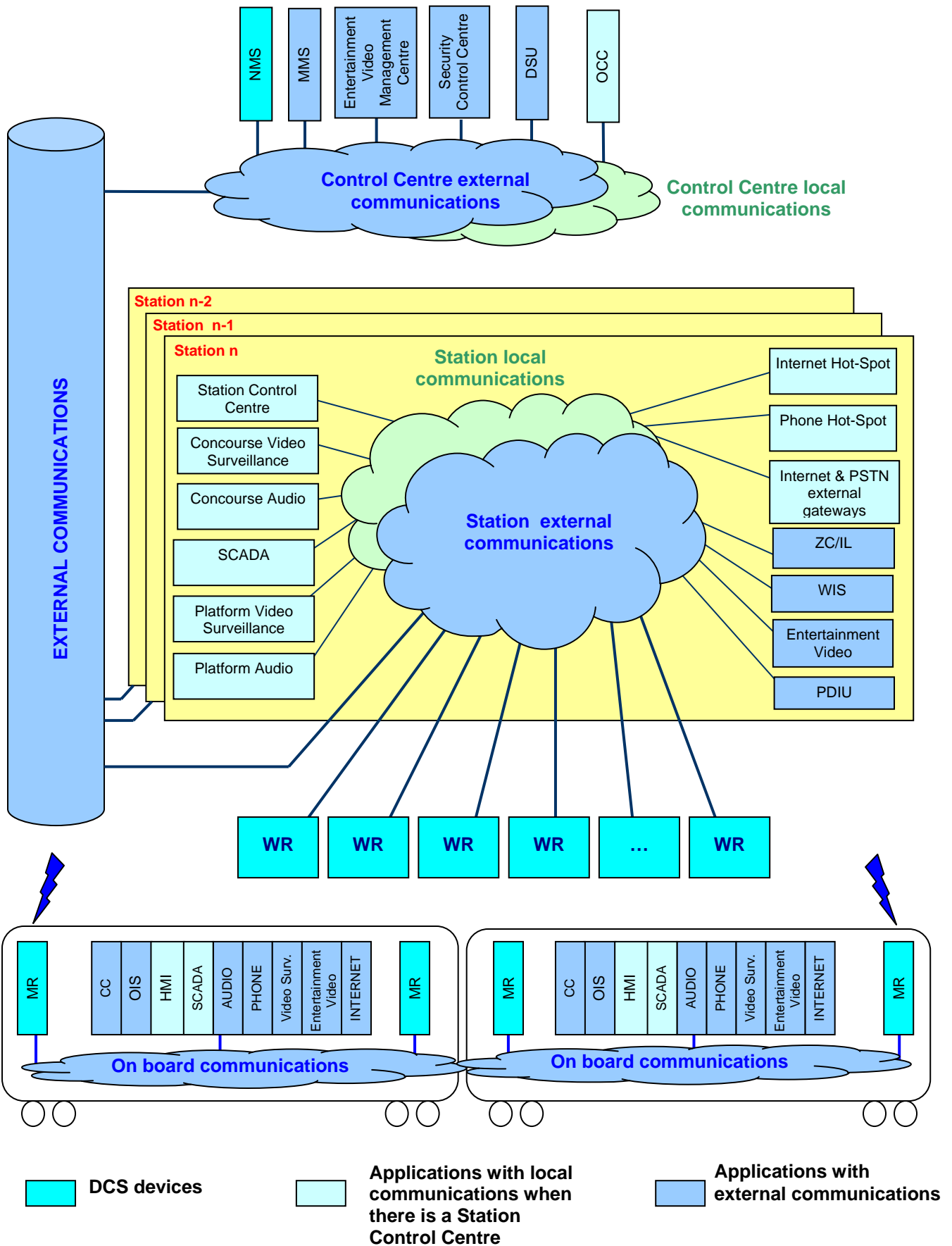
Audio in stations and trains includes Emergency calls, answers to Emergency calls and Public Address.

Entertainment includes also Infotainment.

The Security Control Centre includes Video Security Management and Audio Security Management.

SCADA in stations provides interface to equipment such as fans, lights, power supplies, escalators, etc.

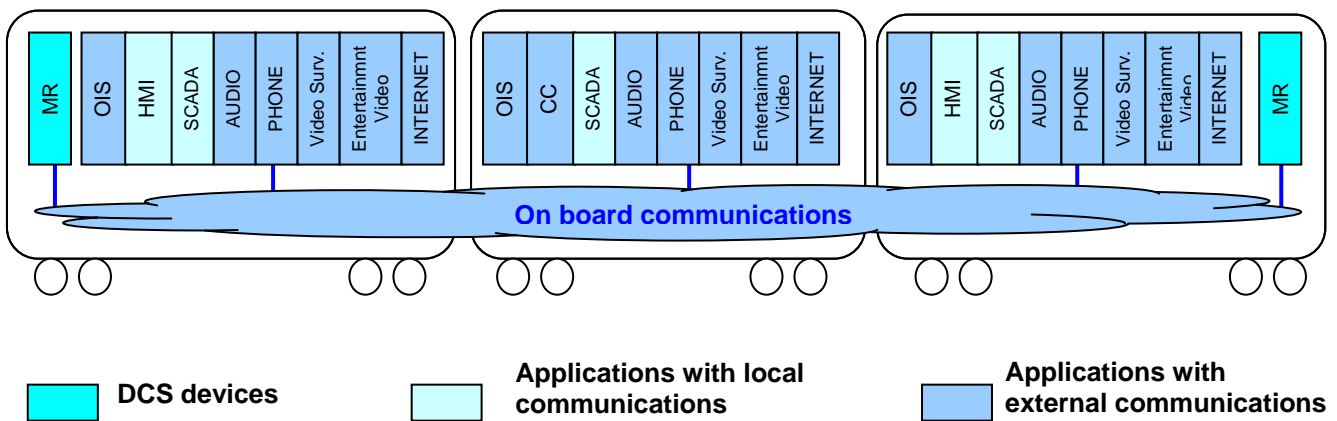
In the following diagram, the mobile radios are drawn only at each train extremity, however it is not compulsory to have only this location for the radios.



Other architectures are possible with the external phone and Internet gateway located only in one or a few stations, or at the OCC. This would have the benefit to concentrate in one point the protection to the external world and to decrease the number of such equipment, but will increase the throughput needed on the wayside backbone.

B) On-Board DCS application reference architecture

The on-board DCS application reference architecture in this section is related to a single train set. The case of coupled trains is provided in the General DCS application reference architecture section.



3. DCS DESIGN CONSTRAINTS

3.1 Redundancy constraints

- R01 The DCS architecture shall include sufficient internal equipment and connection redundancy to meet the availability requirements.
- R02 Any change of availability level shall be reported to the NMS and MMS.
- R03 Availability level shall be automatically restored upon failure rectification.

3.1.1 Interface Constraints

This section describes constraints related to the connection of redundant equipment to the DCS.

- R01 The use of redundant logical communication channels at the application level (i.e. layers above DCS layers) is fully transparent to the DCS.
- R02 To offer increased availability to the applications requiring it, the DCS shall provide at least 2 separate physical ports reducing common mode of failure in the related communication paths and such that the joint availability meets the requirements of the D40.

3.1.2 Wayside DCS constraints

This section describes specific redundancy related constraints for the wayside DCS.

- R01 The DCS architecture shall be such that when a failure occurs in a redundant section of the DCS, the reconfiguration time will not exceed the value defined in the D40 document.
- R02 When redundancy mechanisms are applied, they shall not introduce a modification of the addressing plan which has been designed to cover redundancy case.

3.1.3 On-Board DCS constraints

This section describes specific redundancy related constraints for the on-board DCS.

- R01 The DCS architecture shall be such that when a failure occurs in a redundant section of the DCS, the reconfiguration time will not exceed the value defined in the D40 document.
- R02 When redundancy mechanisms are applied, they shall not introduce a modification of the addressing plan which has been designed to cover redundancy case.
- R03 As a minimum the DCS shall provide independent radio links, for instance at each end of a train set.

3.2 Train-coupling constraints

This section describe constraints on the DCS resulting from train coupling.

- I01 After the train coupling, the radios located at the coupled extremities may not be transmitting properly. It is therefore necessary to couple the train networks.
- I02 The coupling of train networks can be achieved either by a wired physical connection of the 2 networks or by a radio connection.
- R01 In case the communications between coupled trains are ensured through a radio connection, the DCS shall prevent communication with other trains.
- I03 After train coupling, the overall train network can be either a single sub-network or the combination of 2 connected sub-networks
- R02 If a reconfiguration of DCS (onboard and/or wayside part) is necessary following train coupling, mechanisms applied shall not create a transmission outage of such duration that system operation is impacted.
- R03 Functionality, guaranteed Quality of Service and guaranteed performance of the DCS shall be independent of the train coupling status.
- R04 If a reconfiguration of DCS (onboard and/or wayside part) is necessary following train coupling, Start and End of reconfiguration status shall be reported to NMS and MMS.
- R05 If a reconfiguration of DCS (onboard and/or wayside part) is necessary following train coupling, mechanisms applied shall manage this sequence without any data provided by end users application.
- R06 If a reconfiguration of DCS (onboard and/or wayside part) is necessary following train coupling, mechanisms applied shall not change the addresses used by the end users application.
- I04 Following train coupling, the coupling of the 2 on-board networks in a single network can result in an overall throughput which will be the sum of the throughput of each of the 2 on-board network.
- R07 If necessary, the DCS design should reduce the effect of increased network load due to train coupling, for example, by restricting the communications between the two coupled networks. In that way, the traffic will remain as local as possible.
- R08 If needed, the DCS shall determine if the train has been coupled either by an external information/wiring or by internal means.

3.3 Radio propagation constraints

This section describes radio propagation constraints such as the track environment (tunnel, open air, monotube, bitube, parking area, curves...), and the presence of blocking trains (front, side...), and their effect on the distance between two wayside radio access point.

- I01: For network planning, the coverage level is defined in terms of time and area where the minimum signal criteria are achieved.

I02: Railway environment means here one of cases which could be encountered; that includes the track environment (tunnel, open air, monotube, bitube, parking area, curves...), the presence or not of blocking trains (front, side...) between the wayside and the on-board radios.

R01: DCS shall assume a continuous bi-directional communication radio link for the complete length of track in any railway environments.

R02: The level of radio coverage shall guarantee a minimum signal value in time and area that allow DCS to perform communications or transmissions of data. The minimum value is to be defined according to specific customer requirements.

R03: The ground radio equipment of the system shall provide communications for mobiles when stationary and when travelling at speeds up to the maximum allowable line speed (metro or guided transports)

R04: DCS shall take into account transition of a train from a network or cell to another without affecting calls or data transfers in every railway environment and conditions previously described in this section ; DCS shall also provide a high channel resistance to jamming.

3.4 Security constraints

This section describes security-related constraints such as:

- dedicated physical secured links
- protection of the DCS at the border of the DCS or at the level of the radio
- centralized security management system

Security – but not safety– must be considered at network level. Safety can be considered only at upper OSI layer or application level.

Regarding security, the only services required from the DCS are (for open Networks):

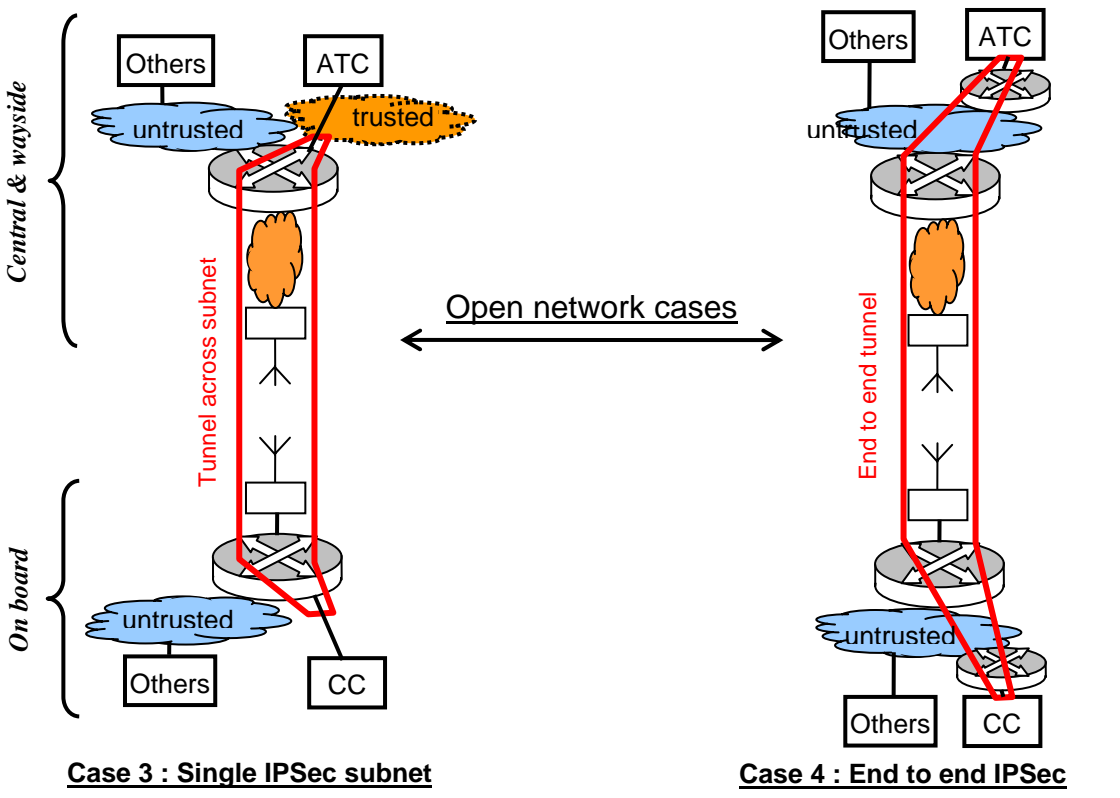
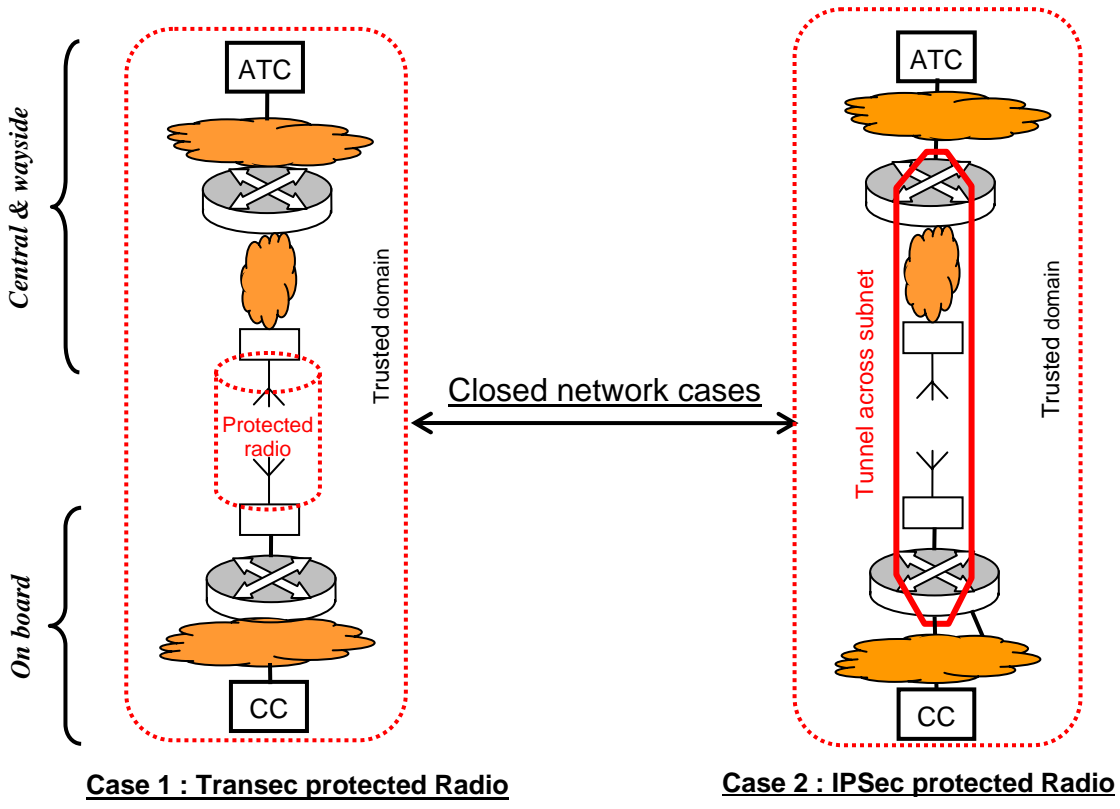
- Authentication, against emulation and masquerading
- Protection against eavesdropping
- Protection against denial of service (from repetition to flooding).

In order to support any kind of services and any users, the DCS has to be considered as an open system as defined in CENELEC EN 50159-2. However, if only limited critical set of services are provided, the DCS can be considered as a closed network if the radio link is sufficiently protected.

If the border of the network is vulnerable, security must be enforced from end to end of the DCS or between trusted subnets associated to each end, selectively for critical application servers and clients.

If the border of the network is not vulnerable, security of the radio path may be provided by one of the following:

- a) the radio data link layer, as TRANSEC (see case 1 in the drawing)
- b) the network layer, as COMSEC i.e. IPsec :
 - for a sub-network which encompasses the radio path (see case 2 in the drawing)
 - from end to end of the DCS (see case 4 in the drawing) or between trusted subnets associated to each end (see case 3 in the drawing), selectively for critical application servers and clients



is a router

For simple architecture (see case 3 in the drawing), it is enough to have a single IPSec subnet if the critical applications are connected to this subnet through a direct link or a trusted subnet.

For more complex architecture (see case 4 in the drawing) involving cascaded trusted/un-trusted subnets, the DCS must still provide a global IPSec tunnel between extremities trusted subnets. The security gateways of this global IPSec tunnel must be located in each direction at the first transition from a trusted subnet to an un-trusted subnet.

- R01 For critical applications, the DCS shall provide dedicated secured links.
- R02 If there is a security protection at the network level, authentication must be provided according to IPSec (RADIUS service) or an equivalent level.
- R03 With a closed system dedicated to critical applications, the radio links must be protected either directly by TRANSEC (e.g. specific waveform and scrambling process) or compartmented into an IPSec sub-network (using encryption with secret keys).
- R04 If the border of the network is vulnerable, IPSec using encryption with secret keys must be provided from end to end of the DCS to critical applications which need for it.
- R05 The security services must be managed from a central platform providing key management, periodical renewal, and over the air rekeying (OTAR) if necessary. This central platform must be connected on a trusted part of the ground network, e.g. the same trusted subnet as OCC.
- R06 The technical solutions for security must be coherent with an operational security policy (see D42).

3.5 Performance constraints

This section describes additional performance related constraints.

- R01 DCS shall meet all performances requirements regardless of external parameters, such as train position on the line
- R02 DCS shall be able to support nominal performances under any conditions. If necessary, parallel data routes could be used to carry the traffic

3.6 Other constraints

3.6.1 Power saving mode

- R01 If power saving mode is applied on some DCS devices, the DCS architecture shall always provide a path through fully powered devices to transmit the wake-up order.

3.6.2 Prioritisation

No constraints found on the architecture for the prioritisation.

3.6.3 Level 1 Maintenance

This section describes constraints related to level 1 maintenance.

- R01 It is recommended to locate the WR on station platforms, in order to make the access easier. Only a small number of WR should be located in tunnels between stations.
- R02 On the trains, there should be a specific attention to provide an easy access to communication units.
- R03 Every unit should have a built-in test (BITE).



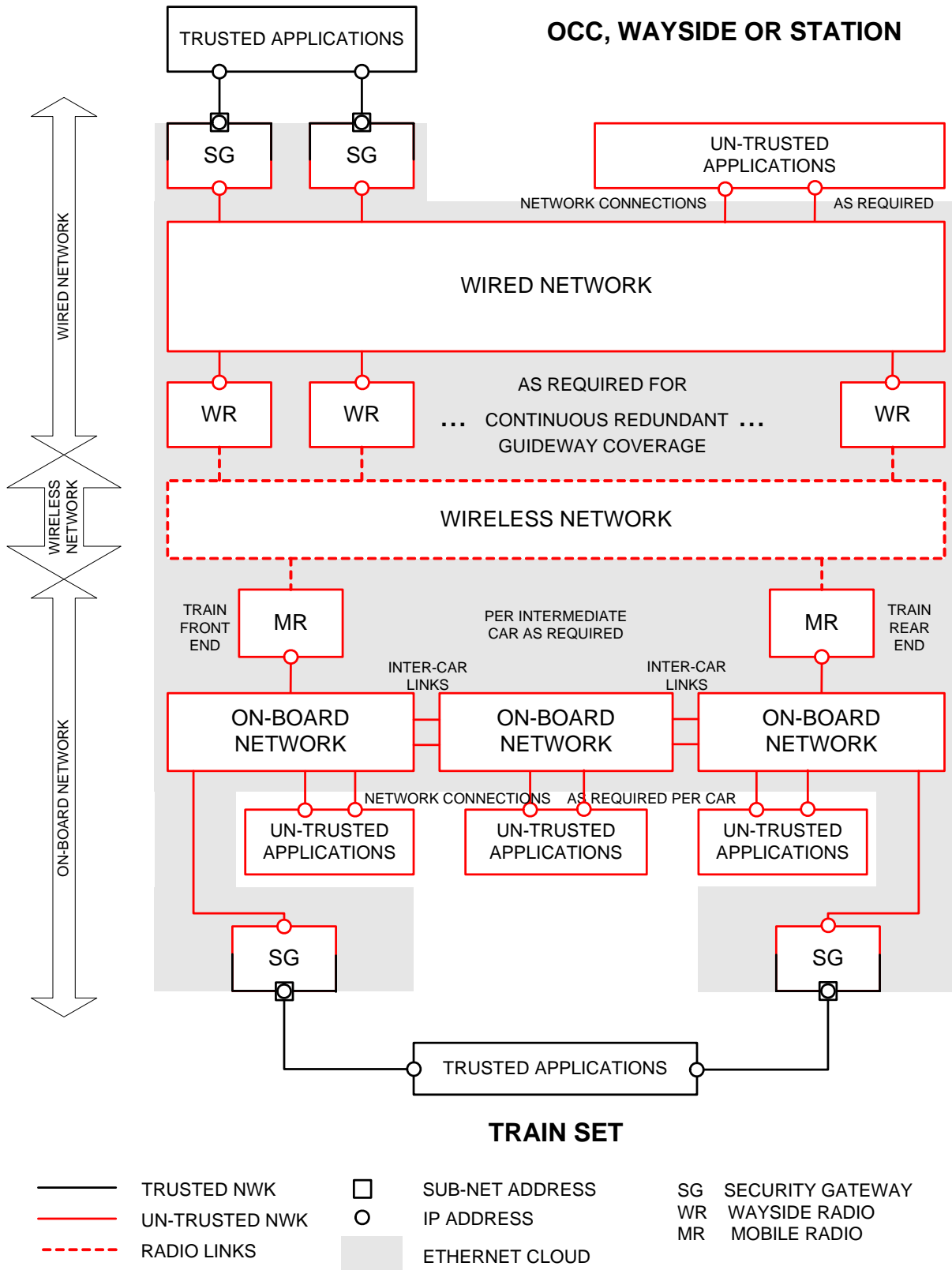
4. ARCHITECTURE AND PRINCIPLES

4.1 DCS Architecture

This section describes the DCS Architecture. This includes the overall architecture and the specific architectures between wayside/station and control centre and for station, on-board and control centre.

The overall architecture shall provide a highly reliable DCS network that takes into account functional, performance, reliability and maintainability requirements previously defined in earlier MODCOMM deliverables.

4.1.1 Overall



In order for application to make connections to the DCS, it is necessary to identify and separate those communications links requiring authentication from those that do not require it. The former are trusted links between pairs of trusted application equipment or application LANs. The later are un-trusted links comprising multiple inter-connection links between un-trusted application equipment.

For trusted applications:

- the data transmitted between trusted applications are all at the same security level,
- there is no multi-level classification of data,
- the network management shall be under the control of security management.

Trusted applications are connected through security gateways (SG). Because of the nature of authentication protocols using separate cipher keys for each link, the trusted links must occur between discrete pairs of trusted application equipment, and therefore only uni-cast packets are allowed to and from trusted equipment.

Un-trusted equipment may be connected anywhere at the edge of the network (but not through a SG). Uni-cast, multi-cast and broadcast packets are allowed to and from un-trusted equipment.

An inviolate rule is that trusted equipment can never communicate with un-trusted equipment over the DCS. In the diagrams un-trusted equipment and networks are shown in red, and trusted equipment is shown in black. The rule is equivalent to stating that a red line can never attach to a black line except through a SG.

Equipment collocated in the same physically secure area can share the same trusted network.

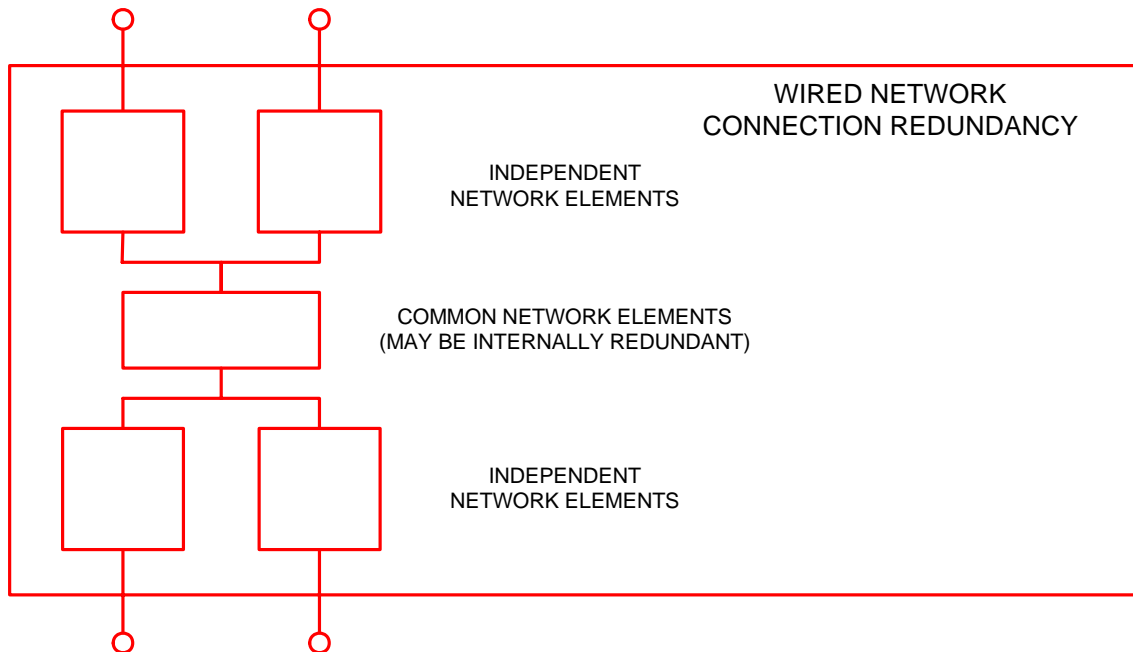
The trusted side of each SG is shown as having a separate sub-net address. This is not essential but is very convenient for redundancy management, for example by routing communications via specific radios.

It is recommended to have at least 2 radio links operating per train consist.

The previous diagram is implying connection of all on-board devices on the same un-trusted network for the whole train with potentially local trusted network per car. Alternatively, if separate trusted is available, then it is considered to be included within the trusted applications.

4.1.1.1 Wired Network

There are many ways to implement the wired network in order to provide improved reliability. One way is to implement completely independent transmission paths for each of the two connections. Another way is to provide partly independent transmission paths, as shown in the following diagram, with some independent element and some common network elements.



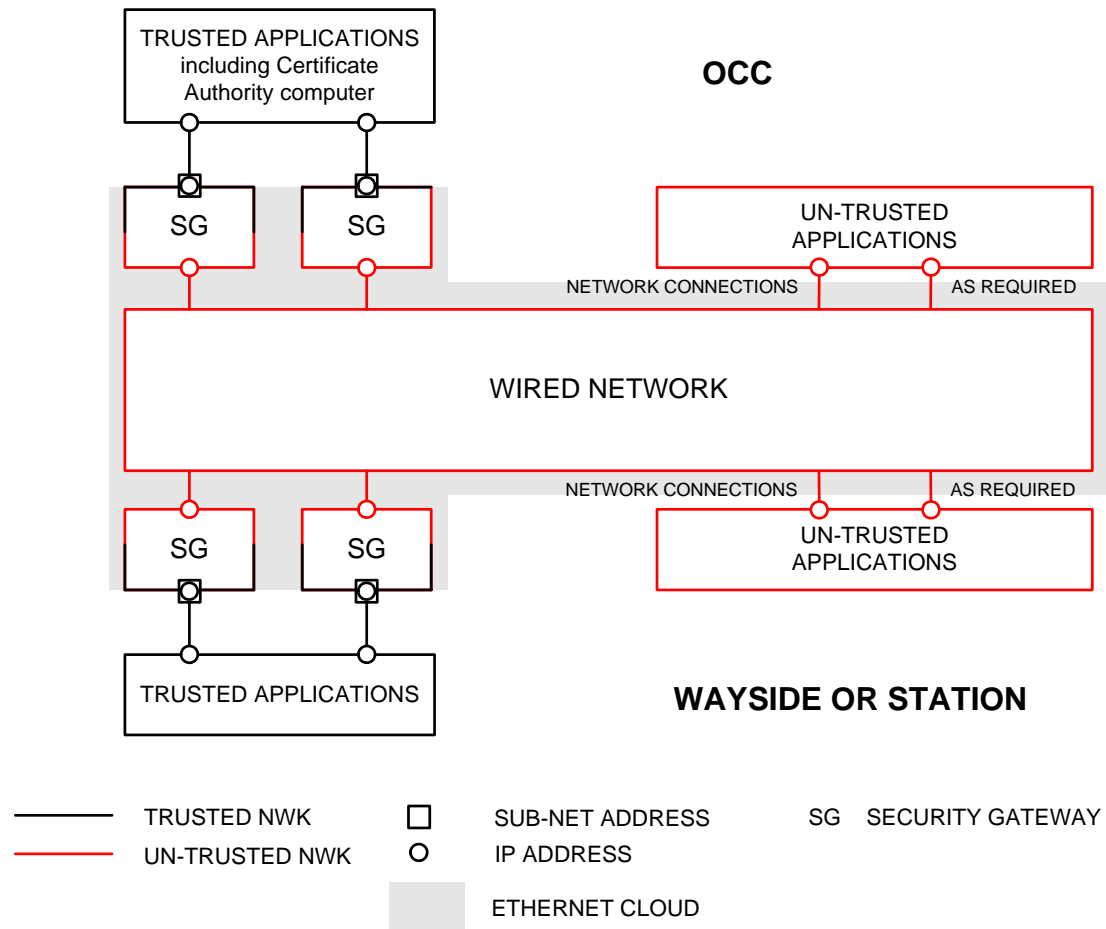
4.1.1.2 Wireless Network

It is not necessary to specify any details about the wireless network between the wayside and on-board networks because it doesn't include any additional device (only radio links).

4.1.1.3 On-board Network

The on-board network shows redundant radio connectivity by having a radio at each end of the train, and shows connectivity between separate train sets (inter-car links). Furthermore, this connectivity is redundant. It is also possible to have trusted connections, via additional SGs, in the middle cars of a train (not illustrated). Beyond this, it is not necessary to specify any details about the on-board network because it can be implemented in a number of different ways.

4.1.2 Wayside or Station to Control Centre

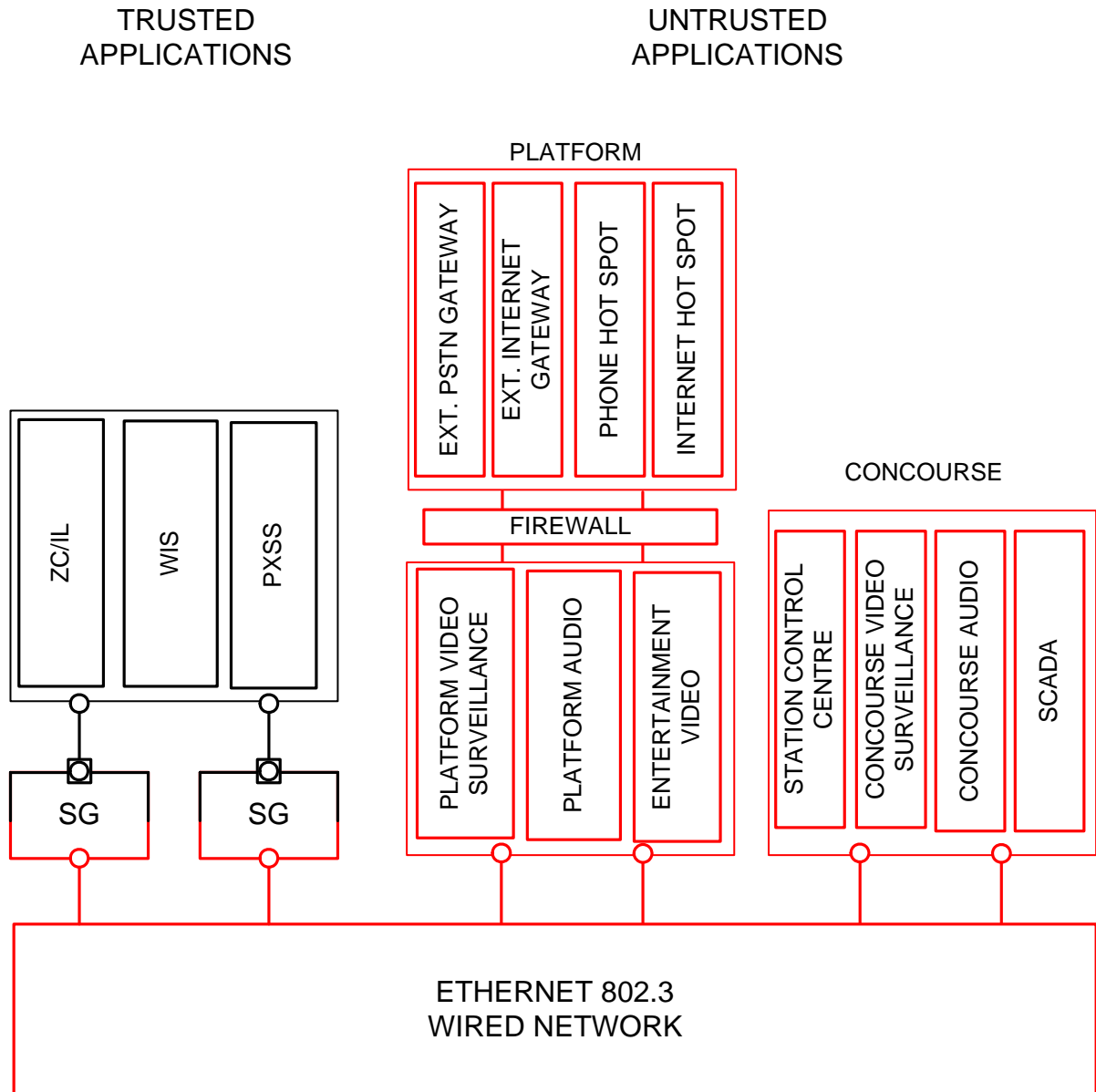


Communications between wayside or station to control centre work entirely over the wired portion of the network.

The same rule for trusted and un-trusted equipment than in section 4.1.1 apply.

4.1.3 Station Equipment

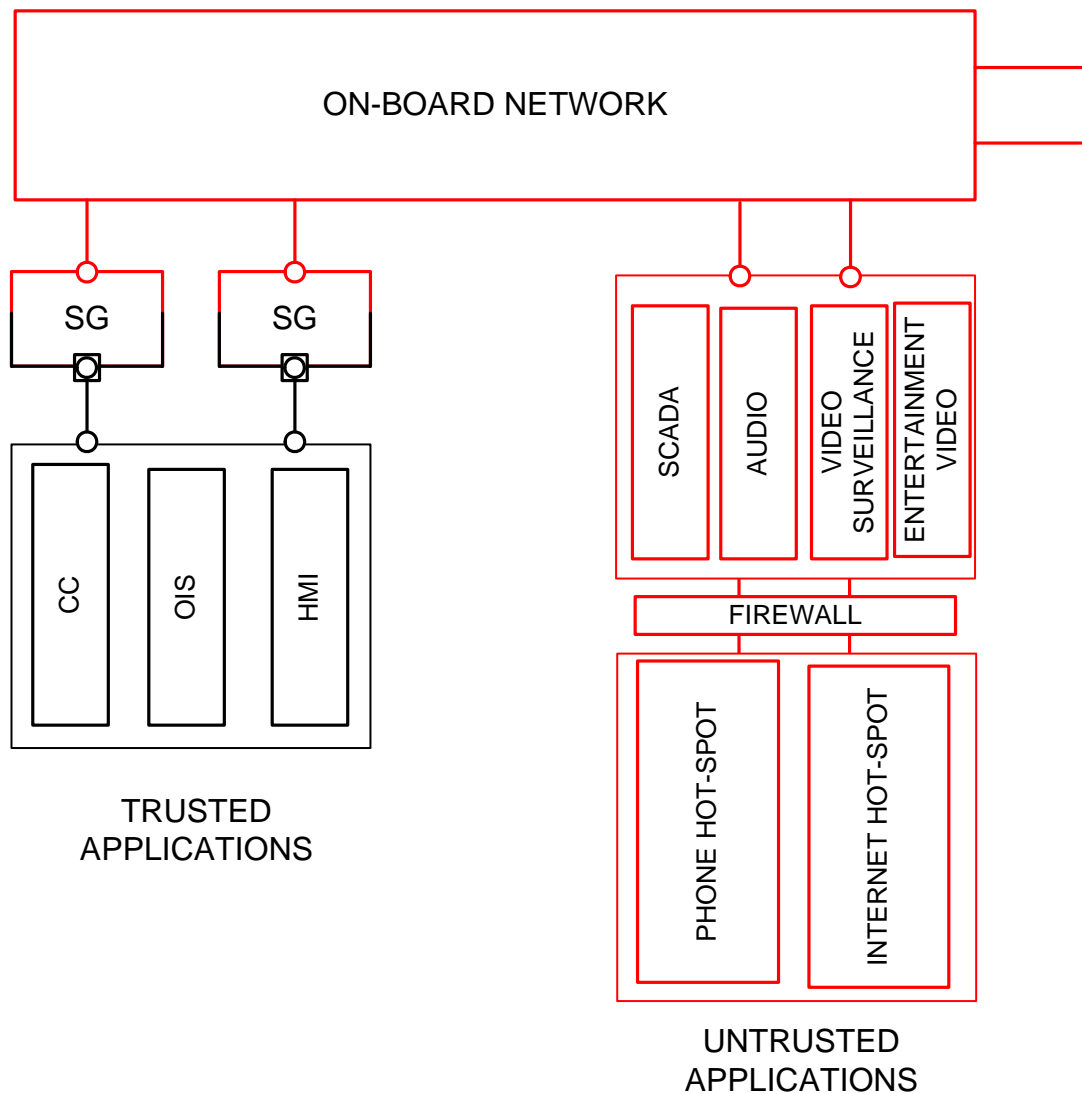
STATION EQUIPMENT



The application equipment that may be used at a station, as listed in section 2.2.5, is categorized into trusted and un-trusted components.

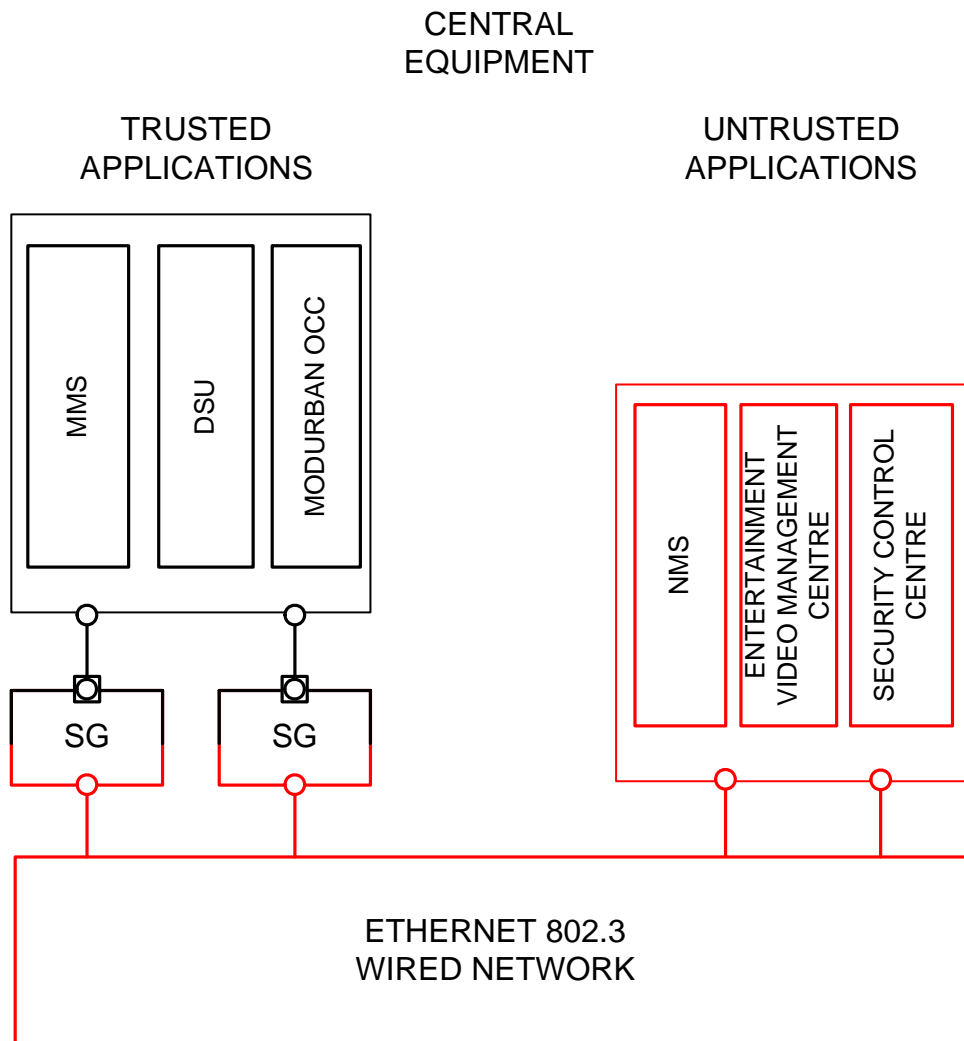
Two or more stations may share the same pair of SG devices.

4.1.4 On-board Equipment



The application equipment that may be used at a station, as shown in section 2.2.5, is categorized into trusted and un-trusted components.

4.1.5 Control Centre Equipment



The application equipment that may be used at a station, as shown in section 2.2.5, is categorized into trusted and un-trusted components.

4.2 Architecture principles

This section gives the architecture principles that are applicable to a MODURBAN DCS.

The main general principles coming from the DCS design constraints analysis are the following :

- The DCS is able to offer increased availability to the applications requiring it, by providing separate physical ports reducing common mode of failure in the related communication paths.
- The DCS provides its functionalities, guaranteed quality of service and guaranteed performance for both coupled or uncoupled trains.
- The DCS radio layout ensures on the complete length of the track, the reception of the minimum signal necessary to provide the required throughput.
- The DCS provides dedicated physical secured links in addition of its basic unsecured links.
- If security services such as key management and periodical renewal, or over the air rekeying (OTAR) are necessary, they are managed from a central platform.

The other principles applicable to the DCS are the following :

- scalability from a small line, to a big line, to several lines
- spectrum efficiency,
- geographic reuse of the resource
- Maximum coverage between WR shall be defined such that the required on-board to wayside throughput is available anywhere between MR and WR
- DCS doesn't prevent to use a variable bit rate
- division of the DCS into sub-networks, at least for train, and for stations



5. OPEN POINTS DESCRIPTION

The description of the D41 Open Points is provided in this section with their relationship to other open points.

Open Point	Description	Links
	No Open Point for the D41 document.	