

5.6.3.2 FDFT Link Gateway

5.6.3.2.1 Basic design and hardware

A physical Mobile Communications Gateway (MCG) shall be implemented on each consist (see /WP3 D3.2/). The support of redundant implementation of MCGs on a consist is not required.

The redundancy functionality between MCGs in a train is not required.

The concept of Train to ground communications shall follow IEC 61375-2-6. If there are options in this normative, either a recommendation or a decision on the way to follow the normative is given in this document.

The MCG shall allow to communicate with other devices in the consist using the Ethernet Consist network (ECN).

The GNSS module shall support the output of the protocol GNSS NMEA (at least version 4.0 shall be supported).

The specific data that shall be provided by the GNSS module to a user (CCU) isn't yet defined and needs to be specified by WP5 (train functions).

Description	Reference to IEC 61375	Justification / Rationale
A Mobile Communications Gateway (MCG) shall be implemented on each consist to provide FDFT Link functionality.		To provide the functionality of the Wireless FDFT-Link, a physical FDFT-Link Gateway shall be provided. It shall be called Mobile Communications Gateway (MCG).
The MCG sub-system shall meet the elements shown in IEC 61375-2-6, chapter 4.4.3, table 3.		
The MCG shall be able to negotiate the power class acc. to (IEEE 802.3af) with the network port of the Ethernet Train Backbone Node (F-ETBN).		In case the device is physically a separate device, it shall support the protocol acc. to 802.3af as a so-called

		powered device (PD).
The MCG shall support the VLAN tagging acc. to IEEE 802.1q for communications with device being connected to the ECN (Ethernet Consist Network) for in consist communications.		VLANs are used to separate communication profiles.
For Train to ground communication the requirements shown in IEC 61375-2-6, chapter 4.2, table 1 shall be met. Exceptions to table 1 are noted in the reference to this requirement.	<X1>	
No redundancy through another MCG located on another consist in the same train shall be considered, as mentioned in IEC 61375-2-6, chapter 4.2, table 1, row 6.	As a reference see <X1>	IEC 61375-2-6 chapter 4.2, table 1, row 6 states a redundancy option using a MCG located in another consist.
Multiple MCGs shall not be considered as mentioned in IEC 61375-2-6, chapter 4.2, table 1, row 5.	As a reference see <X1>	IEC 61375-2-6, chapter 4.2, table 1, row 5 states a redundancy option, which is not required. MCG is neither required for redundancy nor for load balancing as most other components are not redundant either. To save costs.
A trusted platform module (TPM) that is included in the MCG hardware shall be used to securely store authentication keys.		
The TPM technology shall support at least TPM 2.0.		

5.5.4.3.2 FDFT Link Mobile Communication

The MCG shall support the protocols to allow connectivity via Public Mobile Communications Network or Wireless LAN (bearers) to wayside systems, herein referred

as Ground Communications Gateway (GCG) and Wayside Communications Gateway (WCG), to provide connectivity to FDFT Backend systems.

The MCG shall meet all the requirements from bearers.

The MCG shall support the functionality to select a specific mobile network selector service to always manage the active communication channel when more mobile communication network options are available.

The services provided by the MCG shall be always available to the FTFD backend systems via the FDFT link, therefore the FDFT Link shall be available at any time.

The Train Wake-up shall be implemented to ensure communications and wake up at any time. The protocol to support this functionality shall be as defined in IEC 61375-2-3:2024 chapter 6.9 "Wake-up" Option

Description	Justification / Rationale
For the MCG a public cellular network (mobile network) shall be used to provide the data connection (bearer).	
A Wireless LAN (Wi-Fi network) shall be supported as addition to public cellular network (bearer).	
Wireless LAN shall be implemented according to standard IEEE 802.11.	2.4 GHz frequency as general option
The MCG shall only act as Wi-Fi Client in a Wireless LAN environment.	
The MCG shall <u>not</u> use wireless communication standards for railway communication and applications (GSM-R / LTE-R) .	MCG uses solely public mobile network or Wireless LAN instead.
The public cellular network technology shall be state-of-the-art.	Currently, this would mean LTE (4G, 4th generation) as a minimum requirement for cellular network.

	For future use 5G and evolving technologies shall be considered.
A substandard offering machine-to-machine (M2M) communication shall be supported by the MCG. Specifically, this means LTE-M (LTE Cat-M1) for 4G public cellular networks.	This is sufficient for low bandwidth requirements and has the effect of saving power.
If the public cellular network is capable of LTE Cat-M1, it shall be preferred by the MCG.	Prefer use of low power technology. LTE Cat-M1 offers bandwidth from 300 kbit/s up to 1 Mbit/s.
In 5G public cellular network, low power option shall be preferred (NB-IoT 5G or similar).	Prefer use of low power technology; the standard is still evolving
If 4G and 5G public cellular network are unavailable, an <u>option</u> should be provided to fall-back to 2G technology.	This is an <u>option</u> to provide better network coverage. 2G network will likely not play a big role beyond year 2027.
Each entity using the FDFT Link communication shall consider the available bandwidth for LTE Cat-M1 (bandwidth from 300 kbit/s up to 1 Mbit/s).	
Each entity using the FDFT Link communication shall consider the latency for LTE Cat-M1 (typical value of 10-20ms).	Source: 3GPP Release 13
An MCG Network Selector Service (NSS) shall be implemented according to IEC 61375-2-6, chapter 6.3.4.	If more than one bearer (public cellular network

	or Wi-Fi) is available, the selection of radio interface shall be implemented according to IEC 61375-2-6.
If no bearer is available, it must be ensured that a communication network on the wayside is set up by infrastructure operators.	informational; Wi-Fi network or negotiation with public cellular network operators.
The functionality of a SIM card for public cellular network authentication shall be included.	eSIM (embedded SIM card) is preferred
The SIM card shall provide data roaming capability for public cellular networks.	
The bearer shall provide an IPv4 address (IP address) used for communication.	A private IPv4 address is not considered a security feature but is likely to reduce access from the public Internet.
The IP address on the external interface of the MCG can be dynamically assigned and does not need to be public.	Mobile public network or Wi-Fi network
The FDFT Link shall support NAT (Network Address Translation).	The bearer may provide NAT (or Carrier Grade NAT, CGNAT) functionality, if a private IP address or a dedicated

	space is assigned to the external interface of the MCG. Eg. this is defined in IETF RFC 1918 and IETF RFC 6598.
IPv6 support shall be considered. The same rules apply to IPv6 as to IPv4 addresses.	
If IPv6 is used, a transition technology shall be implemented by the bearer to reach IPv4 endpoints if required.	An IPv4 endpoint could be the FDFT Link I/F of the FDFT Backend.
The services provided by MCG shall be always available to the FDFT backend systems via the FDFT link.	Even when consist is in energy saving mode.
An MCG Train Wake-up Service as described in IEC 61375-2-6, chapter 6.3.6 shall be implemented to ensure continuous communication capability and wake up.	Even when the consist is in energy saving mode.

5.6.3.3. FDFT Link Interface

IT security level 4 (SL 4) as defined in IEC 62443-3-3 applies.

Rationale:

SL 4 – Prevent the unauthorized disclosure of information to an entity actively searching for it using sophisticated means with extended resources, IACS specific skills and high motivation.

Remark: In the current situation, SL4 is the expected required security level.

Every consist shall use a unique private key for authentication.

The FDFT link shall always be initiated by the MCG, as no incoming communication through public interfaces shall be available on the MCG for IT security reasons.

The MCG shall use DNS to initiate connections to wayside systems.

On wayside systems, the authentication information is challenged against a PKI (Public Key Infrastructure), which does not need to be publicly recognised, but must be known and trusted by all systems in the GCG/WCG participating in the authentication.

Description	Justification / Rationale
The Requirements for Board to Ground communication shall be fulfilled as described in DIN EN 61375-2-6 Chapter 4.2 Table 1.	Additional requirements or specifications are described below.
No IP Ports (TCP or UDP) shall be open on the MCG on the external interface of the MCG.	No services are offered on public interfaces of MCG.
All incoming connection requests on the external interface of the MCG shall be dropped.	No services are offered on public interfaces of MCG.
A connection for the FDFT Link shall only be initiated by the MCG.	A transaction in the FDFT Link can be connected in both directions.
FDFT Link connections shall be initiated using a DNS hostname (FQDN).	No static IP address shall be configured to allow change of service IP on the landside.
The requirements for the FDFT Link connection shall be met according to DIN IEC 62443-3-3.	
As the FDFT Link transmits safety related information and uses a public mobile radio network, the criteria for the FDFT Link shall comply with chapter 5.15 of IEC 62443-3-3.	
FDFT Link requires the protection according to SL 4 (security level 4) as defined in IEC 62443-3-3.	

The FDFT Link shall protect the integrity of information including cryptography according to IEC 62443-3-3, chapter 7.3.3.1	
Requirements for Identification and Authentication shall be considered based on IEC 62443-3-3, chapter 5.	SL to be defined based on the requirements of the application as described in the normative.
Keys for authentication shall be secured by a Trusted Platform Module as a hardware measure.	TPM 2.0 or better
Multifactor authentication is required by security level 4 (SL 4) in IEC 62443-3-3. The authentication key stored in TPM is one factor. An additional factor shall be chosen.	Eg. SIM card, ID of MCG (MAC), or any static identification.
To securely handle a large number of consists, the use of Public-Key-Infrastructure as described in IEC 62443-3-3, chapter 5.10 shall be implemented.	
A PKI (Public Key Infrastructure) shall be used to authenticate a large number of consists according to criteria explained in IEC 62443-3-3, chapter 5.11.	
Every consist requires a unique and genuine private key / account to authenticate against wayside systems.	For authentication against GCG/WCG.
The PKI parameters shall be set up and kept state-of-the art.	This included algorithms, key lengths, and other services like revocation.
The PKI or CA (Certificate Authority) does not require to be an internationally recognized root CA.	The PKI can be self-hosted / self-signed.

FDFT Link Data / MCG function

The MCG shall provide network connectivity and data services from and to the consist via Radio interfaces. It shall provide Firewall services and supports zones as described in IEC 62443-3-3.

The MCG shall provide basic services to subsystems on the consist, like time source and position information through a GNSS module.

Description	Justification / Rationale
The MCG shall support and provide shared communication (as a router/gateway) to be used as described in IEC 61375-2-6, chapter 4.6.1.2.	Communication by many devices on the (same) consist is possible
The MCG shall act as a firewall for all interfaces and zones to control and separate traffic flows as described in IEC 62443-3-3 chapter 9.4.	
The MCG's IT security architecture shall be aligned with the concepts defined in IEC 62443, especially IEC 62443 part 3-3.	
The MCG shall provide functionality of an Application Layer Gateway ("broker service architecture") as described in IEC 61375-2-6, chapter 5.2.	
The MCG shall provide access from subsystems on the consist, attached to the ECN to FDFT backend services.	E.g: from a telematics device to communicate with FDFT backend.
The MCG shall provide access from FDFT backend services to subsystems on the consist attached to the ECN.	
The MCG shall access subsystems on the consist via VLANs in the Ethernet Consist Network (ECN) through the Train Backbone Node (F-ETBN).	
Each transaction using FDFT Link communications shall classify to either use the MCG as an ALG or as a shared communication (router). See IEC 61375-2-6 for details.	Define for each application separately how to communicate
The GNSS receiver shall provide the following information as a minimum: • latitude & longitude • altitude • time • speed & direction	

accuracy of position (accuracy value or error estimate, including when a satellite fix is obtained.)	
The MCG shall act as time source via the network using NTP (RFC5905) as protocol.	Based on time obtained through GNSS.
Proposal: The MCG shall synchronize itself to the UTC as received thru the GNSS receiver.	
The MCG shall share position data using standard protocols via network connection to other subsystems on the consist.	Either forward NMEA 0183 data or via gpsd (TCP/IP). For example used by a telematics device.
The MCG shall provide TLOS (Train Location Service) as described in chapter 6.3.2 of IEC 61375-2-6.	

FDFT Link Data / Requirements for GCG function

A GCG provides DNS services (among other services and functions). An MCG registers or updates it's consist address using DNS with the IP address assigned to the FTFT Link interface of the MCG. Services on the consist will be available to the FTFD backend through this registered address/hostname.

GCG also is a key part in the PKI (Public Key Infrastructure).

Description	Justification / Rationale
The GCG shall be reachable via DNS FQDN.	The FQDN is statically configured in MCGs that use this GCG.
Every operator shall provide a FQDN for the GCG endpoint to be able to handle connections from their respective consists.	The FQDN is statically configured in MCGs that use

	this GCG.
The MCG shall update the ground DNS server to register its consist identification with the IP address assigned to the wireless interface according to IEC 61375-2-6, chapter 6.3.1.4.	The registration shall be done using nsupdate according to IEEE RFC 2136.
No address registration via DNS for Train Journey shall be implemented as suggested in IEC 61375-2-6, chapter 5.3.5.2.	Not required
The numbering of FQDN shall follow the recommendation in 61375-2-6, chapter 5.3.5.1.	An example for consist addressing via DNS: UIC318112345670 .tcndns.oebb.at for consist 31 81 1234 567-0
Each GCG shall know and trust each Root CA to which it must authenticate.	
Each GCG shall have access to revocation services.	Eg. CRL, OCSP or comparable.