UNISIG

ERTMS/ETCS
EuroRadio FIS **FRMCS Communication Functional Module**
REF: SUBSET-037-3 ISSUE: 4.1.4 DATE: 11 April 2025

Company	Technical Approval	Management approval
ALSTOM		
AZD		
CAF		
HITACHI RAIL STS		
MERMEC		
SIEMENS		
THALES		

1 MODIFICATION HISTORY

Issue	Section Number	Modification / Description	Author
4.0.0	-	Baseline 4 1st release version	ER WG
4.0.1	4, 5, 6.2,1, 6.3.2, 6.3.4, 6.4.	Extensions for FRMCS V2	ER WG
4.1.1	All	Changes according to the first EECT review for V2	ER WG
4.1.2	All	Changes according to the second EECT review for V2	ER WG
4.1.3	6.2.3.1.4, 6.3.4.1.5	Editorial changes	ER WG
4.1.4	Table 4	Add parameter “User data” according to CRxxxx	ER WG

2 TABLE OF CONTENTS

3 GENERAL ASPECTS

3.1 Scope

3.1.1.1.1 This document (Subset-037-3) is applicable for data transmission over FRMCS without safety responsibility.

3.1.1.1.2 In particular Subset-037-3 does not define:

- The application functionality and application information flow.
- The architecture of the radio communication system.
- Security aspects are specified in [Subset-146].
- Safety aspects as these are specified in [Subset-037-2].

3.2 Acronyms and abbreviations

3.2.1.1.1 For general ERTMS/ETCS terms, definitions and abbreviations refer to [Subset-023]. New terms and abbreviations relevant and used in this FIS are specified here.

Abbreviation	Meaning
API	Application Programming Interface
AU1	First Authentication message
AU2	Second Authentication message
CFM	Communication Functional Module
CS	Circuit Switched
DI	Disconnect
DT	Data
FFS-V3	For Further Study to be clarified in FRMCS V3 specification
ID	Identity
ITU	International Telecommunication Union
MTU	Maximum Transfer Unit
O&M	Operation and Maintenance
OSI	Open System Interconnection
PDU	Protocol Data Unit
PS	Packet Switched
RTO	Retransmission TimeOut
SFM	Safe Functional Module
TCEPID	Transport Connection EndPoint Identifier
TP	Transport Protocol
TSAP	Transport Service Access Point
TU	Trackside Unit (e.g. RBC)

3.3 Definitions

3.3.1.1.1 For general ERTMS/ETCS terms, definitions and abbreviations refer to [Subset-023]. New definitions relevant and used in this FIS are specified here.

FUNCTIONAL MODULE
Set of functions contributing to realize the same global task.

MESSAGE AUTHENTICATION CODE (MAC)
An authenticator which is sent with a message to enable the receiver to detect alterations made to the message since it left the sender and to verify that the source of the message is as claimed. The MAC is a function of the whole message and a secret key.

Note: The terms FRMCS on-board/trackside (defined in [Subset-023]) and On-Board/Trackside FRMCS terms (used in FRMCS specifications) can be used interchangeably.

3.4 References

This FIS incorporates by dated or undated references, provisions from other publications. The relevant parts of these normative references are cited at the appropriate place in the text and the publications are listed hereafter. For dated references, subsequent amendments to or revisions of any of these publications apply to this FIS only when incorporated in it by amendment or revision. For undated references, CCS TSI Annex A applies.

Reference	Title	Author	Issue
FRMCS FFFIS	UIC; FRMCS FFFIS – Form Fit Functional Interface Specification	UIC	
RFC 791	Internet Protocol, RFC791 aka IETF STD 5, last update 2/2013 (RFC6864)	IETF	8/1981
RFC 9293	Transmission Control Protocol	IETF	10/2024
RFC 1122	Requirements for Internet Hosts – Communication Layers, last update 01/2020	IETF	10/1989
RFC 2018	TCP Selective Acknowledgment Options, last update 01/2020	IETF	10/1996
RFC 8200	Internet Protocol, Version 6 (Ipv6), last update 02/2020	IETF	07/2017
RFC 2883	An Extension to the Selective Acknowledgement (SACK) Option for TCP, last update 02/2020	IETF	07/2000
RFC 5482	TCP User Timeout Option, last update 07/2022	IETF	03/2009
RFC 6633	Deprecation of ICMP Source Quench Messages, last update 10/2015	IETF	05/2012
RFC 7323	TCP Extensions for High Performance, last update 12/2018	IETF	09/2014
Subset-023	Glossary of Terms and Abbreviations	UNISIG	
Subset-037-1	EuroRadio FIS – GSM-R CS/PS Communication Functional Module and Coordinating Function FRMCS/GSM-R	UNISIG	
Subset-037-2	EuroRadio FIS – Safety Functional Module	UNISIG	
Subset-098	RBC-RBC Safe Communication Interface	UNISIG	
Subset-146	Security Layers for ETCS Applications	UNISIG	

4 REFERENCE ARCHITECTURE

4.1.1.1.1 The Communication Functional Module (CFM) determines the necessary functions and capabilities to make use of FRMCS. Figure 1 contains a detailed reference architecture of the radio communication sub-system. The service interfaces and the protocol interfaces are defined.

4.1.1.1.2 Figure 1 shows the reference architecture for EuroRadio providing FRMCS communication. Interface (1c) is the interface between EuroRadio and the FRMCS on-board (OB_{app}). Interface (1d) is the interface between the EuroRadio and the FRMCS trackside (TS_{app}). The interfaces are specified be [FRMCS FFFIS] and encompasses the user plane to exchange user data as well as the control plane to manage necessary information for communications (FRMCS APIs).

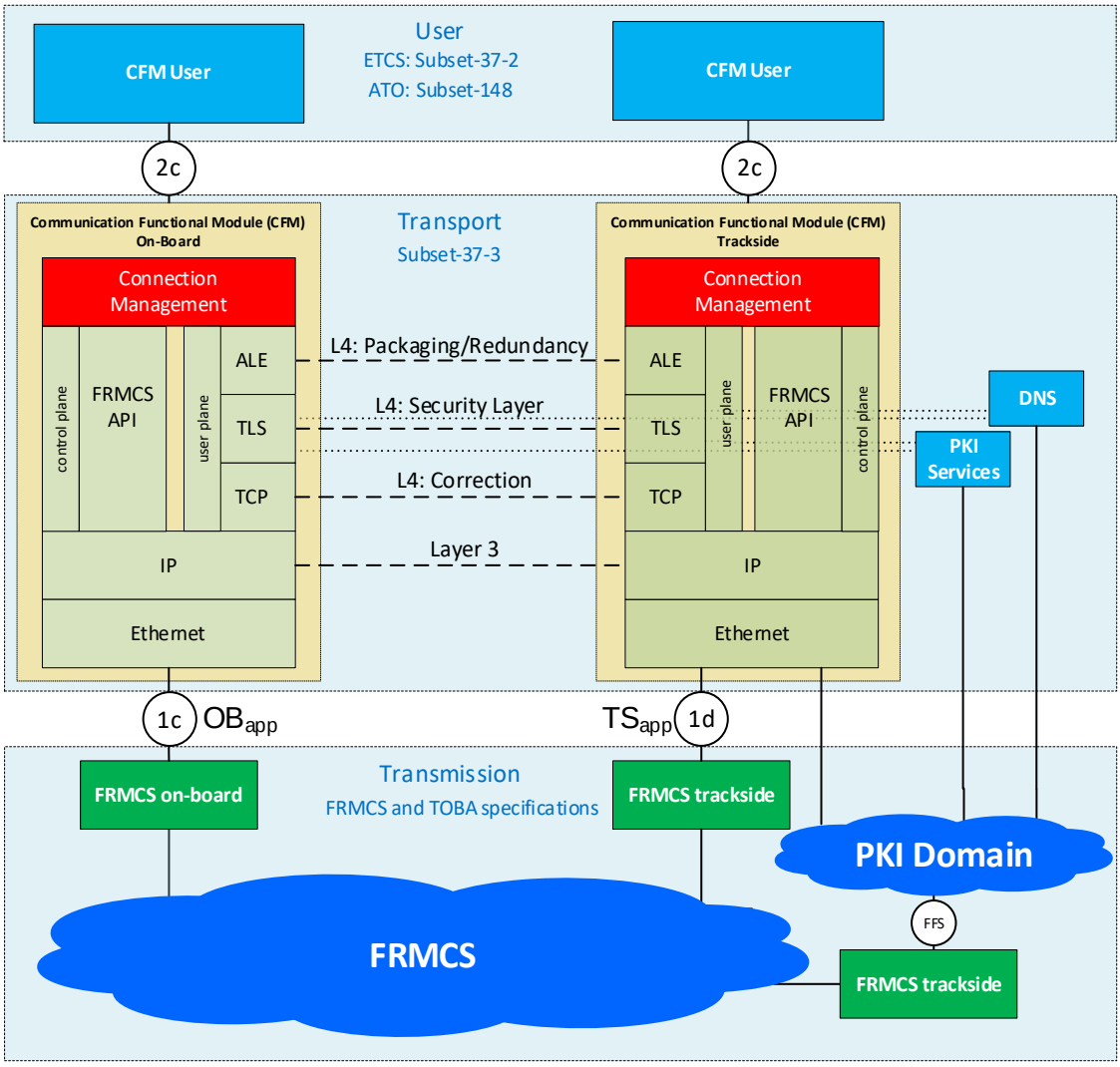

Figure 1 Reference architecture of EuroRadio

4.1.1.1.3 Interface (2c) is the interface between the Communication Functional Module (CFM) and the CFM User and it is in the scope of this specification.

4.1.1.1.4 Logical peer entity interfaces Security Layer, Layer 4 (Transport), Layer 3 (Network) are mandatory for interoperability. The interface is specified in terms of protocol data units and communication relevant aspects of module functionality.

4.1.1.1.5 Additional to the application related communication the TLS protocol layer needs IP Connectivity to the support functions “DNS and PKI Services”.

5 INTERFACE TO FRMCS

5.1.1.1.1 CFM shall use Loose Application regime and consider "OB_{APP}/TS_{APP} API Services" according to [FRMCS FFFIS].

5.1.1.1.2 The network layer protocol shall support IPv6 [RFC 8200].

5.1.1.1.3 The network layer protocol shall support IPv4 [RFC 791].

5.1.1.1.4 The used IP version shall correspond to the version used by the local network.

5.1.1.1.5 The data link layer shall be realised according to [FRMCS FFFIS].

5.1.1.1.6 The following table summarise the data link layer characteristics needs to be supported by the FRMCS system:

Table 1 Data Link Layer characteristics

	communicationCategory	Used for
1	ATO: "operativATO" ETCS: "operativETCS"	Operative data of the application
2	"HOME"	PKI and, KMS connectivity to the home network

Note: The handling of "communicationCategory" is FFS-V3.

6 COMMUNICATION FUNCTIONAL MODULE

6.1 General

6.1.1.1.1 This chapter specifies the Communication Functional Module (CFM) and its services. The CFM covers the OSI layers 4 (transport layer).

6.1.1.1.2 The CFM specify a functional interface and the related information flow. Implementation of CFM does not necessarily need to strictly use the specific model described by the subset.

6.1.1.1.3 A CFM instance provides a single user service.

6.2 Service definition and Interface to the CFM User

6.2.1 General Description

6.2.1.1.1 This interface (2c) is internal between the CFM and one CFM User.

6.2.1.1.2 Before entering service, the CFM shall be registered to the FRMCS on-board/trackside.

6.2.1.1.3 The first local registration to the FRMCS on-board/trackside will be managed in the CFM internally.

6.2.1.1.4 A deregistration/ reregistration functionality could be provided additionally to enable a controlled log off from the FRMCS on-board/trackside during the time the CFM User goes into an inactive mode (e.g. “isolation”, “standby”, “no power” for ETCS).

6.2.1.1.5 The CFM will support one-to-one connections only.

6.2.1.1.6 Connection establishment and release shall be triggered by the CFM User.

6.2.1.1.7 In case a connection is not established or is dropped; CFM User shall retry.

Note: If an error is persistent according to paragraph 6.2.6.1.5, the coordinating function specified in [Subset-037-1] may determine to retry using an alternative communication mode.

6.2.1.1.8 It shall be possible to establish multiple connections to different remote CFM Users.

6.2.2 Model of communication services

6.2.2.1.1 The communication services that a CFM offers to the CFM User are based on the services provided by the transport layer of TCP/IP reference model [RFC 9293]. These services concern:

- Transport connection establishment/release
- Reliable data transmission for packets ≤ 64 K octets
- Secured data transmission
- Transparent data transmission

6.2.2.1.2 A CFM instance communicates with the CFM User through a Transport Service Access Point (TSAP) by means of transport service primitives.

6.2.3 Service primitives for Connectivity Status

6.2.3.1.1 Two service primitives are provided to inform the CFM User about the status of IP Connectivity

- to request Connectivity status and
- to indicate Connectivity status

Table 2 Service primitives for connectivity status

Primitive Parameter	T-CONNECTIVITY.request	T- CONNECTIVITY.indication
Connectivity state		X
X Mandatory parameter (0 – no connectivity; 1 – connectivity provided)		

6.2.3.1.2 By means of the service primitive “T-CONNECTIVITY.request” the CFM User is able to request the connectivity status to the FRMCS network.

6.2.3.1.3 The status of the connectivity is indicated by the service primitive “T-CONNECTIVITY.indication” to the CFM User.

6.2.3.1.4 The connectivity indication can also be provided independently of a request, at any change of connectivity (e.g. after power-up or after loss of connectivity, see 6.4.2.1.4).

6.2.4 Service primitives for Connection establishment

6.2.4.1.1 The process of establishing a transport connection is initiated at the time when the CFM User requests a connection set up to the CFM. This service is accessed through the service primitive T-CONNECT.request with its associated parameters at the TSAP.

6.2.4.1.2 The following table gives the service primitives used for connection establishment and their corresponding parameters (see Table 3).

Table 3 Service primitives of the communication layer for connection establishment

Primitive Parameters	T-CONNECT request	T-CONNECT indication	T-CONNECT response	T-CONNECT confirm
TCEPID		X	X(=)	X
Called address: Called ETCS ID type Called ETCS ID	 X X	 X X		
Calling address: Calling ETCS ID type Calling ETCS ID	 X X	 X(=) X(=)		
Responding address: Responding ETCS ID type Responding ETCS ID			 X X	 X(=) X(=)
AU1 (see [Subset-037-2])	X (ETCS only)	X(=) (ETCS only)		
AU2 (see [Subset-037-2])			X (ETCS only)	X(=) (ETCS only)

X	Mandatory parameter.
(=)	The value of that parameter is identical to the value of the corresponding parameter of the preceding transport primitive.
ETCS ID type:	see [Subset-037-1], Table 3, Octet 4
ETCS ID:	see [Subset-023] and [Subset-037-1], Table 3, Octet 5-7, User ID (3 octet value)

6.2.4.1.3 The parameter TCEPID (Transport Connection End Point Identifier) is provided locally to distinguish between different transport connections.

6.2.4.1.4 The parameter ETCS ID type together with ETCS ID is unique within the scope of ERTMS data application. The ETCS IDs are used by the transport layer during connection establishment. The ETCS ID type and ETCS ID identifies the CFM User.

6.2.4.1.5 The Calling ETCS ID identifies, together with the ETCS ID type, the transport connection initiator. The Called ETCS ID identifies together with the ETCS ID type the called CFM user. The responding ETCS ID identifies the accepting/responding CFM user, which was locally selected by the responding transport entity.

6.2.4.1.6 The following figure shows the sequence of transport service primitives at TSAP for connection establishment:

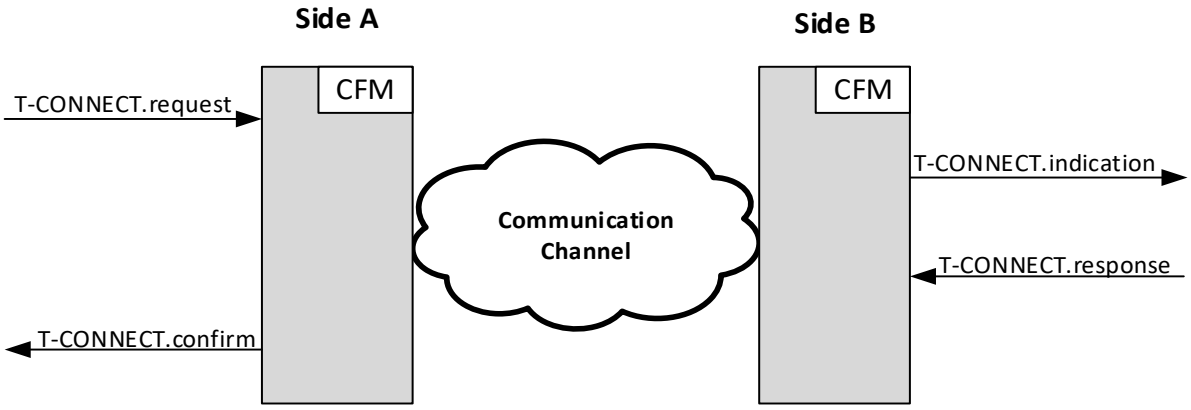

Figure 2: Sequence of primitives for connection setup

6.2.4.1.7 An unsuccessful connection establishment will be indicated to the CFM User by the T-DISCONNECT.indication (see 6.2.6).

6.2.5 Service primitives for data transfer

6.2.5.1.1 The data transfer service is provided after a successful transport connection setup and is handled by the communication stack directly. This service is accessed through the service primitive T-DATA.request with its associated parameters at the TSAP. The CFM provides transparent and reliable transfer of user data in both directions simultaneously and hides to the CFM Users the way in which the data are handled internally. The following table gives the service primitives of the communication layer used for data transfer:

Table 4: Service primitives of the communication layer for data transfer

Primitive Parameters	T-DATA.request	T-DATA.indication
TCEPID	X	X
User Data	X	X

6.2.5.1.2 A request for data transfer is made by the CFM User (after a successful transport connection set up) using the T-DATA.request service primitive, with user data as a parameter. These data are delivered to the intended user using the primitive T-DATA.indication with user data as a parameter.

6.2.5.1.3 The following figure shows the sequence of transport service primitives for the data transfer.

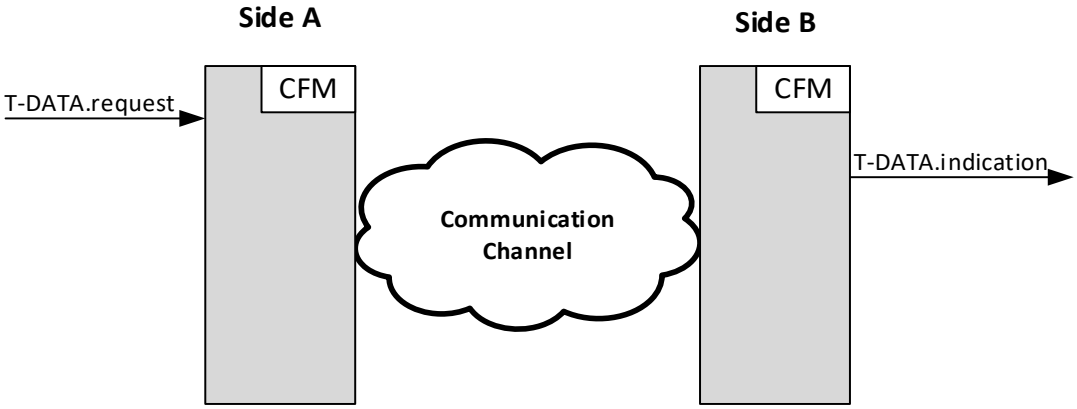

Figure 3: Sequence of primitives for data transfer

6.2.6 Service primitives for connection release

6.2.6.1.1 The transport connection release is provided by the communication layer through the service primitive T-DISCONNECT.request. The connection release is indicated to the CFM User using the service primitive T-DISCONNECT.indication. The connection release is indicated to the CFM User as a consequence of a disconnection request issued by the user (normal release), as a consequence of connection establishment rejection or because of a network failure.

6.2.6.1.2 The following table gives the service primitives used for connection release.

Table 5: Service primitives of the communication layer for connection release

Primitive Parameters	T-DISCONNECT.request	T-DISCONNECT.indication
TCEPID	X	X
Reason		X (1)
User Data	X(U)	X(=)
(1): It shall be used in the error case.		

6.2.6.1.3 The following figure shows the sequence of transport service primitives at TSAP for connection release.

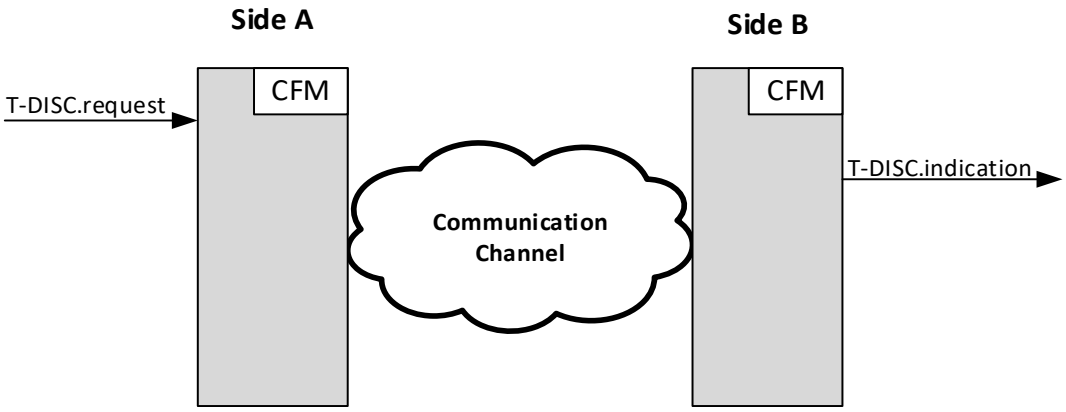

Figure 4. Sequence of primitives for connection release initiated by a CFM User

6.2.6.1.4 If an error occurs in the CFM or if the CFM receives an indication of an error by the FRMCS system. the errors can be ignored, locally logged or indicated to the CFM user.

6.2.6.1.5 If there is a problem with connection or connection establishment, the CFM should try by itself to recover the problem. Only if the problem cannot be solved, (i.e. the transport connection cannot be established), the CFM shall:

- inform the CFM User by a T-DISCONNECT.indication with a release cause according to the following table
- release the connection by using the “Closure of a session” feature according to [FRMCS FFFIS], if the corresponding FRMCS connection is ongoing.

Table 6: Error causes of the CFM

Reason/ code		Sub-reasons		comment
Normal release	Code =0	0	Normal release	
Persistent error	Code = 1	1	No further information	Connection not possible
Temporary Error	Code = 2	1	No further information	CFM User should retry
Note: All other reason/sub-reason values are reserved.				

6.3 FRMCS Communication stack

6.3.1 Introduction

6.3.1.1.1 This section provides a precise specification of the communication protocols of the user plane.

6.3.1.2 Control of the Communication Stack

6.3.1.2.1 The communication Stack shall be controlled by the Connection Management by the following primitives:

Note: In the following “client” refers to the calling side, “server” to the called side.

Note: For the call flows see Figure 5 to Figure 7 in clause 6.4.3.

Table 7 Service primitives of the communication layer for connection establishment

Primitive Parameters	T-COM. Listen	T-COM. Start	T-COM. StartAck[1)]	T-COM. Release	T-COM. ReleaseAck
TCEPID		X	X(=)	X	X(=)
own IP address	X				
Local FRMCS on-board/trackside IP address		X			
Calling address: Calling ETCS ID type Calling ETCS ID		 X X			
Called address: Called ETCS ID type Called ETCS ID		 X X			
Response address Response ETCS ID Response ETCS ID type			 X X		
AU1 (Safety Layer)		X (ETCS only)			
AU2 (Safety Layer)			X (ETCS only)		
X Mandatory parameter.					

6.3.1.2.2 To detect incoming connection an instance of the protocol stack has to be bound to the port. This is initiated with the primitive T-COM.Listen.

6.3.1.2.3 The client uses T-COM.Start primitive to request a connection to the server. The successful connection establishment of the connection will be indicated using the T-COM.StartAck primitive.

6.3.1.2.4 On the server side the T-COM.Start primitive indicates an incoming connection to the connection management. The connection will be accepted with the T-COM.StartAck primitive.

6.3.1.2.5 With the T-COM.Release primitive the communication stack shall be controlled released after transmitting all stored user information.

6.3.1.2.6 The release of the communication stack after T-COM.Release shall be indicated by the T-COM.ReleaseAck primitive to the Connection Management.

6.3.1.2.7 A malfunction of the communication stack shall be indicated to the Communication Management with the T-COM.Release.

6.3.2 Adaptation Layer Entity (ALE)

6.3.2.1 **Functions**

6.3.2.1.1 The main functions of ALE are:

- Establishment and Release of the user plane connection.
- Guaranteed packet structure for packet size lower or equal to 64 K octets. Larger packet size is a matter of protocol user specification.
- Monitoring of channel availability.

6.3.2.1.2 All the above ALE functions are based on [Subset-098] (RBC-RBC Safe Communication Interface), using the requirements specified in Table 8. The paragraphs below explain the adaptation of Subset-098 for on-board to trackside safe communication.

Table 8. Applicability conditions of Subset-098

Section	Applicability conditions
§ 1 Modification History	Not relevant.
§ 2 Table of Contents	Not relevant.
§ 3 introduction	Not relevant.
§ 4 Reference architecture	Not relevant.
§ 5 Safe Functional Module	Not relevant.
§ 6 Communication Functional Module	All applicable except for the following rows of this table.
§ 6.1 General	Not relevant, however not only RBC-RBC Safe Communication Interface, but generic on-board and trackside equipment.
§ 6.2.1.1.1	Systems are assumed both fixed and mobile.
§ 6.2.1.1.2	Physical redundancy not supported on vehicle side.
§ 6.3.1.1.1	Running not only on ground-based systems.
§ 6.3.1.1.4	The diagram in figure 28 shows an example for a fixed connection, not over FRMCS.
§ 6.3.2.1.3	Only Class D.
§ 6.3.2.1.4	One single physical link only, with only one TCP connection, no redundancy used.
§ 6.3.3 Class A request	Not relevant.
§ 6.3.4.1.1	A request for a Class D quality of service shall result in the Adaptation Layer attempting to make only one TCP connections to the remote Adaptation Layer entity. This connection shall be used to transfer all data and control messages. The safe connection shall operate only on this link. The exact details of how this link shall be monitored and managed are contained in §6.6.
§ 6.4.1.1.3	Managing of the redundancy is not applicable.
§ 6.5.2.1.1	Transport priority is not used.
§ 6.5.2.2.1	Specified in chapter [Subset-098].
§ 6.5.2.5.4	TCP_LISTEN_ON_PORT specified in [Subset-098].
§ 6.5.2.6.1	Every connection between two subsystems is realised through only one transport connection.
§ 6.6.1 Class A (optional for implementation)	Not relevant.
§ 6.6.2	Class D is used. One single physical link only, with only one TCP connection, no redundancy used.
§ 6.8	Specified in chapter 6.3.3
§ 6.8.3.1.2	Ipv6 and IPv4 is mandatory
§ 6.9.3.1.1	Specified in chapter [Subset-098].
§ 7 INFORMATIVE ANNEX	Not relevant.

6.3.2.2 **Redundancy of the ALE Server physical interfaces**

6.3.2.2.1 The ALE Redundancy feature will not be used for Euroradio.

6.3.2.3 **Local Redundancy**

6.3.2.3.1 Local redundancy for FRMCS onboard/trackside is FFS-V3.

6.3.2.4 **Connection Monitoring**

6.3.2.4.1 Standard TCP Keep Alive shall be used, together with other TCP parameters and features, see Table 9.

6.3.3 Security Layer

6.3.3.1.1 The communication between On-Board and Trackside User shall be secured.

6.3.3.1.2 Authentication shall be done for both sides (i.e. mutual).

6.3.3.1.3 Packets shall be protected against modification. Use of encryption to achieve confidentiality of exchanged data is not mandatory. A client shall provide to the server a list of supported ciphers which shall include at least one cipher with and one without encrypting confidentially and the server shall return to the client the selected cipher from that list.

Note: The decision (to be done by the trackside) to use encryption providing data confidentially should be based on a risk analysis.

6.3.3.1.4 The communication shall be protected against replay attacks.

6.3.3.1.5 The configuration of the security layer depends on the using application. See [Subset-146, Annex A] for details.

6.3.4 Transport Layer

6.3.4.1.1 The transport layer protocol shall be TCP.

6.3.4.1.2 Depend on the application the following ports shall be used:

ETCS: 7913
ATO: 7914

6.3.4.1.3 In the following Table 9, Mandatory (M) and Optional (O) TCP Features are specified from ETCS operation point of view.

Note: If the GPRS and the FRMCS stack are running on the same kernel some of the TCP parameters in Table 9 are dependent.

6.3.4.1.4 The following adaptation should be done for ATO:

- The user data traffic of ATO is different compared to ETCS, i.e., for ATO there is no requirement that the time between two consecutive messages shall not exceed a set value (T_NVCONTACT). That is, transmitted data can remain unacknowledged for a longer time. Consequently, the TcpUserTimeout should be set to a higher value for ATO traffic.

6.3.4.1.5 Limits and recommended values are reused by GPRS, adapted values for the FRMCS channel are FFS-V3.

Note: The configurability per connection is analysed from the Linux TCP implementation point of view. Other implementations could have other restrictions. This analysis (marked in grey) is FFS-V3.

Table 9. Applicability conditions of TCP

	Feature	RFC	M/O	Value	Comments
1	Initial RTO	9293 1122	M	>= TCP_RTO_MIN < TCP_RTO_MAX (Recommended: = TCP_RTO_MIN)	Also known as “TCP_timeout_init” *Note: not configurable per connection*
2	Minimum Retransmission Timeout	9293 1122	M	1-5s (Recommended: 3 s)	TCP_RTO_MIN: The RTO is not allowed to be lower than this value *Note: not configurable per connection*
3	Maximum Retransmission Timeout	9293 1122	M	>=5s (Recommended: 5 s)	TCP_RTO_MAX: Should be set to a value that defines the maximum allowed time before a forced retransmission *Note: not configurable per connection*
4	Karn and Jacobson's algorithm, with exponential back-off	1122	M	Used	Standard TCP feature to compute RTO *Note: not configurable per connection*
6	TcpMaxConnectRetransmissions	9293 1122	M	3	Number of SYN-packet retries; also known as “TCP_SYN_retries” *Note: not configurable per connection*
7	TcpMaxDataRetransmissions	9293 1122.	M	1-5 (Recommended: 2)	Also known as “TCP_retries2” *Note: not configurable per connection* The detection time range is (1+TcpMaxDataRetransmissions) * [TCP_RTO_MIN, TCP_RTO_MAX], i.e. for recommended values [9,15] s.
8	TcpKeepAliveTime	9293 1122	M	10-20 s (Recommended: 10 s)	The interval to wait before probing the idle connection *Note: configurable per connection*
9	TcpKeepAliveInterval	9293 1122	M	2-5 s (Recommended: 2 s)	The interval to wait before retrying the probe after an initial failure to respond: *Note: configurable per connection*
10	TcpKeepAliveProbes	9293 1122	M	2-4 (Recommended: 2)	The maximum number of times to retry the probe *Note: configurable per connection* *Note 2: Expected disconnect time for recommended value is TcpKeepAliveTime + TcpKeepAliveInterval*TcpKeepAliveProbes = 14s*
11	TcpUserTimeout	9293	O	>=10 (Recommended: 11 s)	The TCP user timeout controls how long transmitted data may remain unacknowledged before a connection is forcefully closed. It is checked during RTO update. The detection time range is [TcpUserTimeout , TcpUserTimeout + min(TcpUserTimeout, TCP_RTO_MAX)], i.e. for recommended values [11,16] s. *Note: configurable per connection* *Note 2: the recommended value of 11 is chosen in order to cover delays in relation of RTO timeout.*
12	TcpSack	2018 2883	M	enabled	Selective Acknowledgement *Note: not configurable per connection*

	Feature	RFC	M/O	Value	Comments
13	TcpTimestamps	7323	M	disabled	*Note: not configurable per connection*
14	TcpNoDelay	1122 6633	M	enabled	Disables Nagel's algorithm which concatenates small messages before sending them
15	TCP Push Bit	9293	M	enabled	Force the processing of the receiver buffer *Note: not configurable per connection*
16	Max TCP segment size	9293	M	<= 1416 (Recommended: = 1416)	Maximum value is MTU - sizeof(max TCP Header) - sizeof(max IP Header) Where guaranteed MTU=1500 byte, sizeof(max TCP Header)=60 byte, sizeof(max IP Header) = 24 byte *Note: configurable per connection*
17	TcpEarlyRetrans	5827	M	<=2 (Recommended: 0)	Controls the mode of retransmissions in certain widely available TCP implementation. Should not be used for EuroRadio. Note: not configurable per connection.

6.3.5 Overhead of PDUs

6.3.5.1.1 The safety layer (used for ETCS only, see [Subset-037-1]) adds a header (1 octets) and the MAC (8 octets) to the user data (≤1023 octets).

6.3.5.1.2 The ALE sublayer adds a 10-octet header (or more, if ALE Packet Type equals 1 or 2) to the user data.

6.3.5.1.3 The secure transport layer adds a 24-octet header (or more) to the user data.

6.3.5.1.4 The IP layer adds a header of 20 or 24 octet (Ipv4) or 40 octets (Ipv6) to the user data.

6.3.5.1.5 The packet segmentation of TCP will be reassembled by the ALE protocol.

6.4 Management of Communication Functional Module

6.4.1 Configuration management

6.4.1.1.1 TCP Configuration Parameters shall be set according to Table 9.

6.4.1.1.2 Application type, ETCS ID / ETCS ID type and StaticId (see [FRMCS FFFIS]) shall be set according to the values given by the Infrastructure Manager / Railway Undertaker.

6.4.1.1.3 For the CFM, the IP address of the OBAPP/TSAPP control plane shall be preconfigured.

6.4.1.1.4 Configuration parameters for PKI services are FFS -V3.

6.4.1.1.5 The FRMCS Connection Establishment timer shall be set to FRMCS_CED = 5s (FRMCS Connection Establishment Delay).

6.4.2 Registration and Connectivity Status functionality

6.4.2.1.1 The registration to the FRMCS on-board/trackside after Power-On shall be managed in the CFM internally without an external trigger by the CFM User.

6.4.2.1.2 The Application Type according to [Subset-037-1], Table 5, shall be mapped to the Application Category as follows:

Table 10. Application Type mapping

Application Type	Application Category [FRMCS FFFIS], Table 6
0x10 (ERTMS/ETCS level 2)	etcs
0x30 (ATO/ATO communication)	ato

6.4.2.1.3 This registration shall be done as described in [FRMCS FFFIS] as “Local Binding”.

Note: Details of TLS handling are FFS-V3.

6.4.2.1.4 The connectivity status shall (On-Board) / should (trackside) be monitored using the notifications “FtdAvlNotif” for Transport Domain and “FsdAvlNotif” for Service Domain (see [FRMCS FFFIS]).

6.4.2.1.5 Service is available if both statuses are “TRUE”.

6.4.2.1.6 The status shall be stored.

6.4.2.1.7 After an initial indication the CFM User should be informed if requested and in case of a status change.

6.4.3 Connection Management

6.4.3.1.1 Similar as OB_{APP} / TS_{APP} use the “sessionId”, the communication stack control interface use “TCEPID“ to identify a connection. Because it is a one-to-one relationship the value of “sessionId” should be reused for “TCEPID” or a mapping function has to be implemented.

6.4.3.1.2 To provide incoming connections the FRMCS communication stack shall be started using the T-COM.Listen primitive.

6.4.3.1.3 If the CFM is used with the Safety Layer according to [Subset-037-2] the SaPDU AU1, received with the T-CONNECT.request primitive, shall be transmitted in the connection establishment of the ALE protocol to the remote user. The remote user will response with the SaPDU AU2.

6.4.3.1.4 All errors related to the connection management shall be indicated to the CFM User according to clause 6.2.6.

6.4.3.2 Outgoing Connections

6.4.3.2.1 Operative outgoing connections shall be triggered by the CFM User with the T-CONNECT.request primitive.

6.4.3.2.2 To establish the user plane the “Opening a session” feature according to [FRMCS FFFIS] shall be used.

6.4.3.2.3 The remote address is:

"id<ETCS-ID>.ty<ETCS ID Type>.cc<NID_C>.ertms"

	formatted as
ETCS-ID	6-digit lowercase hex ASCII string
ETCS-ID type	2-digit lowercase hex ASCII string
NID_C	3-digit lowercase hex ASCII string

Example: id031123.ty08.cc00c.ertms

6.4.3.2.4 The communicationCategory shall be set according to the first entry of Table 1.

6.4.3.2.5 On success the "sessionId" shall be stored. In all other cases a temporary error shall be indicated to the CFM User according to clause 6.2.6.

6.4.3.2.6 If the successful establishment of the session was confirmed with the OpenSessionFinalAnswer the FRMCS communication stack shall be started using the T-COM.Start primitive providing the "Local FRMCS on-board IP address" (known by the "Session start" feature), the calling and called ETCS address information and the SaPDU AU1, otherwise a temporary error shall be indicated to the CFM User.

6.4.3.2.7 If the communication stack acknowledges the start-up the CFM User shall be informed using the T-CONNECT.confirm primitive, otherwise a temporary error shall be indicated to the CFM User according to clause 6.2.6.

6.4.3.2.8 The FRMCS Connection Establishment shall be supervised by a timer set to FRMCS_CED (see 6.4.1.1.5).

6.4.3.3 Incoming Connections

6.4.3.3.1 If utilising the Host to Host Application interface (OB_{APP}, TS_{APP}) mode of [FRMCS FFFIS], then an incoming FRMCS connection will be indicated by the FRMCS on-board/trackside by an IncomingSession notification and supported by the CFM according to [FRMCS FFFIS].

6.4.3.3.2 **Note:** Handling of End-to-End channel, especially the association of control and user plane is FFS-V3. When the connection management receives the T-COM.Start:

- The establishment of the transport link and the ETCS address information of the remote entity shall be indicated to the CFM User using the T-CONNECT.indication primitive, otherwise a temporary error shall be indicated to the CFM User according to clause 6.2.6.

6.4.3.3.3 If the CFM User answers with the T-CONNECT.response the connection will be acknowledged to the communication stack using the T-COM.StartAck primitive.

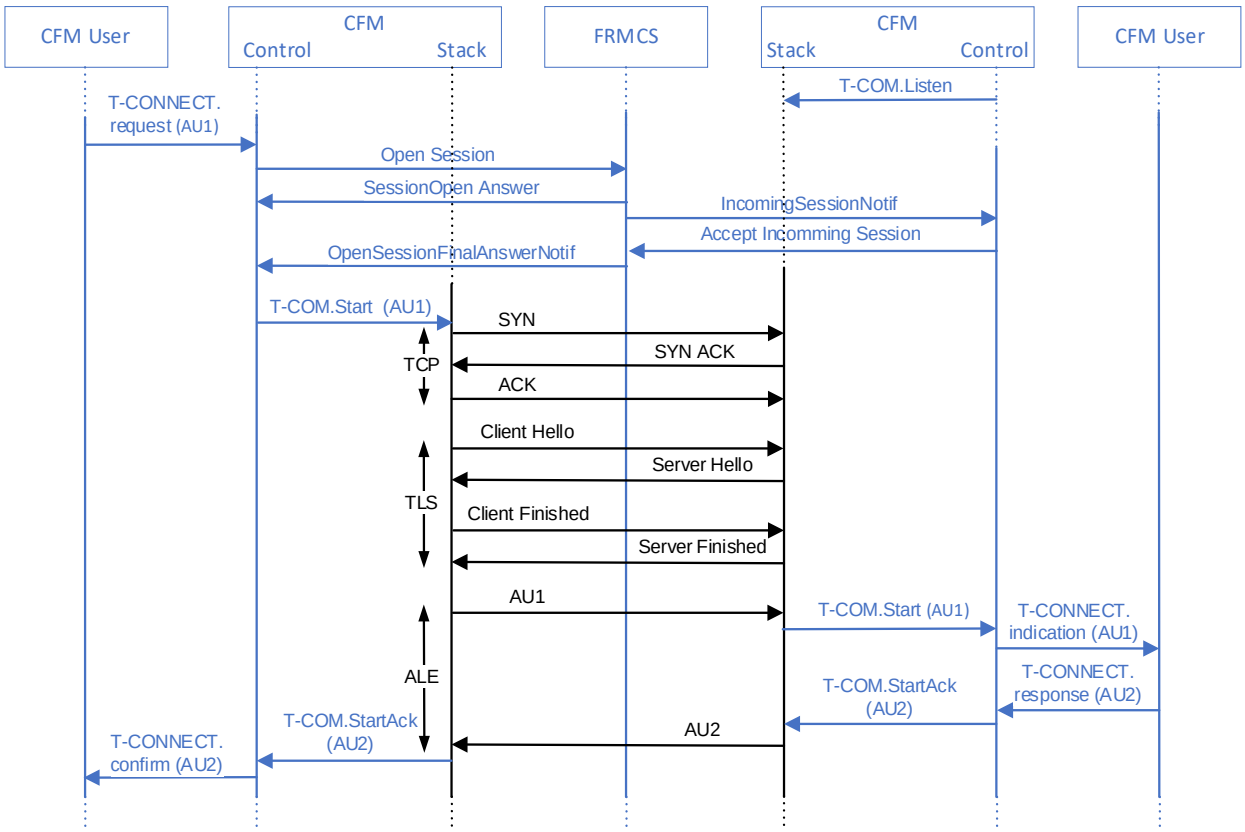

Figure 5: Connection establishment handling (Host to Host mode)

6.4.3.4 Outgoing Disconnect

6.4.3.4.1 If the CFM User initiates the disconnect using the T-DISCONNECT.request the CFM shall initiate the release of the communication stack using the T-COM.Release primitive.

6.4.3.4.2 After receiving the T-COM.ReleaseAck the service connection shall be released using the “Closure of a session” feature according to [FRMCS FFFIS].

6.4.3.5 Incoming Disconnect

6.4.3.5.1 An incoming disconnect will be indicated by the “DI” information of the ALE protocol. It shall trigger the TLS/TCP release and shall be indicated to the control management using the T-COM.Release.

6.4.3.5.2 The control management will inform the CFM User using the T-DISCONNECT.Indication and acknowledge the T-COM.Release. This acknowledgement is for information only.

6.4.3.5.3 If the FRMCS on-board/trackside initiates a disconnect using the “sessionClosureNotif” notification according to [FRMCS FFFIS] the disconnect shall be indicated to the CFM User using the T-DISCONNECT.indication primitive.

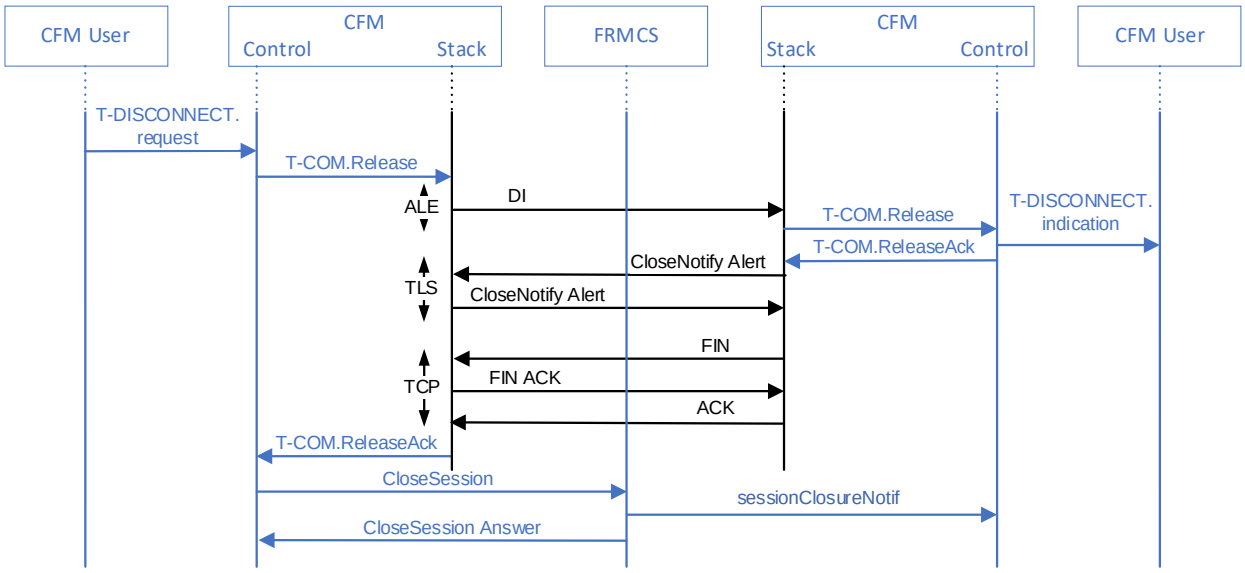

Figure 6: Connection Disconnect handling (Host to Host mode)

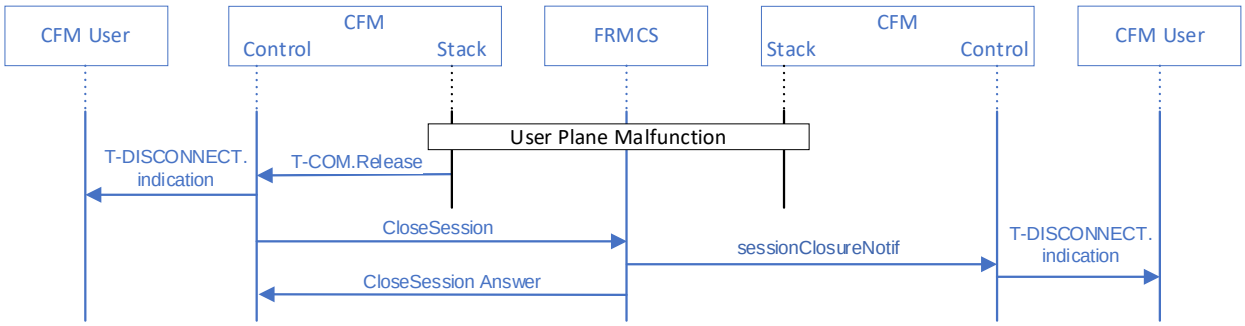

Figure 7: Connection Malfunction handling (Host to Host mode)

6.4.4 Deregistration functionality

6.4.4.1.1 If the CFM User is going to an inactive mode, the CFM should inform the network using the “De-Register” function according to [FRMCS FFFIS]. The FRMCS on-board/trackside will close the event stream.

6.4.4.1.2 After reactivation of the CFM User a new registration will be necessary (see clause 6.4.2).

Note: The trigger for deregistration and reregistration are in the responsibility of implementation. Unintended restarts of CFM (i.e. no Local deregistration happens) are not covered by this chapter.

6.4.5 Error logging

6.4.5.1.1 Diagnosis and error logging is a matter of the implementation.

6.4.6 DNS and PKI Services

6.4.6.1.1 Connectivity to DNS and PKI Services shall be established using the “Session start” feature in Host to Network mode according to [FRMCS FFFIS].

6.4.6.1.2 The communicationCategory for this session shall be set according to second entry of Table 1.

6.4.6.1.3 The IP network address (termed “network prefix” in IPv6 and “subnet” in IPv4) received upon a successful FRMCS (network) “Session start” request, shall be used by the requesting CFM as network prefix (or IPv4 subnet part) of destination IP addresses for IP packets associated with respective FRMCS (network) connection.

Note: The IPv6 Interface Identifier (or IPv4 host address part) of the destination address is considered transparent and hence will not be translated by FRMCS.