Title and contract N°	WP4 T4.4	C592
Author :	**Brice Gombault**	**SYSTEREL**
Diffusion :		
Object :	**Safety analyse of Subset 026, Section 3.5, Management of Radio Communication (MoRC).**	

1. EVOLUTION OF THE DOCUMENT

Issue Number Date	Section Number	Modification / Description	Author
1A 04-10-13	All	Creation	BGO
2A 15-10-13	All	Revised according to comments	BGO

2. CONTEXT

As defined in the SUBSET-088 v2.3.0, the role of ETCS is

To provide the Driver with information to allow him to drive the train safely and to enforce respect of this information.

Thus the Core Hazard is defined as

Exceedance of the safe speed or distance as advised to ETCS.

One way is the “KERNEL-6 Manage communication session failure” which results an “RADIO (INFILL) Transmission data consistency failure (safety related transmission function)”

3. SYSTEM MODEL FROM SRS

This chapter describes the MoRC function from the SRS subset-026-3, issue 3.3.0.

3.1. Functional decomposition

This chapter summarises the role of the different functions.

Function	Role
register mobile terminal	Used to register the Mobile Terminal to a Radio Network.
set-up safe connection	Used to set-up the safe connection according to EURORADIO specification.
establish communication	Used to establish a communication with trackside equipment.
maintain communication	Used to maintain the communication with trackside equipment.

terminate communication	Used to terminate the communication with trackside equipment.
release safe connection	Used to release the safe connection according to EURORADIO specification.
notify driver	Used to notify the driver of the state of radio communication.

3.2. Interfaces of the MoRC function

3.2.1. Physical components

The MoRC function interacts with 4 units:

- Mobile Terminal
- Radio Bloc Centre
- Radio Infill Unit
- Driver Module Interface

3.2.2. Data

This chapter describes data used by the MoRC function.

Input data	Description
start_of_mission - train is rejected* - the driver closes the desk*	A start of mission occurs. * If one of these events occurs during Start of Mission, the termination of the communication shall be performed.
end_of_mission	End of Mission is performed.
trackside_establishment_request	The establishment of the communication is ordered from trackside (RBC, RIU or balise groups).
trackside_terminating_request	The terminating of the communication is ordered from trackside.
trackside_terminating_ack	After reception of Termination_com_session_msg, the trackside considers the communication session terminated and sends an acknowledgement to the on-board.
mode_change	The change of mode has to be reported to the RBC.
manual_change_level	The driver has manually changed the level to 2 or 3.
front_end_change_level	The train passes a level transition border (from level 2/3 to level 0, NTC, 1) with its front end.
end_of_radio_hole	The train front reaches the end of an announced radio hole.
start_of_radio_hole	The train front reaches the start of an announced radio hole.
trackside_system_version	The system version from the trackside.
init_com_session_msg_in - time-stamp - Last Relevant Balise Group	The message Initiation of communication session from the trackside.
radio_network_identity	Radio Network identity.

power-up	The train is switch-on.

Internal data	Description
communication_established	A communication is already established.
communication_lost	Communication session is considered as terminated due to loss of safe radio connection.
communication_lost_delay	Maximum time to maintain a communication session in case of failed re-connection attempts
RBC_id	The identity of the RBC.
RBC_phone_number	The telephone number of the RBC.
communication_request	The action to be performed (establish/terminate the session).
spleeping_units	Used in sleeping mode.
RIU_id	The identity of the RIU.
RIU_phone_number	The telephone number of the RIU.
phone_number	The telephone number of the train.
supported_versions	List of supported system versions.
max_establishment_try	The number of times to try to establish a safe radio connection.
max_repetition_msg	Repetition of radio messages (i.e. excluding the first sending)
msg_repetition_delay	Waiting time before radio message repetition
radio_connection_status	Status of the connection from EURORADIO
last_radio_network_identity	Last Radio Network identity.

Output data	Description
init_com_session_msg_out	The message Initiation of communication session to the trackside.
termination_com_session_msg	Termination of communication session message to the trackside.
version_msg	The version independent message to the trackside indicates “No compatible version supported”.
session_established_report_msg - phone_number	The session established report message to the trackside. The phone_number is only sent when the train establish the communication.
radio_setup_request	Request the set-up of a safe radio connection with the trackside.
radio_release_request	Request the release of a safe radio connection with the trackside.
connection_stat_msg - No Connection - Connection Lost / Set-Up failed - Connection Up	Information to the driver about the status of the safe radio connection.
version_error_flag	Error flag to inform the driver of a system version error.

3.3. FMEA

The worksheet includes the following columns:

- **#:** Identification number of the raw of the table,
- **Function**: Function/sub-function to be analysed,
- **Failure mode** (and related outputs): The following failure modes are considered for the outputs of each function:
    - Absence: the function is not carried out on request,
    - Loss: the function was carried out but it stops,
    - Inadvertent: the function is performed when not requested,
    - Degraded: the function does not meet its requirements (it could be due delay, outputs corrupted, address error, …),

  Note: for some functions, some of these modes can be not relevant. In this case, the mode is not considered.
- **Effect**: Direct effect of the failure mode on function outputs and at system level,
- **Hazard**: Indicate if the hazard identified could happen (Yes or No),
- **Detectability**: Indicate if the detectable/Undetectable,
- **SIL**: Deduced Safety Integrity Level of the function. SIL-4 if the Hazard is Yes, else SIL-0,
- **Safety Criteria**: Safety Criteria defining the need to eliminate or mitigate risks. The measures can be preventive, palliative or corrective,
- **Comments**: Free comments to clarify the content of the row.

Suppositions on analyse:

- The absence of communication is safety related at system level.

#	Function	Failure mode	Effect	Hazard	Detectability	SIL	Safety Criteria	Comment
1	register mobile terminal	Absence	The Mobile Terminal is not registered to the radio network. Communication with trackside equipment is not possible.	yes	Detectable	SIL-4	REQ_FMEA_ID_001 The Mobile Terminal shall be safely registered to a Radio Network.	
2		Loss	The Mobile Terminal is not registered to the radio network. Communication with trackside equipment is not possible.	yes	Detectable	SIL-4	REQ_FMEA_ID_002 The driver shall be safely informed of the state of the radio communication (resulting of the different steps: registration of the Mobile Terminal to the Radio Network, establishment of the communication, end of communication).	
3		Inadvertent	The Mobile Terminal changes form a radio network to another during an active communication. The active communication with trackside equipment fails.	yes	Detectable	SIL-4	REQ_FMEA_ID_003 If a communication through a Radio Network is active, registration to another Radio Network mustn't be performed.	
4		Degraded	The Mobile Terminal is not registered to the radio network. Communication with trackside equipment is not possible.	yes	Detectable	SIL-4	REQ_FMEA_ID_001 The Mobile Terminal shall be safely registered to a Radio Network. REQ_FMEA_ID_002 The driver shall be safely informed of the state of the radio communication (resulting of the different steps: registration of the Mobile Terminal to the Radio Network, establishment of the communication, end of communication).	

#	Function	Failure mode	Effect	Hazard	Detectability	SIL	Safety Criteria	Comment
5	set-up safe connection	Absence / Loss / Degraded	The radio connection is not safe. Corruption of data may occur.	yes	Detectable	SIL-4	REQ_FMEA_ID_004 A safety protocol shall be used to performed communication between Mobile Terminal and Radio Network.	
6		Inadvertent	An active communication with trackside equipment fails due to the set-up of the safe connection.	yes	Detectable	SIL-4	REQ_FMEA_ID_005 If a communication with trackside equipment is active, set-up of safe radio connection with another trackside equipment mustn't be performed. Exception in case of handover with RBC.	
7	establish communication	Absence	Communication with trackside equipment is not performed.	yes	Detectable	SIL-4	REQ_FMEA_ID_006 Communication session with trackside equipment shall be safely established.	
8		Loss	Establishment of communication is not complete.	yes	Detectable	SIL-4	REQ_FMEA_ID_002 The driver shall be safely informed of the state of the radio communication (resulting of the different steps: registration of the Mobile Terminal to the Radio Network, establishment of the communication, end of communication).	
9		Inadvertent	An active communication with trackside equipment fails due to the establishment of a new communication.	yes	Detectable	SIL-4	REQ_FMEA_ID_007 Establishment of communication session shall be performed when no communication is active. Exception in case of handover with RBC.	

#	Function	Failure mode	Effect	Hazard	Detectability	SIL	Safety Criteria	Comment
10		Degraded	The communication is not correctly established (wrong trackside equipment called, wrong system version used)	yes	Detectable	SIL-4	REQ_FMEA_ID_006 Communication session with trackside equipment shall be safely established.	
11	maintain communication	Absence / Loss / Inadvertent / Degraded	Communication is lost in case of loss of safe radio connection.	yes	Detectable	SIL-4	REQ_FMEA_ID_008 Communication session shall be safely maintained.	
12	terminate communication	Absence / Loss / Degraded	Communication with another trackside equipment is not possible.	yes	Detectable	SIL-4	REQ_FMEA_ID_009 Terminate a communication session shall be safely defined.	
13		Inadvertent	Transmission of data with trackside equipment fails.	yes	Detectable	SIL-4	REQ_FMEA_ID_002 The driver shall be safely informed of the state of the radio communication (resulting of the different steps: registration of the Mobile Terminal to the Radio Network, establishment of the communication, end of communication). REQ_FMEA_ID_009 Terminate a communication session shall be safely defined.	
14	release safe connection	Absence / Loss / Degraded	No safety impact as communication is terminated.	no	-	-	-	

#	Function	Failure mode	Effect	Hazard	Detectability	SIL	Safety Criteria	Comment
15		Inadvertent	Transmission of data with trackside equipment fails.	yes	Detectable	SIL-4	REQ_FMEA_ID_010 The release of the safe radio connection with trackside shall be performed only when the communication session is terminated.	
16	notify driver	Absence / Degraded	The driver is not informed of the state of the radio connection.	yes	Detectable	SIL-4	REQ_FMEA_ID_002 The driver shall be safely informed of the state of the radio communication (resulting of the different steps: registration of the Mobile Terminal to the Radio Network, establishment of the communication, end of communication).	
17		Loss / Inadvertent	NA	-	-	-	-	

4. SYSML MODEL

The model used is BitHub\model_evaluation\model\SCADE_Siemens\MoRC_System\MoRC_System

4.1. Functional decomposition

Function	**Comment** (*equivalence with function defined in §3.1)*
SessionStateManager	*(notify driver)*
EstablishingACommunicationSession	*(establish communication)*
MaintainingACommunicationSession	*(maintain communication)*
TerminatingACommunicationSession	*(terminate communication)*
RegisteringToTheRadioNetwork	*(register mobile terminal)* *(set-up safe connection)* *(release safe connection)*

4.2. Data

SysML Data	**Comments** (*equivalence with data defined in §3.2.2)*
Input flow	
OBU_Status	Inputs from onboard unit (OBU) components: Status, time...
- powerAvailable	*(power-up)*
- M_Mode	*(mode_change)*
- M_Level	*(manual_change_level)* *(front_end_change_level)*
- systemVersionIsCompatible	*(trackside_system_version)*
- radioHoleStatus	*(start_of_radio_hole)* *(end_of_radio_hole)*
OrderToRM	Orders to MoRC from onboard or RBC
- orderFromOnboard	*(start_of_mission)* *(end_of_mission)*
- messageFromRBC	*(trackside_establishment_request)* *(trackside_terminating_request)* *(trackside_terminating_ack)* *(init_com_session_msg_in)*
- NID_RBC_ID	*(RBC_id*

RadioNetworkIDs	Radio network IDs memorized, from Driver, from Trackside *(radio_network_identity*
- radioNetworkID_memorized	
- radioNetworkID_fromDriver	
- radioNetworkID_fromTrackside	
SafeRadioComStatus	Status of the safe radio communication
- setupEstablished	*(communication_established)* *(communication_lost)*
- mobileHWConnectionStatus	*(radio_connection_status)*
Output flow	
RM_Status	Actual status of the Management of Radio Communication
- radioComSessionEstablished	*(session_established_report_msg)*
- mobileSWStatus	*(connection_stat_msg)* *(version_error_flag)*
OrderToRBC	Orders to RBC from MoRC
- messageToRBC	*(init_com_session_msg_out)* *(termination_com_session_msg)* *(version_msg)*
SafeRadioComCmd	Control commands to the safe radio communication and to the mobile
- requestSetup	*(radio_setup_request)*
- releaseSetup	*(radio_release_request)*
- mobileHWCmd	
- actualRadioNetworkID	*(radio_network_identity)* *(last_radio_network_identity)*
- memorizeTheLastRadioNetworkID	*(last_radio_network_identity)*

4.3. SEEA

Considering the similarities of the SysML Model and the safety model defined in section 3, no SEEA analyse will be performed on SysML Model for the moment.

5. SAFETY CRITERIA

REQ_FMEA_ID_001

The Mobile Terminal shall be safely registered to a Radio Network.

REQ_FMEA_ID_002

The driver shall be safely informed of the state of the radio communication (resulting of the different steps: registration of the Mobile Terminal to the Radio Network, establishment of the communication, end of communication).

REQ_FMEA_ID_003

If a communication through a Radio Network is active, registration to another Radio Network mustn't be performed.

REQ_FMEA_ID_004

A safety protocol shall be used to performed communication between Mobile Terminal and Radio Network.

REQ_FMEA_ID_005

If a communication with trackside equipment is active, set-up of safe radio connection with another trackside equipment mustn't be performed. Exception in case of handover with RBC.

REQ_FMEA_ID_006

Communication session with trackside equipment shall be safely established.

REQ_FMEA_ID_007

Establishment of communication session shall be performed when no communication is active. Exception in case of handover with RBC.

REQ_FMEA_ID_008

Communication session shall be safely maintained.

REQ_FMEA_ID_009

Terminate a communication session shall be safely defined.

REQ_FMEA_ID_010

The release of the safe radio connection with trackside shall be performed only when the communication session is terminated.

6. TRACEABILITY OF SAFETY CRITERIA WITH SRS

Safety criteria	**SRS section**
REQ_FMEA_ID_001	**§3.5.6**; §3.5.6.1; §3.5.6.3; §3.5.6.5; §3.5.6.6; §3.5.6.7
REQ_FMEA_ID_002	§3.5.3.8-b; **§3.5.7**; §3.5.7.1; §3.5.7.2;
REQ_FMEA_ID_003	§3.5.6.5
REQ_FMEA_ID_004	§3.5.1.1; §3.5.2.2
REQ_FMEA_ID_005	§3.5.3.5.2
REQ_FMEA_ID_006	**§3.5.3**, §3.5.3.2, §3.5.3.4.1, §3.5.3.5.2, §3.5.3.7, §3.5.3.8
REQ_FMEA_ID_007	§3.5.3.5.2
REQ_FMEA_ID_008	**§3.5.4**
REQ_FMEA_ID_009	**§3.5.5**
REQ_FMEA_ID_010	§.3.5.5.2-c

END OF DOCUMENT