OPENETCS

Safety analyse: calculate of train position and orientation function

Confidentiality	Reference	Version	Pages Number	Last modification
Confidentiel	**C693_ASS**	**2A**	**27**	**14/08/2014**

	Name	**Visa**	**Date**
Writer	O. Hervillard		
Verification			
Approbation			

Summary

Figures

1. PREAMBLE

1.1. Object

This document has for aim to describe safety analyses performed, to determine safety requirements, needed for the calculate train position and orientation function.

The scope of safety analyses is:

- The description of the function;
- The failure mode and effects analysis of the function.

1.2. History

Indice Date	Autor	Chapter	Modifications
1A	O. Hervillard	Tous	Création du document

1.3. Diffusion

Name	Society
Équipe projet C593	SYSTEREL

1.4. Applicable documents

No apply

1.5. Reference documents

Doc	Title	Reference
[R1]	WP3-Initial-Architecture.di	SysML model
[R2]	ETCS Application Level 2 - Safety Analysis Part 1 - Functional Fault Tree	SUBSET-088 v2.3.0

1.6. Terminology and abbreviation

FMEA	Failure mode and effects analysis
BH	Boundary Hazard
LRBG	Last Relevant Balise Group

2. METHODOLOGY

This chapter has for aim to explain the FMEA method realized for the safety analysis of the calculate train position and orientation function.

2.1. FMEA

FMEA is a hazards evaluation method based on studies (research and evaluation), for each unique function, of failure modes.

For each failure mode studied, effects on others functions / sub-functions, system effects and safety requirements linked are defined.

Analysis is performed in table format:

N°	Function	Failure mode	Effect	Gravity	Boundary Hazard	Safety requierement	Current action	Recommanded action	Comment

For each function, these parameters must be identified:

- failures mode;
- their direct effects of the failure mode on the outputs of the system;
- their gravity (Gr.);
- their safety requierements;
- boundary Hazard;
- current action to counter the failure mode;
- recommanded action to counter the failure mode;
- free comment to clarify the contents.

The following failure modes are considered for each function:

- erroneous data (authenticity error);
- crosstalk (authenticity error);
- corrupted data (incl. ill-formed data, ambiguous data, etc);
- stale data;
- absence (no execution of the function, no update of a data, absence of a data, etc);
- presence (presence of a function, presence of a data).

The following levels of gravity are defined:

- 0, if there is no impact on the safety of the whole system, or if the system is safer under these conditions;
- 1, if there is an impact on the safety of one channel, and the safety of the whole system is then reduced;
- 2, if the conditions lead to a BH.

If level of gravity is 2, safety requirements must be defined to delete the failure mode.

3. CALCULATE TRAIN POSITION AND ORIENTATION FUNCTION

3.1. Function description

Calculate train position and orientation function receives information from LRBG passed and from odometry data. During a trip and with this information, the function determines the train position and orientation.

The function is composed of two processus:

- Manage Balise Information, manages information from balises and determines the train orientation;
- Manage Train Position, calculates train position due to manage balise information data.

Functional analyses presented in this document are based on SysML model from [R1].

3.2. Safety objectives

3.2.1. Boundary Hazard

A Boundary Hazard (BH) expresses the conditions on the interfaces that could lead to a hazard. For Calculate train position and orientation process, one Boundary Hazard was identified:

BH_1: Incorrect determination of train location reference to LRBG.

This Boundary Hazard is identified in [R2] and in the following fault tree:

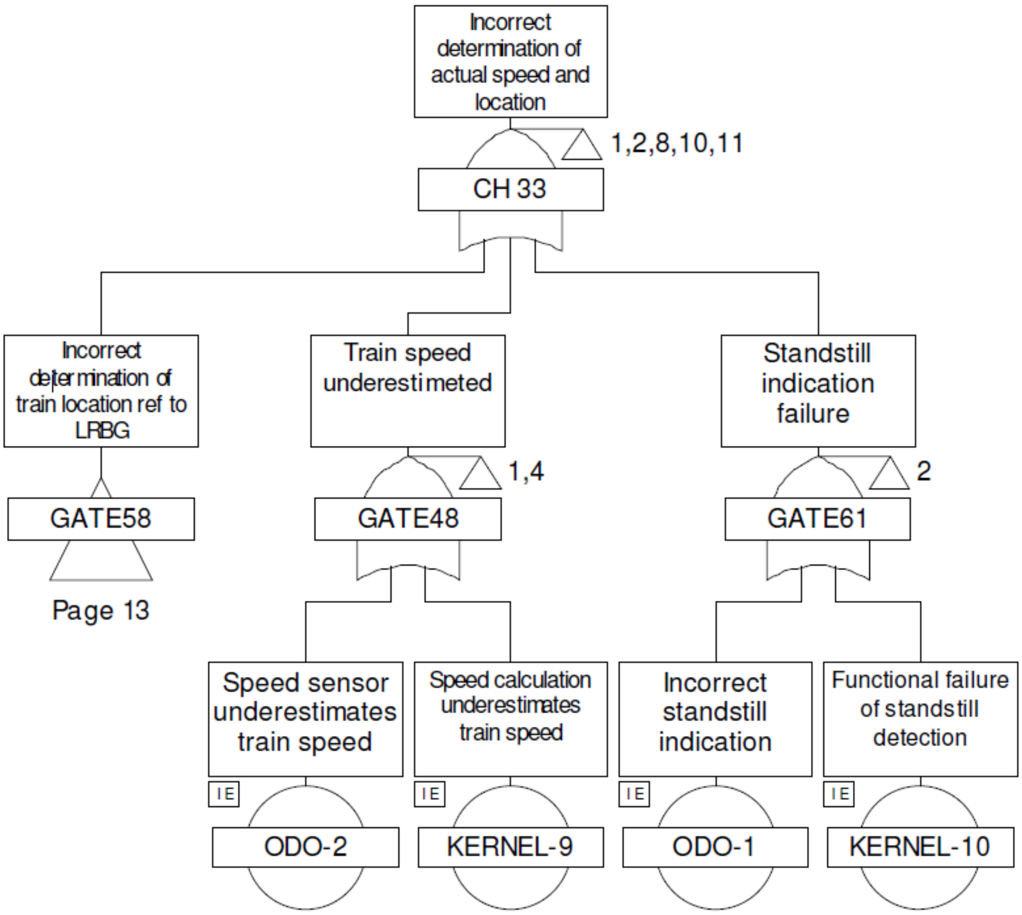
Incorrect determination of actual speed and location
1,2,8,10,11
CH 33
Incorrect determination of train location ref to LRBG
GATE58
Page 13
Train speed underestimeted
1,4
GATE48
Standstill indication failure
2
GATE61
Speed sensor underestimates train speed
IE
ODO-2
Speed calculation underestimates train speed
IE
KERNEL-9
Incorrect standstill indication
IE
ODO-1
Functional failure of standstill detection
IE
KERNEL-10

fig. 1: Fault Tree, [R2]

3.2.2. Safety hypothesis

[H 1] Analysis presented in this document are focusing on safety accepts and not on security accepts. In other words, malicious acts are not considered.

3.3. Manage Location Related Information

3.3.1. Process description

This process has five modules:

- PerformEuroBaliseDecoding;
- BuildBGMessage;
- CheckBGConsistency;
- DetermineBGorientation_LRBG;
- SelectUsableInfo;

PerformEuroBaliseDecoding module has for aim to collect data from balise transmission module, to create the TelegramHeader from these data and to give driver information (If an invalid balise has been received the BTM will pass the Balise information to this function, in this situation the driver has to be informed).

BuildBGMessage has for aim to create “balise group message” from TelegramHeader, balises information, train information and odometry information.

CheckBGConsistency has for aim to check the BG message.

DetermineBGorientation_LRBG has for aim to determine the train orientation from checked BG message

SelectUsableInfo ?

3.3.2. Safety requierement identifiers

All the safety requirements identified within this document are recapped in §3.4. Identifiers are noted as [MTP_ASS_XXX], XXX is the identifier number of the requirement and MLRI for Manage Location Related Information.

3.3.3. AMDE

N°	Function	Failure mode	Effect	Gravity	Boundary Hazard	Safety requierement	Current action	Recommanded action	Comment
	PerformEuroBaliseDecoding	Absence	Impossibility to calculate the position and the orientation of train.	1		MLRI_ASS_005	CheckBGConsistency		
		Loss	Missing output data or wrong output data	2		MLRI_ASS_002 MLRI_ASS_005	CheckBGConsistency		
			Impossibility to calculate the position and the orientation of train.	1		MLRI_ASS_005	CheckBGConsistency		
		Inadvertance	Stale data used.	2		MLRI_ASS_001 MLRI_ASS_005 MLRI_ASS_006			
			Non-existent error detected.	0					Available impact

N°	Function	Failure mode	Effect	Gravity	Boundary Hazard	Safety requierement	Current action	Recommanded action	Comment
		Degraded	Missing output data or wrong output data	2		MLRI_ASS_002 MLRI_ASS_005	CheckBGConsistency		
			Stale data used.	2		MLRI_ASS_001 MLRI_ASS_005 MLRI_ASS_006			
		Non-stop	Stale data used. Wrong output data	2		MLRI_ASS_002 MLRI_ASS_005 MLRI_ASS_006			
			Non-existent error detected	0					Available impact
	BuildBGMessage	Absence	No message available, impossibility to calculate the position and the orientation of train.	1		MLRI_ASS_005	CheckBGConsistency		

N°	Function	Failure mode	Effect	Gravity	Boundary Hazard	Safety requierement	Current action	Recommanded action	Comment
		Loss	Incomplete message or with error, impossibility to calculate the position and the orientation of train.	2		MLRI_ASS_003 MLRI_ASS_005	CheckBGConsistency		
		Inadvertance	Stale data used.	2		MLRI_ASS_002 MLRI_ASS_005 MLRI_ASS_006			
			Non-existent error detected	0					Available impact
		Degraded	Wrong output data	2		MLRI_ASS_005			
			Stale data used.	2		MLRI_ASS_005 MLRI_ASS_006			

N°	Function	Failure mode	Effect	Gravity	Boundary Hazard	Safety requierement	Current action	Recommanded action	Comment
			Incomplete message or with error.	2		MLRI_ASS_003 MLRI_ASS_005			
		Non-stop	Stale data used.	2		MLRI_ASS_002 MLRI_ASS_005 MLRI_ASS_006			
			Non-existent error detected	0					Available impact
	CheckBGConsistency	Absence	Existent error no detected	2		MLRI_ASS_005			
			Impossibility to calculate the position and the orientation of train.	0					Available impact
		Loss	Message unchecked. Existent error no detected.	2		MLRI_ASS_004 MLRI_ASS_005			
		Inadvertance	Stale data used.	1		MLRI_ASS_003 MLRI_ASS_005 MLRI_ASS_006			

N°	Function	Failure mode	Effect	Gravity	Boundary Hazard	Safety requierement	Current action	Recommanded action	Comment
			Non-existent error detected	0					Available impact
		Degraded	Existent error no detected	2		MLRI_ASS_005			
			Introduction of error.	2		MLRI_ASS_005			
			Non-existent error detected.	0					Available impact
		Non-stop	Non-existent error detected.	0					Available impact
			Stale data used for the train position and orientation calculation.	2		MLRI_ASS_003 MLRI_ASS_004 MLRI_ASS_006			
	DetermineBGorientation_LRBG	Absence	Impossibility to calculate the train orientation.	1		MLRI_ASS_005			

N°	Function	Failure mode	Effect	Gravity	Boundary Hazard	Safety requierement	Current action	Recommanded action	Comment
		Loss	Incomplete calculation of orientation	2		MLRI_ASS_005			
			Wrong orientation calculation	2		MLRI_ASS_005			
		Inadvertance	Stale data used.	2		MLRI_ASS_004 MLRI_ASS_006			
			Impossibility to calculate the train orientation. Non-existent error detected.	0					Available impact
			Wrong orientation calculation.	2		MLRI_ASS_005			
		Degraded	Wrong orientation calculation.	2		MLRI_ASS_005			
			Wrong input data used.	2		MLRI_ASS_004 MLRI_ASS_005 MLRI_ASS_006			
			Incomplete orientation calculation.	2		MLRI_ASS_005			

N°	Function	Failure mode	Effect	Gravity	Boundary Hazard	Safety requierement	Current action	Recommanded action	Comment
		Non-stop	Stale data used	2		MLRI_ASS_004 MLRI_ASS_005 MLRI_ASS_006			
			Non-existent error detected.	0					Available impact

3.3.4. Safety requirement

The purpose of this chapter is to resume safety requirements linked with the calculate train position and orientation function.

Safety requirements are identified below:

#	Safety requierement
MLRI_ASS_001	PerformEuroBaliseDecoding process must be able to check : - The good definition (parameters values and file format requierement) - completeness; - data integrity; - version; of these input data.
MLRI_ASS_002	BuildBGMessage process must be able to check : - The good definition (parameters values and file format requierement) - completeness ; - data integrity ; - version, Of these input data.
MLRI_ASS_003	CheckBGConsistency process should be able to check : - The good definition (parameters values and file format requierement) - completeness ; - data integrity ; - version, Of these input data.
MLRI_ASS_004	DetermineBGorientation_LRBG process should be able to check : - The good definition (parameters values and file format requierement) - completeness ; - data integrity ; - version, Of these input data.
MLRI_ASS_005	As explain in the SUBSET-091, onboard equipments must have a failure rate < 10-9 f/h. Thus, SIL 4 process should be applicable for : - PerformEuroBaliseDecoding ; - BuildBGMessage ; - CheckBGConsistency ; - DetermineBGorientation_LRBG.

#	Safety requierement
	Process.
MLRI_ASS_006	To avoid using stale data, input data of each module should be deleted at the end of the process.

3.4. Manage Train Position

3.4.1. Process description

This process has three modules:

- ValidDataDirect module;
- CalculateTrainPosition module;
- ManagePositionReport module.

ValidDataDirect module has for aim to check input data whose will be sent to CalculateTrainPosition module.

CalculateTrainPosition has for aim to calculate train position from balises information, train information and odometry information.

ManagePositionReport has for aim to manage errors during the calcul of the train position. This module generates a rapport with parameters used for the position calculation, train position, train information and errors detected.

Rapport must include at least information identified in: 3.6.5.1.2/subset-06-3.

This process is described on the following figure:

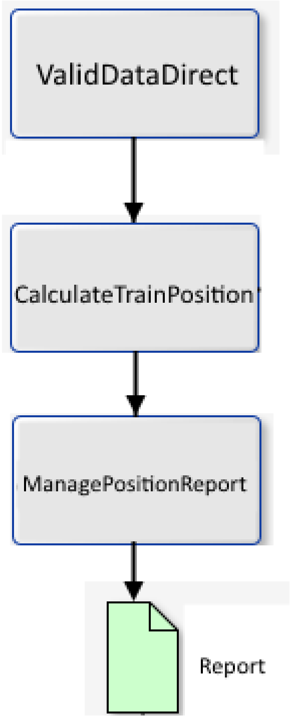

fig. 2: Manage Train Position Process

3.4.1. Safety requierement identifiers

All the safety requirements identified within this document are recapped in §5. Identifiers are noted as [MTP_ASS_XXX], XXX is the identifier number of the requirement (MTP for Manage Train Position).

3.4.2. AMDE

N°	Function	Failure mode	Effect	Gravity	Boundary Hazard	Safety requierement	Current action	Recommanded action	Comments
1.	Calculate Train Position	Absence	Train position information unavailable.	1		MTP_ASS_004	Manage Position Report		
2.			No calculation of train position, stale data of train position used by others modules.	2	BH_1	MTP_ASS_002 MTP_ASS_003 MTP_ASS_004 MTP_ASS_006			
3.		Loss	Incomplete data of train position. Stale data used by Manage Position Report.	2	BH_1	MTP_ASS_002 MTP_ASS_004 MTP_ASS_007			
4.			Train position information unavailable or with partial information.	1		MTP_ASS_002 MTP_ASS_004 MTP_ASS_006	Manage Position Report		
5.		Inadvertance	Stale data used, wrong calculation of train position.	2	BH_1	MTP_ASS_001 MTP_ASS_004 MTP_ASS_006 MTP_ASS_007	Manage Position Report		

N°	Function	Failure mode	Effect	Gravity	Boundary Hazard	Safety requierement	Current action	Recommanded action	Comments
6.			Input data unavailable. Impossibility to calcul train position.	0		MTP_ASS_004			Availabilyt impact
7.		Degraded	Wrong train position information.	2	BH_1	MTP_ASS_004 MTP_ASS_007	Manage Position		
8.			Train position information unavailable or with partial information. Stale data used by the module Manage Position Report.	1		MTP_ASS_002 MTP_ASS_004 MTP_ASS_005 MTP_ASS_006 MTP_ASS_007			Availabilyt impact
9.		Non-stop	Input data unavailable to calculate train position. Nonexistent errors detected.	0		MTP_ASS_004			Availabilyt impact
10.			Stale data used, wrong train position calculated.	2	BH_1	MTP_ASS_001 MTP_ASS_004 MTP_ASS_006 MTP_ASS_007	Manage Position Report		

N°	Function	Failure mode	Effect	Gravity	Boundary Hazard	Safety requierement	Current action	Recommanded action	Comments
11.	Manage Position Report	Absence	No detection of errors	2	BH_1	MTP_ASS_004			
12.			Train position information not saved.	1		MTP_ASS_004			Impact sur la disponibilité
13.		Loss	No detection of errors	2	BH_1	MTP_ASS_004			
14.			Train position information not saved.	1		MTP_ASS_004 MTP_ASS_006			
15.		Inadvertance	Nonexistent errors detected.	0		MTP_ASS_004			Impact sur la disponibilité
16.			Stale input data used, wrong train position information.	2	BH_1	MTP_ASS_002 MTP_ASS_007			
17.		Degraded	No detection of errors	2	BH_1	MTP_ASS_004			
18.			Nonexistent errors detected.	0		MTP_ASS_004			Impact sur la disponibilité

N°	Function	Failure mode	Effect	Gravity	Boundary Hazard	Safety requierement	Current action	Recommanded action	Comments
19.			Train position information not saved.	1		MTP_ASS_004			
20.			Wrong train position information.	2	BH_1	MTP_ASS_004			
21.		Non-stop	Nonexistent errors detected.	0		MTP_ASS_004			Impact sur la disponibilité
22.			Stale date used, wrong train position information.	2	BH_1	MTP_ASS_004 MTP_ASS_007			
23.	ValidDataDirect	Absence	Stale date used by CalculateTrainPosition module. Wrong train position information.	2	BH_1	MTP_ASS_001 MTP_ASS_004 MTP_ASS_006 MTP_ASS_007	Manage Position Report		
24.			Data unavailable for module Calculate Train Position, calculate of train position impossible.	1		MTP_ASS_004 MTP_ASS_005	Manage Position Report		
25.		Loss	Stale date used by CalculateTrainPosition module. Wrong train position information.	2	BH_1	MTP_ASS_001 MTP_ASS_004 MTP_ASS_005 MTP_ASS_007	Manage Position Report		

N°	Function	Failure mode	Effect	Gravity	Boundary Hazard	Safety requierement	Current action	Recommanded action	Comments
26.			Data unavailable for module Calculate Train Position, calculate of train position impossible.	1		MTP_ASS_004 MTP_ASS_005	Manage Position Report		
27.		Inadvertance	Manage Position Report : Nonexistent errors detected.	1		MTP_ASS_001 MTP_ASS_004 MTP_ASS_005 MTP_ASS_007	Manage Position Report		Availability impact
28.			Calculate train position: Stale date used by CalculateTrainPosition module. Wrong train position information.	2	BH_1	MTP_ASS_001 MTP_ASS_004 MTP_ASS_005 MTP_ASS_007	Manage Position Report		
29.		Degraded	Calculate train position: Stale date used by CalculateTrainPosition module. Wrong train position information.	2	BH_1	MTP_ASS_001 MTP_ASS_004 MTP_ASS_005 MTP_ASS_007	Manage Position Report		
30.			Input data unavailable for CalculateTrainPosition. Impossibility to calcul train position.	1		MTP_ASS_001 MTP_ASS_004 MTP_ASS_005 MTP_ASS_007	Manage Position Report		

N°	Function	Failure mode	Effect	Gravity	Boundary Hazard	Safety requierement	Current action	Recommanded action	Comments
31.		Non-stop	Calculate train position : Stale date used, Wrong train position information.	2	BH_1	MTP_ASS_001 MTP_ASS_004 MTP_ASS_005 MTP_ASS_007	Manage Position Report		

3.4.3. Safety requirement

The purpose of this chapter is to resume safety requirements linked with the calculation train position and orientation function.

Safety requirements are identified below:

#	Safety requierement
MTP_ASS_001	CalculateTrainPosition process must be able to check : - The good definition (parameters values and file format requirement) - completeness ; - data integrity ; - version, Of these input data.
MTP_ASS_002	ManagePositionReport process must be able to check : - The good definition (parameters values and file format requirement) - completeness ; - data integrity ; - version, Of these input data.
MTP_ASS_003	ValidDataDirect process should be able to check : - The good definition (parameters values and file format requirement) - completeness ; - data integrity ; - version, Of these input data.
MTP_ASS_004	As explain in the SUBSET-091, onboard equipments must have a failure rate < 10-9 f/h. Thus, SIL 4 process should be applicable for : - Calculate Train Position ; - Manage Position Report ; - ValidDataDirect. Process.
MTP_ASS_005	ManagePositionReport report should contains as minimum information describe in the Subset-06-3 chapter 3.6.5.1.2
MTP_ASS_006	ManagePositionReport should be able to indentify this kind of error : - Input data unavalaible for the CalculateTrainPosition module; - Stale data used by CalculateTrainPosition - Failure of CalculateTrainPosition and ValidDataDirect.

#	Safety requierement
MTP_ASS_007	To avoid using stale data, input data of CalculateTrainPosition and ManagePositionReport process should be deleted at the end of ManagePositionReport process.

FIN DE DOCUMENT