Functional Hazard Analysis (FHA) as basis for safety requirement definition: The ETCS case study

Abstract: This paper aims to demonstrate the application of FHA for railway industry application as part of RAMS program implementation based on the standard EN 50129 concept. Such risk analysis enables to predict the effect of the safety critical element, which may trigger a major accident such as collision or derailment. In addition, it´s possible to define the level of safety integrity necessary for such safety critical element. In order to demonstrate the FHA concept application a cases study concerns ETCS will be demonstrated

Key Words: FHA, SIL, Risk Matrix, THL, ETCS

Author: Dr. Eduardo Calixto, ECC, Germany

1 - Risk Analysis Methods

The Risk Analysis started around middle of twenty centuries in different industries with different approaches like:

- In 1960's - Aerospace Industry with Quantitative Risk Assessment methods, Nuclear Industry with Probabilistic Risk Assessment approach,
- In 1970's - Chemic Industry with Quantitative Risk Assessment and Seveso directive,
- In 1980's - Oil and Gas Industry with Quantitative Risk Assessment and Safety Case,

The other industries such as railways followed the established approaches, methods, customized the risk management standards and adapted the risk analysis methods to their characteristics and requirements.
The risk methods are part essential to the risk assessment and aims to identify the hazards, assess and evaluate the risk. Such risk methods are qualitative or quantitative approach.
In the first case, a group of specialists identifies hazards and qualify risk based on risk matrix. In the second case, despite hazards being identified qualitatively based on specialist opinion, risk is calculated by mathematical methods. The risk analysis methods can also be classified as deductive or inductive. The deductive risk analysis methods first identify the hazards or incidents and then their causes, consequences and when the risk mitigation is necessary, some recommendations are proposed. The inductive risk analysis methods first define process deviation, equipment failures, incident or accident and after the causes, which lead to an incident or accident. The most usual qualitative risk analysis methods applied to railways are:

- ***PHA*** (Preliminary Hazard Analysis) is a qualitative inductive method, which identifies hazards, causes, consequences, detections and propose recommendations. In some cases, PHA has a risk assessment based on risk matrix, where probability (or frequency) is related to the causes and severity that is related to consequences.

• ***FMEA*** (Failure Mode Effect and Analysis) is a qualitative inductive method, which identifies equipment failure modes, causes, detection and finally consequences. In FMEA case, when focus is safety, will be regarded unsafe failures, that means failure that cause an unsafe condition of equipment that can trigger an accident.

• The ***Functional Hazard Analysis*** is a qualitative deductive risk analysis, which is a very important method concerning electric and electronic equipment in the railway industry. The first step is to describe the equipment function and further the functional failures, hazard, cause and consequences. Such method addresses the recommendation to the equipment functional safety requirement achievement as well as defined the test to be carried out to confirm and validate such function. In the railway industry, such method is correlated with the SIL analysis because enable a SIL definition depends on the Tolerable hazard level.

• ***HAZOP*** (Hazard Operability) is a qualitative inductive method, which identifies deviation, causes and finally Hazard consequences. In HAZOP case, the deviation applied to railway assets are: interface, time, action, limit, high level, and high flow. In fact, the HAZOP method defines guide words such as high, low, partial, absent, no and combine with such defined parameters.

The most usual quantitative risk analysis methods applied to railways are:

• The ***FTA*** (Fault Tree Analysis) that is a quantitative deductive method, which identifies the top event, that is an incident or accident and go into further detail about the combination of event that trigger such top event. Such combination is defined by logical gates based on "Boolean Logic" that basically, define the combination of basic events.

• ***ETA*** (Event Tree Analysis) is a quantitative inductive method, which identifies initiate the event, an incident or hazard and furthers the sequence of events that can trigger one or more accident scenario.

• ***LOPA*** (Layer of Protection Analysis) is a quantitative inductive method, which identifies initiate event (an incident or hazard) and furthers the sequence of layers of protection that can avoid accidents.

• ***SIL*** (Safety Integrity Level) is a quantitative deductive method, which identifies the probability of failure on demand that one specific SIF (Safety Instrumented Function) must achieve in order to mitigate risk to an acceptable level. In case of the railway industry, the SIL is applied to a different context. Therefore, each electric and electronic element function needs to be assessed based on the Tolerable Hazard Level, which is related to a SIL category which varies from 1 to 4.

• The ***Bow Tie*** is a quantitative deductive method, which identifies the causes and consequences of incidents as well as control and recovery measures. This method defines accidents causes combined as well as the sequence of events that results in the final accident scenario.

In the railways industry case, the main reference for the risk management and risk methods are the standards EN 50126 and EN 50129 (for Electric and Electronic equipment). The table 1 describes all risk methods application and additional safety task along the railway asset life cycle.

Similar to the RAM program part, it´s necessary to have a safety plan, which will describe the safety, organizational structure, the safety team members' responsibilities, the internal and external organizational interface, the safety index, the applied risk methods described, the activities schedule, the safety verification and validation test schedule and final deliverables and the safety Case.

During the concept phase, once established the safety requirement during the BID, the equipment supplier selection take place. After the suppliers are defined, all activities defined in the safety plan need to be implemented and followed up during the asset life cycle.

During the design phase, the safety KPI are verified based on different risk methods. It is also important to understand that, from a safety point of view, reliability is associated with unsafe failure for many systems such as signaling, bogie, brakes and TCMS. Therefore, the safety indexes are not only risk and SIL level, but also reliability, that is unfortunately not demonstrated as part of safety and risk analysis.

The "DFMEA" is also important because the DFMEA recommendation tries to avoid unsafe failures caused by bad material quality, bad design, bad configuration that can trigger accidents.

On "System Validation phase" functional test need to be implemented to demonstrate that all critical functions fail safely. In addition, during the warranty period, the safety and reliability index will be validated.

It´s also important to update the risk analysis during the operational phase and whenever the system is modified. The "reliability data base" about unsafe failures must be implemented as part of the FRACAS system to support futures risk analysis.

During operation, the preventive maintenance, test and inspection play an important hole in risk mitigation. Therefore, all preventive maintenance, test and inspection tasks defined during the RCM analysis in design phase must be implemented and be part of the asset management system as will be discussed in chapter 10.

Table 1 Safety tasks through asset life cycle
Source: EN 50126

LIFE CYCLE PHASE RELATED	GENERAL TASKS	PHASE RELATED Safety TASKS
1. Concept	_Establish Scope and purpose of Railway project. _Define Railway project concept. _Undertake financial analysis & feasibility studies. _Establish Management.	_Review previous achievement, safety performance (previous HazLog, PHA, SIL). _Consider Safety implication of the project. _Review Safety policy & safety target.
2. System definition and application conditions	_To establish a system mission profile. _Prepare system description. _Identify operation & maintenance strategy. _Identify operation conditions. _Identify maintenance conditions. _Identify the influence of existing infrastructure constraints.	_Establish Safety Plan (overall). _Evaluate past experience data for Safety. _Perform Preliminary Hazard analysis. _Define tolerability of risk criteria. _Identify the influence on RAM of existing infrastructure constraints.
3. Risk Analysis	_Undertake project related Risk Analysis	_Perform System Hazard & Safety Risk Analysis _Set-up Hazard Log, Perform Risk Assessment
4. System requirements	_Undertake requirement analysis. _Specify system (overall requirements). _Specify Environment. _Define system demonstration & acceptance criteria (overall requirement). _Establish a validation plan. _Establish Management, Quality & Organizational requirements.	_Specify System Safety requirement (overall). _Define Safety acceptance criteria (overall). _Define system functional Structure. _Establish the RAM program. _Establish RAM management.
5. Apportionment	_Apportion system requirement.	_Apportion system safety, target & requirements.

of system requirements	_Specify subsystem & component acceptance criteria. _Define sub-system & component acceptance criteria.	_Specify subsystem & component safety requirement. _Define sub-system & component safety, acceptance criteria. _Update system safety plan.
6. Design and implementation	_Undertake requirement analysis. _Specify system (overall requirements). _Specify Environment. _Define system demonstration & acceptance criteria (overall requirement). _Establish a validation plan. _Establish Management, Quality & Organizational requirements.	_Implement Safety Plan by reviewing, Analysis, testing and Data assessment, addressing:. Hazard log, Hazard analysis & risk assessment _Justify safety related design decision.. _Undertake Program control, covering: Safety management, Control of sub-contractors, supplier. _Prepare generic Safe case control, covering: Prepare (if applicable) generic application safe case
7. Manufacturing	_Perform Production Planning, Manufacture, Manufacture and Test Sub-assembly of components _Prepare documentation _Establish training	_Implement safety plan by: review, analysis, testing & data assessment. _Use Hazard Log.
8. Installation	Assemble System Installation	
9. System Validation (including safety, acceptance and commissioning)	_Commission _Perform probationary period of operation _Undertake training	Prepare application specific safety case.

2 – Functional Hazard Analysis

The Functional Hazard Analysis (FHA) aims to define the system functions and function failures associate with hazards to support the safety function requirement definition. The system function will have more than one sub functions and all hazards associated with each function must be assessed. The function is the description of the system propose, in other words, what such system does. Whenever the Functional hazard analysis is carried out, the scope will be only the safety associated function, that means, the function, which can lead in an accident in case of loss, partial loss, wrong action or unintended action.

The basis for the Functional Hazard Analysis is the Preliminary hazard analysis, which describes the hazards which need to be associated with each system function. Based on EN 50129, the FHA focus on safety-related electronic systems (including sub-systems and equipment) for railway signaling applications. The nonelectric and electronic equipment will follow the PHA and can be assessed in more detailed in other risk analysis level, such as System Hazard Analysis or Failure Mode and Effect Analysis.

The system is the high-top level and depends on the EE configuration different systems can be defined under the FHA scope. The system encompasses one or more hardware and software and have an interaction with other system. Usually, there´s a confusion when the FHA is being carried out to go into detailed considering the hardware or software, but that will be the further step after the FHA. Actually, all functions considered in the FHA are of course associated with some hardware or software, but the intention is not to depict such information at this level. The figure 1 describes the sequence of safety analysis including the input and output of the Functional Hazard Analysis, which is part of hazard analysis and risk assessment.

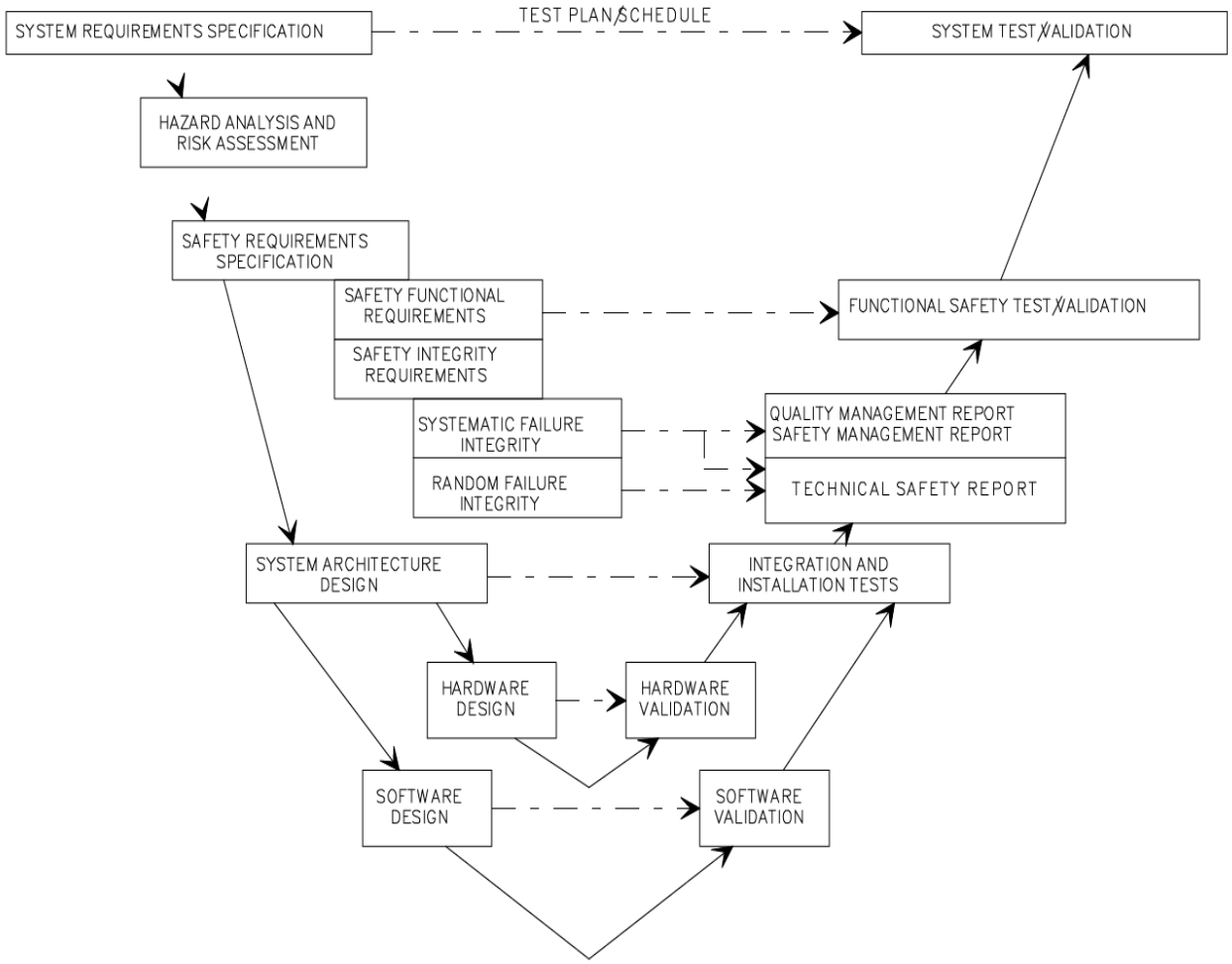

Figure 1 - Example of design and validation portion of system life-cycle Source: EN 50129 (2003).

2 – Risk Analysis and evaluation

Regarding the qualitative risk approach, is important to understand that different equipment in railway industry has different life cycle time and such systems requires different values of frequency in risk matrix. Even though, the standard EN 50126 establishes an example of risk matrix six per five as well as the quantitative risk requirement that must be followed by Railway industry. As shown the table 1 below.

			Hazard Severity Level			
			Insignificant	Marginal	Critical	Catastrophic
			IV	III	II	I
Frequency of occurence	Frequent	A	Undesirable	Intolerable	Intolerable	Intolerable
	Probable	B	Tolerable	Undesirable	Intolerable	Intolerable
	Occasional	C	Tolerable	Undesirable	Undesirable	Intolerable
	Remote	D	Negligible	Tolerable	Undesirable	Undesirable
	Improbable	E	Negligible	Negligible	Tolerable	Tolerable
	Incredible	F	Negligible	Negligible	Negligible	Negligible

Table 2 - Risk Matrix
Source: EN 50126

In order to define the risk level, it´s necessary to understand the severity and frequency classification applied to the risk matrix. The, severity classification must describe all parties affected in the case of an accident, such as employees, passenger and environment. The table 2 shows an example of severity category based on EN-50126 definition.

Table 3 - Hazard Severity Level
Source: based on EN-50126.

Description	Abbreviation
Catastrophic : Fatalities and/or multiple severe injuries and/or major damage to the environment.	I
Critical : Single fatality and/or severe injury and/or significant damage to the environment.	II
Marginal : Minor injury and/or significant threat to the environment.	III
Insignificant : Possible minor injury or minor system damage.	IV

The table 4 shows six categories of frequency of occurrence of hazardous categories regarding aspects like personal safety, and environment. In some risk analysis the probability category can also be applied. In fact, for the specialist point of view, it´s easier to estimate the frequency rather than the probability. The probability is a very subjective value to be estimated and depends too much of each one perception. By the other hands, the frequency is easier to be estimated because is related with the number of occurrences along the life cycle. However, the most important point is to have an agreement amongst the involved part, which will be part of the risk analysis and also receive the risk analysis form vendors. Therefore, the risk concepts, as well as risk matrix definition must be agreed before to carry out any type of risk method, which apply the risk matrix.

Table 4 - Frequency of occurrence of hazardous events
Source: based on EN-50126.

Description	Abbreviation / rating	Frequency
Frequent: Likely to occur frequently; the hazard will be continually experienced	**A**	10-4≤ F < 10-3
Probable: Will occur several times; the hazard can be expected to occur often	**B**	10-5≤ F < 10-4
Occasional: Likely to occur several times; the hazard can be expected to occur several times	**C**	10-6≤ F < 10-5
Remote: Likely to occur somewhere in the system lifecycle; the hazard can be reasonably expected to occur.	**D**	10-7 ≤ F < 10-6
Improbable: Unlikely to occur but possible; the hazard can be assumed it may exceptionally occur	**E**	10-8 ≤ F < 10-7
Incredible: Extremely unlikley to occur; it can be assumed the hazard may not occur	**F**	10-9 ≤ F < 10-8

3 – FHA ETCS onboard case study

The safety requirement defined for the system must be allocated to the system function. The functional hazard analysis at the system level produces the functional safety requirement as well as the safety integrity level requirement considering the random system failures as will be discussed in the next item. The functional safety requirement must be validated by the test firstly in the hardware and software level and after at the system level after hardware and software integration as described in figure 1. The table 5 shows an example of the Functional Hazard Analysis applied to the European Train Control System (ETCS). The first column shows the column reference number, which is related to the possible accident causes by some specific sub-function failure. The second columns show the functions of the ETCS. The third column shows the sub-functions of each ETCS function. The fourth column shows the function failure mode, such as total loss of the function and wrong information or command. The fifth column shows expected frequency of the functional failure mode, that is defined based on the frequency of the occurrence table defined in table 4. The sixth column shows the scenario, which describe the situation of the train such as: stopped, moving at low speed or moving at high speed. In order to capture the worst scenario, the FHA considered only the scenario “Train moving in high speed”. The seventh column shows the potential accident caused by the functional failure, which in the worst-case scenario are derailment and collision. The eight columns show the accident effect severity classification based on the table 1 definition, which in case of train collision or derailment is expected more than one fatality and several serious injuries. The ninth column shows the risk level definitions based on the risk matrix defined in table 1, which consider the frequency (table 4) and severity (table 3) combination. The column tenth shows the functional safety requirement to mitigate such unacceptable risk. The eleventh column shows the frequency after the safety functional mitigation implemented. The twelfth columns show the severity, which is not mitigated because once the accident, such as collision and derailment happen, the effect will be the same. The thirteenth columns show the new risk level after the functional requirement implemented based on the table 1 classification, which consider the frequency (table 4) and severity (table 3) combination. After this stage, based on the Functional hazard analysis the Tolerable Hazard level and the associated safety Integrity Level will be defined as well as the SIL allocation for the hardware and software.

Table 5 - ETCS on board Functional Hazard Analysis

N°	Function	Sub-Function	Failure Mode	Frequency	System Effect	Scenario	Potential Accident	Hazard Severity Level	Risk Level	Safety Function Requirement	Frequency	Hazard Severity Level	Risk Level
1	2	3	4	5	6	7	8	9	10	11	12	13	14
1	1 - Train position detection	1.1 - Localize the train position by the Carborne Controller	Loss of position detection function.	Occasional	The Carborne Controller doesn't know train position	Train traveling in high speed	Derailment or Collision	I	Intolerable	1 - Driver must be warned in case of Loss of train position detection function by visual and auditive alarm. 2. Train position detection /calculation function must have redundant configuration to mitigate the risk of total loss of this function.	Improbable	I	Tolerable
2			Erroneous Detection	Occasional	The Carborne Controller sends wrong train location	Train traveling in high speed	Derailment or Collision	I	Intolerable	3 - Driver must be warned in case of corrupted position detection/calculation function by visual and auditive alarm.	Improbable	I	Tolerable
3		1.2 Track trains by the Zone Controler.	Loss of track function.	Occasional	The Zone Controller doesn't know train position	Train traveling in high speed	Derailment or Collision	I	Intolerable	4 - Driver must be warned in case of Loss of track detection/calculation function by visual and auditive alarm. 5 - Train track detection/calculation function must have redundant configuration to mitigate the risk of total loss of this function.	Improbable	I	Tolerable
4			Erroneous track	Occasional	The Zone Controller sends wrong train location	Train traveling in high speed	Derailment or Collision	I	Intolerable	6- Driver must be warned in case of Loss of detection function by visual and auditive alarm.	Improbable	I	Tolerable
5	2 . Train separation	2.1 - Ensure the safe train separation distance continuously	Loss of safe separation function	Occasional	The Zone Controller does not locate the train and consequently trains are not safe separately	Train traveling in high speed	Collison	I	Intolerable	7 - Driver must be warned in case of Loss of detection function by visual and auditive alarm . 8- Train separation detection/calculation function must have redundant configuration to mitigate the risk of total loss of this function.	Improbable	I	Tolerable
6			Wrong separation command	Occasional	Tre train are not safe separated in the same zone	Train traveling in high speed	Collision	I	Intolerable	9 - Driver must be warned in case of corrupted track detection/calculation function by visual and auditive alarm.	Improbable	I	Tolerable
7	3 . Train Overspeed protection	3.1 - Supervise train speed	Loss of train speed supervision	Occasional	The drivers is unknow about the train overspeed	Train traveling in high speed	Derailment	I	Intolerable	10 - Driver must be warned in case of Loss of speed detection/calculation function by visual and auditive alarm. 11 - Train speed detection/ calculation function must have redundant configuration to mitigate the risk of total loss of this function.	Improbable	I	Tolerable
			Wrong train speed information	Occasional	The drivers is wrong informed about the train overspeed	Train traveling in high speed	Derailment	I	Intolerable	12 - Driver must be warned in case of speed detection/ calculation function corrupted by visual and auditive alarm.	Improbable	I	Tolerable

The further step concerning the safety requirement is to define the functional safety architecture, which need to comply with the functional safety requirement. Therefore, it will be possible later to define technical safety requirement for the hardware and software levels as well as the technical safety configuration. The figure 2 below shows the functional safety architecture based on the functional safety requirement. The validation will be based on tests, which demonstrate the functional safety requirement firstly in the hardware and software level later on at the system level.

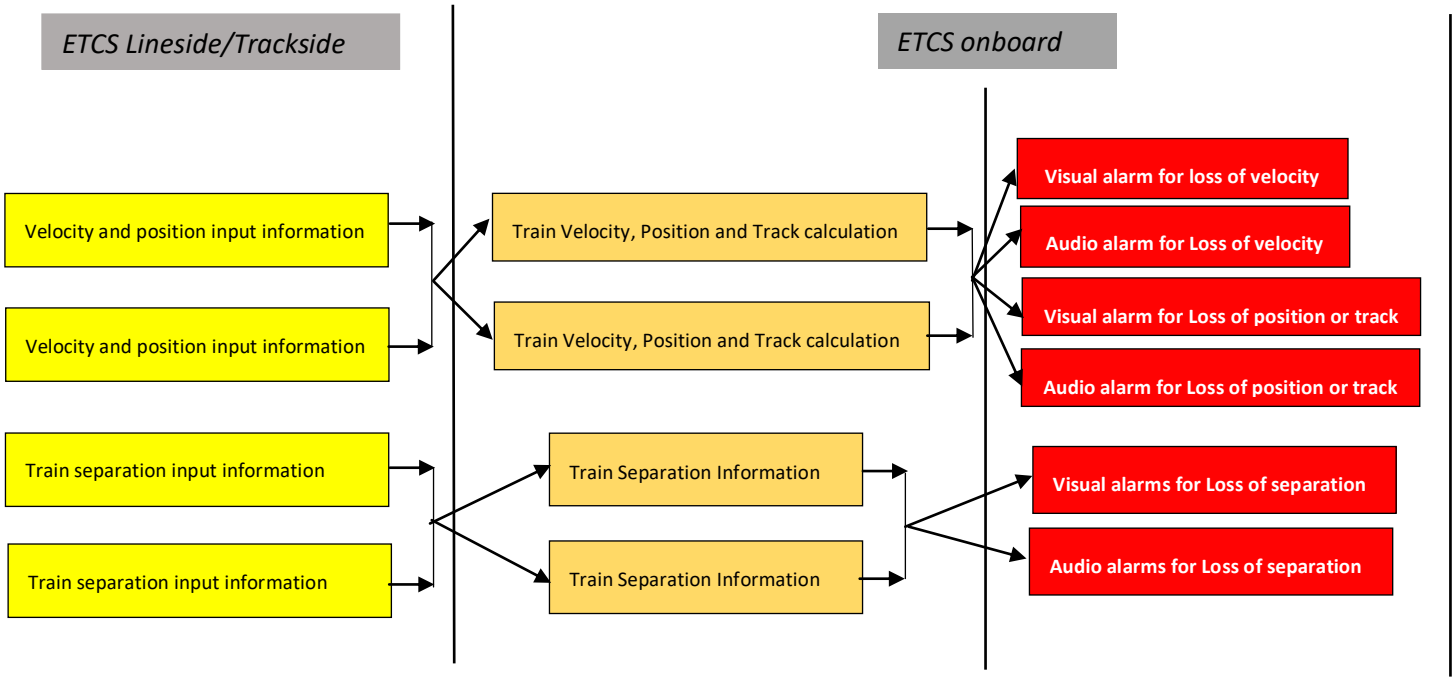

Figure 2 - Functional Safety Architecture

5– Conclusion

The paper achieves the main objective that was to demonstrate the FHA application to railway safety critical electrical and electronic physical assets. The FHA has the main objective to assess the electric and electronic safety function and enable to establish the safety requirement for the different safety function. Therefore, the ETCS case study was applied to demonstrate the FHA application considering the main hazard related to ETCS equipment function as well as to establish the necessary requirement to mitigate the risk. In doing so, the Functional safety architectures established based on such functional requirement. The next step is to define the safety integrity level for each function based on the tolerable hazard level considering the established risk classification. Such application will be demonstrated in the next technical paper.

The Functional Hazard Analysis has as main advantages:

- To enable the functional safety requirement;

- To define the functional safety architecture based on functional safety requirement;
- To establish the basis for the SIL selection;
- To establish the basis for the hardware and software SIL allocation;
- To define the basis for the functional safety verification and validation test.

The FHA drawbacks are:

- Depends on specialist experience to define all functional safety function failures;
- Since being a qualitative analysis can be overestimate that will influence on more effort than necessary in the functional safety design;
- Since being a qualitative analysis can be underestimated that will influence on less effort in the functional safety design;

References

Calixto, Eduardo. Safety Science: Methods to Prevent Incident and worker Health Damage at Workplace. ISBN-13: 978-1608059539 Bentham Science.

EN 50126, Railway applications – The specification and demonstration of reliability, availability, maintainability and safety (RAMS). Part 1: Basic requirements and generic process. Part 2: Guide to the application of EN 50126-1 for safety (CLC/TR). Part 3: Guide to the application of EN 50126-1 for rolling stock RAM (CLC/TR), 1999.

EN 50128, Railway applications – Communication, signalling and processing systems – Software for railway control and protection systems, 2001.

EN 50129, Railway applications – Communication, signaling and processing systems – Safety related electronic systems for signaling, 2003.

ETCS level 2, http://www.mermecgroup.com/protect/atpatc-systems/630/ertmsetcs-level-2.php

ISO 9001 Quality Management. ISO. International Organization for Standardization. Retrieved 2 October 2015.