Research and Practice on Digital Development and Management of Road Vehicles Functional Safety

Yinshu Wu[1, a], Yue Qin[1, b] and Chenxing Ouyang[1, c]

[1]CATARC (Tianjin) Automotive Engineering Research Institute Co.,Ltd., Tianjin, China

[a]wuyinshu@catarc.ac.cn

Abstract

This paper introduces the current situation of road vehicle functional safety development and management and the pain points in its practice. Based on this, it systematically combs the demand analysis and overall design of the digital process of functional safety development and management, and takes the concept stage as an example to introduce its digital practice process in detail, which has theoretical and practical significance for the standardization and digitalization of road vehicle functional safety development and management.

Keywords

Functional safety development; Digital process; Functional Safety Concept Phase.

1. INTRODUCTION

With the continuous development of modern science and technology, the degree of electrification and intelligence of automobiles is getting higher and higher, and the functions and systems of automobile models are increasing. In view of this, the International Organization for Standardization has formulated the international standard ISO26262 for functional safety of automotive electronic and electrical systems with reference to the basic standard IEC61508 for functional safety of electronic, electrical and programmable devices, which has been implemented for many years. This standard is a functional safety standard for road vehicles and is applicable to all safety related systems composed of power, electronic and programmable electronic devices that provide safety related functions on road vehicles. As many countries in Europe and the United States have written automobile safety into their regulations, the major OEMs and component suppliers in the foreign automobile industry attach great importance to automobile functional safety. They have implemented the ISO26262 standard within the enterprise, formed their own functional safety team, developed a development and verification process that meets the requirements of the functional safety standard, and made the development process and products conform to the ISO26262 standard, so as to meet the safety needs of automobile products in operation. In the functional safety development standard, the development life cycle is divided into concept stage, system level, hardware level and software level according to the system engineering V process. The development life cycle is divided into multiple stages, each stage includes input, process requirements, tools and methods used, and verification requirements. At present, the functional security development in the industry mainly relies on Office tools, which are cumbersome to operate and low in the utilization rate of data derivation. It is urgent to use the online electronic platform system to manage the functional security development projects.[2]

2. STATUS QUO OF DEVELOPMENT AND MANAGEMENT OF ROAD VEHICLE FUNCTIONAL SAFETY

In the safety standard IEC 61508, the concept of safety is "no unacceptable risk". Functional safety focuses on the safety of electronic and electrical system functions. To achieve this goal, the first version of road vehicle functional safety standard ISO 26262 was released in 2011 [1]. In 2017, in the national standard GB/T 34590, the development goal of functional safety was defined as that there was no unreasonable risk caused by the harm caused by the abnormal performance of electronic and electrical systems. ISO 26262 standard covers all safety related applications in the development of automotive electronics and electronics, and formulates all safety related activities throughout the life cycle of the vehicle. ISO 26262 standard puts forward corresponding functional safety requirements from requirements, including conceptual design, software and hardware design, to final production and operation, which cover the entire life cycle of the vehicle, so as to ensure that the functional failure of safety related electronic products will not cause danger.[3][4]

In production and operation. During the whole life cycle of maintenance and scrapping, ISO26262 guarantees the functional safety performance objectives of automotive electronic control products that meet the technical requirements of functional safety by specifying process parameter consistency, qualified production/operation/maintenance tools, strict production/operation/maintenance processes, standard use information, etc. At the same time, ISO 26262 also ensures the consistency and reliability of the functional safety performance of electronic control products by specifying the development interface, definition of safety requirements, configuration, change, verification, software and hardware tools/components required by the support process, which are similar in nature to the similar characteristics of the quality management system.

To sum up, we can see that functional safety is a systematic and complete system, with very strict internal logic. Any adjustment to any part of it may cause damage or loss to the overall logic chain. According to the research, the functional safety development in the industry mainly relies on Office tools, which are cumbersome in operation and low in data derivation rate. The existing digital platform for the development and management of automotive functional safety is mainly based on foreign software, with high tool costs, and lacks the full life cycle functional safety development project management capabilities. Auto engine manufacturers, primary and secondary suppliers urgently need a standardized, systematic, procedural and convenient online management platform. Next, this paper will give a detailed introduction to the digital practice in the conceptual stage of the functional security development process.

3. OVERALL DESIGN AND PRACTICE OF DIGITAL PROCESS FOR ROAD VEHICLE FUNCTIONAL SAFETY DEVELOPMENT AND MANAGEMENT

3.1. Requirements Sorting and Function Abstraction

Software requirement analysis is the initial stage of formal software development, which relates to the development and maintenance of the whole software and is a very important part of the whole software development. The demand research is carried out from the business requirements, user requirements and functional requirements of the digitalization of automobile functional safety development and management. Clarify the necessity of vehicle functional safety development, user characteristics and sort out specific functional modules

The concept phase in the process provides the initial security requirements for functional security development, which is the basis and key link in the entire product development process. This system combs the requirements of the ISO26262 standard and the business logic at the conceptual stage, and abstracts the overall functions of the system into six modules, namely, login, home page, functional security management, functional security development, functional security database, and system management.

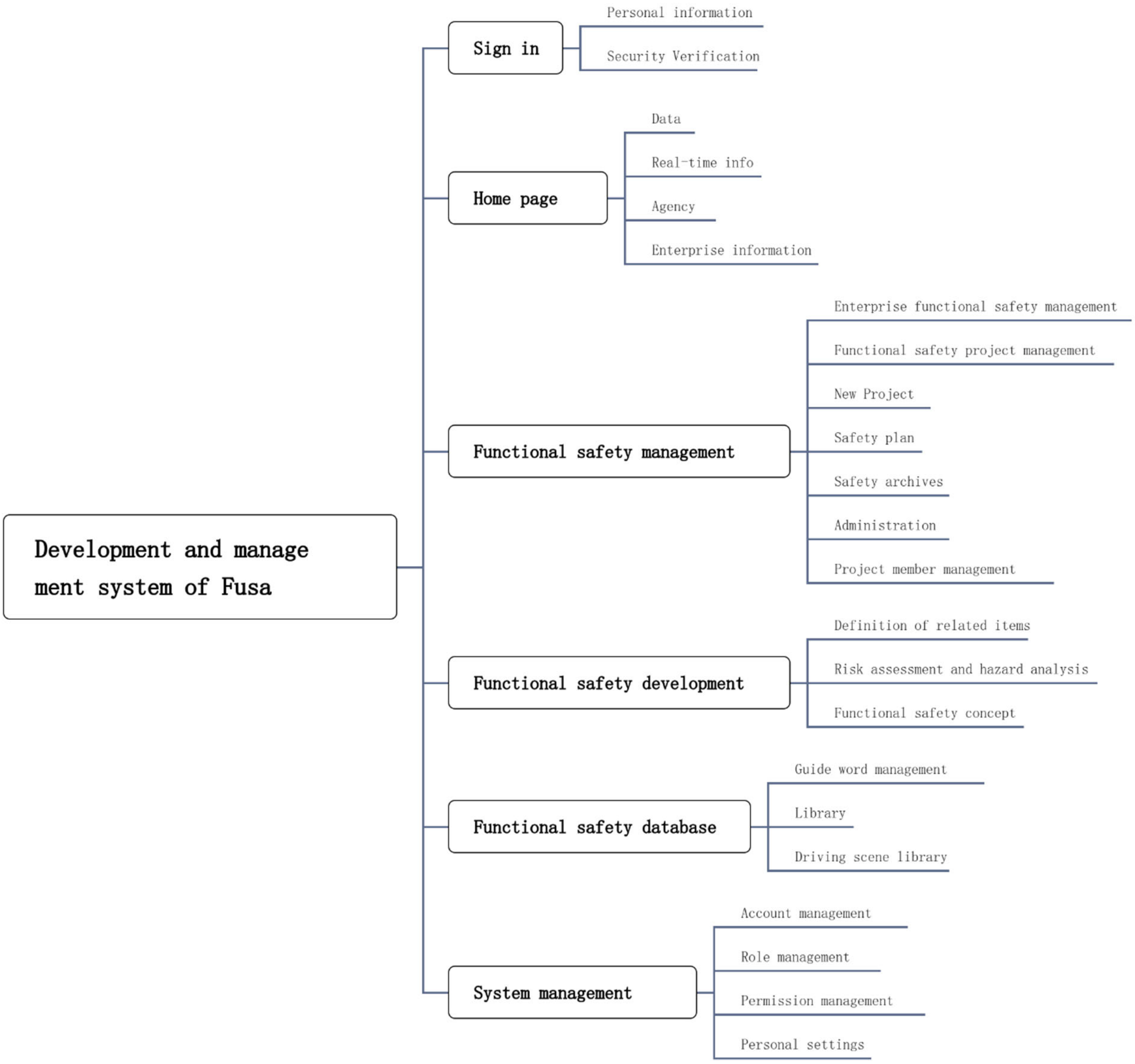
Development and management system of Fusa
Sign in
Personal information
Security Verification
Home page
Data
Real-time info
Agency
Enterprise information
Functional safety management
Enterprise functional safety management
Functional safety project management
New Project
Safety plan
Safety archives
Administration
Project member management
Functional safety development
Definition of related items
Risk assessment and hazard analysis
Functional safety concept
Functional safety database
Guide word management
Library
Driving scene library
System management
Account management
Role management
Permission management
Personal settings

Figure 1. System Function Module Diagram

The main functions of the system are as follows:

(1) User identity, role authentication login, permission management settings

(2) The homepage kanban can preview user basic information, user project data statistics kanban, functional security business messages, and enterprise messages.

(3) Implement a platform based multitask, multi-user, large concurrent work environment

(4) The systematic project management process, combined with the requirements of functional safety lifecycle project management in ISO26262, realizes the rules and processes from project information management, personnel management, output management and other aspects

(5) It integrates the development of vehicle functional safety concept, including related item definition, HARA, HAZOP, scene library, S E C value evaluation and FTTI strategy algorithm.

(6) Realize visual image editing and expression, support parametric configuration of architecture diagram components, map parameters to the analysis process, and complete the association between front and back diagrams and table data.

(7) Standardized template management shall be carried out for the data generated in the functional security development stage. Data includes: function library, scene library, guide vocabulary, and security target base library.

3.2. Overall Design

The system adopts B/S (browser/service mode) structure, which is a network structure mode after the rise of WEB. It has the advantages of convenient maintenance, strong distribution, simple development, and can be operated anywhere. The expansion of the system is very easy, meeting the requirements of multi-user and multi task parallel development of the system. The analysis and design of the system adopts object-oriented technology, which has the advantages of easy maintenance, high efficiency and easy expansion. In terms of design mode, the system adopts MVC (Model View Controller) design mode, where M refers to business model, V refers to user interface, and C refers to controller. The MVC mode is used to separate M and V code, which has the characteristics of low coupling, high reusability, fast deployment, and high maintainability. It is mainly used for the development of Web applications, and is currently the main mode of software development.[1]

3.3. General Framework

Planning a complete system overall framework that can meet the requirements of the functional safety development management system is a prerequisite for all work, is also the basis for laying the system performance, and is crucial for the development of a software system. The system architecture should be layered and organized, and the system functions should be modularized and low coupled, so that it can be modified, reused and deployed more easily and quickly according to the actual needs, thus meeting the requirements of the future elastic expansion of the system.

The system is specifically divided into application framework, technical framework and system framework. The application framework meets the requirements of access control, permission management, user management, basic application services of other applications, and application templates of form templates and interface templates; The technical framework is divided into login authentication, exception handling, database connection, log management, cache processing, data encryption and Struts framework, JSP tag, UI application technology framework and technology; The system framework is the server operating system and database. The overall framework of the system is shown in Figure 2:

4. DETAILED SYSTEM DESIGN AND INTERFACE

4.1. Main Interface

The overall layout of the page adopts the T-shaped layout shown in the above figure, in which the system logo is placed on the top, the system copyright can be placed on the bottom, the left side of the middle is the navigation menu of the system, and the right side of the middle is the display part of the content. The advantages of this layout are clear page structure, clear primary and secondary, and emphasis on order.

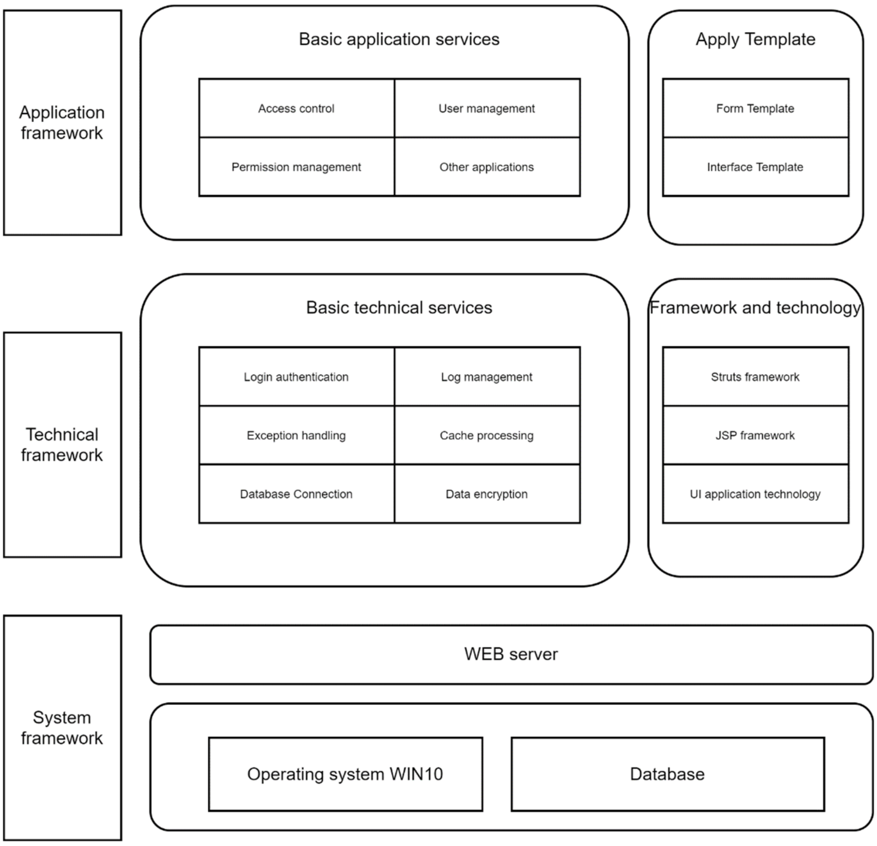

Figure 2. Overall Framework of the System

4.2. Detailed Design of Modules in The Conceptual Stage of Functional Safety Development

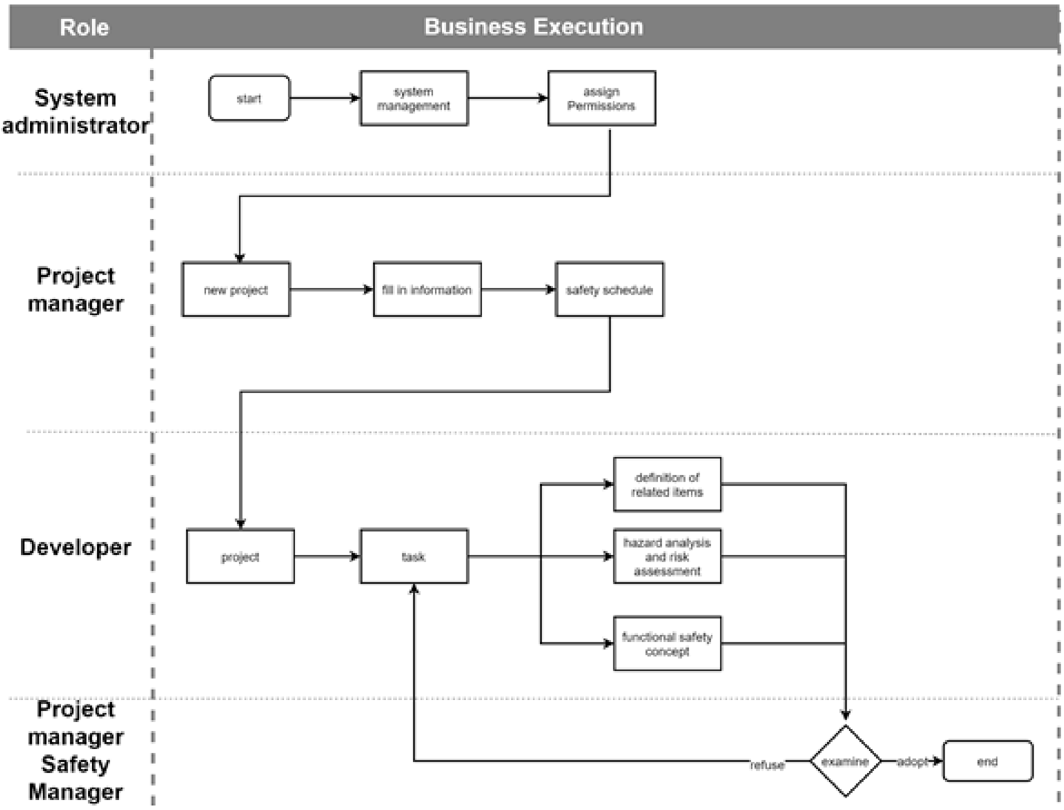

Figure 3. System Flow Chart

After the project manager assigns the tasks of the concept phase to the engineer, the engineer opens the project list of the functional security development module and enters the task list. Each task has a designated engineer. The engineer enters the product interface to work according to his assigned task to complete the corresponding task list. In the concept stage, different operation interfaces are displayed according to account permissions. The function list can be added, edited, deleted, imported, etc. Import can import local function files and foreground database functions. Before importing, you can download the template and then import it. The content button "View Details" pop-up box displays activation conditions, status charts, signals, etc., which can be added, deleted, or modified. The activation conditions can also be queried.

Hazard analysis and risk assessment mainly include failure analysis, hazard analysis, scenario analysis, risk assessment, safety objectives, verification review report - HAZOP, verification review report - HARA, and verification review report - safety objectives.

(1) Failure analysis: To enter the page, you need to import a function node first, add a guide word after importing the function, edit the failure form corresponding to the guide word, and finally submit to complete the current task.

(2) Hazard analysis: according to the failure form of each function, edit the corresponding impact on the whole vehicle, possible hazards and safety related contents. Submit the current task after editing.

(3) Scenario analysis: specify a scenario library for each function. You can select a scene library from the database or add a scene library. The new scene library is only valid for the current function. Submit the current task after specifying the scene library.

(4) Risk assessment: each failure form and scenario arrangement and combination of each scenario library generate risk assessment data, edit SEC analysis and safety target data of each risk assessment, and submit the current task after editing. Excel data of risk assessment can also be exported.

(5) Safety objective: safety objective data is obtained by merging risk assessment data, and the same safety objective is merged. Submit the current task after checking.

(6) Hazard analysis and risk assessment verification report: three verification review reports will be generated after WP302 data is completed, namely HAZOP, HARA and safety objectives. The three validation review reports need to be reviewed to see whether they meet the requirements, whether they pass the review and fill in the review comments.

The concept of functional safety mainly includes functional safety requirement analysis, functional safety requirement matrix and functional safety verification report. Confirmation of functional safety requirements is based on multiple states, such as motion mode, safety state, emergency operation and fault tolerance time of related items. The concept of functional safety also includes safety measures such as safety mechanisms, which are implemented in the architecture elements of related items, and their contents are specified in the functional safety requirements.

(1) Functional safety requirement analysis: the basic data comes from the combined safety objectives of hazard analysis and risk assessment. Each safety objective includes relevant functions and failure forms, system architecture diagram, fault tree analysis, safety level of relevant components, hardware architecture metrics, and determined functional safety requirements. Generally speaking, a related item can be simply described as environment, vehicle and driver model. The purpose of safety design is to reduce risks in related items by exporting various driving scenarios. First, determine the possible hazard scenarios of vehicles, consider the environmental conditions and driving conditions, and combine the possible

hazards in relevant items. The identified hazard scenarios shall be divided by hazard analysis and risk assessment, and then the safety objectives and ASIL levels shall be obtained.

(2) Functional safety requirement matrix: summarize the functional safety requirements of each safety objective, combine the same functional safety requirements, select the highest ASIL level, and form a requirement matrix. The safety matrix is automatically imported from the conceptual safety requirement table, and each safety objective has a safety requirement table. All the conceptual requirements of safety objectives are listed together to form a safety matrix

(3) Functional safety verification report: the data is obtained from the functional safety concept data. It is necessary to edit whether the traceability of safety objectives is met, the ability to reduce cargo and avoid hazardous events, and review.

5. CONCLUSION

The electronic and electrical components of modern automobiles are becoming more and more complex, with higher integration and more and more failures. After a series of evolution of automobile safety system, the concept of functional safety has been paid more and more attention by OEMs. The digital practice of automobile functional safety development management realizes the working system of management, development and test life cycle, the online multi-user, multi task full process working mode, the automatic association of business data logic, management traceability, automatic coordination and embedded professional analysis tools. It effectively solves the pain points of traditional development methods, thus improving the working efficiency of developers and shortening the time to market.

REFERENCES

[1] Lv Guanyan, Li Fenhua. The Design of Campus Supermarket Management System under MVC Framework [J]. Computer Age, 2022 (04): 123-125. DOI: 10.16644/j.cnki.cn33-1094/tp.2022.04.034.

[2] Huan Hongsheng Safety Requirements in Automobile Design and ISO 26262 Standard [J]. Monitoring and Maintenance, 2012 (10): 12-13.

[3] Peng Fei ISO26262 New Ideas for Ensuring Vehicle Functional Safety [J] Automobile and accessories. 2015 (37).

[4] Vehicle Functional Safety Analysis [J] Song Yu. Internal combustion engine and accessories. 2018 (15).

[5] Huey Der Chu, Yu Shu Hu ISO 26262 - Vehicle specific functional safety standards [J] Quality Monthly, 2012, 48 (8): 15-20.