Application of PREEvision in Functional Intelligent Safety Design for Integrating Automotive Electronic and Electrical Architecture

Xuan Zhou¹, Zhiwen Hou¹, Xianghu Meng¹, Xin Zhou¹, Jia Fang¹ and Zhifa He²
¹Xuzhou XCMG Automotive Manufacturing Co., Ltd, Xuzhou 221000, China.
²China Automotive Technology and Research Center Co., Ltd, Tianjin 300300, China.
*Corresponding author: sacredking@163.com

Abstract. With the increase of people's attention to car safety and the introduction of functional safety, designers have changed their thinking from fault-based to functional-based safety architecture design. PREEvision, an architecture design tool, can integrate automotive electronic and electrical architecture design and integrate functional safety design into it, which greatly simplifies the design process and design time, and at the same time can also reduce the probability of product failure to improve security.

1. Introduction
With the increasing complexity of automotive systems, we are facing new challenges in the field of system safety engineering. We often interact with electronic/electrical (E/E) system in the design of automobile architecture, and its possible failure may have great safety consequences and impact. Based on these problems, ISO 26262 is formulated to meet the specific requirements of road vehicle safety critical system. It is suitable for a complete vehicle safety life cycle: management, development, production, operation, service and retirement. It provides a method to determine vehicle safety integrity level (ASIL) based on vehicle specific risk, which is a risk classification scheme defined in the standard, which is used to analyze and classify the impact of specific potential hazards. One of the biggest advantages of PREEvision application software is that it can combine the function safety, architecture design and preview. Prevision follows the international standard of functional safety iso26262, meets the requirements of modeling and analysis of functional safety development, and supports the whole process of functional safety development [1].

2. Functional safety standard iso26262
More and more electronic/electrical (E/E) systems with safety functions are being integrated on modern vehicles, which increases the complexity of the system and increases the risk of the system. Therefore, it is very important to make product development and product development process more pragmatic and efficient. Iso26262 standard is a vehicle life cycle based on functional safety, including the concept stage, product development and the design stages after the launch. And PREEvision is mainly used in the whole design concept stage, including the definition of related items, safety life cycle start-up, hazard analysis and risk assessment, and functional safety concept [2]. In addition, more and more OEMs require their suppliers to comply with functional safety standards such as ISO 26262. To support the achievement of
functional safety, best practices in systems engineering, project management, and quality assurance are required.

3. **Preevision support for functional safety**

PREEvision can manage the complexity of E/E system conceptual design, and make every step of development have two-way traceability. The whole design is carried out in the same tool, which makes the source of development data and security analysis single, and can ensure the consistency between the functional safety design and all the architecture development products referenced, and record the security design process according to the safety concept.

4. **Realization of lka system function security based on preevision**

The following is an example of functional security process analysis of lane keeping assist system in PREEvision. LKA system is defined as warning the driver when the vehicle starts to deviate from the current lane without receiving the turning signal, and the system will implement the measures to keep the current Lane in case of emergency. Lane keeping aid project definition: the first step of functional safety design is project definition, and the first goal of project definition is to define and describe the project, such as feature characteristics, function interaction, operating mode and vehicle driving status, etc., the project definition also needs to collect all the information related to project design and safety analysis: the role of the project and its description; The connection between this system and other functions, such as steering lights and emergency warning lights; The requirements for each function, e.g. signal requirements for other projects; The initial architecture and outline of the project; Other non-functional parameters, such as pressure resistance, housing, etc. This section is designed in the PREEvision model requirements layer.

![Figure 1. Design of functional Security requirement layer for PREEvision](image-url)
The second goal is to have a better understanding of the project so that every activity defined in the security lifecycle can be performed. You can define it by charting: create a new and selected project definition system diagram under the Security Analysis catalog in the PreEvision model, Figure 2. PreEvision software brings its own mapping association feature, which core the project requirements defined by the previous requirements layer to the relevant modules in the project definition diagram. The project defines it as a preparation for the next step in hazard analysis and risk assessment.

![Figure 2. LKA project definition](image)

Hazard and operability study (HAZOP): Risk and operability study: Risk and operability research, HAZOP is a qualitative analysis method used to systematically investigate the possibility of failure and identify possible failures in the system. HAZOP is a good preparation for Hazard Analysis and Risk Assessment (HARA) because it uses a very systematic approach to derive and classify hazard events, resulting in hazard events for subsequent hazard analysis hazard assessment. We can complete the HAZOP design in the HAZOP editor table of the PreEvision-specific model, Figure 3.

![Figure 3. HAZOP analysis table](image)

Hazard analysis and risk assessment (HARA): The purpose is to identify and classier hazards in the project definition and to develop security objectives to prevent or mitigate risks in order to avoid anticipated hazards.ISO26262-3 mentions that HARA's main task is to identify and classify hazardous events and use them to derive appropriate system security objectives. The hazard description is done in the Risk Analysis Editor in PreEvision. It has been determined above that hazard events will also be used for hazard analysis and risk assessment (HARA). In PreEvision, the basic structure of hazard...
analysis and risk assessment is first created, and the component mapping in the project definition is assigned to hazard analysis. Create a hazardous event in the Hazard Analysis Editor and automatically assign the operating scene and the created safety target to it, Figure 4.

State analysis is the identification of all relevant operating conditions and operating patterns (Note: For this we only need to consider one hazard, one potential failure) when the project's failure causes the hazard to occur, a running state determines the actual application objectives of the project and the expected security behavior. For example, an ordinary car cannot expect to be safe and easy to operate at high speeds on a highway. The factors to be considered in state analysis and hazard identification are as follows: vehicle use scenarios, such as: highway driving, urban driving, parking, rural roads; Environmental conditions: e.g. friction on the road surface, side wind; reasonably foresee drivers and road users (for possible injuries); Cooperation with the control system (for fault-avoidance control).

Hazard identification: 1) The identification and confirmation of project hazards must be systematic and detailed; 2) FMEA is used for the identification of hazards for analysis; 3) the most important thing for the identification, description and environment of hazards must be from the vehicle safety level. For example, "the airbag may be switched on at high speed" instead of "a screw in the airbag system may be loose" because the same hazard may be caused by a different cause.

Hazard classification and ASIL rating recognition: the severity (S), exposure (E), and controllability (C) are determined by the results of prior state analysis and hazard identification. Figure 5.

Functional safety concept (FSC) functional safety concept: The functional safety concept is a system concept designed to achieve safety objectives, with the aim of deriving functional safety requirements from safety objectives and then assigning safety objectives and functional safety requirements to the system's electrical and electronic architecture or external risk reduction measures to ensure that the required functionality is safe. The security objectives and security features written must now be improved
according to the functional security requirements. Figure 6 creates functional security requirements in the PREEvision requirements layer. Then create a requirement map between security objectives and functional security requirements so that the content can be continuously traced.

![Figure 6. Functional security requirements](image)

Security objectives: The tracking view (dangerous events) in Figure 7 supports refining or decomposing safety targets. In addition, it prevents errors and insouciances through ASIL decomposition's automatic validation mechanism, highlighting the corresponding table cells if there is an invalid ASIL decomposition.

![Figure 7. Tracking view (hazardous events)](image)

Functional safety decomposition: Key safety levels with the Automotive Safety Integrity Level (ASIL) can be expressed as the functionality of the system. One security requirement for an ASIL can be broken down into two security requirements. To achieve this, an effective combination must be observed, as in Figure 8, which is done automatically with the help of ASIL-Decomposition.

![Figure 8. ASIL analysis](image)

Technical safety concept (TSC) security technology concept: PREEvision -based functional security design in this step, the concept of functional security is refined into a technical security concept, and security features in the logical functional architecture are assigned to the technology architecture, including the inference and implementation of technical security requirements. In the PREEvision tool, this is done by mapping logical functions to the hardware system. Therefore, all the necessary technical safety requirements are inferred. Consistency checks provide a reasonable ASIL rating. The technical security requirements are derived from FMEA analysis, which need to determine the following system attributes under the initial functional framework: external interfaces, such as communication and user interfaces; Limitations of environmental conditions or functional limitations, system molding construction requirements. Hardware security technology design in PREEvision can be modeled in detail to the device level. Electrical components are created in the hardware principle layer and then the
technical safety requirements and safety mechanisms are assigned with the mapping function. You can also create detailed software security concepts, which are done at the software architecture layer. Technical security requirements, failures, and security mechanisms can be detailed to ports, interfaces, and data elements that are allocated through mapping capabilities.

Safety Analysis: FMEA (Failure Mode Impact Analysis): Use FMEA to identify design failure patterns, see how they affect product operation, and identify measures to mitigate failures, a critical step is to predict potential failure patterns for the product. Unlike other tools, PREEvision can be analyzed and optimized using existing system designs, which significantly reduces the cost of performing and maintaining consistent analysis. This traceability of software, such as traceability between failures and security mechanisms, can also be easily implemented and effectively maintained throughout the development lifecycle. The main factor affecting FMEA is the Composite Index (RPN), which sorts content by RRPN (Risk Priority) values (from highest to lowest), rather than by structure in FMEA tables. RPN- S-O-D, wherein S-Severity O-occurrence (Occurrence) D-Detected is difficult to detect (Detection). FMEA causes can be linked to FMEA results in the same FMEA failure mode when FMEA analysis is performed. Typically, the FMEA structure is not built in the model view, but in an edited table tailored to the FMEA analysis, as shown in Figure 9. The software's own export capabilities also allow you to create a document based on the FMEA for easy data output and management.

5. Conclusion

Starting with the increasing complexity and importance of automotive E/E systems, PREEvision has developed a complete vehicle functional safety design process based on the published ISO 26262 standard to enhance product safety and competitiveness for automotive manufacturers. The functional safety of model-based system engineering method is highly traceable in PREEvision model view. The integration of functional safety design with the design of electronic and electrical architecture will certainly play a more important role in the vehicle design process.

References
[1] Yin Zhenhua, Tang Fengmin, Zhou Tao. The development and application and research of functional safety in PREEvision. Automotive Appliances, 2018 (1).
[2] Wang Junming, Zhou Hongwei. The concept design of lane keeping assistance based on ISO26262 is designed. Journal of Chongqing Jiaotong University (Natural Sciences Edition), 2019, 38 (03): 135-142.
[3] Zhao Zhenglan. Pure electric vehicle torque control safety concept and torque monitoring model. Journal of Automotive Engineering, 2018, 008 (003): 229-234.
[4] Shen Ximing. XX model automotive safety system development project risk management. 2016.