Functional safety evaluation of battery anagement system based on probability of failure per hour

Mingsheng Chen 1,a, Zhimao Ming 1,b, Guixiong LIU 2,c* Hongpei Li2,d
1Guangzhou GRG metrology and test Co., Ltd., Guangzhou, Guangdong, China
2South China University of Technology, Guangzhou, Guangdong, China
aemail: chenms@grgtest.com, bmingzm@grgtest.com
cemail: megxliu@scut.edu.cn, d201920100482@mail.scut.edu.cn

Abstract: In order to identify functional safety property of battery management system, safety integrity level of BMS research is performed by average frequency of a dangerous failure of the safety function. The result shows that: currently, functional safety has been research at home and abroad, through evaluation system of road vehicle and electrical, electronic, programmable electronic safety-related systems. So, safety integrity level could be analyzed quantitatively by a functional relation, which is established among tolerable hazard frequency, demand rate on safety-related protection system, dangerous failure of average frequency and safety integrity level. Based on tolerable hazard frequency and the demand rate on safety-related protection system, safety integrity level of a BMS is evaluated as level II.

1. Introduction
With the gradual development of electric vehicles in the automotive industry, the functional safety concerns of the vehicle and its key components are also increasing, especially the functional safety of the power battery and its management system. The current reference to the functional safety of road vehicles[1,2] and electrical and electronic safety-related systems[3,4] of international and domestic standards for functional safety, are proposed related evaluation system framework and process. Current research and applications are mainly focused on the function of instrumentation in the petrochemical field[5], or limited by practical application scenarios[6] and objects[7]; and the selection and implementation of specific verification methods [8,9] are mostly qualitative analysis, lacking quantitative research[10,11]. In this paper, the average frequency of dangerous failure model[12] is used to quantitatively analyze the functional safety[13] characteristics of the battery management[14] system under the conditions of tolerable dangerous frequency and the requirement rate of safety-related protection system, in combination with the evaluation system of the functional safety integrity classification of the Battery Management System (BMS).

2. Functional safety of vehicles and electrical and electronic systems

2.1. Functional safety of road vehicles
As for the functional safety of road vehicles, the current national standard is GB/T 34590-2017 Road Vehicles - Functional Safety, which corresponds to the international standard ISO 26262-2011 Road vehicles - Functional safety. The newly promulgated ISO 26262-2018 Road vehicles - Functional safety abolishes the weight limit of the model and extends its coverage to other vehicle categories,
including heavy road vehicles, trucks, buses and motorcycles. It also includes guidelines for the design and use of semiconductors in automotive functional safety environments, providing additional support for digital and analog components, programmable logic devices (PLDs), multi-core processors and sensors, and semiconductor suppliers.

2.2. Functional safety of electrical and electronic systems
The current national standard for functional safety of electrical and electronic systems is GB/T 20438-2017 Functional safety of electrical/electronic/programmable electronic safety-related systems, and the corresponding international standard is IEC 61508 2010 Functional safety of electrical/electronic/programmable electronic safety-related systems. In order to consider various types of safety strategies, systems with different technologies (e.g. mechanical, hydraulic, pneumatic, electrical, electronic, programmable electronic, etc.) should be used to ensure safety. It is necessary to consider not only the components in a single system, but also the combination of different safety-related systems. Since the potential risks and complexity of safety-related systems vary considerably from one application area to another, the safety measures required for a specific application should be determined after grasping the basic principles of the standard and application-specific elements.

3. Functional safety features

3.1. Tolerable Risk Frequency
The Tolerable Hazard Frequency is numerically the reciprocal of the service life (in hours). In this paper, the tolerable hazard frequency is based on the Mandatory End-of-Life Standard for Motor Vehicles, which was implemented in 2013: "8 years for small and micro-taxi passenger cars, 10 years for medium-taxi passenger cars, 12 years for large-taxi passenger cars; 13 years for bus passenger cars; 15 years for special school buses; 20 years for large and medium-sized non-operating passenger cars (except large sedans); there is no limit on the number of years of use for small and micro non-operating passenger vehicles, large non-operating sedans, and wheeled special mechanical vehicles."

3.2. Security protection system requirement rate
Whether the security protection system request rate has achieved a tolerable risk level in the absence of additional protective measures needs to be determined by accident risk classification. And the risk level is divided into four levels, risk level I is intolerable risk; risk level II needs further study to determine the tolerable level; risk level III and risk level IV are tolerable risk. In this study, the safety protection requirement rate and the number of accident risks are numerically corresponding to the BMS fault diagnosis items; the BMS fault diagnosis items include basic items such as battery temperature shown in Table 1 and expandable items such as insulation resistance, i.e. with reference to GB/T 38661-2020 Technical Conditions of Battery Management System for Electric Vehicles. In the actual battery system design and fault diagnosis needs confirmation process, BMS safety protection requirements should not be limited to the items listed in the standard.

Table 1 BMS troubleshooting basic items[15]

| No. | Failure state                                                                 | Diagnostic projects                                      |
|-----|-------------------------------------------------------------------------------|----------------------------------------------------------|
| 1   | Battery temperature greater than set limit                                    | High battery temperature                                 |
| 2   | Battery temperature is less than the lower set limit                         | Low battery temperature                                   |
| 3   | Secondary cell(cell packs)/voltage greater than the upper voltage setting limit | High voltage of battery cells (cell packs)               |
| 4   | Secondary cell(cell packs)/voltage less than the upper voltage setting limit   | Low voltage of battery cells (cell packs)                 |
| 5   | The consistency deviation of battery cell (cell group) is greater than the set condition | Secondary cells (cell groups) large consistency bias         |
| 6   | Charging current (power) is greater than the maximum charging current (power value) | High charging current (power)                             |
| 7   | Discharge current (power) greater than the maximum discharge current (power value) | High discharge current (power)                            |
3.3. Average frequency of hazardous failures

Based on the determination of the frequency of tolerable hazards and the requirement rate of the safety protection system, the average frequency of hazardous failures of individual safety-related protection systems can be expressed as [3]:

\[ PFH = \frac{F_t}{F_{np}} \]  

Where \( PFH \) is Average frequency of hazardous failures per hour, \( F_t \) is Tolerable Risk Frequency, \( F_{np} \) is security protection system requirement rate in the absence of additional protective measures.

3.4. Security integrity level

Safety Integrity Levels (SILs) are typically classified into four levels, with Level 4 being the highest and Level 1 being the lowest. For the specified parameters of the safety integrity level target, the object of this study, the battery management system, is a safety-related system in continuous operation mode. The hourly average frequency of dangerous failures for its specific safety functions corresponds to the safety integrity level, as shown in Table 2.

Table 2 Relationship between average frequency of failure and safety integrity level [3]

| Average frequency of hazardous failures per hour | Rank |
|-------------------------------------------------|------|
| \([10^9, 10^8)\) | 4    |
| \([10^8, 10^7)\) | 3    |
| \([10^7, 10^6)\) | 2    |
| \([10^6, 10^5)\) | 1    |

4. Algorithms and analysis

With reference to the 15-year service life of a vehicle of the type described above, i.e., 131,400 hours, the tolerable hazard frequency at this time is:

\[ F_t = \frac{1}{131400} \approx 7.61 \times 10^{-6} \]

According to GB/T 38661-2020 Battery Management System Technical Conditions for Electric Vehicles, there are 7 basic BMS fault diagnosis items and 11 expandable items, so the required rate of safety-related protection systems is numerically consistent with them.

\[ F_{np} = 7 + 11 = 18 \]

In combination with the above conditions, using equation (1), the average frequency of dangerous failures can be calculated as.

\[ PFH = \frac{F_t}{F_{np}} \approx 4.23 \times 10^{-7} \]

According to the calculation \( 4.23 \times 10^{-7} \in [10^{-7}, 10^{-6}) \), the BMS security integrity level is level 2 against Table 1.

Based on the results of a BMS safety integrity level calculation that has been obtained, the risks to the control system must be identified and analyzed through a risk analysis process. The risks are then mitigated using a variety of implementable work programs until the overall risk is reduced to an acceptable level. The permissible level of risk is one of the items in the safety requirements and is expressed as the probability of failure of the target hazard at a specific time, corresponding to different SIL levels. SIL 4 is the most reliable and SIL 1 is the least reliable in terms of the execution of safety functions, and the higher the SIL level is, the higher the probability that the equipment will execute safety functions correctly, and the higher the SIL level is, the higher the safety and reliability, but the economic cost will increase. In addition, the higher the SIL level of the system, the higher the hardware failure margin is required to ensure that safety issues are kept under control in the event of a failure of part of the BMS equipment.
5. Conclusions
This paper quantitatively evaluates the functional safety of a BMS using a mathematical model of the average frequency of dangerous failures, combined with the functional safety characteristics of the BMS. The main conclusions are.

(1) In the current evaluation system based on the functional safety of road vehicles and electrical and electronic systems, GB/T, IEC and ISO standards need to determine safety measures according to specific application scenarios to reduce the risk level when they are implemented.

(2) For the parameters of functional safety features, the functional relationship between the average probability of failure, the frequency of tolerable hazards and the requirement rate of safety-related protective systems constitutes the theoretical basis for determining the safety integrity level of BMS.

(3) After calculating the average failure probability for the functional safety of a battery management system, it is determined that the safety integrity level is level 2, which provides a reference basis for subsequent risk analysis and control decisions.

In addition to the quantitative analysis of the average frequency of hazard failure in this paper, there are semi-quantitative and qualitative analysis methods for the functional safety assessment technique.

Acknowledgments
This paper is one of the stage results of the Guangdong Key Areas R&D Project Power Battery System Testing and Evaluation Technology Research (2019B090908003).

References
[1] Road vehicles Functional safety: part 9 Safety integrity level oriented and safety oriented analysis of vehicles Standardization Administration of China (SAC) -2017.
[2] ISO Road vehicles - Functional safety: Part 9: Automotive safety integrity level (ASIL)-oriented and safety-oriented analyses- 2018.
[3] Functional safety of electrical and electronic programmable electronic safety-related systems: part 5 Example of method for determining safety integrity level Standardization Administration of China (SAC) -2017.
[4] IEC Functional safety of electrical / electronic / programmable electronic safety-related systems: Part 5: Examples of methods for the determination of safety integrity levels -2010.
[5] Jia, Y.C.(2017) Safety Integrity Level Selection and Validation Methodology for Safety Instrumented Functions. Chemical Automation and Instrumentation,12: 1118-1121.
[6] Liu, X.D.(2010) Overview of security integrity of critical security systems. Safety and electromagnetic compatibility,6: 53-57.
[7] Chen, H.(2011) Research on the application of security integrity level analysis methods. Petrochemical automation,47: 23-25.
[8] Yu,W.G.,Wu,S.G.,Bo,L.Y.(2018) Safety Instrumented System SIL Validation Method Selection and Implementation. Electrotechnology,24: 130-133.
[9] Zhou, R.Y.,Zhong,A.,Ren,J.Z.(2014) Comparative Study of Methods for Determining Security Integrity Levels for Security Systems. China Production Safety Science and Technology, 10: 67-73.
[10] Chen,X.F.(2015) Comparative Study of Security Integrity Level Validation Methods for Security Systems. China Petroleum and Chemical Standards and Quality, 35: 36-39.
[11] Xi,Y.(2014) A Bayesian Network Based Study on Safety Integrity Level Verification of Safety Instrumented Systems. Southwest University, Chongqing.
[12] Wang Y.K Liu Z.X.(2016) Reliability assessment of safety instrumentation system for high demand mode[J]. China Mechanical Engineering,27(01):101-104+108.
[13] Zhu,W.J,Shi,Y.J.(2020),Lei,B. Functional safety analysis and design of BMS for lithium-ion battery energy storage system. 9(01):271-278.
[14] Zhang,B.L.(2019) Functional safety-based battery management system architecture design for
electric vehicles. Beijing Jiaotong University.

[15] Battery management system for electric vehicles Standardization Administration of China (SAC)-2020.