Functional safety research of battery management system based on risk graph methods

Mingsheng Chen¹,a, Guiting Xie¹,b, Zhimao Ming¹,c, Guixiong Liu²,d*, Wei Li²,e
¹Guangzhou GRG metrology and test Co., Ltd, Tianhe, Guangzhou, Guangdong, China
²School of Mechanical and Automotive Engineering, South China University of Technology, Tianhe, Guangzhou, Guangdong, China
*aemail: chenms@grgtest.com, bemail: xiegt@grgtest.com, cemail: mingzm@grgtest.com
eemail: 201921002251@mail.scut.edu.cn
*Guixiong Liu.d: email: megxliu@scut.edu.Cn

Abstract. In order to clarify the functional safety integrity hierarchy of the battery management system, this paper uses risk map analysis to qualify the battery management system failure event of an alarm device. The relationship among six risk parameters and four levels of safety integrity are built through specific risk. Thirteen contents are detailed and in according to four risk parameters. The results show that the functional safety outcomes of the battery management system can be classified into seven categories, and safety integrity was determined to be level I using the ten mapped paths in the risk map.

1. Introduction
In recent years, new energy electric vehicles have developed rapidly, and are widely used in road transportation. The power battery, as the core component of new energy electric vehicles, determines the performance of electric vehicles[1]. With the increasing development of battery management systems in the new energy electric vehicle industry, the functional safety standards related to the safety of road vehicles[2-3], and electrical and electronic promulgated and implemented at home and abroad are also being improved[4-5]. The battery management system, as an electronic device that monitors and manages the battery, is an important factor in the safety of the entire vehicle[6]. Current research on functional safety integrity is mainly focused on petrochemical[7], process control, mechanical devices, instrumentation and other fields, while less research has been conducted on battery management systems for electric vehicles[8-9]. In order to qualitatively study the functional safety of the battery management system, this paper uses risk map analysis to classify the safety integrity level of the battery management system of electric vehicles, taking into account the functional safety characteristics of the battery management system.

2. Battery management system functional safety
Battery management system (BMS) failure is a key factor in the frequent occurrence of electric vehicle safety accidents. The core function of BMS is to monitor the battery voltage, temperature and other information in real time and make the battery work in a safe state[10]. BMS is the core component to ensure the safety of the battery system and even the safety of the whole vehicle, a safe
and reliable BMS is essential to prolong the life of the vehicle's power battery. It is of great significance to improve the safety performance of the vehicle by improving the service life.

2.1 Battery management system and its functions
BMS is an important link between the vehicle power battery and the electric vehicle, and its main function is to detect and manage the battery, monitor the battery temperature, voltage and charge state, and provide communication, safety, cell balancing and management control for the battery to ensure that the battery can be kept in the best working state and prolong the life of the battery.[11]. BMS is a system with communication interface with application equipment, which transmits real-time battery information to the subsystem and provides data basis for the overall system strategy.[12]. BMS is mainly used to measure voltage, current signal monitoring, battery pack temperature, insulation resistance, high-voltage interlock, charge and health status estimation, equalization and battery power limiting, as well as relay control, thermal control, fault diagnosis and alarm, and fault-tolerant operation. The technical identification of BMS functions is a risk parameter for subsequent system failures related to functional safety. Theoretical basis for the work on judgement and path mapping.

2.2 Functional safety assessment methodology
Functional safety assessment methods are currently divided into three main categories: qualitative, semi-quantitative and quantitative. No single method is currently available for all applications, so it is necessary to make choices as needed. These include: risk mapping method, hazard event severity matrix, protection layer analysis, and average hazard failure probability method. In order to ensure that the risk of the subject can be reduced to a specified quantitative value and the assessment result is higher than the tolerable risk requirement, and without considering the common cause failure and other protective layers, the risk map method is used in this paper for the qualitative study of the safety integrity level of the battery management system.

3. Risk map analysis
The risk matrix approach is a qualitative risk assessment analysis method that integrates the likelihood of a hazard occurring and the severity of the harm to assess the risk. It is a tool for risk visualization and is widely used in the field of risk assessment by listing the hazard states to be assessed and selecting a hazard level for each hazard state and estimating its probability of occurrence[13].

3.1 Model Composition
The mathematical model expression for the risk map is:

\[ R = (f, C) \]  

In the formula 1, \( R \) is the risk in the absence of safety-related systems, \( f \) is the frequency of dangerous events in the absence of safety-related systems, \( C \) is the consequence of a hazardous event.

Three additional risk parameters can be derived from this, \( F \) is the frequency, duration of exposure to the hazard area, \( P \) is the probability that a hazardous event cannot be avoided, \( W \) is the probability of an undesired event. The above parameters are the basic components of the risk map analysis method.

3.2 Implementation programme
The specific implementation steps are as follows, firstly, the starting point of the risk reduction assessment is defined; secondly, the mapping path is derived from the consequences of the hazardous event; then the next extension is made to correspond to the frequency, time, and probability of unavoidable hazardous event exposure to the hazardous area; and finally, the safety integrity level classification table is listed for the probability of undesired events. A typical risk map expression is shown in Figure 1, a indicates that there are no special security requirements, b indicates that an electronically programmable electronic safety-related system does not meet the requirements.
The risk map approach makes it difficult to consider the likelihood of associated failures between the source of the requirement and the equipment used in the EEPSS. This may result in an overestimation of the effectiveness of the EEPSS. A calibration of the risk map that includes a higher than annual requirement rate may result in a higher SIL requirement derived using the risk map than the requirement, at which point alternative analysis methods should be considered.

3.3 Risk parameter correspondence category
In order to concretize the qualitative determinations of the risk map, the categories were decomposed during the preparation process with reference to the risk parameters in order to form a clear mapping for the path to the final safety integrity rating. A typical risk parameter to category correspondence would be:
- Consequences (C): C1-3 indicates minor injury, serious injury and death of personnel, respectively;
- Frequency and duration of exposure to hazardous areas (F): F1-2 indicate low and high frequencies, respectively;
- Potential to avoid dangerous events (P): P1-2 possible and almost impossible, respectively;
- Probability of an undesired event (W): W1-2 express small and large probabilities, respectively.

4. BMS risk map analysis
Risk map analysis, in conjunction with the functional safety characteristics of the BMS, establishes risk parameters and relationships with safety integrity levels by considering tolerable risks associated with specific hazards. Combining the BMS risk parameters with the category correspondence, specific entries corresponding to the parameters in terms of consequences, frequency and duration of exposure to the hazard zone, probability of avoiding a hazardous event, and probability of an undesired event are sorted out. Using the mapped paths in the compiled risk map, the functional safety integrity level of the BMS can be determined.

4.1 BMS risk map
Based on the actual working conditions and functional categories of the BMS as described above, the risk map mapping with the BMS safety-related system failure as the starting point of the assessment and containing 10 risk parameter outputs is shown in Figure 2.
For the necessary risk reduction estimates for safety-related systems, forty, total seven types of safety integrity assessment results can be specified by specifying the safety integrity level that should be met by the safety-related systems of the BMS through each indication in the scale. Among them, the specific correspondence between risk parameters and categories is shown in Table 1.

### Table 1 BMS risk parameters correspond to categories

| Risk parameter | Categories                      |
|----------------|--------------------------------|
| Consequences ($C$) | \begin{align*}
C_1 & : \text{minor injuries} \\
C_2 & : \text{One person seriously injured} \\
C_3 & : \text{One to three deaths} \\
C_4 & : \text{More than three deaths}
\end{align*} |
| Frequency and duration of exposure in hazardous areas ($F$) | \begin{align*}
F_1 & : \text{Rarely exposed} \\
F_2 & : \text{Frequent exposure} \\
P_1 & : \text{Absolutely possible} \\
P_2 & : \text{Unlikely} \\
P_3 & : \text{Impossible}
\end{align*} |
| Potential to avoid dangerous events ($P$) | \begin{align*}
W_1 & : \text{Infinitesimal probability} \\
W_2 & : \text{Small probability} \\
W_3 & : \text{High probability} \\
W_4 & : \text{Quite high probability}
\end{align*} |

### 4.2 BMS Functional Security Integrity Level

By considering the tolerable risks associated with specific hazards, combined risk parameters and relationships with safety integrity levels are established. Using the ten mapping paths in Figure 2, the forty, total seven functional safety assessments of the battery management system can be identified to provide technical support for the BMS functional safety integrity research work. For example, the thermal runaway event triggered by the failure of the BMS fault diagnosis and over-temperature protection alarm device can form the $C_2 \rightarrow F_2 \rightarrow P_1 \rightarrow W_2$ mapping path. The consequences of a BMS safety-related system failure are one person seriously injured and relatively infrequent exposure to hazardous areas, but it is entirely possible for personnel to avoid hazardous events, and the probability of an undesired event is quite small. According to Figure 2, this state corresponds to a BMS safety integrity level of one.

### 5. Conclusion

In this paper, a functional safety study of battery management systems for electric vehicles was carried out using the qualitative analysis of risk maps. The main conclusions are obtained as below:

1. As the core functional component of the "battery system" of an electric vehicle, the functional safety assessment of the battery management system is beneficial to the risk control work of the whole
vehicle. The starting point of the risk reduction assessment is the key boundary condition in the functional safety assessment of the battery management system.

(2) A risk map constructed from parameters such as the consequences of a hazardous event, frequency of exposure, likelihood of a hazardous event, and probability of undesired occurrence can be used to assess the level of safety integrity of a BMS functional safety system. No safety requirements and the inability of a safety system to meet the requirements are the two limit results of the risk map assessment output.

(3) The risk map analysis method for qualitative functional safety analysis of battery management systems is suitable for scenarios where the required rate of calibration is less than once a year.

In addition to the qualitative analysis method of risk map studied in this paper, the technical means of functional safety research of battery management system also includes semi-quantitative and quantitative analysis methods. Issues such as the differences between qualitative and quantitative analysis methods and application conditions should be further explored.

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] Tian, J., Gao H.B., Zhang Y.Q., etc. (2020) Research of life prediction methods for power Li-ion battery in electric vehicles. Chinese Journal of Power Sources, 44: 767-770.
[2] Road vehicles - Functional safety: Part 9: Automotive safety integrity level (ASIL)-oriented and safety-oriented analyses - 2018.
[3] Road vehicles - Functional safety - Part 9: Automotive Safety Integrity Level (ASIL)-oriented and safety-oriented analyses - 2017.
[4] Functional safety of electrical/electronic/programmable electronic safety-related systems: Part 5: Examples of methods for the determination of safety integrity levels - 2010.
[5] Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 5: Examples of methods for the determination of safety integrity levels - 2017.
[6] Zhu, W.J., Shi Y.J., Lei, B. (2020) Functional safety analysis and design of BMS for lithium-ion battery energy storage system. Energy Storage Science and Technology, 9: 271-278.
[7] Chen, X.F. (2015) A comparative study of security integrity level validation methods for security systems. China Petroleum and Chemical Standard and Quality, 35: 36-39.
[8] Yu, W.G., Wu, S.G., Bo L.Y., etc. (2018) Selection and Implementation of SIL Verification Method for Safety Instrument System. Electric Engineering, 39: 130-133.
[9] Chen, H., Jia, Y., Xu, X.L., etc. (2011) The Application Study of Safety Integrity Level Analysis Methods. Automation in Petro-Chemical Industry, 47: 23-25.
[10] Zou, C., Zhu, Q. (2019) Introduction and Research of Battery Management System of Electric Vehicles. Electric Engineering, 40: 176-177+180.
[11] Song, W.J., Lv, J., Luo, W., etc. (2017) Research progress in Li-ion battery pack inconsistency control. Battery Bimonthly, 47: 303-306.
[12] Zhang, M.Y., Wu, W., Song, Y.B., etc. (2020) Security level evaluation system for wireless local area network access devices. Journal of Tsinghua University (Science and Technology), 60: 371-379.
[13] Shen, M., Gao, Q., Wang, Y., etc. (2019) Design and analysis of battery thermal management system for electric vehicle. Journal of Zhejiang University (Engineering Science), 53: 1398-1406+1430.