GB

GUIDANCE TECHNICAL DOCUMENT FOR

STANDARDIZATION OF THE PEOPLE'S REPUBLIC OF CHINA

ICS 43.040

CCS T 35

GB/Z 42285-2022

Road vehicles - ASIL determination guidelines for electrical and electronic system

道路车辆 电子电气系统 ASIL 等级确定方法指南

Issued on: December 30, 2022 **Implemented on: July 01, 2023**

Issued by: State Administration for Market Regulation;
Standardization Administration of PRC.

Table of Contents

Road vehicles - ASIL determination guidelines for electrical and electronic system

1 Scope

This document presents methods for determining the ASIL (Automotive Safety Integrity Level) of electrical and electronic systems in road vehicles. Determining ASIL (Automotive Safety Integrity Level) of electrical and electronic systems is required by GB/T 34590.3-2022.

This document applies to safety-related systems, which incorporate one or more electrical/electronic systems, as installed on mass-produced road vehicles other than mopeds.

2 Normative references

The contents of the following documents constitute the essential provisions of this document through normative references in the text. Among them, for dated references, only the version corresponding to the date applies to this document; for undated references, the latest version (including all amendments) applies to this document.

GB/T 34590 (all parts) Road vehicles - Functional safety

GB/T 34590.1-2022 Road vehicles - Functional safety - Part 1: Vocabulary (ISO 26262-1:2018, MOD)

GB/T 34590.3-2022 Road vehicles - Functional safety - Part 3: Concept phase (ISO 26262-3:2018, MOD)

3 Terms and definitions

The terms and definitions as defined in GB/T 34590.1-2022, as well as the following terms and definitions, apply to this document.

4 Hazard analysis and risk assessment

4.1 Identification of hazards

Hazard analysis and risk assessment (HARA) is an analysis process, that identifies potential hazards and combines them with operating scenarios, to form a set of specific hazard events, assessing the risk of each hazard event, to determine its ASIL level and safety goals.

The definition of dependent item is a prerequisite for HARA. Hazard identification can be achieved, through different hazard analysis techniques. This document gives examples of hazard identification, using Hazard and Operability Analysis (HAZOP) techniques. HAZOP is an exploratory analysis method, which can be used to identify and evaluate the abnormal performance of dependent items; helps to check the operation of dependent items at the vehicle level, in a structured and systematic way. This analysis method adds appropriate introductory words to each function of dependent item, to assume its different abnormal performance, which can lead to hazards, meanwhile the hazards may be harmful to the occupants of the target vehicle, other vehicles and their occupants, or other persons at risk, for example, the potential hazards to the pedestrians, cyclists, or maintenance personnel in the vicinity of the target vehicle.

Other effective methods can also be used, to identify relevant hazards. This document does not recommend or support a specific hazard identification method. Hazard identification is part of hazard analysis and risk assessment. Appendix A describes the motion behavior of the vehicle, along different axes.

The following is an example of the application of a simple HAZOP method, to identify hazards, which are caused by potential abnormal performance of dependent items. For example, based on the function described in the definition of dependent item, consider the role and capability of the dependent item actuator, then assume the following abnormal function of the dependent item.

a) Loss of function - When required, no function is provided.

b) Provide wrong function, when required:

1) Wrong functions - More than expected;

2) Wrong functions - Less than expected;

3) Wrong function - Opposite direction.

c) Unexpected functions - Provide functions when not required.

e) When evaluating certain vehicle operating scenarios, a combination of factors may be required, to cause a hazard to cause a specific injury. A vehicle operation scenario may be composed of several factors; some of these factors may be closely related. For the combination of factors that form the prerequisites of a hazardous event, the correct value of the exposure probability can only be calculated, after identifying the relationship between each factor.

Example: For a scene with snow and ice, there is a high correlation with the reduction of pavement friction. If the exposure probability of the scene with snow or ice for the reduction of road friction is considered to be E2 levels independently of each other, THEN without these two exposure probability factors rated as E2, an exposure probability lower than E2 is equivalent (for scenes with snow and ice). Treating these linked scenarios as independent might lead to inappropriate downgrading of the exposure probability.

f) In the hazard analysis and risk assessment, do not consider the hazards that have been covered by the safety regulations of the workplace for maintenance personnel, as well as all hazards caused by dependent items that are being repaired (see Note 1 in 4.1).

g) The defined hazardous events shall be specific enough, to ensure accurate definition of the degree of harm and determination of controllability.

- A scene can be divided into several newly added specific scenes (may lead to different S and C parameters);
- If the analysis results of multiple scenarios related to the same hazard are similar or identical, these scenarios shall be combined for analysis;
- The above guidelines shall not be used, to artificially increase or decrease exposure probability factors;
- This does not require an exhaustive examination of every possible combination, it is sufficient to consider typical vehicle operating scenarios and include those that lead to the highest ASIL level.

4.2.3 Step 2: Determine severity

4.2.3.1 General information

According to GB/T 34590 (all parts), the "severity" level of potential harm, which is caused by a specific hazardous event, can be defined as one of the four levels shown in Table 5. These "severity" levels are a general classification, to provide guidance on assigning an ASIL for a given hazardous event.

Often, "severity" levels are difficult to define exactly. Because, the "severity" result

hazard event. The development of this hypothetical scenario involves multiple sources of information, including but not limited to expert analysis and judgment, analysis of technical reports, particularly relevant accidents or analysis of test, simulation and historical accident data. Appendix B provides some general information, that can be used to assign the appropriate "severity" level to motion control hazards, at a given vehicle level.

4.2.3.2 Guidance on assignment of "severity" to crash-related hazards

During the hazard analysis and risk assessment process, assigning a "severity" level requires expert assessment and consideration of a representative sample of various traffic conditions, vehicle speeds, road conditions. Due to continued advances in vehicle road and crash-related active and passive safety technologies, as well as increased education and law enforcement on road user safety behaviors, analysis of historical accident data tends to overestimate future measures targeting injury risk AND may also do not contain suitable data for a new and different scenario. In these cases, models can be used, to incorporate new scenarios in the context of historical data, in order to better predict outcomes.

In general, the risk of injury to road users increases as the collision speed increases. For planar collisions, the estimation of the velocity difference (ΔV), before and after the collision, which is available in some historical accident databases, can assist the evaluation of the "severity" of the accident. Consideration may be given to replacing ΔV with other pre- and post-crash estimators (e.g., energy-equivalent velocity, relative vehicle/object velocity), and to account for other crash characteristics such as vehicle overlap and crush/intrusion. Appendix B provides some general guidance, that may assist in the "severity" rating. For non-planar crashes, such as rollovers, other available criteria depending on the hazard scenario can be used for the "severity" assessment. The examples given in GB/T 34590.3-2022 can also be used, as a reference for the assignment of "severity".

When determining the likely "severity" level of a crash from historical data, the available data relevant to the system under development shall be analyzed. For example, the balance between driver and vehicle control is changing, due to the introduction of new active safety features, that automatically intervene in vehicle dynamics, in certain specific crash-imminent environments. Therefore, as new features are applied, current data may not reflect suitable results. When determining the "severity" and ASIL level, the vehicle or system manufacturer shall analyze all technologies, that are applied to a specific vehicle.

The "severity" levels of the hazardous events, that are representative of the various scenarios considered, are to be documented in the hazard analysis and risk assessment document.

Note 1: The "probability of exposure" needs to be considered to set the "severity" level related to it. For a certain driving condition, if a value higher than the "severity" level

accidents, due to abnormal performance of the new system, if applicable, can be compared with existing relevant accident data. The test subject's response behavior to the hazard can then be assessed, to derive a preliminary level of controllability.

Overestimation of severity, probability of exposure, controllability parameters and derived ASIL levels needs to be avoided, which may result in the reduction, or even elimination, of functions or features that are beneficial to overall safety. Also avoid underestimating severity, probability of exposure, controllability parameters, derived ASIL level; otherwise, it may lead to insufficient safety requirements.

Appendix C provides examples of hazard analysis and risk assessment for electric power steering (EPS) assistance functions.

Appendix D provides examples of hazard analysis and risk assessment for drive and transmission functions.

Appendix E provides an example of a hazard analysis and risk assessment for a suspension control function.

Appendix F provides examples of hazard analysis and risk assessment for brake and parking brake functions.

4.3 Relationship between safety goals and safety status

When performing a Hazard Analysis and Risk Assessment, the output is a set of safety objectives to ensure safe operation. The definition of these safety goals considers avoiding or mitigating the potential harm, that may be caused by the abnormal function of dependent items; the controllability measurement can be used for the definition of safety goals. In a functional safety concept or a technical safety concept, a safe state and associated safety measures are appropriately defined, to achieve safety goals in the event of a failure of the dependent item. A "hazard analysis and risk assessment" for a safe state is not always required, although the hazards of a safe state can be derived from a "hazard analysis and risk assessment", when the safe state coincides with a specific failure at the dependent item level. Therefore, inconsistencies may arise, as both the safety goal and the safety state are derived from consideration of failure behavior, at different points in the safety life cycle. For the consistency of the safety profile, it is recommended to avoid the safety state from violating the safety goal. This recommendation can be achieved, by different formulations of safety goals and individual safety states. For example, a safety goal could be "avoiding loss of the emergency braking function without warning", whilst a safety state could be "disabling the function and notifying the driver that the function is not available". In this safe state, an alarm mitigates the consequences of loss of function, because the driver becomes aware that the function is no longer available. The safety concept and HARA shall be consistent; otherwise, it will have a negative impact on the safety file. If the safety status of this safety goal

Appendix B

(Informative)

Guidelines for severity rating

B.1 General introduction

This Appendix contains general information on assigning severity levels to vehicle movement control hazards, that form part of the hazard analysis and risk assessment. However, the content in this Appendix is not exhaustive and complete, which shall be noted in the application.

The assignment of severity levels may involve a variety of sources of information, including (but not mandatory or limited to): expert analysis and judgment, analysis of specific relevant crash or crash test technical reports, simulation tests, or historical crash data. Crash accidents, lab tests, road tests and other test data provide objective, reliable, repeatable results. Simulation testing can provide direction, for pre-crash scenarios and the relative contributions of many factors and interactions that typically occur in crash events. Analysis of historical traffic accident data can provide overall guidance on accident frequency and injury likelihood, for various crash accident scenarios. However, inherent limitations make it impossible to make precise predictions about future conditions.

For scenarios based on vehicle collision accidents, GB/T 34590.3-2022 defines the concept of severity levels, based on the injuries suffered by personnel in collision accidents (see Table B.1). GB/T 34590.3-2022 refers to the Abbreviated Injury Scale (AIS) (which assigns a severity score of 0 ~ 6 to a single injury); takes the "probability of injury" of a specific AIS level as an example, for assigning S0 ~ S3 severity levels. AIS that determines injuries to some or all road users, which are involved in traffic accidents within a geographic location, is provided in some historical accident databases. The collection of these accident data is usually a small sample size; the case selection criteria vary by location.

In order to properly use damage ratings, which are derived from available accident databases, the inherent limitations of the data sources shall be analyzed. The use of accident data to support severity ratings requires a solid understanding of the data collected and the limitations of the data available, to ensure that appropriate methods are used and results are properly interpreted.

In general, literature publications and real-world analysis of different global crash accident databases reveal the principle, that crash severity increases with relative speed. For this reason, a higher driving speed may increase the possibility of a collision accident, at a higher relative speed, which consequently lead to an increase

in the possibility of injury. However, there may be wide variation, when considering the definition of speed intervals for the allocation of S0 ~ S3, based on different sources of accident history data and specific crash screening criteria. These variations may be due to regional differences in the traffic environment, changes in sampling criteria for accident history data, or consideration of other factors such as available crash attributes, crash types, occupant restraints equipped or used.

Technical and practical considerations, for the use of historical accident data available in the literature or in specially developed analyzes to support severity ratings, include:

- For deep accident databases, case sampling criteria and collected data vary globally. The discrepancy in the analysis results of different databases may be partly due to the variation of sampling criteria.

- The size of the sample size shall be considered, to better understand the uncertainty in the accident sampling process, because the sampling process varies with each available database. In particular, the low frequency of crashes to the highest injury severity, in existing deep accident databases, may limit any injury classification and thus the assignment of supporting severity.

- Selection of sample population (level of analysis). For a given set of crashes, the damage ratings for the crash, for the vehicle involved, for the road user, for the vehicle user may vary, based on the highest injury severity recorded. That is to say, for any set of specific crash accidents, the specific severity injury rating, which is calculated at the crash level, vehicle level or occupant level, is different.

- According to Note 1 of 6.4.3.2 in GB/T 34590.3-2022, the severity classification should take into account the possible injuries, which are suffered by all participants involved in the accident.

- Many data, which is collected after the crash that may be related to the risk of injury, are unknown before the crash, so these data cannot be used in the pre-crash scenario. Examples include occupant characteristics (e.g., older occupants are generally at higher risk of injury than younger occupants, in similar crashes) and crash object characteristics (e.g., lightly loaded versus fully loaded large commercial vehicles, the collision energy potential is different).

- Estimation of collision energy after a collision accident (for example: relative vehicle speed, equivalent vehicle speed for obstacle avoidance):

  - Calculations are not necessarily performed for each vehicle (for example: in the current case of trailer collision accidents, if the collision object is a medium/heavy truck, no relative speed estimation is available);

  - Not necessarily consistent with the occupant impact pulse, which may be

- Although accidents are sampled, according to a well-defined method, there are some deviations compared with official statistics, which can be compensated by standardized and published weighting methods.

- For the use of the existing database to determine the accident severity of vehicles still under development, it needs to consider the active and passive safety and road infrastructure improvements, that occurred during this period. One possible way to influence this progress is to consider only recent models or vehicles with certain systems (e.g., ABS, ESC, air curtains, pedestrian protection).

- A given hazardous condition may lead to a range of possible accident scenarios. Analysts should avoid detailed analysis, that can only be predicted a posteriori and cannot be predicted in hazard analysis and risk assessment.

Based on each individual analysis of the above data sources, a discrete set of velocity ranges is generated for severity levels S0 ~ S3. Table B.1 shows the summary results of the independent analysis, defining the minimum and maximum speed ranges for each of the severity levels S0 ~ S3. Those ranges shown in Table B.1 reflect the overlap of discrete velocity ranges, which are produced by different analyses, which may be due to differences in available data sources and analysis methods. These differences may include:

- Regional driving mode and environment;

- Crash selection criteria for the deep accident database;

- Extrapolation from deep accident databases to wider populations;

- Composition of regional vehicle teams;

- Vehicle selection criteria (for example: vehicle age, equipment for specific vehicle technologies, such as airbags);

- Definition of collision type (frontal collision, side collision, rear collision) (for example: damaged plane, direction of impact force);

- Classification of collision types (for example: amount of overlap);

- Included collision objects and classifications;

- Passenger wrapping (e.g., seat position, restraint use);

- Occupant characteristics (for example: age);

- Included non-occupant injury results (for example: pedestrians, occupants on other vehicles).

Appendix C

(Informative)

Example of hazard analysis and risk assessment of steering function

C.1 General

This Appendix provides examples of hazard analysis and risk assessment for electric power steering (EPS) assistance functions. C.3 provides a HAZOP analysis, to identify abnormalities in EPS function, that correspond to hazards at the vehicle level. C.4 provides some examples of EPS malfunctions, resulting hazards at the vehicle level, associated ASIL levels. This Appendix does not represent a transition to functionally complete hazard analysis and risk assessment, but rather a subset of functional safety hazards for EPS functions, to provide guidance.

Note: This Appendix contains examples of ASIL levels for selected hazardous events. The determination of ASIL level shall be determined, through negotiation between relevant parties. Appendix B of GB 17675-2021 gives the minimum requirements for the steering system.

C.2 Definition of dependent items: Overview of functional concepts

The EPS function assists the driver in providing directional control of the vehicle to the steering wheels, while reducing the amount of steering effort required by the driver to steer the vehicle. EPS measures driver intent at the steering wheel; processes it simultaneously with other inputs from the vehicle, to provide steering torque assistance. The scope of this analysis is assuming that, the EPS system has a mechanical steering connection; when the power assist function of the EPS is lost, it can still support the driver to steer the vehicle manually.

C.3 HAZOP analysis

Table C.1 lists the HAZOP analysis, to identify dysfunctional manifestations of the EPS assist function. Table C.2 lists the mapping from EPS functional abnormalities to vehicle hazards.

This is an excerpt of the PDF (Some pages are marked off intentionally)

------ The End ------