Research on Design Method of Safety Components in Grader Control System

Yanjie Xue*, Zhiqiang Hou
Jiangsu XCMG engineering machinery research institute co. LTD, Xuzhou, Jiangsu, 221000, China
yangying@xcmg.com, E-mail: xgxueyanjie@163.com

Abstract. Motor grader is one of the important equipment for modern road mechanization construction. The performance of its control system directly affects the quality after road construction. At the same time, the safety of the product is equally important as the basic attribute of the product. In order to get better product safety performance, most countries have formulated a series of standards to regulate the design process. This article introduces the design method and relevant requirements of the control system safety in the EU standards, and explains the method, model and basic process of the control system safety design using the safety components of grader control system as an example.

1. Introduction
The control system is the main component of the grader, with the development of technology and intelligence, the product structure is more complicated and the integration is higher, the combination of electrical, hydraulic and mechanical structures is becoming closer and closer. The control system serves as the centre of the grader, the structure of the command system is also increasingly complex. However, the more complex the machine, the higher the probability of failure or danger, so the higher the safety design requirements are. The relevant safety components of the control system are mechanical control system components that provide safety functions. Its design and evaluation are related to the safety of the entire product. The safety design of the control system can avoid unpredictable or potentially dangerous situations, so it is very important.

2. Design method of relevant safety components of control system
The relevant safety components in the grader control system refer to the components in the system that respond to safety-related input signals and generate safety-related output signals. It consists of hardware and software and can be independent of the machine control system or integrated with the machine control system. Motor grader control system can use electrical, hydraulic, pneumatic and mechanical technologies or a combination of multiple technologies.

Typical causes leading to product hazardous conditions include: inappropriate design or modification of control system logic, temporary or permanent defects or failures of one or several components of the control system, changes or failure of the power source of the control system, selection and design of control devices and improper location. Typical examples of danger caused by improper control system design include: unexpected start, uncontrolled speed change, moving parts unable to stop, protection failure, etc.
2.1. The design process of the safety components of the control system
In order to prevent the dangerous situation of the product and realize the safety function, the design goal of the safety components of the control system is to reduce the risk of the product to an acceptable level. According to the requirements in ISO 12100, the risk reduction can adopt an iterative method, as shown in Figure 1.

Figure 1 Illustration of risk reduction iteration method

2.2. Determine the performance level
The ability of a safety component to perform a safety function is expressed by determining the performance level PL. For each SRP / CS or SRP / CS combination selected to perform a safety function, the PL should be estimated. The PL value of SRP / CS should be determined by estimating the following parameters. These parameters related to the evaluation process can be divided into the following two groups:
1) Quantifiable parameters, including the average dangerous failure time MTFFD value of individual components, diagnostic coverage rate DC, common cause failure CCF, structure;
2) Non-quantifiable parameters that affect the performance of SRP / CS, including the performance of safety functions under fault conditions, safety-related software, systematic failures, and environmental conditions.

2.3. SRP / CS block diagram of typical safety functions
After identifying the safety function of the control system, the specific composition of SRP / CS should be identified. The typical safety function diagram illustrates that the relevant safety components of the control system are composed of the following aspects.
SRP / CSa—input;
SRP / CSb—logic / processing;
SRP / CSC—output / power control element;
iab, ibc—interconnection method.
3. Safety risk assessment

According to the EU Machinery Directive, manufacturers must carry out a risk assessment of machinery, and the design and manufacture of products must consider the results of the risk assessment. Risk assessment refers to the work of quantifying the impact and loss of people's life, life, property and other aspects caused by the event before the risk event. For grader product design, it is very important to identify and manage risks in advance. Therefore, graders should also identify and manage various risks at the beginning of design.

The safety risk assessment can refer to Appendix 1 of the Machinery Directive 2006/42/EC and the Class A standard ISO 12100. The basic workflow is shown in the figure 3.

3.1. Risk identification

After determining the mechanical limits, the basic step of any mechanical risk assessment is to systematically identify hazards (permanent hazards and unexpected hazards), hazardous conditions, and / or hazardous events that are reasonably foreseeable at all stages of the machine's life cycle.

Only after the hazard has been identified can measures be taken to eliminate the hazard or reduce the risk. In order to realize hazard identification, it is necessary to identify the actions performed by the machine and the tasks performed by the operators interacting with it, while considering the different components, the mechanism or function of the machine, the materials to be processed, and the use environment.
3.2. Risk estimate

The likelihood of a risk occurring usually depends on personnel behaviour or technical failure. In most cases, the estimation of the probability of a dangerous event should be based on reliability prediction data or historical data of similar products. But sometimes, the low probability of accidents does not mean that the probability of danger is low. In order to determine how dangerous the screened risk is, the risk should be quantified. The method of risk estimate as shown in Figure 4.

1—The starting point for evaluating the effect of safety functions on risk reduction;
L—has little effect on risk reduction;
H—has a great effect on risk reduction;
PLr—Performance level required by.
Risk parameters:
S—the severity of the injury;
S1—minor (usually recoverable injury);
S2—serious (usually irreversible injury or death);
F—Frequency and / or duration of exposure to danger;
F1—Rarely-infrequently and / or short exposure time;
F2—Frequent-continuous and / or long exposure time;
P—Avoid danger or limit the possibility of injury;
P1—Possibility under certain conditions;
P2—Almost impossible.

Figure 4 Risk diagram of PLr for determining safety function requirements

For example, in terms of the risk of overloading, if the degree of injury is "severe S2", if it is not managed, the frequency of occurrence will be higher than "F2", but under effective management, it is still more likely to avoid its occurrence, it is possible to be "P1", therefore, the risk level of overloading can be evaluated as "d" according to the above judgment conditions.

3.3. Risk reduction

In order to reduce the risk, you can use the technical solutions in the technical standards, or you can use the proprietary technology of each enterprise. As long as you can provide sufficient evidence to prove that after taking measures, the risk level has dropped to a controllable level, you can solidify the program, to form a document to ensure the long-term implementation of the measure[4].

4. Design of safety functions

According to the risk assessment, the load sensing system of the grader should comply with the requirements of PL = d as specified in the Class B standard ISO 13849-1, which provides a comprehensive safety assessment from components to the system, to quantify the safety of the system through the system safety level (PLr), mean time to dangerous failure of each channel (MTTFd), system diagnostic coverage (DC), common cause failure prevention (CCF) and other parameters. The relationship between PL and categories of channels, DC and MTTF is shown in Figure 5.
Description:
1—MTFFD of each channel = low;
2—MTFFD of each channel = medium;
3—MTFFD of each channel = high.

Figure 5 The relationship between PL and the category of each channel, DCavg and MTFFD

In order to meet the requirements of PL = d, when designing a safety control system, it needs to be designed through four main steps. First, the MTTF should be high level, and then if the structure type (Category) is the second type DC should be at a medium level; if the structure type is Type 3, then DC can be at a low level. ISO 13849-1 also provides detailed classification data, which can be used to quantitatively classify PL according to the data in Table 1.

|        | Average probability of dangerous failure per hour (1/h) |
|--------|--------------------------------------------------------|
| PL     |                                                        |
| a      | 10^-5 ≤ PL ≤ 10^-4                                     |
| b      | 3 × 10^-6 ≤ PL ≤ 10^-5                                |
| c      | 10^-6 ≤ PL ≤ 3 × 10^-6                                |
| d      | 10^-7 ≤ PL ≤ 10^-6                                    |
| e      | 10^-8 ≤ PL ≤ 10^-7                                    |

4.1. Determine the type of safety control system
The third structural type (Cat. 3) of ISO 13849-1 requires that its design should be such that a single fault in any of these components will not cause the loss of the safety function, and a single fault should be detected at or before the next instruction on the safety function.

4.2. Mean Time Between Failure
There are multiple calculation methods for mean time to failure (MTTFD). In this case, the component manufacturer determined 10 based on the corresponding product test method standards of the components reach the average number of cycles when they fail dangerously (B10D = 3795891 operations), then the MTTFD of the components can be calculated by B10D and n_op (average number of operations per year)\[5\].

The following assumptions are made in the application of components: h_op is the average working time, the unit is hour / day, it is assumed here that the component works on average 6 hours per day; d_op is the average working time, and the unit is day / year. It is assumed here to work 6 months per year, that is, 180 days; t_cycle is the average working time (such as the switching of the valve) between the starting points of two successive cycles of the component, the unit is seconds / cycle, and each detection cycle is about 20 seconds / cycle, then

\[
n_{op} = \frac{d_{op} \times h_{op} \times 3600}{t_{cycle}} = \frac{6 \times 180 \times 3600}{20} = 194400 \text{ S/h} \tag{1}
\]
So the dual-channel MTFFD = 97.5 year, and this data belongs to a high range.

4.3. Diagnostic coverage
Diagnostic coverage refers to a measure of diagnostic effectiveness, which is the ratio between the failure rate of diagnosable dangerous failures and the failure rate of all dangerous failures. Generally, DC can be estimated by FMEA or similar methods. DC is divided into four levels: none (DC < 60%), low (60% ≤ DC < 90%), medium (90% ≤ DC < 99%) and high (DC ≥ 99%).

In this case, based on the data provided by the component supplier, the diagnostic coverage of the single-channel feedback loop is 65%. According to the DC and MTTF of the components in the system, the DC$_{avg}$ of the entire system is calculated by the formula:

\[
DC_{avg} = \frac{DC_1}{MTTF_1} + \frac{DC_2}{MTTF_2} = \frac{0.65}{195} + \frac{0.65}{195} = 0.65
\]

Therefore, the DC of the system is low.

4.4. Common cause failure CCF
According to the definition, common cause failure refers to the failure of different products caused by the same event, and these failures have no causal relationship with each other. Because Cat.3 structure design adopts redundant design, and through separation and isolation, it can avoid CCF and meet the requirements [6].

According to the above results: MTFFD = high, DC = low, the structural design meets the requirements of Cat. 3, therefore, the performance level PL of the safety control system is determined according to Figure 4 in this article.

5. Conclusion
Through the selection of components such as mean time to failure, diagnosis coverage, common cause failure, etc., the required safety level is finally achieved. This series of evaluation and design process can maximize the reliability of the safety function of the hierarchical control system, which is a quantifiable, easy to detect and mature design process.

References
[1] ISO 12100:2010, Safety of machinery — General principles for design — Risk assessment and risk reduction [S].
[2] ISO 13849-1:2015, Safety of machinery — Safety-related parts of control systems — Part 1: General principles for design [S].
[3] ISO 19014-1:2018 Earth-moving machinery—Functional safety—Part 1:Methodology to determine safety-related parts of the control system and performance requirements [S].
[4] EN 474-1:2006+A5:2018, Earth-moving machinery-safety [S].
[5] Shao Shanfeng, Li Yuhe, Wang Wenbo, Wu Guoxiang. (2016) Research on Intelligent Control System of Fully Hydraulic Grader. Control technology, 72-74.
[6] Liang Yuhong. (2014) Design of Electro-hydraulic Control System for Automatic Leveling of Grader. Mechanical Engineers, 4:73-75.