Research on Product Elements' Safety-Critical Degree

by Wu Qiong and Lyu Mingrui
China

According to system safety practice, the safety of a system is a designed characteristic. Therefore, the role of safety in the lifecycle of the system is important to consider during the design phase. There are many factors affecting product safety, and each of them plays a part in determining a product's overall safety. It's important to locate isolate key elements that influence a product's overall safety, and design with those factors in mind, as well as the time, cost and effectiveness of their influence on the design phase.

The concept of "safety-critical" has long been a part of the system safety field, and scholars from different countries have studied safety-critical items in a system; unfortunately, the concept can be somewhat subjective and, often, disagreement occurs. These judgments can be affected by many factors and can cause inaccurate assumptions about which parts are critical, as well as encourages deviation in product development and maintenance that can cause serious consequences to product safety.

Effective control of a product's safety mainly relies on paying efficient and continuous attention to safety-critical items, from the design and research phase until disposal.

To evaluate the role that an individual part plays in a system's safe operation, its "safety-critical degree" gives information to the product's designers and maintainers. These designations of safety criticality help determine the elements that need to be controlled in an efficient way — especially in a large system — and aid in locating which parts play the most important roles in the safety of the entire system.

This article attempts to quantify the degree to which a safety-critical element affects the safety of an entire system.

Range of This Study

The product mentioned in this article is an electromechanical product that can be broken down into subsystems, assemblies, subassemblies and components. We assume human error and environmental influences are acceptable (they are not factored into this discussion). The material's condition is either "failure" or "no failure." It's a conditional probability that the item's failure results in a mishap. We only consider the occasion of a mishap caused by failure.

Defining "Safety-Critical" and "Safety-Critical Degree"

Standards and references in the field of safety typically identify the existence of safety-critical items and their importance in product safety research. However, there is no systematic analytic approach to locating the "critical" part, so most scholars and engineers complete their research using subjective judgment. This judgment can be influenced by many factors, including the professional's experience and ability.

Unfortunately, this method makes it difficult to decide precisely which element is "more critical" among all the different components that play a critical role in the system. Different researchers can easily come to different conclusions on which element is most critical to the safety of the system.

To measure the level of an element's safety criticality, we must look at the definition of "safety-critical degree" as defined by MIL-STD-882E. This is the level of influence that an element's failure has on the safety of a product.

Every element has its own safety-critical degree; that is, each element influences product safety, just to different degrees. Researchers can establish a baseline for determining safety-critical elements according to a product's function and safety requirements. There can be more than one safety-critical element.

Measurement of an Item's Safety-Critical Degree

Reliability focuses on the system's status *before* an element's failure, while safety focuses on the element's impact on the system *after* failure takes place. For our purposes here, we are focusing on the situations in which an element's failure causes mishap. When failure occurs, reliability and safety become the same issue, differing only on one point: Failure(s) leading to one mishap is a conditional probability. The element's failure can cause a mishap, but sometimes it only affects the system's function to a certain degree, without danger. Here, we consider only failures that can cause a mishap with direct losses.

Because an element's failure mode differs, the level of a failure's impact on a mishap and the relationship

between failure and mishap also varies. Here, we use the effect of an item's failure mode and its significance coefficient in a fault tree to express the measurement of its safety-critical degree.

Research Ideas

- *Apply failure mode(s) and effect(s) and criticality analysis (FMECA) to the target element and compute the effects of each failure mode that can directly cause mishap* — FMECA can help us identify all the failure modes in a relatively objective way; we can then obtain each failure mode's effects on a potential mishap, which is its contribution to a mishap, by employing criticality analysis.
- *Construct fault trees and compute the criticality significance coefficient of base events* — We adopt fault tree analysis (FTA) to determine the relationship between the potential occurrence of a given top event and the failure modes we identified earlier.

  Our purpose is to express the level of the element's failure mode's effect on a mishap, which is the function of the significance coefficient. It tells us that by controlling a particular item, we can deduce the probability of a mishap's occurrence most efficiently.

  In fact, picking the significance coefficient among structure, cut sets, probability or the criticality of significance coefficient depends on the research's application. The first two significance coefficients — that is, the structure significance coefficient and the cut sets significance coefficient — are the only options to apply when lacking data support. Considering the calculating complexity, the cut sets significance coefficient is more applicable.

  Here, we use the criticality significance coefficient as an example to show how critical each element's failure can be to its top event. The criticality significance coefficient is expressed as the ratio of the occurrence probability's relative changing rate to the base event and top event.
- *Apply weighted summation to failure mode's effect and its criticality significance coefficient, and express the element's safety-critical degree afterwards* — Normally, failure modes can contribute to more than one mishap, so we need to synthesize the effects and the criticality significance coefficient of all failure modes to obtain the safety-critical degree for a target element.

The Calculation of a Failure Mode's Effects

While analyzing a product's composition, function and operational principle, we analyze the target item with FMECA to find out all the failure modes affecting the product's safety. The failure modes are those that can directly cause mishaps.

For those failure modes, we can achieve the logical relationship between failure effects and failure rates after CA analysis: In one failure mode, the expression of an element's failure effect is expressed in formula (1):

$$C_m(i) = \beta\alpha\lambda_p t \times 10^6 \quad (1)$$

where i is the failure mode with a certain effect, α is the failure mode's relative frequency, β is the probability that failure causes consequence and λ_p is the element's failure rate.

In this case, we are able to compute each failure mode's effects in a more quantitative way when the system has integral failure rates.

Fault Tree Construction to Obtain the Criticality Significance Coefficient

Analyzing failure modes, failure states, failure factors and failure consequences on the foundation of FMEA is our first task. We then construct fault trees after finding all the possible mishap types that an element's failure can cause.

Significance analysis is applied to base events; after obtaining the qualitative significance of structure and cut sets, and the quantitative significance of probability and criticality, we have the base event's criticality significance coefficient expressed in formula (2):

$$I_g^c(i) = \frac{q_i}{P(T)} \cdot I_g(i) \quad (2)$$

where $I_g^c(i)$ is the criticality significance coefficient of the base event, i, $I_g(i)$ is the probability significance coefficient for event i, $P(T)$ is the probability of the top event's occurrence and q_i is the probability of the base event, i.

The Synthesis of an Element's Safety-critical Degree

One product can have multiple failure modes, and the combination of those failure modes can lead to different types of mishaps, with each mishap in relation to one fault tree. In each fault tree, each failure mode has a different significance coefficient.

The base event's criticality significance coefficient here only refers to the criticality significance coefficient of a certain failure mode in a certain fault tree. Also, the failure mode effecting $C_m(i)$ only refers to the effects of certain failure mode. To obtain the failure

mode's effects and the criticality significance coefficient of a target element, the synthesis of *all* failure modes' effects and their criticality coefficient in *all* fault trees must be considered.

To combine the element's failure modes effects and criticality significance coefficient, we must eliminate the influence of the target's original dimension and magnitude to make the result commensurable. Here, we apply the standardization method to $C_m(i)$ and as expressed in formula (3), to get $C_m'(i)$ and $I_g^{c'}(i)$.

$$C_m'(i) = \sqrt{\frac{1}{n-1}\sum_{i=1}^{n}(C_m(i) - \overline{C}_m)^2},\ \overline{C}_m = \frac{1}{n}\sum_{i=1}^{n} C_m(i)$$

$$I_g^{c'}(i) = \sqrt{\frac{1}{n-1}\sum_{i=1}^{n}(I_g^c(i) - \overline{I}_g^c)^2},\ \overline{I}_g^c = \frac{1}{n}\sum_{i=1}^{n} I_g^c(i) \quad (3)$$

We employ the weighted summation method here. In formula (4), we assume item *A* has *n* kinds of failure modes, and that there are *k* types of mishaps that those failure modes can result in. The effect of the failure mode *i* in fault tree *j* is $C_m(i)_j$ and the criticality significance coefficient of *i* in fault tree *j* is $I_g^c(i)_j$.

Failure modes = {1, 2 … i … n}
Mishap types = {1, 2 … j … k} (4)

Therefore, the element's criticality significance coefficient $S_c(A)$ is as shown in formula (5):

$$S_c(A) = \sum_{i=1}^{n}\sum_{j=1}^{k} C_m'(i)_j \cdot I_g^{c'}(i)_j \quad (5)$$

The quantification result for an element's safety-critical degree (as shown here), can offer professionals an objective reference that is more scientific and systematic, rather than a subjective judgment on which items to manage first by sorting or ranking them in descending order.

The Extension Research of Safety-critical Degree

After quantifying an element's safety-critical degree, we can further research the application of the safety-critical degree and its characteristics. Sometimes, a small change in an element's safety-critical degree can have a critical impact on the safety of the entire product. Therefore, we need to know *which* safety-critical elements share the same safety-critical degree so that the design of those elements can be prioritized to improve the overall safety of the products within the constraints of operational effectiveness, suitability, time and cost.

In practical systems, an element's failure rate in an electromechanical product changes with abrasion and aging, and different elements can affect each other. Consequently, the probability that a mishap caused by failure, along with a base event's qualitative structure significance and an element's criticality significance coefficient change with time. The composite safety-critical degree, therefore, is a time-dependent function. We attempt to convey this logical relationship through a dynamic fault tree, and search for the point at which an element's critical degree has a sharp change. When successful, we will be able to find the best timing to control product safety.

Conclusion

The impact of a safety-critical element can affect product safety at different levels; therefore, the criticality of these elements to systems differs, as well. Determining the safety-critical degree is a way of measuring to reflect this discrepancy.

Not only do critical components affect safety, but each element, to a degree, can affect a product's safety. Designers can distribute risks to increase product safety by rationally arranging elements by their degree of importance during the development phase.

The definition of "safety-critical degree" and the new explanation of "safety-critical element," based on the measurement of the former being made an exploration step, is a tentative solution to the gap in the "measurement" of product safety research.

About the Authors

Professor Wu Qiong has been a researcher in the field of safety science for nearly 30 years at the Shenyang Aerospace University. He is a Safety Assessor Class I and was a member of the first group of certified safety engineers. He is a member of China's Safety Science and Engineering Education Steering Committee, and serves as an editorial board member for China's core journals *China Safety Science Journal* and *Safety and Environment*. He attended the University of Southern California as a visiting scholar for further study from 1987 to 1988, and he has been dedicated to the research of system safety, risk management, and its application to product safety assessment and insurance practice.

Lyu Mingrui works on the safety certification of products in TüV Rheinland (China) Ltd. She was a postgraduate student of Professor Wu at the Shenyang Aerospace University, and has been conducting research on the assessment of product safety.