A method for analysis and assessment of system safety based on hazardous source

Bohua Li [a], Shiyu Gong [b] and Guopeng Song [c]

College of Information System and Management, National University of Defense Technology, Changsha 410073, China

[a]lbhwindy@outlook.com, [b]yiyue@189.cn, [c]rocsgp@163.com

Keywords: Hazardous source; safety requirement; accident scenario.

Abstract. Hazardous source will exist according to the characteristic or operational need of the system, and the existence of hazardous source is the fundamental reason of accident occurrence. Hazardous source needs to be identified, and the corresponding safety requirement should be proposed. Assuring the source under control will effectively decrease system safety risk to what could be accepted. Based on the root or source, analysis and assessment of system safety will be more accurate and precise. This paper introduces a method or process for analysis and assessment of system safety, and each procedure is introduced in details.

1. Introduction

Safety is an emergent property of complex system according to the interaction of corresponding elements [1]. The occurrence of accident is related to not only the single components but also human factor, management factor and interaction of components. Therefore it is necessary for complex system to use system theory to analyze. STAMP, proposed by Leveson, has offered a new valuable approach to solving the safety problem along with basic systems theory concepts.

The hazardous source is the fundamental reason of accident occurrence. Many complex systems inevitably include a variety of sources because of work characteristic or operational need, especially weapon equipment system. For example, missile system includes inflammable, explosive and even poisonous propellant, and its engine will produce vibration, noise and heat when it is working. Obviously, hazardous source is indivisible organic parts of complex system and its running environment. Thus how to control the sources is the key point for safety of system, as it is impossible to absolutely eliminate the sources.

This paper proposes a more systematic safety analysis process based on hazardous source, so that the analyst could take measures to prevent accident at root. Section 2 clarifies that the hazardous source is the fundamental reason of accident occurrence. Section 3 introduces how to identify hazardous source of system. Section 4 provides a method to propose safety requirement accordingly. Section 5 presents the safety risk assessment method based on accident scenario model. At last, the entire work in this paper is concluded in Section 6.

2. Hazard and Accident

The process of accident occurrence is one of how hazardous source becoming uncontrolled. It is a dynamic process that transforming the safety state to accident state. The hazard state is the intermediate state and also the key state. To better understand why the hazardous source is the fundamental reason of accident; it is needed to turn to some common related definition. The definition of mishap is an unplanned event or series of events resulting in death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment, and hazard is any real or potential condition that can cause injury, illness, or death to personnel; damage to or loss of a system, equipment or property; or damage to the environment (MIL-STD-882D). Hazard is the precursor to mishap. A hazard will change to the mishap in some condition. It is always confusing to distinguish hazard from mishap. For example, it is a hazard that worker could be electrocuted by

touching exposed contacts in electrical panel containing high voltages, however it is a mishap that worker was electrocuted by touching exposed contacts in electrical panel containing high voltage[2].

A hazard is comprised of Hazardous Element (HE), Initiating Mechanism (IM) and Target and Threat (T/T) [2]. Hazardous Element, or hazardous source, is the root of accident, such as propellant of engine. Initiating Mechanism is all kinds of inadequate control or constraint. Target and Threat is the person or thing that is vulnerable to injury and/or damage, and it describes the severity of the mishap event. Every component is necessary for accident. The process of occurrence of accident is shown in fig. 1.

Fig. 1 The process of occurrence of accident

In the process of engineering design and management, if any component of hazard could be eliminated, the corresponding accident will be eliminated at the same time. However, there exists no absolute safe system, especially when it comes to weapon equipment system. For decreasing the safety risk, the number of hazardous sources, the probability of IMs and the severity of T/T should be decreased. So the next steps are identifying hazardous source, proposing corresponding safety requirement and identifying accident scenario. The final work in this procedure is analyzing and assessing.

3. Identification of hazardous source

According to the prior section, the first step of safety research is identifying all the potential hazardous sources. Hazardous source is the root of hazard and accident and the physical state of hazardous state. Its existence may be due to the material used, work characteristic and operational need of system. It cannot be completely eliminated. Whatever you summarize, if there is not boundary of quantity, the hazardous source is everywhere[3]. Safety is the emergent property of system. It is required to identify, analyze, control and retrain hazardous source so that the safety risk could be accepted.

Combined with the character of weapon equipment and stressing the internal factor of system, the definition of hazardous source is the materials that include a hazard category and may lead to accident when some IMs happened. The hazard categories could refer to the fifteen hazard categories proposed in *Engineering handbook for system safety* [4], as shown in Table 1.

Table 1 Hazard categories

Number	Hazard category	Number	Hazard category
1	Environment hazard	9	Pollution
2	Heat	10	Material metamorphism
3	Pressure	11	Fire
4	Poison	12	Exposure
5	Vibration	13	Electric
6	Noise	14	Acceleration
7	Radiation	15	Machinery
8	Chemical reaction		

How to identify the system hazardous source could be considered in following ways:

Identify hazardous sources according to hazard category table. If a component of system has one or more hazard categories, then the component is a hazardous source. For example, the engine of spacecraft includes hazard categories about vibration and heat; the propellant includes hazard

categories about poison, fire, exposure. So these hazardous sources are urgent to be considered in the design stage.

Identify hazardous sources according to the lessons of experience. It is easily to identify some hazardous source through analyzing the hazard and mishap information of similar system. For example, in 1992 and 1995, the reason of the accidents that LM-2 twice failed to launch the communication satellite is due to the resonance vibration of cowling and satellite, and then it led to the exposure of satellite engine. According to this lesson, the cowling must be considered as a hazardous source in the system design.

Identify hazardous sources according to the general safety design standards and handbooks. They are made according to the potential accident and hazardous sources. For example, according to the design standard that the high-voltage wires must be enclosed through insulator, the high-voltage wires is the hazardous source.

The hazardous sources cannot be completely eliminated. The system should be used in positive ways, and at the same time, the hazardous sources must be controlled. After identifying hazardous sources, the corresponding safety requirement should be proposed.

4. Safety requirements

The function of safety requirement is to set constraints on hazardous sources. A safe system has to owe adequate safety requirements for hazardous sources. The complete safety requirement could be proposed according to the following steps:

Step 1: the proposition of preliminary safety requirement

After identifying the hazardous sources, the preliminary safety requirement should be proposed according to the properties of hazardous sources and the potential outcomes. Through corresponding information, the safety requirements that include component failures, performance deterioration, human factor and management factor should be proposed. And on the other hand, combined with performance of sub-node, the more concrete requirement should be proposed according to the decomposition of parent node. The requirements of sub-node have inheritance. If new requirements are found, the feedback is necessary for improvement of design.

Step 2: description of node behavior

The behavior description includes two procedures. In the first stage, it is necessary to describe the related parameters that are about physical, chemical, performance and so on. There are two ways to describe these parameters. One way is using function such as $Y = f(X, S, t \cdots)$ and $S = g(X, S, t \cdots)$, where Y the output of component is; X is the input; S is the performance of component; and t is the running time. Other way is using computer language for those parameters that are qualitative or have complex modification. For example, IF-THEN could be used. In the second stage, it is necessary to describe the behavior of system running. It could be described through Function Model(FM), Configuration flow graphs(CFGs) or IDEF0. For example, the functional behavior for propellant discharging may be described as Discharging Valve Open→Emit→Propellant Tank Empty. The functional behavior for parachute opening may be described as Resisting Force Parachute Open→ Stabilizing Parachute Open → Leading Parachute Open → Master Parachute Inflate → Master Parachute Open. With more detailed behavior described, it is easier to find the missing requirement.

Step 3: verification of safety requirement

After the description of component behavior, it is necessary to verify the safety requirements for ensuring completeness and integrity of requirement. The control flaw is divided into three types shown in Table 2.

It is necessary to analyze every feedback of adjacent levels of system. According to the component behavior and control flaw table, the requirement could be verified.

Complete safety requirements could effectively prevent hazardous sources uncontrolled from happening. It could optimize the system design combined with engineer design, and at the same time decrease the safety risk.

Table 2 Control flaw table

Number	Classification
A	Inadequate Enforcement of Constraints (Control Actions)
A.1	Unidentified hazards
A.2	Inappropriate, ineffective, or missing control actions for identified hazards
A.2.1	Design of control algorithm(process) does not enforce constraints
A.2.2	Process models inconsistent, incomplete, or incorrect (lack of linkup)
A.2.3	Inadequate coordination among controllers and decision makers
B	Inadequate Execution of Control Action
B.1	Communication flaw
B.2	Inadequate actuator operation
B.3	Time lag
C	Inadequate or missing feedback
C.1	Not provided in system design
C.2	Communication flaw
C.3	Time lag
C.4	Inadequate sensor operation (incorrect or no information provided)

5. Safety assessment based on accident scenario

Accident is a set of events and its occurrence has certainty. Some targeted measure could be taken to decrease the safety risk in practical project if the reason of process of accidents could be completely recognized. Safety assessment based on accident scenario includes initiating event identifying, accident scenario developing, scenario risk assessing and so on. It could clearly describe the reason, the process and all kinds of factors that may influence system safety. System-theoretic view of STAMP is added for improving the completeness of identification of accident scenario. The process includes three steps.

Step 1: the identification of initiating event

Initiating event is the root of an accident and the beginning of a scenario. The fatal accident may be omitted if the initiating event cannot be completely identified. There are two parts of initiating events according to the safety requirements. One part is the violation of safety requirement of bottom component. Bottom component is the minimum unit of hazardous source decomposing, and the violation of requirement is the fundamental reason of hazardous source uncontrolled. The other part is the violation of safety requirement of intermediate component, but the bottom component is nominal through simulation. The reason may be the interaction of component.

Step 2: the establishment of scenario

Accident will occur when a series of constraints (or safety requirement) are not enforced or enforced inadequately. According to the definition of accident scenario and the process that accident occurs, there are two methods to establish accident scenario:

Using Event Tree Analysis. ETA is a deduction analysis method. It could get the potential accident scenario from the given initiating event, and then could qualitatively and quantitatively assess the system. It is fit for multi-factor and multi-target complex systems. For example, in 1979, ETA was used to analyze Three Mile Island Nuclear Generating Station accident, and achieved good results. However, ETA has strong subjectivity, so the completion of scenario is decided by the knowledge of analysts and the information of system.

Using the control loop. Many feedback control loop exist in adjacent level. The requirements of parent node should be decomposed to the sub-nodes, and states of sub-nodes should be fed back so that parent node could update the requirements in time. Every feedback control loop includes four

parts: Controller, Actuator, Controlled Process, and Sensor. After the identification of initiating event, the accident scenario could be identified according to the process of transmitting information of control loop. For instance, sensor failure → inadequate feedback → inaccurate information to controller→inaccurate order to actuator→inaccurate control to the controlled process→system crash →accident happening.

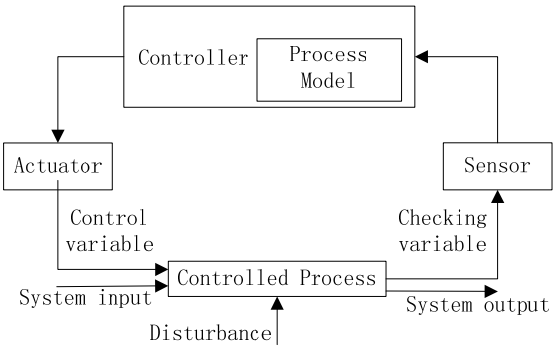

Fig. 2 Feedback control loop

After the establishment of accident scenario, analyst should figure out the probability of inadequate control, and assess the system risk. Assuming the accident severity of accident scenario L_i is C_i, and the probability is P_i, the system risk R will be $R = \sum_{i=1}^{n} C_i * P_i$. If system risk is unacceptable, the design needs to be improved, in order to decrease the system risk.

6. Conclusion

This paper introduces a safety analysis and assessment method based on hazardous source. Because hazardous source is the root of accident, it is better to identify all accident scenarios and decrease the probability and severity of accident from the root. It can put forward safety requirement for hazardous source in the design stage. Besides, it can also propose corresponding constraint measure with the engineering design. The future work may be improving the extent of analysis through simulation.

References

[1] N. Leveson, Engineering a safer world: Systems thinking applied to safety, Mit Press, 2011.
[2] C. A. Ericson, Hazard analysis techniques for system safety: John Wiley & Sons, 2005.
[3] Shen Li, "Study on the Combination of Major Hazard Theory with Practice," China Safety Science Journal, vol. 18, pp. 166-170, 2008.
[4] G. Z. 97, Engineering handbook for system safety [S], 1997.