Available online www.jocpr.com

Journal of Chemical and Pharmaceutical Research, 2014, 6(3):645-651

Research Article

ISSN : 0975-7384
CODEN(USA) : JCPRC5

A quantitative evaluation method of safety based on argument

Dajian Zhang, Minyan Lu and Nan Wu

School of Reliability and System Engineering, Beihang University, China

ABSTRACT

Many of the specific safety evaluation methods, such as Failure Mode and Effects Analysis, Preliminary Hazard Analysis, Safety Checklist, are used in the schematic design phase. Being applied as concrete techniques in a micro level, it is difficult for them to provide sufficient confidence about safety in the actual use of products. This paper presents a new quantitative safety evaluation method based on argumentation technique. First, we discuss the basic principles and the theoretical basis of our method. Then, the basic steps of evaluation are given. Finally, through a case study, we verify the feasibility and effectiveness of the method. The results show that our quantitative method can be used as a comprehensively analysis method which includes many factors from the high level, such as design, management, human factors, environments. Compared with traditional approaches, our contribution presents a new way to assist decision makers, such as product designers and project managers, to make their decisions more objectively, reasonably, effectively.

Key words: Safety; quantitative; evaluation; argument

INTRODUCTION

For industries like Astronautics, Aeronautics and Chemical Engineering, the importance of system safety is self-evident. In recent years, with the frequent occurrence of disastrous accidents like the bullet train collision, nuclear radiation caused by Fukushima earthquake and coal mine gas explosion, research and practice of safety-related theory, technology and method once again became the focus of employees in design, management, and high-risk industries, and leads the continuous improvement of all kinds of safety work.

The safety features of products usually depends on two aspects: technology and management, after years of development and evolution, safety design technology has been increasingly complete, and gradually forms a methodology represented by the specific technology of Failure Mode and Effects Analysis (FMEA), Preliminary Hazard Analysis (PHA), Safety Checklist (SCL), Hazard and Operability Study (HAZOP), Common Cause Analysis (CCA), Operation Hazard Analysis, Functional Hazard Analysis (FHA), Zonal Safety Analysis (ZSA), Accident Tree Analysis (ATA), Event Tree Analysis (ETA), Fault Tree Analysis (FTA) [1-4]. Standards like GJB900 and GJB/Z99 is a comprehensive solidification of existing technology results. However, catastrophic accidents still occur.

According to relevant statistics, more than half of the hazard events are induced by management other than design. So, although we can evaluate the safety level of the product using the safety analysis methods discussed above[5], these methods only takes the design elements into account, without any analysis of the management level in the whole process of product development and use. As a result, the credibility of conclusion of product safety level evaluation is questionable.

In recent years, a proof method based on objectives has arisen internationally, aiming to evaluate whether the system was safe or not. This method focuses on the objectives which the system wants to meet, and is based on proof and use evaluation as a link. By establishing the connection between the objectives and the evidence provided through systematic and clear evaluation, this method can demonstrate that the system meets the requirements of the objectives. This method can not only evaluate safety level during the whole cycle of product from product development to use, but also takes many factors that has impact on safety such as technology and management into account, thus explains the security level the product can reach systematically. In Europe, this kind of method based on objectives has been widely used in the military, petroleum, railway, nuclear energy, Marine and other industries. In these industries, it is used to prove the safety properties of key systems, also known as the safety case.

This paper uses demonstrate advantages and principles of safety case for references, the author analyzes and puts forward a quantitative evaluation method of safety based on argument (EMOSBOA in short). This method can intuitively and comprehensively evaluate the level of system safety, it is a more complete macroscopic evaluation technology than micro safety technology such as FMEA. As an effective supplement to the existing safety evaluation system, this method can directly apply to safety critical systems such as airplane approach and landing navigation.

In this paper, the follow-up structure arrangement is as follows: In the second section, we will present the basic concept of safety case; in the third section, we will present the principle and theoretical basis of EMOSBOA method; in the fourth section, we will present the overall framework of EMOSBOA method; in the fifth section, we will present an application example of EMOSBOA method; in the sixth section, we will present the conclusions and point out the future work.

SAFETY CASE AND ARGUMENT TECHNOLOGY

Safety case is a documented evidence entity, it is to illustrate the system is safe enough in a specific tasks or in a specific environment through a convincing and effective argument[6]. A safety case usually consists of three main parts: Claim (Objectives), argument, inference and evidence. Its basic structure as shown in the figure below:

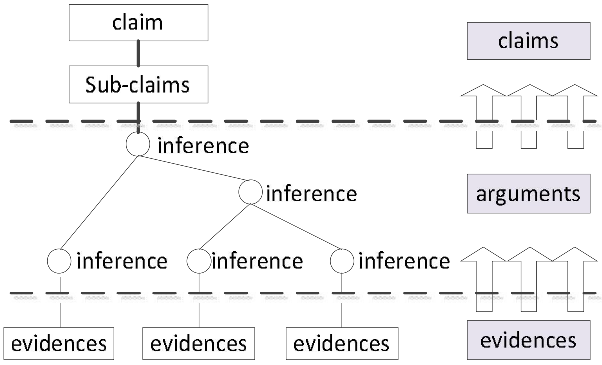

Fig.1:Basic structure of safety case

(1) Claim is a statement on the system properties, it points out the objectives that the system must meet [8]; (2) Evidence is any information or fact that can show whether a belief or proposition is true or effective. It has a very wide range of coverage, it can be based on established scientific principles, or based on the previous experience. It can be technical, and also can be other non-technical information such as laws, regulations etc. Under the background of safety case, evidence may take the form of a hypothesis as a constraint of some conditions provide convenience for creating an argument; (3) Argument is the link between claim and evidence, it shows the relationship and the basis between the general objective of safety case and evidence integrated entity.

The three elements in safety case model are connected with and based on each other. An argument without any support of evidence is illusive, baseless and unconvincing. Similarly, evidence without the support of argument is unexplainable, unable to show any proof capability, thus unable to show whether the claim is satisfied.

Since the proposal of safety case, there has been many ways to express safety argument, such as Natural Language Representation, Table Representation, Claim Structure, Goal Structuring Notation and so on. The most widely used method is Goal Structuring Notation (GSN in short). It is a graphical representation of argument brought by researchers at the University of York, UK. It provides rich graphical symbols, and it can clearly show the elements in the safety arguments (claims, evidence, background, etc) and the relationship between them [7,8]. Major GSN graphic elements can be roughly divided into two kinds: Node Element and Connector Element. A goal node contains a claim or statement about system properties, a solution node contains supported evidence of the stated claim. These two kinds of nodes are the core of the GSN and also the backbone of the argument. Strategy node, background node and assumption node belong to auxiliary nodes, they provide the necessary information for the chain of argument/support between goal nodes and solution nodes. GSN connector between the node elements is used to establish a relationship, forming a clear argument/support network structure, namely a goal structure. After ten years of development, GSN has been widely used in many fields of safety critical industries such as astronautics, railway, defense, etc. And it has achieved good results. The draft of the standards have been widely discussed, now in the middle of finishing process [9]. In the near future, with the standard formally come out, GSN will be further promoted to a broader field of application and development.

Table 1:Basic symbols of GSN

symbols	relevant interpretation
▭	Goal: a GOAL illustrates the objectives of safety case, should be expressed as a simple predicate,and whether it can be answers with yes or no, usually consists of top-level goal and sub-goals.
○	Solution: It describes the evidence of an objective is satisfied. It can be directly used to solve the goal, without the need for a decomposition to the goal. Solutions can be conclusion of independent analysis, evidence or review report and the reference design material, etc.
▱	Strategy:considered to be a rule to solve the goal. The goal can be solve by strategy, divide the goal into a series of solutions through strategy.
→	SupportedBy: express the relationship of support or evidence. Support relationship indicates a goal is supported, evidencerelationship indicates the goal and the evidence are connected. Used in between goals, goals and strategies, goals and solution.
◇	Unfinished node: Can be further analyzed.

SAFETY QUANTITATIVE EVALUATION PRINCIPLE AND THEORETICAL BASIS BASED ON SAFETY CASE

In order to quantitatively evaluate the safety of system/events, we should first determine the quantitative index of the safety system/events. In classic safety analysis technology such as FMEA, indexes like hazard severity level, hazard probability level, Probability of hazard event, etc [5,10]. The quantitative evaluation indexes sufficiently estimated the technical problems for the design phase, but it failed to take into consideration of the elements of management in the whole cycle. This paper is based on claims of system/event properties in safety case, and use the credibility of the claim as the quantitative index to measure the safety level of system/events reached, thus to conduct a comprehensive quantitative evaluation in technology and management level. Principle analysis diagram as shown in figure 2.

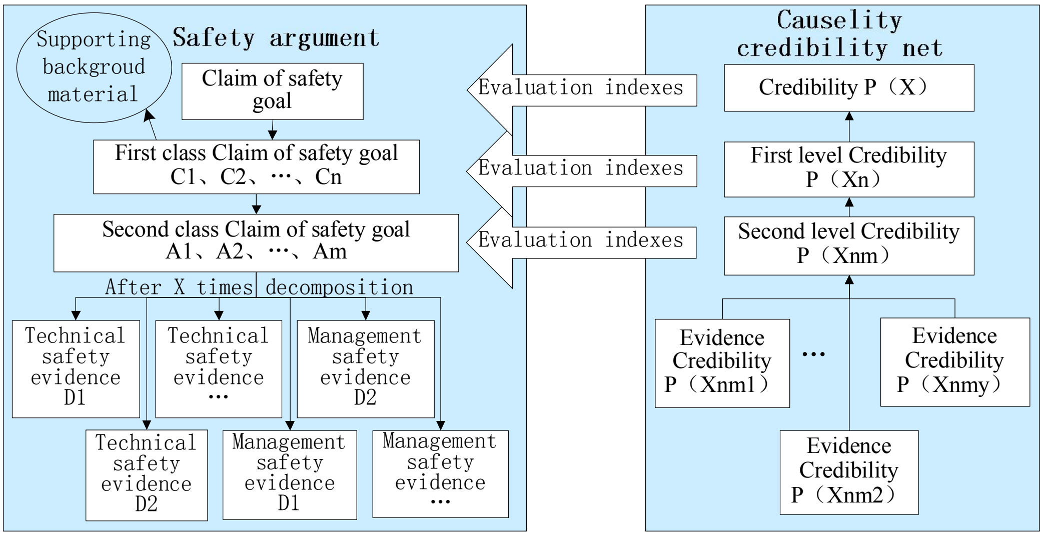
Supporting backgroud material
Safety argument
Claim of safety goal
First class Claim of safety goal C1、C2、…、Cn
Second class Claim of safety goal A1、A2、…、Am
After X times decomposition
Technical safety evidence D1
Technical safety evidence …
Management safety evidence D2
Technical safety evidence D2
Management safety evidence D1
Management safety evidence …
Evaluation indexes
Evaluation indexes
Evaluation indexes
Causelity credibility net
Credibility P（X）
First level Credibility P（Xn）
Second level Credibility P（Xnm）
Evidence Credibility P（Xnm1）
…
Evidence Credibility P（Xnmy）
Evidence Credibility P（Xnm2）

Fig.2:Principle of quantitative evaluation method of safety based on argument

As is shown in the figure, in EMOSBOA, the key is the transformation betweenthe goal and safety quantitative evaluation index. The claim of safety case (namely argument goal) is usually a true/false proposition expressed with a syntax format like <noun phrase><verb phrase>. The noun phrase of the proposition shows the subject of the claim, while the verb phrase in the proposition defines the predicates, used for making assertions to the subject. The most commonly used declaration form can be described as "XX system is safe" or "XX operation event is safe". Using the method of GSN to complete the construction of a safety case is the sign of completing the contents of the claim. On this basis, we can conduct a quantitative analysis of safety case argument framework to get the causation creditability net, and finally calculate the creditability of a claim. With the reliability migration of net, we can iteratively calculate the creditability of system or the safety claim of an operation event, thus obtaining the evaluation conclusion.

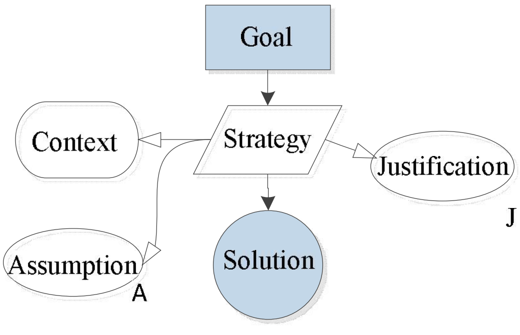

Fig.3:The basic model diagram of safety case

Figure 3 is the basic model diagram of safety case using GSN methods. The shaded area, Goal and the Solution, is essential elements the figure of the model, the rest of the diagram are the auxiliary elements. The reliability of all the evidence entities (Solution) in safety case can be characterized by a set of random variables X＝{X1, X2, …, Xn}. The evidence entities hierarchically and causally support and argue the claim of the objective (Goal), therefore, the credibility of the claim of the objective is P (X), a joint probability distribution of X. Assuming that evidence Xi are independent between each other, using the chain rule, we can get:

$$P(X_1,\cdots,X_n) = P(X_1)P(X_2|X_1)\cdots P(X_n|X_1,X_2,\cdots,X_{n-1})$$
$$= \prod_{i=1}^{n} P(X_i|X_1,X_2,\cdots,X_{i-1})(1)$$
$$= \prod_{i=1}^{n} P(X_i|\mathrm{parents}(X_i))$$

In safety case, every evidence entity or level claim represents a random variable, the connector between them represent the direct dependencies between the variables. Each variable is supplemented with a probability distribution, we can express the dependence degree between all levels of claims (Goal) and its related evidence entities (Solution) using conditional probability distribution. In fact, each Solution node has two states: “happen (Y)” or “not happen (N)”, through the recursive iteration of basic model diagram in safety case, we can get the credibility of the top event Goal claim when all the evidences “happen”. In this process, “Strategy” and other auxiliary elements can be used to help determine the value range of $P(X_i|\mathrm{parents}(X_i))$.

STEPS OF QUANTITATIVE SAFETY EVALUATION

The steps of EMOSBOA are implemented as figure 4.

First, we should transform the safety problem that needs to be evaluated to True or False proposition in syntax format like <noun phrase><verb phrase>. For instance, “A bullet-train running at 350 kilometers per hour on Beijing-Guangzhou line is safe”, or “The recently designed nuclear power system under the condition of the 8 magnitude earthquake is safe”, etc.

Second, use GSN model elements to construct the structured and modular framework from the top down. In this process, we should fully considering the safety-ensuring measures in both technical elements like design elements, personnel elements, environment elements, method elements, manufacture element and management elements, find as much evidence to support the credibility of the top event proposition statement. GSN model basic instructions are shown in table 1.

Third, regard parent and child nodes in the argument framework as random variables, the connector between them as causation relationship, and finally we get a causation net based on argument.

Fourth, determine the net parameters of causation net, namely the probability distribution of the variables. Some of these parameters can be achieved through data analysis, some can be obtained directly from the characteristics of the evidence, and the other can be obtained through expert consultation. The conditional probability of the variables constitutes the conditional probability tables (CPT).

Fifth, calculate the creditability probability of the root node according to formula 1, we can get the creditability degree of initial proposition, it can be used as safety evaluation index of systems or events. For instance, after calculation, Design Project A achieved the creditability of “A bullet-train running at 350 kilometers per hour on Beijing-Guangzhou line is safe” is 95%, Design Project B achieved the creditability of “A bullet-train running at 350 kilometers per hour on Beijing-Guangzhou line is safe” is 80%, so we have reason to believe that the safety level of Design Project A is much higher than that of Design Project B, and we should accept A.

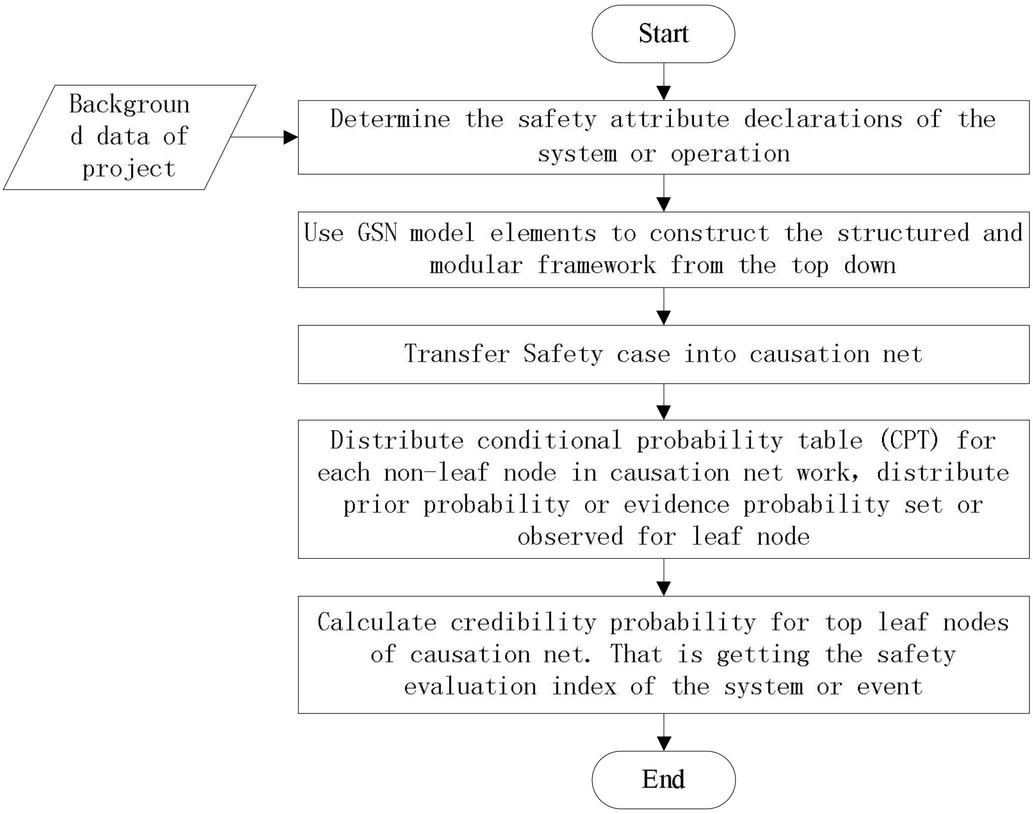
Start
Background data of project
Determine the safety attribute declarations of the system or operation
Use GSN model elements to construct the structured and modular framework from the top down
Transfer Safety case into causation net
Distribute conditional probability table (CPT) for each non-leaf node in causation net work, distribute prior probability or evidence probability set or observed for leaf node
Calculate credibility probability for top leaf nodes of causation net. That is getting the safety evaluation index of the system or event
End

Fig.4: Flowchart of quantitative safety evaluation based on argument

APPLICATION EXAMPLE

In today's society, safety of civil aviation aircraft flight is closely related to everyone's life, especially in the landing phase, the high incidence phase of flight safety accident. On July 6th 2013, Asiana airlines plane crash in San Francisco international airport, it also happened in the landing phase. We can evaluate “The plane land safely under the influence of the outside environment” using the method introduced in this paper. Considering various factors including man, machine,materials,method and environment, we can build the GSN framework as shown in figure 5. After converted to causation net, we can get figure 6. In figure 6, the lower nodes are the parent nodes of the upper nodes, the upper nodes are the parent nodes of the lower nodes. The child nodes are dependent to parent nodes. The probability and conditional probability of the variables are shown in table 2.

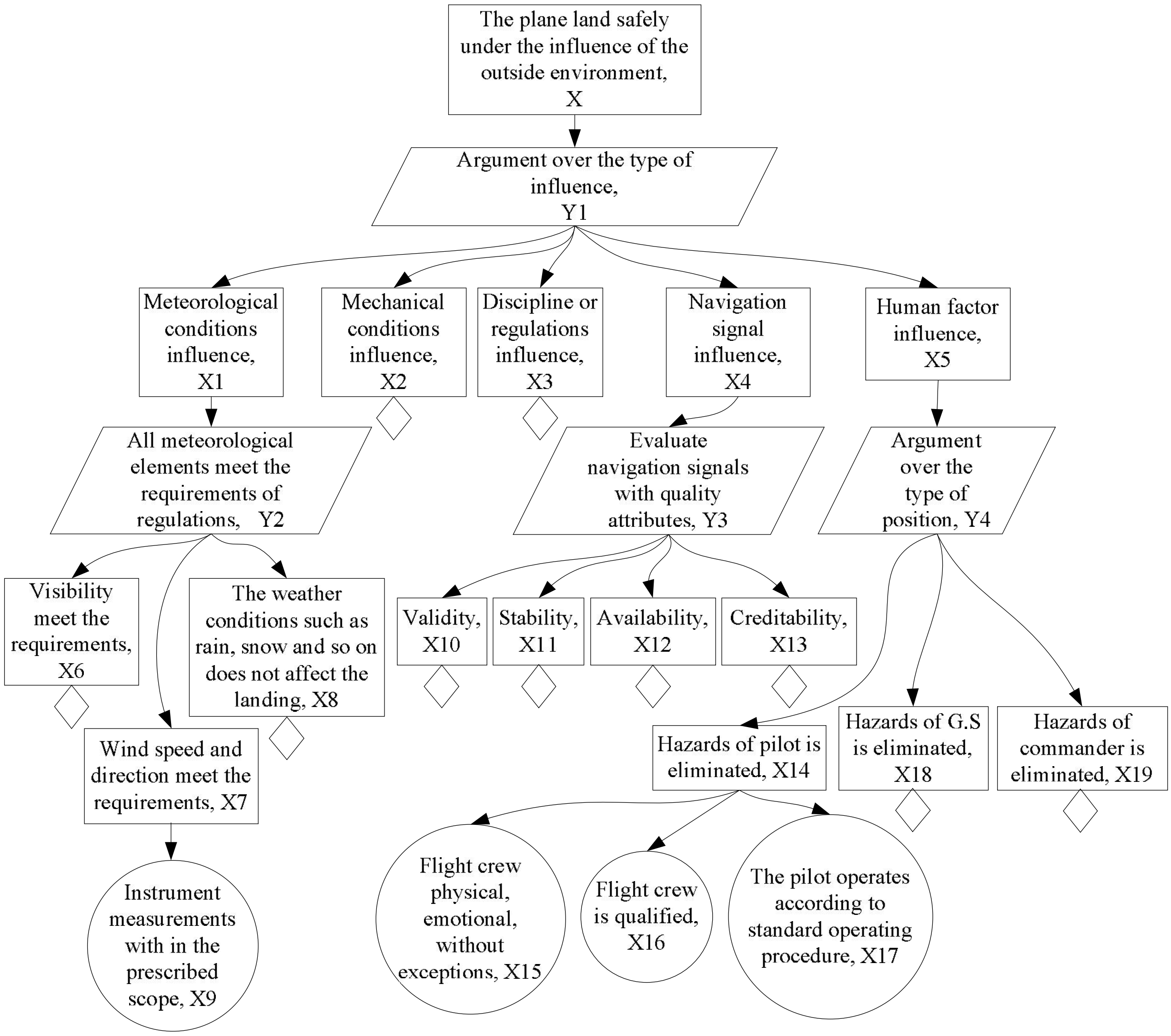
The plane land safely under the influence of the outside environment, X
Argument over the type of influence, Y1
Meteorological conditions influence, X1
Mechanical conditions influence, X2
Discipline or regulations influence, X3
Navigation signal influence, X4
Human factor influence, X5
All meteorological elements meet the requirements of regulations, Y2
Evaluate navigation signals with quality attributes, Y3
Argument over the type of position, Y4
Visibility meet the requirements, X6
The weather conditions such as rain, snow and so on does not affect the landing, X8
Wind speed and direction meet the requirements, X7
Instrument measurements with in the prescribed scope, X9
Validity, X10
Stability, X11
Availability, X12
Creditability, X13
Hazards of pilot is eliminated, X14
Hazards of G.S is eliminated, X18
Hazards of commander is eliminated, X19
Flight crew physical, emotional, without exceptions, X15
Flight crew is qualified, X16
The pilot operates according to standard operating procedure, X17

Fig.5: Flowchart of quantitative safety evaluation based on argument

Table 2: The probability or conditional probability of each variable

Probability or conditional probability	**Method to obtain**
P(X9) = P(X7)=0.80	
P($X1\|X6,X7,X8$)=0.98	Analyze statistical data
P(X6)=0.83	Analyze statistical data
P(X8)= P(X2)=0.95	Analyze statistical data
P($X4\|X10,X11,X12,X13$)=1	obtained directly form characteristics of the evidence combined with strategy Y3
P(X10)= P(X13)= P(X16)=1	obtained directly form characteristics of the evidence
P(X11)= P(X12)= P(X3)=0.99	Analyze statistical data
P($X14\|X15,X16,X17$)=0.90	From expert consultation
P(X15)=0.98	Analyze statistical data
P(X17)=0.97	Analyze statistical data
P($X5\|X14,X18,X19$)=1	obtained directly form characteristics of the evidence combined with strategy Y4
P(X18)=0.94	Analyze statistical data
P(X19)=0.96	Analyze statistical data
P($X\|X1,X2,X3,X4,X5$)=0.99	From expert consultation

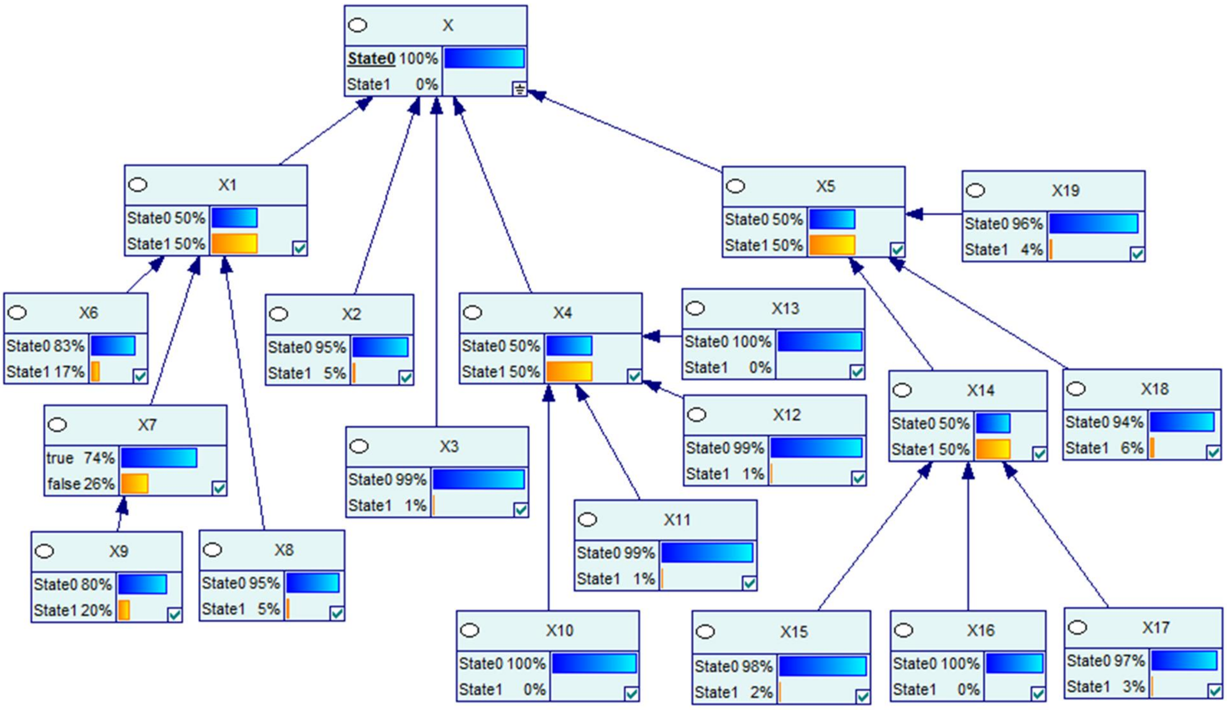

Fig.6:Causal network

By utilizing the reasoning of Bayesian network, we can calculate the credibility ofour top goal,safe land under the influence of environment. In this case, the credibility of our top goal is 0.8.

CONCLUSION

This paper proposes a system safety evaluation method based on the model of argument, it is centered on hazard, linked with argument to set up a safety evaluation framework. And then quantitatively evaluates system safety with Bayesian network, takes the landing stage as an object for the application example to test its feasibility and validity. Results indicate that EMOSBOA can intuitively and reasonably show and confirmed the system's safety level. And this method can provide a useful tool for the risk decision of system.

REFERENCES

[1] Yuanhui WANG. *System Safety Engineering*.Tianjin university press,**1999**.
[2] Donghong ZUO, Kaiqing GONG.*System Safety Engineering*.Chemical Industry Press,**2004.**
[3] Baozhi CHEN. *System Safety Assessment and Prediction*.Metallurgical Industry Press,**2005.**
[4] Jifa GU, Liyan ZHAO. *Systems Engineering and Electronics*, v.21, n.8, pp.28-31,**1999**
[5] Jun LU. *Safety assessment, analysis and research of Civil aircraft flight control system*.School of Astronautics in University of Civil Aviation China,**2009.**
[6] Bishop P, Bloomfield R. *In Industrial Perspectives of Safety-critical Systems*, pp.194-203,**1998**.
[7] Kelly T, Weaver R. *In Proc of Dependable Systems and Networks*, **2004**.
[8] Kelly T. *Arguing Safety – A Systematic Approach to Managing Safety Cases*. University of York, **1998**.
[9] Goal Structuring Notation Working Group. *GSN Community Standard Version 1*. **2011.**
[10] Feng WANG. *System safety analysis methods of front landing gear system*. School of Astronautics in University of Civil Aviation China,**2009.**
[11] Hongzhi WU. *Journal of South China Normal University*,v.5, pp.23-27,**2003.**
[12] Hitchcock D.*Argumentation*, v.19, n.3, pp. 373-391,**2005.**