Modeling and application of risk assessment considering veto factors using fuzzy Petri nets

Reference:
Zhou Jianfeng, Reniers Genserik.- Modeling and application of risk assessment considering veto factors using fuzzy Petri nets
Journal of loss prevention in the process industries - ISSN 0950-4230 - 67(2020), 104216
Full text (Publisher's DOI): https://doi.org/10.1016/J.JLP.2020.104216
To cite this reference: https://hdl.handle.net/10067/1703470151162165141

Fuzzy risk assessment with veto factors

Jianfeng Zhou[a, *], Genserik Reniers [b, c, d]

a. School of Electromechanical Engineering, Guangdong University of Technology, Guangzhou 510006, China
b. Faculty of Technology, Policy and Management, Safety and Security Science Group (S3G), TU Delft, 2628 BX Delft, The Netherlands
c. Faculty of Applied Economics, Antwerp Research Group on Safety and Security (ARGoSS), Universiteit Antwerpen, 2000 Antwerp, Belgium
d. CEDON, KULeuven, 1000 Brussels, Belgium

Abstract: Risk assessment is important for plant safety, and fuzzy set theory is useful for such assessment because many safety factors have fuzzy characteristics. In this study, veto factors for risk assessment are taken into account. Weighted fuzzy Petri-net with inhibitor arcs is proposed to model relationships between safety factors and establish the risk assessment structure considering veto factors. Definitions of WFPN as well as the enabling rule and execution rule are provided. The modeling approach for the assessment combining normal factors with veto items is discussed. The proposed fuzzy risk assessment approach is illustrated by an example of assessing the safety of production installations and process technique of plants that deal with hazardous chemicals. Veto factors and non-veto factors are presented and the assessment structure based on WFPN is established. Using the factor data of a plant, a safety value is obtained through the operation of WFPN and the verification of the approach is discussed.

Keywords: risk assessment; veto factors; fuzzy set; weighted fuzzy Petri-net

1. Introduction

Risk assessment, also known as "safety assessment", is a technology to detect hazards, analyze harmful factors and possible consequences, predict the risk of a system, and suggest reasonable safety measures. It is very important to the safety production of plants and the safety supervision of government departments. Many legislations, governments and international organizations, such as the SEVESO directive, OSHA (occupational safety and health administration), and the United States Environmental Protection Agency (US EPA), have established regulations and programs, which require manufacturers to perform a safety analysis to ensure that major accident hazards have been identified and appropriate safety measures have been taken.

There have been many fatal accidents resulting from an inadequate safety assessment in the past decades, causing great property losses and casualties. For instance, one of the worst industrial disasters in recent U.S. history occurred in the BP Texas City Refinery on March 23, 2005. Fifteen people were killed and 180 were injured by explosions and fires, and financial losses exceeded $1.5 billion (CSB, 2007). According to the final report issued by the CSB (2007), the main reason of the accident was the lack of process safety measures and insufficiency of risk reduction measures. As another example, crude oil leaking from an underground pipeline entered the drainage of Qingdao City of China, and led to a series of explosions and fires on November 22, 2013. The accident killed 62 people and injured another 136. According to the official accident investigation report, the direct cause was the rupture of the pipeline. Defects in the design of pipeline and drainage systems, inadequate supervision of pipelines, weak awareness of safety among maintenance workers, and inefficient emergency response

[*]Corresponding author.

processes were potential causes of the accident.

Many methods have been used to assess safety, such as Fault Tree Analysis (FTA) (NUREG, 1981), Failure Mode and Effects Analysis (FMEA) (Stamatis, 2003), Event Tree Analysis (ETA) (Beim and Hobbs, 1997), Markov chains (Mechri et al., 2011), and Bayesian networks (Leu and Chang, 2013). The safety assessment of a plant often involves many factors, many of which are characterized by uncertainty or fuzziness. Therefore, fuzzy set theory was introduced in many fields of safety assessment. For example, fuzzy set theory was combined with fault tree analysis to estimate the occurrence probability of accidents (Wang et al. 2013; Cheliyan and Bhattacharyya, 2018). In failure mode and effect analysis (FMEA), the fuzzy set method was utilized to deal with uncertainties (Lin et al., 2014; Jiang et al., 2017). Fuzzy logic was also employed during event tree analysis to reduce uncertainties (Huang et al., 2001; Ramzali et al., 2015). Fuzzy Markov chain was utilized to solve the problem of imprecision in safety assessing (Mechri et al., 2011), and fuzzy-based HAZOP (Hazard and Operability Analysis) was adopted for analyzing process hazards and risk evaluation (Fuentes-Bargues et al., 2016).

In addition to combining with conventional safety assessment techniques, fuzzy set theory was also widely used in comprehensive safety assessment which uses safety factors and weights to make a general assessment of the safety level of systems or objects. Guo et al. (2009) developed a comprehensive evaluation model which integrates with a three-layer BP neural network to evaluate equipment criticality. Hanss and Turrin (2010) proposed an approach based on fuzzy arithmetic to solve uncertainties of epistemic type in modeling and analysis of systems. Zeng et al. (2017) used fuzzy comprehensive evaluation method to evaluate the sustained casing pressure (SCP) risk in gas wells.

So far, fuzzy safety assessment, especially fuzzy comprehensive assessment, focuses on the combined role of various factors in safety assessment, and veto factors have hardly been taken into account. In the safety management, there may be situations in which, in assessing some safety conditions, certain safety factors are of particular importance and are not to be tolerated by safety management if they are not satisfied, even if other safety factors are satisfied well. For example, to assess the operation process of all jobs of a plant, the main factors to consider are whether the operation processes are based on the analysis of hazardous and harmful substance, whether the operation processes are issued to the relevant jobs, and whether the head of the plant or his designated technical person in charge approves and issues the operation processes, etc. However, if there is a job which has not an operation process, the assessment result of the operation process of the plant is not qualified even if the operation process assessment results of other jobs are very good. These safety factors if they are not satisfied they cannot be tolerated are the vetoes of the corresponding safety conditions, that is, if these factors are not satisfied, the assessment results of the corresponding safety condition will take the worst value directly. To the best of our knowledge, in the existing studies, there is no study on risk assessment with veto factors. The veto factors will influence relationships between safety factors and the structure of safety assessment, and conventional safety assessment methods can hardly deal with them.

Petri-net is a powerful modeling and analysis tool to describe various relationships among parts of a system. It can use elements like places, transitions, arcs and tokens to establish a graphical model, and has strict mathematical expressions. Various technologies of system description and system behavior analysis can be carried out by Petri-nets. In addition to expressing knowledge, Petri-net can also show the reasoning process. In the beginning, Petri nets are mainly used in modeling and analysis of discrete event systems. In order to model and analyze more complex systems, many extensions are proposed on the basis of ordinary Petri-net. To express and analyze uncertain knowledge, some researchers integrated fuzzy set theory with Petri-net to form fuzzy Petri-net (FPN) (Albert and Senen, 1994; Chen, 2002; Liu et al., 2017). In this study, FPN is utilized to assess safety considering veto factors as it can well describe the problem of assessment with veto factors.

The remaining parts of this paper are organized as follows. In Section 2, problems of safety assessment when veto factors are taken into account are briefly discussed. In Section 3, the definitions of WFPN as well as the corresponding enabling rule and the execution rule are provided. The modeling approach of safety assessment with veto factors is discussed. An illustrative example of the application of this approach is presented in Section 4. The conclusions of this work are given in Section 5.

2. Assessment problems with veto factors

When veto items are taken into account in safety assessment, some new problems may emerge. Veto factors are usually handled differently from non-veto factors. For an assessment with non-veto factors, a common requirement is to make a comprehensive assessment, that is, to consider the influences of multiple factors at the same time. Different factors have their own weights according to the importance to the assessment item, and the relationship between the factors is "AND". However, for veto factors, the relationship between them is usually “OR”, that is, when one of the veto factors is satisfied, the corresponding assessment item is vetoed (the minimum assessment value is usually taken).

For an assessment item, when veto factors are satisfied, the non-veto factors assessing the same item do not work; when none of the veto factors is satisfied, the non-veto terms can be used to make a comprehensive assessment of the item. That is, to assess an item, veto factors and non-veto factors are mutually exclusive.

The general fuzzy assessment methods only consider the comprehensive influence of various factors, so they are difficult to model and analyze the relationships between factors at the same time when veto factors are considered. In this work, Petri-net is used to model and analyze the assessment problem with veto factors.

3. WFPN approach

A method of extending Petri-net is to introduce a special arc called inhibitor (David and Alla, 2010). An inhibitor arc is a directed arc connecting a place p to a transition t. Different from normal directed arcs, its end is marked by a small circle. Fig.1 shows a Petri-net with a normal arc and an inhibitor arc. In this figure, the inhibitor arc between p_1 and t_1 represents that transition t_1 is only enabled if place p_1 does not contain any tokens and p_2 which connects to t_1 through a normal directed arc has at least one token. This mechanism can be adapted to integrate with fuzzy Petri-nets to meet the requirements of assessment with veto items.

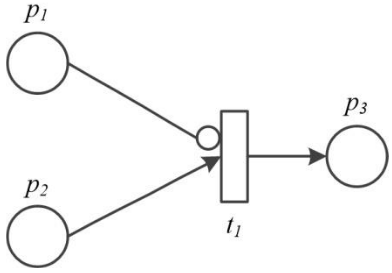


Fig. 1 A Petri-net with a normal directed arc and an inhibitor arc

3.1 Definitions

Combining the inhibitor arcs with the WFPN given by Chen (2002), the WFPN is redefined as follows:

Definition 1:

$$WFPN = (P, T, I, O, F, M)$$

Where,

1) $P=\{p_1, p_2, ..., p_n\}$, is a finite set of places, which corresponds to propositions in the fuzzy theory.

2) $T=\{t_1, t_2, ..., t_m\}$, is a finite set of transitions, corresponding to rules in the fuzzy theory. $P \cup T \neq \emptyset$, and $P \cap T = \emptyset$.

3) $I: P\times T \rightarrow [0, 1]$, defines the arcs from places to transitions. I is divided into two sets, I_N representing normal directed arcs and I_I representing inhibitor arcs. The value of an arc (p_j, t_i) defines the weight $w_{ij} \in [0, 1]$ of the input place p_j of transition t_i, and the default value is one. If (p_j, t_i) for j=1, 2, …, k are normal arcs of transition t_i, then

$$\sum_{j=1}^{k} w_{ij} = 1$$

4) O: defines the directed arcs from transitions to places, representing rules to propositions.

5) F: is an n×q dimensional matrix, representing fuzzy values (memberships) of n places in q evaluation levels of the Petri-net. Its element $f_{ij} \in [0, 1]$ is the membership value of place p_i in level j. $F(p_i)$ represents membership vector in place p_i.

6) M: is the marking vector, representing the marking of the Petri-net. A marking of a WFPN indicates the tokens in places. As places in a WFPN represent states, a place can have at most one token. Thus, if place p_i has a token, $M(p_i)$=1, otherwise, $M(p_i)$=0. The initial marking is denoted as M_0.

Places, transitions and arcs in WFPN are represented as icons, where, places are represented with circles, transitions are denoted as rectangles, and directed arcs indicate the impacts between places and transitions. The end of a normal directed arc is an arrow, and the end of an inhibitor arc is marked by a small circle.

With the definition of the WFPN above, the transition enabling and execution rules can be defined. Denote input places of transition t (input transitions of place p) and output places of transition t (output transitions of place p) as •t(•p) and t•(p•), respectively.

In Fig.1, if place p_1 has a token, transition t_1 cannot be enabled to execute. This mechanism cannot directly model the mutex relationship between veto factors and non-veto factors in a risk assessment. Thus, the enabling and execution of transitions with inhibitor arcs are slightly improved in this work. For assessment problems, the veto factor represented by p_1 should also be able to activate transition t_1 (at this time p_2 should be inhibited) and the execution of t_1 should output a value (a worse value comparing the output when p_2 works) reflecting the veto to p_3. Thus, we define the enabling rule and the execution rule as follows:

Definition 2 (Enabling rule): A transition t_j in WFPN is enabled if any of the following conditions is satisfied:

(i) $M(p_i)=1$, for any $p_i \in \bullet t_j$ and (p_i, t_j) is a normal directed arc
and $M(p_k)=0$, for $p_k \in \bullet t_j$ and (p_k, t_j) is an inhibitor arc.

(ii) At least one of places $p_k \in \bullet t_j$ satisfies $M(p_k) = 1$, for (p_k, t_j) is an inhibitor arc.

There are two situations that can enable a transition to execute. If every place connecting to transition t_j through normal directed arc has one token, and all places connecting to transition t_j through inhibitor arcs have no token (rule i), transition t_j is enabled. Rule ii indicates that if one of the places connecting to transition t_j through inhibitor arc has a token, transition t_j is enabled. But in these two situations, the execution of transition t_j is different, which is determined according the execution rule.

For the sake of the following discussion, the membership vectors $F(p_i)$ for $p_i \in \bullet t_j$ and (p_i, t_j) is a normal directed arc are expressed as matrix $F_N(t_j)$, and corresponding weights of p_i on t_j are denoted by $W_N(t_j)$.

Definition 3 (Firing/execution rule): If a transition t_j in WFPN is enabled, it can fire/execute. The execution of an enabled transition t_j in marking M changes the marking into M', satisfying

$M(p_i) = M'(p_i)$, for $p_i \in \bullet t_j$

$M'(p_i) = 1$, for $p_i \in t_j \bullet$

And

$F(p_i) = W_N(t_j) \times F_N(t_j)$, for $p_i \in t_j \bullet$ and t_j is enabled by rule (i),

$F(p_i) = F(p_k) \times w_{ki}$, for $p_i \in t_j \bullet$ and t_j is enabled by rule (ii), and $F(p_k) \times w_{ki}$ has the smallest defuzzified value for $p_k \in \bullet t_j$ and $M(p_k)=1$.

3.2 Modeling

(1) WFPN modeling

Using WFPN, relationships between safety factors, which can build a structured reasoning mechanism using fuzzy reasoning can easily be modeled. Fig. 2 shows WFPN models of basic logical relationships "AND" and "OR".

According to the firing/execution rule of WFPN, the membership vector of p_t in Fig. 2 (a) can be deduced by the following formula:

$$F(p_t) = W_N(t_1) \times F_N(t_1) \tag{1}$$

Where, $W_N(t_1) = [w_1 \quad w_2 \quad \dots \quad w_n]$, and

$$F_N(t_1) = \begin{bmatrix} F(p_1) \\ F(p_2) \\ \dots \\ F(p_n) \end{bmatrix} = \begin{bmatrix} f_{11} & f_{12} & \cdots & f_{1q} \\ f_{21} & f_{22} & \cdots & f_{2q} \\ \dots \\ f_{n1} & f_{n2} & \cdots & f_{nq} \end{bmatrix}$$

for each factor has q assessment levels.

In Fig. 2 (b),

$$F(p_t) = W_N(t_k) \times F_N(t_k)$$

for defuzz($W_N(t_k) \times F_N(t_k)$) = min (defuzz($W_N(t_1) \times F_N(t_1)$), defuzz($W_N(t_2) \times F_N(t_2)$), …, defuzz($W_N(t_n) \times F_N(t_n)$), $1 \le k \le n$.

where, defuzz() is a defuzzification function which converts fuzzy values to crisp values.

As in the safety assessment studied in this work, the "OR" relationship exists between the veto items, the min() function which returns the minimum value among crisp values is used to determine the veto item which has the greatest impact on the target.

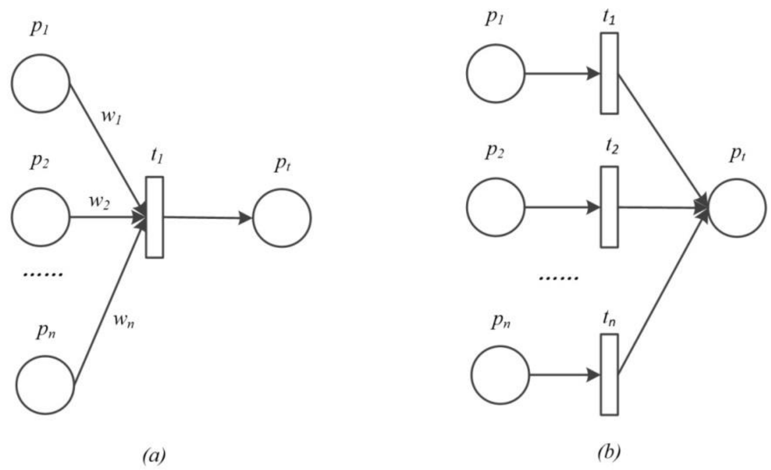


Fig. 2 Modeling of relationships between factors

Combining the "AND" model and the "OR" model, we can establish the structure for safety assessment with veto factors. Fig. 3 illustrates the assessment for the factor represented by place p_t. There are n normal factors expressed by $p_1, p_2, \ldots, p_n$ and two veto items represented by p_{v1} and p_{v2}.

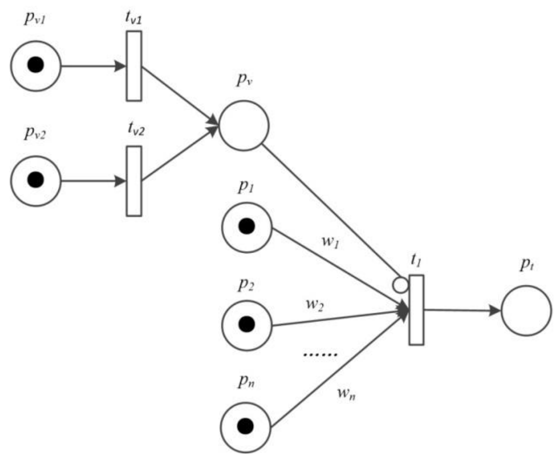


Fig. 3 Assessment structure combining normal factors and veto items

It should be noted that during the assessment shown in Fig. 3, transition t_1 is initially enabled by normal factors expressed by $p_1, p_2, \ldots, p_n$, and a token with assessment value will be put into p_t after t_1 executes. When place p_v gets a token, t_1 may have finished the assessment with $p_1, p_2, \ldots, p_n$. Thus, the operating mechanism of an assessment is determined as follows:

(i) After the execution of a transition, tokens in places connecting to the transition will not be removed, this is in line with the firing/execution rule of WFPN model.

(ii) The condition for the termination of an assessment is that the values of all places are no longer updated.

In this way, transition t_1 can still continue to execute after an execution, as long as the enabling rule is satisfied.

(2) Fuzzy assessment

The basic structure of fuzzy safety assessment based on WFPN is shown in Fig. 4, which consists of the following components:

i. The fuzzifier decomposes input safety assessment variables with crisp numbers and maps the crisp numbers into fuzzy sets using membership functions. An example of membership functions is presented in Fig. 5, where, there are five assessment levels, namely very good, good, medium, bad, and very bad, for input crisp numbers range from 1 to 5. In particular, the fuzzy number of a veto factor in this condition can be set to (1 0 0 0 0) which means definitely very bad.

ii. The fuzzy reasoning module maps input fuzzy sets into fuzzy output sets. It follows fuzzy arithmetic operations of a WFPN model discussed above.

iii. The defuzzifier provides a process of converting fuzzy sets into crisp outputs. There are several defuzzification processes in literature such as the Smallest, Middle, and Largest of Maximum (SOM, MOM, LOM) method or the centroid method (Klir and Yuan, 1995; Yager, 2002). In this study, the centroid method which is a centre average defuzzifier for defuzzification is utilized as it gives mean value of the fuzzy sets. Centroid defuzzification returns the center of area under the curve. If the area is considered as a plate of equal density, the centroid is the point along the horizontal axis about which this shape would balance. It is mathematically represented as:

$$d^* = \frac{\int_d uf(u)du}{\int_d f(u)du}$$

Where, d^* is the defuzzified value, u is the output fuzzy set, and $f(u)$ is the membership function.

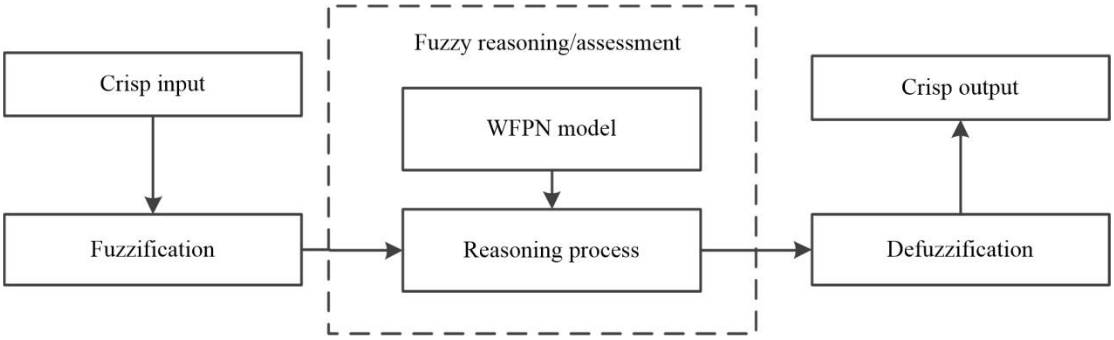


Fig. 4 The structure of fuzzy safety assessment system

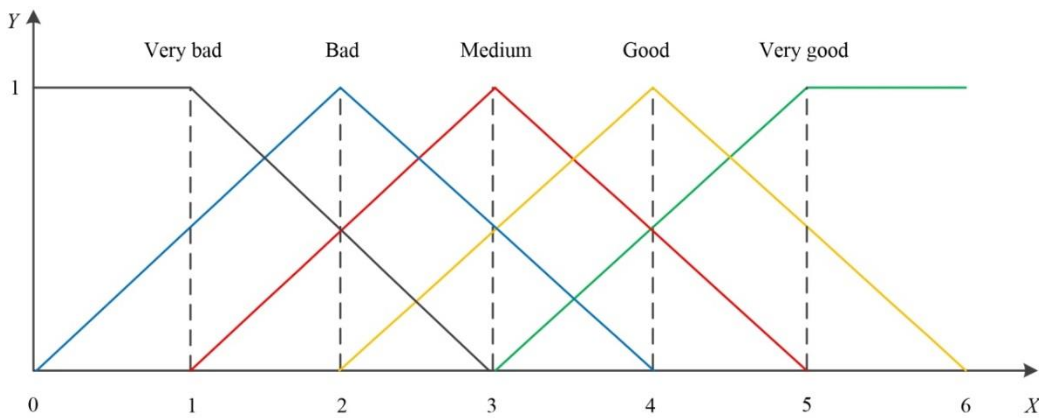


Fig. 5 Membership functions for assessment levels

4. Illustrative example

The safety of production installations and process technique is an important part of plant safety, and is taken as an example to illustrate the proposed safety assessment approach.

Carrying out the standardization of work safety in the enterprises of the chemicals industry is an important means to improve the safety management level of the enterprises and ensure the safety of life and property. Since 2005, the Work Safety Administration Bureau of China (WSABC) has issued the standard for the standardization of work safety of hazardous chemicals enterprises (Trial), and has carried out nationwide standardization of the enterprises. In 2011, WSABC also issued the assessment standard for standardization of work safety of hazardous chemicals enterprises, which requires hazardous chemicals enterprises to carry out standardization work in work safety from 11 areas which are called 11 level A factors, including organizations and responsibilities, management system, management of risk, training and education, accidents and emergency response, and so on. In the assessment standard, the 11 level A factors are divided into 55 level B factors. The assessment is conducted using a scoring method, and each B-level factor has several scoring points. In the assessment standard, different veto items are also established for level A and level B factors. If the sub-items for a certain level factor are satisfied with a full score, but a veto factor of that factor is met, the score of this factor is 0.

The original factors of the work safety standardization assessment of chemical enterprises are too many to illustrate the proposed approach. This paper selects the production installations and the process technique related factors to construct the illustrative example. Most assessment factors have fuzzy characteristics, and the fuzzy assessment method can better reflect the characteristics of each factor. The factors for the safety assessment of production installations and process technique (F0) are determined as shown in Table A.1. Two levels of safety factors are listed in the table for assessing the top factor F0. Although many second-level factors still have lower level factors, as an example, they are not divided downwards in this work. In this work, the production installations and the process technique (F0) are assessed from seven aspects which are expressed as the first level factors, including production installation construction (F1), safety facilities (F2), special equipment (F3), process technique safety (F4), key installations and key parts (F5), inspection and maintenance of installations (F6), and scrapping (F7). Each first-level factor contains several second-level factors. In Table A.1, the explanation of the factors shows the composition of the second-level factors.

In this work, the weight of each factor is determined according to the score assigned to each factor in the work safety standardization assessment, and each second-level factor is assigned 1 to 5 scores according to the degree of conformity. The factors are fuzzified using the method showing in Fig. 5.

There are several veto factors for the safety assessment of production installations and process technique as listed in Table A.2. According to their vetoing factors, they can be divided into two categories, one is the veto factors for top factor F0, the other is the veto factors for the first-level assessment factors. If one veto factor is satisfied, the factor it vetoes will obtain the minimum assessing score.

According to the above safety assessment factors, the WFPN model is established as shown in Fig. 6. The weight of each factor in the assessment is marked on the arc, and the default is 1.

Table 3 shows the scores of non-veto factors for the assessment of a plant.

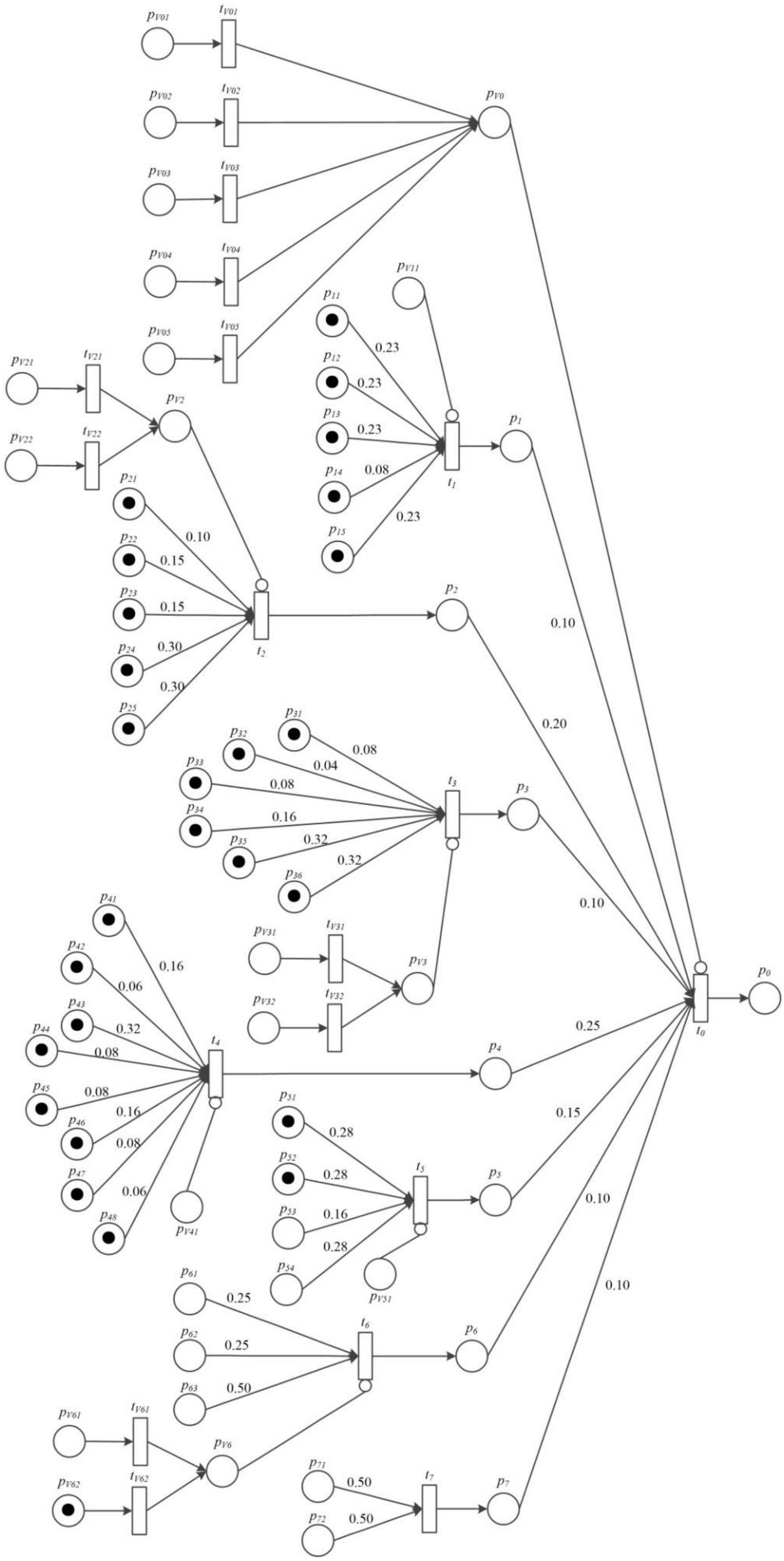


Fig. 6 WFPN model for the safety assessment of production installations and process technique

Table 3 Quantified values of safety assessment factors

Factor	Score	Membership vector	Factor	Score	Membership vector
F11	4	(0 0 0.5 1 0.5)	F12	3.5	(0 0.25 0.75 0.75 0.25)
F13	4.5	(0 0 0.25 0.75 0.75)	F14	3	(0 0.5 1 0.5 0)
F15	4.5	(0 0 0.25 0.75 0.75)	F21	3	(0 0.5 1 0.5 0)
F22	4	(0 0 0.5 1 0.5)	F23	3.5	(0 0.25 0.75 0.75 0.25)
F24	3	(0 0.5 1 0.5 0)	F25	3	(0 0.5 1 0.5 0)
F31	5	(0 0 0 0.5 1)	F32	4.5	(0 0 0.25 0.75 0.75)
F33	5	(0 0 0 0.5 1)	F34	4	(0 0 0.5 1 0.5)
F35	3.5	(0 0.25 0.75 0.75 0.25)	F36	5	(0 0 0 0.5 1)
F41	3.5	(0 0.25 0.75 0.75 0.25)	F42	4	(0 0 0.5 1 0.5)
F43	4	(0 0 0.5 1 0.5)	F44	3	(0 0.5 1 0.5 0)
F45	3	(0 0.5 1 0.5 0)	F46	4	(0 0 0.5 1 0.5)
F47	3.5	(0 0.25 0.75 0.75 0.25)	F48	3	(0 0.5 1 0.5 0)
F51	4	(0 0 0.5 1 0.5)	F52	3	(0 0.5 1 0.5 0)
F53	4	(0 0 0.5 1 0.5)	F54	4.5	(0 0 0.25 0.75 0.75)
F61	4	(0 0 0.5 1 0.5)	F62	5	(0 0 0 0.5 1)
F63	1	(1 0.5 0 0 0)	F71	4	(0 0 0.5 1 0.5)
F72	4.5	(0 0 0.25 0.75 0.75)			

Suppose the veto item V62 in Table A.2 (Inspection and maintenance formality is not gone through properly) is met, thus the membership vector of V62 is set to (1 0 0 0 0). The tokens of places are marked in Fig. 6. Through the fuzzy operations of WFPN model, the defuzzified value (centroid) in place p_0 is 3.3963, which is shown in Fig. 7. The result indicates that the safety of production installations and process technique of this plant is almost in the middle of "medium" and "good".

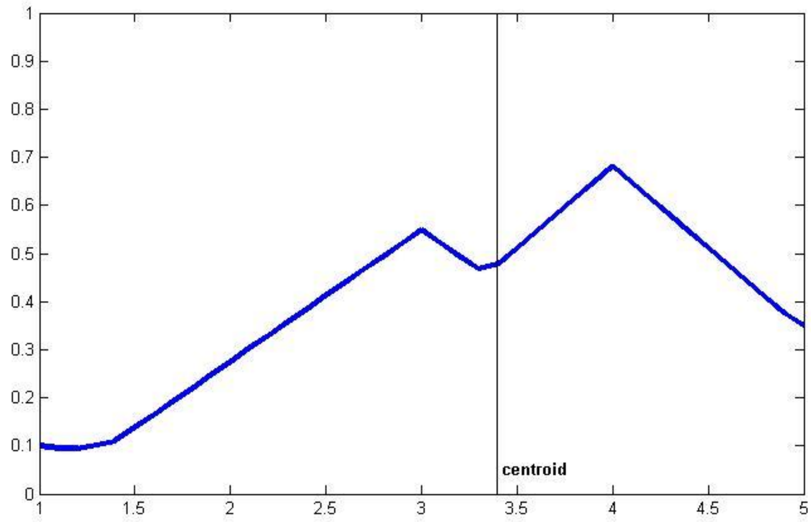
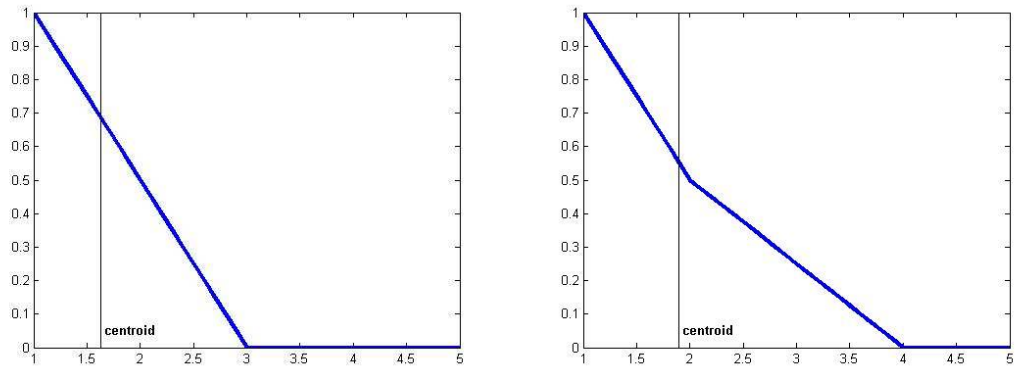


Fig. 7 Centroid defuzzification result of place p_0

For the verification of the proposed safety assessment approach, the fuzzy operation shown by Eq.

(1) and the assessment structure shown in Fig. 4 are consistent with the normal fuzzy assessment. Thus, the assessment without veto factors can be considered correct and the following discussion focuses on the assessment with veto factors.

According to the requirement of safety assessment, if a veto factor is satisfied, the upper factor it assesses should be vetoed, that is, the vetoed factor should be given a score less than (or at least equal to) that assessed by corresponding non-veto factors. Take the assessment of factor F6 (inspection and maintenance of installations) as an example, there are three non-veto factors F61, F62 and F63, and two veto factors V61 and V62. In the WFPN model, V61 and V62 correspond to p_{v61} and p_{v62}, respectively. If any of V61 and V62 is satisfied, the corresponding place (p_{v61} or p_{v62}) is set an initial fuzzy vector (1 0 0 0 0), and the assessment of non-veto factors is inhibited, so that place p_6 will obtain the result fuzzy value (1 0 0 0 0). Its defuzzified centroid value is 1.633, which is shown in Fig. 8 (a). Suppose there are no veto factors, the assessment is only based on the three non-veto factors, and assume they all take the lowest score 1. The fuzzy vector obtained using membership functions is (1 0.5 0 0 0). Using the WFPN model, the assessment result of p_6 is also (1 0.5 0 0 0), whose corresponding defuzzified centroid value is 1.896 and is shown in Fig. 8 (b).



(a) (b)

Fig. 8 Centroid defuzzification result of place p_6. (a) assessment result with veto factors. (b) assessment result without veto factors

It can be seen that even if all the non-veto factors take the minimum value, the result assessed without veto factors is less than that assessed with veto factors. Obviously, we can get similar results for other factors assessed with veto sub-factors. Thus, the proposed WFPN based safety assessment approach can meet the requirements of assessment with veto factors.

5. Conclusions

Assessing the safety of a plant often involves many factors, for example, the factors for assessing accident likelihood including installations, management, and environment, and the factors for assessing accident consequence, such as safety distance, personal protective equipment, and emergency response. Many of these factors are characterized by uncertainty or fuzziness, and fuzzy safety assessment is widely used in many fields of safety assessment.

In some situations, the veto factors should be considered in safety assessment, as they have key influences on the safety, which are difficult to reflect only by weights. If veto factors are taken into account in safety assessment, there are mutually exclusive relationships and "AND" and "OR" relationships between factors. However, it is difficult to set up the assessment structure with veto factors in common fuzzy safety assessment methods. Petri-net is a powerful tool on modeling relationships between parts of a system, and is taken as a modeling tool in this study.

An approach based on weighted fuzzy Petri-net with inhibitor arcs is proposed for safety assessment with veto factors. The definitions of WFPN including definitions of enabling rule and execution rule are presented. How to establish the WFPN based structure for safety assessment with veto factors is discussed. Fuzzy arithmetic operations are reflected in the WFPN model.

The safety of production installations and process technique is one important part of plant safety. It is taken as an example to illustrate the proposed safety assessment approach. Two levels of veto factors are considered in this safety assessment. The WFPN model is established and used to assess the safety of a plant, and the verification of the approach is discussed. It can properly deal with assessment problem considering veto factors and provide reasonable result.

Acknowledgment

This work is supported by National Natural Science Foundation of China (No. 71673060).

References

Albert J. B., Senen B., 1994. Fuzzy Reasoning Supported by Petri Nets. IEEE Transactions on Fuzzy Systems 2(2), 135-150.

Beim, G.K., Hobbs, B.F., 1997. Event tree analysis of lock closure risks. Journal of Water Resources Planning and Management ASCE 123, 137-198.

Cheliyan, A.S. Bhattacharyya S.K., 2018. Fuzzy fault tree analysis of oil and gas leakage in subsea production systems. Journal of Ocean Engineering and Science 3, 38-48.

Chen S.-M., 2002. Weighted fuzzy reasoning using weighted fuzzy Petri nets. IEEE Transactions on knowledge and data engineering 14(2), 386-397.

CSB, 2007. BP America Refinery Explosion, Final Investigation Report. http://www.csb.gov/file.aspx?DocumentId=345.

David R., Alla H., 2010. Discrete, Continuous, and Hybrid Petri Nets. Springer-Verlag, Berlin, Germany.

Fuentes-Bargues J.L., Gonzalez-Gaya C., Gonzalez-Cruz M.C., Cabrelles-Ramírez V., 2016. Risk assessment of a compound feed process based on HAZOP analysis and linguistic terms. Journal of Loss Prevention in the Process Industries 44, 44-52.

Guo L., Gao J., Yang J., Kang J., 2009. Criticality evaluation of petrochemical equipment based on fuzzy comprehensive evaluation and a BP neural network. Journal of Loss Prevention in the Process Industries 22, 469-476.

Hanss M., Turrin S., 2010. A fuzzy-based approach to comprehensive modeling and analysis of systems with epistemic uncertainties. Structural Safety 32, 433-441

Huang D., Chen T., Wang M.-J. J., 2001. A fuzzy set approach for event tree analysis. Fuzzy Sets and Systems 118, 153-165.

Jiang W., Xie C., Zhuang M., Tang Y., 2017. Failure mode and effects analysis based on a novel fuzzy evidential method. Applied Soft Computing 57, 672-683.

Klir GJ, Yuan B., 1995. Fuzzy sets and fuzzy logic: theory and applications. Prentice-Hall, Inc. Upper Saddle River, NJ, USA.

Leu S.-S., Chang C.-M., 2013. Bayesian-network-based safety risk assessment for steel construction projects. Accident Analysis & Prevention 54, 122-133.

Lin Q.-L., Wang D.-J., Lin W.-G., Liu H.-C., 2014. Human reliability assessment for medical devices based on failure mode and effects analysis and fuzzy linguistic theory. Safety Science 62, 248-256.

Liu H.-C., You J.-X., Li Z., Tian G., 2017. Fuzzy Petri nets for knowledge representation and reasoning: A literature review. Engineering Applications of Artificial Intelligence 60, 45-56.

Mechri W., Simon Ch., Ben Othman K., Benrejeb M., 2011. Uncertainty evaluation of Safety Instrumented Systems by using Markov chains. IFAC Proceedings Volumes 44, 7719-7724.

Mechri W., Simon Ch., Othman K.B., Benreje M., 2011. Uncertainty evaluation of Safety Instrumented Systems by using Markov chains. Proceedings of the 18th World Congress The International Federation of Automatic Control Milano (Italy), August 28 - September 2, 2011.

NUREG, 1981. Fault tree handbook. Report NUREG-0492.

Ramzali N., Lavasani M.R.M., Ghodousi J., 2015. Safety barriers analysis of offshore drilling system by employing Fuzzy Event Tree Analysis. Safety Science 78, 49-59.

Stamatis D.H., 2003. Failure Mode and Effect Analysis: FMEA from Theory to Execution. ASQ Quality Press, Milwaukee, USA.

Wang D., Zhang P., Chen L., 2013. Fuzzy fault tree analysis for fire and explosion of crude oil tanks. Journal of Loss Prevention in the Process Industries 26, 1390-1398.

Yager R.R., 2002. Uncertainty representation using fuzzy measures, IEEE Trans. Syst. Man Cybern. Part B. Cybern. 32, 20-28.

Zeng D., He Q., Yu Z., Jia W., Zhang S., Liu Q., 2017. Risk assessment of sustained casing pressure in gas wells based on the fuzzy comprehensive evaluation method. Journal of Natural Gas Science and Engineering 46, 756-763.

Zhu Y., Qian X., Liu Z., Huang P., Yuan M., 2015. Analysis and assessment of the Qingdao crude oil vapor explosion accident: Lessons learnt. Journal of Loss Prevention in the Process Industries 33, 289-303.

Appendix

Table A.1 Factors for the safety assessment of production installations and process technique (F0)

First level factor	Second level factor	Description
Production installation construction(F1)	"Three simultaneities" (F11)	Safety facilities and the main production installation of a construction project should be designed, constructed and put into use simultaneously.
	Management of all stages of the construction (F12)	According to the relevant laws and regulations of the State Safety Administration, construction projects should be regulated in the establishment stage, the design stage, the trial production stage and the acceptance stage.
	Safety supervision of construction process (F13)	The construction project must be designed, constructed and supervised by units with corresponding qualifications; Effective safety supervision is implemented for the construction process of the construction project, and the construction site has a complete safety inspection record to ensure that the construction process is in an orderly management state.
	Management of changes (F14)	Any change during the construction process should strictly implement the regulations of change management, fulfill the change procedure, and carry out risk management in the whole process of the change.
	Safe technology, process technique or equipment (F15)	Production installations should use advanced, safe and reliable new technology, new equipment and new materials; The newly developed process technique must be verified by expert team and be gradually enlarged to industrial production on the basis of small scale test, pilot test and industrialization test.
Safety facilities(F2)	Safety facility account (F21)	A plant should set up the safety facilities account, and its content should meet the requirements.
	Allocation of safety facilities (F22)	Provide fixed alarm facilities for the detection of flammable and / or toxic gases in areas with flammable, explosive or toxic hazards in accordance with relevant specifications; In accordance with the national standards,

		fire embankment is installed in the flammable liquid tank area, and the embankment is set up in the acid and alkali tank area and anticorrosive treatment is carried out; Allocate fire protection facilities and equipment in accordance with national standards; etc.
	Dedicated management of safety facilities (F23)	All kinds of safety facilities are managed by special people; Management files of safety facilities are established.
	Maintenance of safety facilities (F24)	Safety facilities should be included in the equipment maintenance plan, and maintained regularly with records; Safety facilities shall not be dismantled, misappropriated or abandoned arbitrarily.
	Management of monitoring and measuring facilities/tools (F25)	Establish monitoring and measuring facilities/tools management system; Set up monitoring and measurement facilities account; Calibrate and maintain monitoring and measuring facilities/tools with records regularly.
Special equipment(F3)	Management system of special equipment (F31)	Establish a standardized management system for special equipment in accordance with the provisions of national laws and regulations.
	Ledger and archives (F32)	Establish special equipment accounts and files, including technical information, regular inspection records of special equipment and safety accessories, operation records and failure records, daily maintenance records, etc.
	Registering with the supervisory department (F33)	Before the special equipment is put into use, it shall register with the state special equipment supervision and administration department, and the registration mark shall be placed in the prominent position of the equipment.
	Routine maintenance (F34)	Carry out regular routine maintenance of special equipment, check at least once a month, and keep records.
	Periodical calibration (F35)	Regularly calibrate or maintain special equipment, safety accessories, safety protection devices, measurement and control devices and related ancillary instruments in use.

	Periodic inspection (F36)	A month before the expiration of the validity period of special equipment, a regular inspection requirement shall be put forward to the inspection organization of the special equipment; Special equipment which has not been inspected regularly or is not qualified shall not continue to be used; Place or attach the safety inspection mark to the prominent position of the special equipment.
Process technique safety(F4)	Operator's mastery of process technique safety (F41)	Operators should master safety information of process technique, including: (1) chemical hazard information; (2) process technique information; (3) installation information.
	Operation safety of installations (F42)	A plant shall ensure the safe, reliable and complete operation of the following installations: (1) pressure vessels and pressure pipelines, including fittings and valves; (2) pressure relief and emptying systems; (3) emergency shutdown systems; (4) monitoring, alarm systems; (5) interlocking system; (6) all kinds of moving equipment, including spare equipment, etc.
	Risk analysis of processes (F43)	Plants should carry out risk analysis of process: (1) analyze hazards in process; (2) identify potential accident factors in workplace; (3) control influence of potential failures; (4) analyze human factors.
	Inspection of production installations prior to start-up (F44)	Production installations shall be inspected before operation and safety conditions shall be confirmed.
	Stop of production installations (F45)	Production installations shutdown shall meet the requirements.
	Disposal of hazardous chemicals released from pressure relief or emptying systems (F46)	Hazardous chemicals released from pressure relief or emptying systems should be led to a safe place and disposed properly.
	Emergency disposal of production installations (F47)	Measures to deal with emergency and abnormal situations should be determined in operation procedures; When an emergency occurs, it should be properly handled in accordance with the principle of non-injury to the personnel and, if necessary, the installation should be stopped urgently and the emergency should be reported to the

		relevant parties at the same time.
	Treatment of process parameter deviation (F48)	Operators should be aware of the deviation treatment approaches of process parameters; deviations should be analyzed and corrected timely.
Key installations and key parts(F5)	Management system of key installations and key parts (F51)	Plants should identify key installations and their key parts, and carry out the management mechanism of the contact person for the key installations by plant leaders.
	Safety supervision on key installations (F52)	The contact person has the responsibility of safety supervision and guidance for the key installations and key parts for which he is responsible, including supervising the implementation of production safety policies, laws and regulations, regularly checking the problems existing in production safety, supervising and controlling hidden dangers, supervising the implementation of accident handling, and so on.
	Archives of key installations and key parts (F53)	Establish files of key installations and key parts; clarify responsibilities of all management levels of a plant; make records of supervisions.
	Emergency plan of key installations and parts (F54)	Make emergency plans of key installations and key parts; conduct emergency exercises at specified intervals to ensure that people of operation, maintenance of key installations and key parts can identify and timely handle all kinds of accidents.
Inspection and maintenance of installations(F6)	Inspection and maintenance management system (F61)	Develop and implement inspection and maintenance management system, carry out routine and periodical inspection and maintenance.
	Annual comprehensive inspection and maintenance plan (F62)	Formulate annual comprehensive inspection and maintenance plan; carry out "five determinations", namely determining maintenance plan, determining maintenance personnel, determining safety measures, determining maintenance quality, determining maintenance schedule principle.
	Inspection and maintenance operation procedure (F63)	In carrying out inspection and maintenance operations, the prescribed procedures shall be carried out, including: Before a maintenance

		or repair, identifying hazardous and harmful factors, preparing the inspection and repair plan, handling of procedures for delivery of equipment or facilities for inspection and maintenance; performing safety check during a maintenance or repair; handling the formalities of delivery to production after a maintenance or repair.
Scrapping(F7)	Demolition and scrapping management system (F71)	Plants should strictly implement the management system of dismantling and scrapping production installations, and operators should identify hazardous and harmful factors, draw up demolition plans and obey procedures for handover of demolition installations.
	Cleaning of hazardous chemicals (F72)	All containers, equipment and pipelines that need to be removed should be cleaned and checked before they can be removed; demolition, cleaning and other on-site operations should strictly obey the relevant provisions of work permits, etc.

Table A.2 Veto items for the safety assessment of production installations and process technique

Factor	Veto item	Description
F0	Violated any of the "three simultaneities" items. (V01)	Fail to conduct design check, safety condition analysis or completion acceptance of an installation in accordance with national requirements.
	Design, construction or supervision units are not qualified (V02)	Design, construction, or supervision units do not have qualifications or their qualifications do not meet the requirements.
	Technology, equipment or materials used are eliminated by national decree (V03)	Adopt the technology, equipment and materials prohibited by the state.
	The chemical process technique adopted for the first time has not gone through safety verification (V04)	The chemical process technique adopted for the first time in China has not been proved to be safe.
	There are dangerous processes which are not automatically controlled in accordance with regulations (V05).	The dangerous chemical process techniques determined by the State Administration of Work Safety needs to adopt automatic control technology.
F1	The newly developed production process of hazardous chemicals has been conducted directly in industrial	The newly developed process technique of dangerous chemicals is directly industrialized without the process of small-scale, pilot-scale

	production without required tests (V11).	and industrialized tests.
F2	Overtemperature, overpressure detection, acoustic and / or optical alarm system, and safety interlocking devices are not installed (V21).	Fail to install detection instruments, acoustic and / or optical alarm system, and safety interlocking devices at locations that may cause fire and explosion.
	Gas detection and alarm devices are not installed where toxic or flammable gas may leak (V22).	Toxic or flammable gas leakage alarm devices are not set according to the standard.
F3	Existence of special equipment that is not scrapped in time (V31).	The special equipment which has the hidden danger of severe accident, has no maintenance value, or exceeds the safety technical service life, should be scrapped in time.
	Special equipment that has been scrapped is still in use (V32)	Scrapped special equipment can no longer be used.
F4	Pressure vessels and accessories are not inspected or unqualified (V41).	Pressure vessels and accessories including safety valve or bursting disc should be checked regularly.
F5	Key installations and their key parts are not determined (V51).	Plants involving hazardous chemicals should determine key installations and their key parts for work safety.
F6	There is no inspection and maintenance plan developed (V61).	The inspection and maintenance plan should be made before the inspection and maintenance operation is carried out.
	Maintenance or repair formality is not gone through properly (V62).	Fail to properly handle procedures for delivery of installations/facilities to maintenance or repair before the maintenance or repair, or delivery of installations/facilities to production after the maintenance or repair.