J. Shanghai Jiaotong Univ. (Sci.), 2015, 20(4): 508-512
DOI: 10.1007/s12204-015-1658-z

Systematic Safety Analysis Method for Power Generating Equipment

ZHANG Wei[1*] (张　伟),　*HOU Yue-min*[1,2] (侯悦民)
(1. Department of Mechanical Engineering, Tsinghua University, Beijing 100084, China;
2. School of Mechatronic Engineering, Beijing Information Science and Technology University, Beijing 100192, China)

Abstract: A systematic safety analysis method is presented to guide the whole analysis process starting with safety analysis requirement and ending with technical and economical evaluation of the knowledge model and the arrangement of sensors. The method consists of five phases, including data acquisition on factual evidence and collecting design, manufacturing, and installation data of equipment; establishing knowledge model; measurable analysis and selection of sensors as well cost evaluation; knowledge description; and overall evaluation. The proposed method is used for safety analysis of hydraulic power generating units and the analysis results validate the method very well.

Key words: safety analysis, systematic method, cognition model, technical-physical effects, fault diagnosis
CLC number: TH 17　　**Document code:** A

0 Introduction

Safety is a major concern of enterprises, including human safety, economic safety and equipment safety. Three most common used fault modeling techniques are failure mode and effects analysis (FMEA), fault tree analysis (FTA), and model-based approaches. There is one problem in FMEA, FTA and model-based methods: safety analysis quality relies greatly on the knowledge, skill and expertise of the safety engineer. This paper proposes a systematic safety analysis method to provide a controllable procedure for safety analysis of large complex engineering systems.

The effectiveness and reliability of safety analysis depends greatly on the quality of knowledge model, which is at core of safety analysis. Fuzzy logic network, Markov methods, Bayesian networks are widely used for fault model and fault tree[1] for safety integrity level verification[2], probabilistic operational safety assessment of multi-mode engineering systems[3], failure probabilities and fault feature extraction[4], proactive safety assessments[5], and evaluating the faulty behavioral risk value in large-scale hydropower-construction project[6]. These methods focus on algorithms for fault models. There is one problem in FMEA, FTA and model-based methods: safety analysis quality relies greatly on the knowledge, skill and expertise of the safety engineer. These methods focus on establishing fault tree and fault model, but less on identification of physical effects that fail to take effects. This paper proposes a systematic safety analysis method to establish causal dependencies between fault phenomena, sensor signals, function structure, working structure, technical-physical effects and failure parameters based on cognition model and design methodology. Cognitive psychology has been introduced into safety analysis to model human activities[7]. This paper establishes cognition model of knowledge and constructs a theoretic safety analysis method. The proposed method is used for safety analysis of hydraulic power generating units and the analysis results validate the method very well.

1 Theoretical Foundation of the Method

Three world cognition model and design methodology are used to construct the safety analysis method. Three world cognition model is used as a theoretical framework of knowledge modeling, and design methodology is used to provide logical reasoning of causes of fault phenomena.

According to Popper[8], the cognition process involves three worlds. World I consists of physical bodies, including biological objects. World II is the world of mental or psychological states or processes, or of subjective experiences, including conscious experiences from dreams or from subconscious experiences. World III means the world of the products of the human mind,

Received date: 2014-06-23
Foundation item: the National Natural Science Foundation of China (No. 51175284) and the Science and Technology Program of Education Committee of Beijing Municipality (No. SQKM201211232002)

∗**E-mail:** wei-z@mail.tsinghua.edu.cn

including objective knowledge, descriptive languages, or symbolic representations[8]. Supposing E denotes existence field, A and B are existences, a and b are observable phenomena of A and B respectively. α and β are symbolic representations of A and B respectively. ε is the theory describing the existences of A and B. According to ε, β can be derived from α. Therefore, ε explains why a causes b. E explains how observable phenomena result from failure components.

Equipment have dual nature: physical objects existed in nature and artificial objects designed by human. Therefore, equipment systems belong to both World I and World II. As physical objects in World I, equipment can be described by objective knowledge and symbolic representations in World III through mental activity in World II, i.e. through World II thought processes, World III thought contents can be obtained. Knowledge models are thought contents in World III, while the process of knowledge modeling is a thought process. Then, the question here is how to do this? Mental activities are beyond discussion of this paper, but, fortunately, the relationship between World I and World III can be traced down through the design process of the equipment system, which is the point of the proposed method.

Since the dual nature of equipment systems, the relationship between an equipment system and its description is recorded in the design process. Hence, design methodology is a very important guideline to reconstruct mapping between the structure and the function, or the structure and the failure function.

Design is to produce a product or product description that belongs to World I through mental process that belongs to World II. Equipment are embodiments of design. Hence, the design process can be used to guide knowledge modeling. A widely used design process includes three basic phases: the conceptual design, embodiment design and detail design. The conceptual design results in the basic structure of the equipment systems. The conceptual design starts with establishing a function structure by breaking down an overall function into subfunctions. A subfunction can be fulfilled by one of a number of technical-physical effects. Technical-physical effects can be described quantitatively in terms of physical quantities by means of the physical laws governing the physical quantities involved. Some physical quantities are measurable, while some not. Only measurable quantities can be observed through sensors. The cost of sensors and their installation are also factors of safety analysis. Working structures achieving certain technical-physical effects work together to fulfill the main function of the equipment system. Some functions are main functions, while some functions are auxiliary functions.

The major concern for safety analysis is establishing causal dependencies between a hazard and failures of individual components, which depends on the logic relationship of subfunctions and measurable physical quantities of technical-physical effects. Therefore, a function structure involving logical relationship of subfunctions, technical-physical effects, working structures and measurable signals are required for safety analysis. Figure 1 illustrates the template of function structure. In Fig. 1, arrow lines between two items mean the

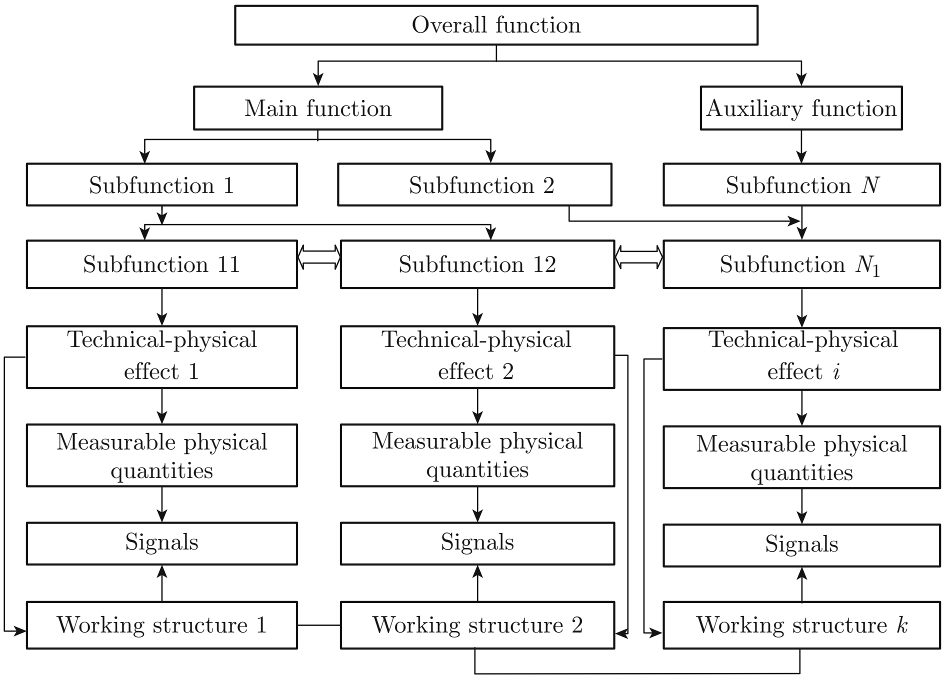

Fig. 1 Functional structure

dependency of these two items. Double arrow blocks mean interactive relation of two items. Lines mean that two substructures are connected to each other.

2 Safety Analysis Method

A systematic safety analysis method is constructed based on the cognition model of safety analysis, which involves five phrases: ① collecting factual data of the object, including customer safety requirement, operation data and fault data of the equipment system, and design and manufacturing knowledge; ② establish knowledge model, including establishing function structure and analyzing functional gain and loss of technical effects; ③ determine observable field, i.e., fault signal signs that can be measured by sensors, including measurable analysis of physical quantities and economical evaluation of measurement scheme, determining measuring points layout and selecting sensors, fault signal signs, and confirming diagnosis parameters and signal feature extraction methods; ④ knowledge representation, including field description of knowledge model (text, diagnosis, fault causal network, hybrid diagnosis tree), knowledge representation and knowledge database; ⑤ overall technical and economical evaluation, including comparison, evaluation, and verification of the signals of sensors and functions, see Fig. 2.

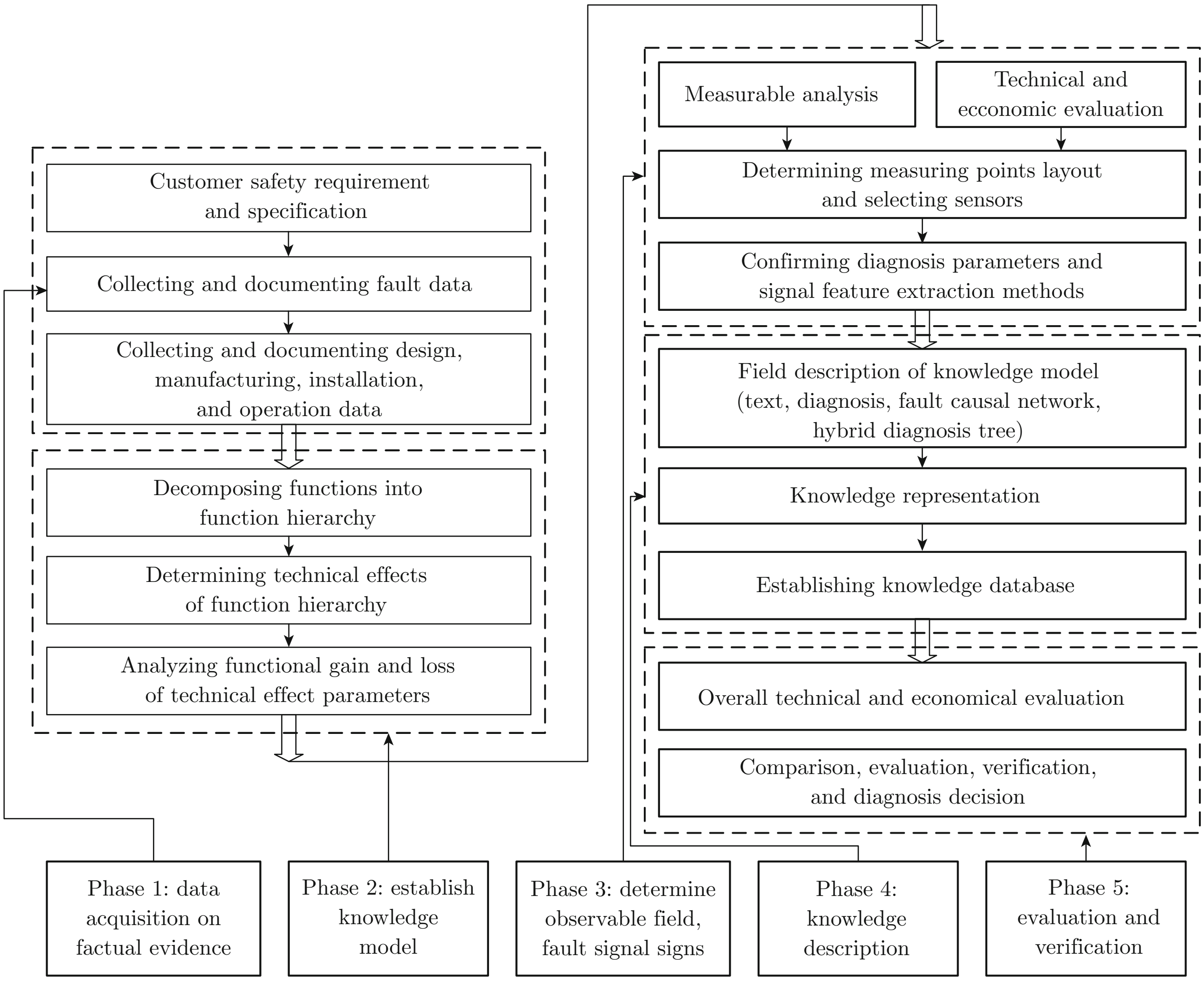
Measurable analysis
Technical and ecconomic evaluation
Determining measuring points layout and selecting sensors
Confirming diagnosis parameters and signal feature extraction methods
Customer safety requirement and specification
Collecting and documenting fault data
Collecting and documenting design, manufacturing, installation, and operation data
Field description of knowledge model (text, diagnosis, fault causal network, hybrid diagnosis tree)
Decomposing functions into function hierarchy
Knowledge representation
Determining technical effects of function hierarchy
Establishing knowledge database
Analyzing functional gain and loss of technical effect parameters
Overall technical and economical evaluation
Comparison, evaluation, verification, and diagnosis decision
Phase 1: data acquisition on factual evidence
Phase 2: establish knowledge model
Phase 3: determine observable field, fault signal signs
Phase 4: knowledge description
Phase 5: evaluation and verification

Fig. 2 Safety analysis method

The quality of the knowledge model depends on function structure and functional gain and loss of technical effects. The technical-physical effects in Fig. 1 are main technical-physical effects. Some other technical-physical effects may companion a main effect or some additional effects have to be added to enable this main effect. Redundancy technical-physical effects may exist for easy manufacturing or operation. Unknown technical effects may also exist because of lack of knowledge. The hierarchy of the technical-physical effects provides causal relationship between function failure and failure components. The relationship is represented hierarchically as Main technical-physical effects, Adjoin technical-physical effects, Additive technical-physical effects, Redundancy technical-physical effects, and Unknown technical-physical effects.

Combining the function structure and the technical-physical effect hierarchy, effects of control parameters of technical-physical effects on function gain and loss can be done and the condition and probability of fault events can be predicted. Control parameters of technical-physical effects are measured by sensors. Working structures fulfilling the main technical-physical effects and auxiliary effects are related to signals of sensors, therefore the relation between specific sensor signal and certain components can be established and the fault cause can be traced down to failure structures.

3 Safety Analysis of Large Hydraulic Power Generating Units

(1) Safety analysis requirement. The customer's requirement is fault diagnosis of the trust bearing of a hydro turbine of large hydraulic power generating units. The problem was the signal alarm of axial displacement frequently warned and the generating unit could not start operation.

(2) Measurable physical quantity. The measurable physical quantity of technical-physical effects is bubble content of the lubricant. The test result of the bubble content is shown in Table 1.

(3) Function structure. The function structure is shown in Fig. 3.

(4) Technical effects of the function structure. Technical effects of the function structure are illustrated in Table 2.

Table 1 Test result of the bubble content of shell turbine oil 30#

Lubricant No.	Unit No.	Bubble content/%	Bubble content standard/%
Shell turbine oil 30#	1#	3.3	10
Shell turbine oil 30#	2#	5.9	10

(5) Diagnosis analysis. According to Table 2, the installation space of trust bearing was within the tolerance, but it was a bit large so that the main technical-physical effect could not take full effect, which caused that oil film force and rigidness decreased. At the same time, addictive technical-physical effect failed to take effect because the additional oil baffle ring of the trust disk was not installed. The oil baffle ring was designed to prevent centrifugal oil so that the higher backpressure can be obtained to assist loading. On the other hand, lubricant oil was mixed with water steam by accident, which caused higher bubble content. The unknown technical-physical effect took effect, which was not reported both in China and outside China. The unknown technical-physical effect was cavitation effect in oil, which developed into cavitation effect and corrosive pitting of bearings.

(6) Measures. The measures that were taken included: changing oil; adjusting installation space of tiles of trust bearing; installing the baffle oil ring.

(7) Result. The unit worked well after taking these measures.

Using the proposed safety analysis method, the fault cause is explained, including the original cause, basic condition, development process of the fault, subsidiary

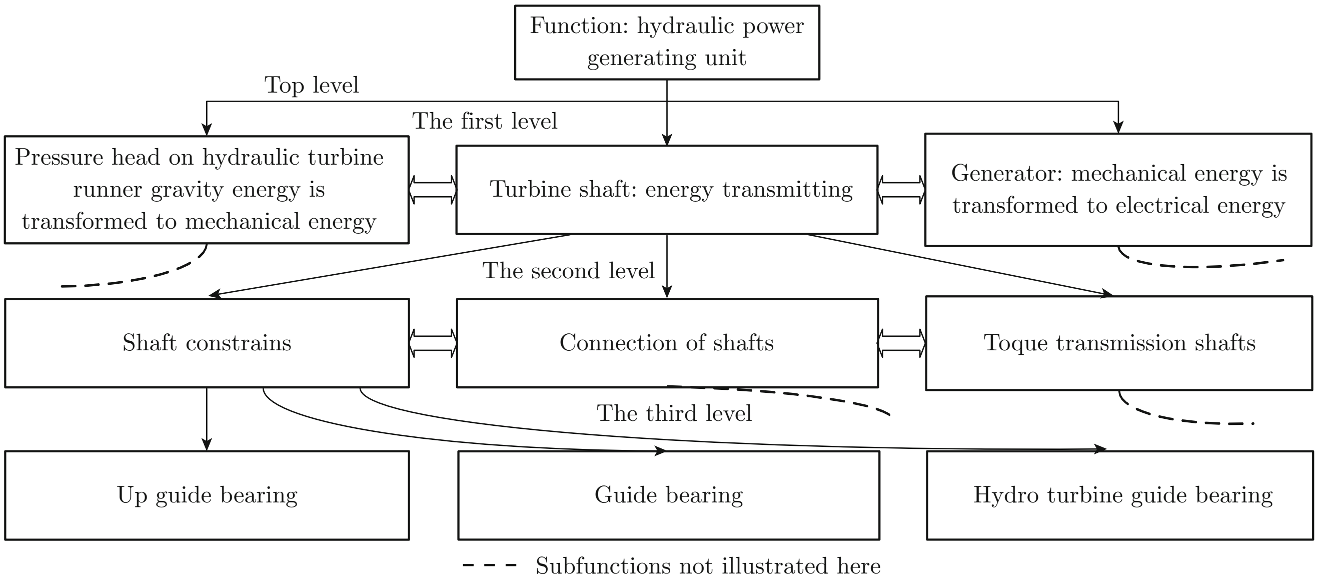
Function: hydraulic power generating unit
Top level
The first level
Pressure head on hydraulic turbine runner gravity energy is transformed to mechanical energy
Turbine shaft: energy transmitting
Generator: mechanical energy is transformed to electrical energy
The second level
Shaft constrains
Connection of shafts
Toque transmission shafts
The third level
Up guide bearing
Guide bearing
Hydro turbine guide bearing
Subfunctions not illustrated here

Fig. 3 The function structure of hydraulic power generating unit

Table 2 Technical effects of function structure

	Technical effects	Objective knowledge	Effects on functions	Control parameters
Function constraint principle of guide bearing	Main technical effect	Fluid thick film dynamic lubrication principle	Three basic factors	Minimum film thickness. Tile temperature and oil temperature of inlet and outlet, and their deference.
	Adjoint technical effect 1	Newton inner friction effect	Temperature rise	Oil temperature of inlet and outlet and difference.
	Adjoint technical effect 2	Temperature viscosity effect of lubricant	Viscosity change against form of film	Oil temperature deference of inlet and outlet.
	Additive technical effect 1	Tiles rub (boundary lubrication and collide)	Contact area and time	Tile temperature and oil temperatures of inlet and outlet, and their variance ratio.
	Additive technical effect 2	Pressure viscosity effect of lubricant	Viscosity change against form of film	
	Additive technical effect 3	Static pressure jack-up device during startup and shutdown process	Jack up in the case of low velocity	
	Additive technical effect 4	Self lubrication or small friction	Babbitt metal or plastic tiles	Friction efficient and pressure ratio.
	Additive technical effect 5	Cooling cycle (oil coolant and forced tile cooling)		Flow of cooling fluid, fluid temperature through the inlet and outlet.
	Unknown technical effect 1	Non-laminar flow?		
	Unknown technical effect 2	Cavitation effect?		
Possible installation condition	Too large clearance (small preload, low oil film rigidness)	Too small clearance (larger preload, high oil film rigidness, too high oil temperature)	Smaller clearance for all bearings (larger preload, high oil film rigidness, higher oil temperature)	Moderate clearance for all bearings or heterogeneous clearances (moderate preload, normal oil film rigidness, normal oil temperature)

cause and the result. Failure structures are tracked down based on function structure and the hierarchical technical-physical effects of the hydraulic power generating unit.

4 Conclusion

This paper proposes a systematic safety analysis method based on three world cognition model and design methodology. The method involves five phases: ①objective knowledge acquisition; ②knowledge modeling; ③measurable analysis; ④knowledge representation; ⑤technical and economical evaluation. The knowledge model is constructed by establishing the hierarchical function structure and hierarchical technical-physical effects. Based on this model, effects of control parameters of technical-physical effects on function gain and loss can be found, and the condition and probability of fault events can be predicted. The proposed method is used for safety analysis of hydraulic power generating units and the analysis results validate the method very well.

References

[1] Abou S C. Fuzzy-logic-based network for complex systems risk assessment: Application to ship performance analysis [J]. *Accident Analysis and Prevention*, 2012, **45**: 305-316.

[2] Shu Y, Zhao J. A simplified Markov-based approach for safety integrity level verification [J]. *Journal of Loss Prevention in the Process Industries*, 2014, **29**: 262-266.

[3] Lin Y, Chen M, Zhou D. Online probabilistic operational safety assessment of multi-mode [J]. *Reliability Engineering and System Safety*, 2013, **119**: 150-157.

[4] Meel A, Seider W D. Real-time risk analysis of safety systems [J]. *Computers and Chemical Engineering*, 2008, **32**: 827-840.

[5] Kazaras K, Kontogiannis T, Kirytopoulos K. Proactive assessment of breaches of safety constraints and causal organizational breakdowns in complex systems: A joint STAMP–VSM framework for safety assessment [J]. *Safety Science*, 2014, **62**: 233-247.

[6] Zhou J, Bai Z, Sun Z. A hybrid approach for safety assessment in high-risk hydropower-construction-project work systems [J]. *Safety Science,* 2014, **64**: 163-172.

[7] Bedny G Z, Harrisy S R. Safety and reliability analysis methods based on systemic-structural activity theory [J]. *Journal of Risk and Reliability*, 2013, **227**(5): 549-556.

[8] Popper K. Three worlds: The tanner lecture on human values [R]. Michigan, USA: The University of Michigan, 1978.