MATEC Web of Conferences **288**, 02001 (2019) https://doi.org/10.1051/matecconf/201928802001
MEAE 2019

Research on risk control method of Spacecraft AIT process based on PFTA

ZHAI Yi*, *SUN* Gang, *Li* Bin, *ZHU* Kaimin, *Wang* Qiang

Beijing Institute of Spacecraft Environment Engineering, Beijing 100094, China

Abstract. In this article, the Process Fault Tree Analysis (PFTA) method is researched, which is about to the risk management of spacecraft Assembly Integration and Test (AIT) process. The method of how to identify the top event and bottom event of Spacecraft AIT process risk and the method of how to assess the risk severity of the bottom event is introduced. The model of risk control matrix is established. From the responsibilities, tools, methods, monitor and other dimensions about the post roles involved of the AIT process, how to establish a risk management system based on the identification, assessment, analysis and control of the whole AIT process is researched. In this risk management system, through technology subject, quantitative topic, process improve, Quality Control (QC) subjects, implementation of product assurance elements, writing Standard Operating procedure (SOP), maintaining system documents, combing knowledge and operation taboo items and other method is used.

1 Introduction

The characteristics of spacecraft production mode are multispecies, small amount, multisystem, long process. As the final step of spacecraft production, AIT has many characteristics such as many operating procedures, many risk items, significant human influence factors, strict quality control requirements, etc. [1] There is still a big gap between risk management and control of AIT operation process that all kinds of problems in AIT production process in aerospace industry at home and abroad indicated. In order to reduce the development risk and improve the development quality, this paper studies the process risk management and control method based on the whole cycle, all elements, and all positions of AIT for spacecraft products.

2 The Meaning of PFTA Risk Analysis Method

2.1 Fault Tree Analysis（FTA）

Fault Tree Analysis (FTA) is a design method to improve system reliability. Through the analysis of hardware, software, environment and human factors that may cause product failure, the fault tree is drawn to determine the various possible combination modes and occurrence probability of product failure. It is a graphic deduction method. It aims at the specific fault state and carries out in-depth logical analysis, visually and intuitively describes the causality of various events within the system, so as to find out the combination of various failure events that cause system failure, and take corresponding preventive measures. [2]

The purpose of FTA is to determine the sequence of failure phenomena to be prevented according to the fault tree diagram, to understand their specific phenomena, and to take preventive measure to prevent the occurrence of undesirable phenomena according to the evaluation [3]. FTA is a commonly used analysis method for quality problems in spacecraft development.

2.2 The Meaning of PFTA

Process Fault Tree Analysis (PFTA) refers to the basic idea of FTA analysis method, takes the potential quality hazard and problems that occurred in the process of spacecraft development as the top event, combines with the process of spacecraft AIT development, further refines the risk items into bottom events, establishes the risk analysis and assessment methods of the whole process, whole cycle and all element of spacecraft AIT, and formulates specific and detailed quantitative control measure about various types of risk bottom events. Finally, the AIT risk management tool method guide is formed to achieve the AIT process risk control and prediction objectives.

3 Risk Identification Based on PFTA

* Corresponding author: xinyii_0303@163.com

https://doi.org/10.1051/matecconf/201928802001

3.1 Risk Items Identification Based on AIT Process of Spacecraft

In order to carry out AIT process risk research on spacecraft, it is necessary to indentify and analyze the risks in turn, formulate and implement strategies and measures to deal with these risks based on the risk possibility degree and its consequences, then monitor and control the implementation process and effect in an appropriate way. Finally, a management system is formed. [4] The iterative four-step risk management process of a project is illustrated in Figure 1.[5]

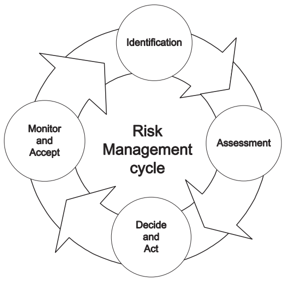


Fig.1 Iterative four-step risk management process of a project

In the process of system design, the logical block diagram, i.e. fault tree, is drawn, so as to determine the possible combination and occurrence probability of system failure, and take corresponding corrective measures, through the analysis of various factors that may cause system failure, including hardware, software, environment, human factors and so on.[6]

3.2 Establishment of PFTA Model

The spacecraft AIT process mainly includes three parts: spacecraft assembly, professional testing and environmental testing. According to the specialty, the case of quality problems occurring in nearly the past ten years are sorted out and classified according to the types of problems. The whole process of spacecraft AIT is systematically analyzed, taking the potential quality hazard and problems as the top events, and using the technical risk identification and control tools such as fault tree analysis. The risk elements are analyzed from five aspects: human, machine, material, method and environment, with the key risk items and key products as the core. The PFTA model is established by decomposing the risk items into bottom events step by step.

The potential quality hazard and problems are the top events of the PFTA model. The top events are decomposed step by step according to the three processes of assembly, professional testing and environmental testing. The quantity and proportion of potential quality hazard and problems in each field in nearly the past ten years are counted. The key risk items and key product items are indentified, and then the sub-fault tree top events are drawn.

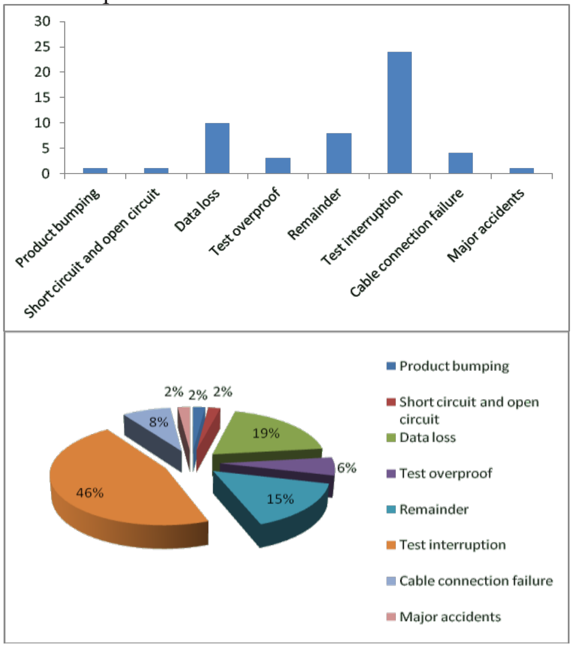


Fig.2 Key risk items statistics of sub fault tree

This method is illustrated by taking the data loss of an environmental test as an example. According to the principle of system composition and structure, the fault mode logic diagram of system failure is drawn, as shown in Figure 3. In this sub-fault tree, the data loss is the top event, sensor anomalies, test data anomalies, heat flow control data anomalies and data storage anomalies that may lead to the top event are intermediate events, eventually, 11 bottom events are formed.

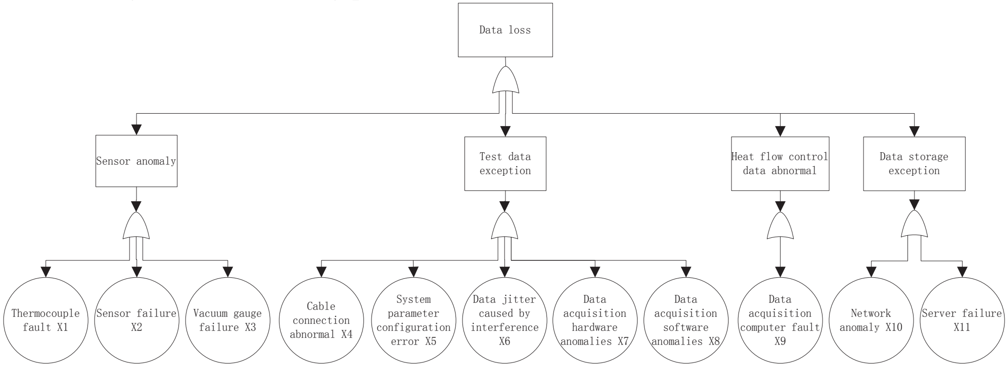

Data loss
Sensor anomaly
Test data exception
Heat flow control data abnormal
Data storage exception
Thermocouple fault X1
Sensor failure X2
Vacuum gauge failure X3
Cable connection abnormal X4
System parameter configuration error X5
Data jitter caused by interference X6
Data acquisition hardware anomalies X7
Data acquisition software anomalies X8
Data acquisition computer fault X9
Network anomaly X10
Server failure X11

Fig.3 Data loss sub-fault tree of environmental test

The structure of this sub-fault tree is relatively simple, and the 11 bottom events are independent of each other. There are 11 minimal cut sets of the sub-fault tree, which are:

G={X1},{X2},{X3},{X4},{X5},{X6},{X7},{X8},{X9},{X10},{X11}.

4 Assessment of Risk Severity

After the PFTA model is established by the above methods, risk severity assessment should be carried out in order to prepare for the subsequent targeted formulation of control measures. The severity of risk includes two factors, one is the likelihood of failure or abnormal occurrence, the other is the severity of consequences caused by the occurrence of risk. Quantitative assessment, qualitative assessment, and risk index and magnitude assessment methods are carried out, according to the actual situation of spacecraft AIT specialty and the different situation of each sub-fault tree.

4.1 Quantitative Assessment

Quantitative assessment is mainly carried out from the likelihood of failure or abnormality. The structural importance of basic cause events is usually the most direct indicator of their impact on target risk events [7].

The structure function of the fault tree is defined as:

$$\phi\ (x_1,x_2\ldots\ldots x_n)=\begin{cases}1, & \text{If the top event occurs}\\0, & \text{If the top event dose not occur}\end{cases}$$

In this functions, n is the number of bottom events in the fault tree, x_1, x_2, ⋯, x_n are the Boolean variables describing the state of the bottom event.

$$x_i=\begin{cases}1, & \text{If the bottom event i occurs}\\0, & \text{If the bottom event i dose not occur}\end{cases}\quad i=1,2,\ldots\ldots n_i$$

The probability importance of the bottom event ‘i’ is:

$$\mathrm{I}_p(i)=\frac{\partial}{\partial q_i}Q(q_1,q_2,\ldots\ldots,q_n)$$

$Q(q_1,q_2,\cdots,q_n)$ is the probability of top event occurrence. Under the condition that bottom event is independent of each other, $Q(q_1,q_2,\cdots,q_n)$ is the function of bottom event $q_1,q_2,\cdots,q_n$. The probability importance of bottom event ‘i’ is expressed as the chance rate of top event occurrence probability when the probability of bottom event ‘i’ changes slightly.

4.2 Qualitative Assessment

Qualitative assessment mainly focuses on the severity of the consequences caused by the occurrence of risks. And four-star assessment is carried out, according to the severity of the consequences of the occurrence of risks.

Table 1. List of four-star assessment

Grade	Severity	Four-star assessment	Risk Description
I	Catastrophic	★★★★	It may result in the loss or basic loss of subsystem functions of spacecraft, which will lead to mission failure or unacceptable degradation. It may cause work life severely reduced, such as design life is reduced by more than 50%. It may cause a great delay in the development progress, such as affecting the AIT progress for 15 days. It may cause casualties. It may cause heavy property losses.
II	Critical	★★★☆	It may cause a significant decline in the main functions of the subsystem, which has a significant impact on the completion of tasks. It may cause major damage or loss to major flight system components or ground devices. It may cause a major delay in the development progress, such as affecting the AIT progress for 10-15 days. It may cause major damage or loss to public or personal property. It may cause long-term harmful effects on the environment. It may cause work life considerable reduced, such as design life is reduced 25%- 50%.
III	Significant	★★☆☆	It may cause a decline in the functions of the subsystem, which has some impact on the completion of tasks. It may cause minor damage to other equipment. It may cause a delay in the development progress, such as affecting the AIT progress less than 10 days. It may cause minor damage to public or personal property. It may cause a temporary effect on the environment.
Ⅳ	Negligible	★☆☆☆	It is a secondary risk and has little impact on the completion of tasks.

4.3 Risk Index and Magnitude Assessment

Risk Index and Magnitude Assessment is multiplied by the four scores as likelihood, severity precognition and pressing to indicate the degree of risk. According to the 4-level scoring system standard, the threshold of 1-4-

level assessment standard is set, and the severity of risk is divided. [8]

Table 2. Standard List of Risk Assessment Integrated Code

Score	Likelihood	Severity	Precognition	Pressing
1	It will not happen at all.	The effect is very low, slight damage, not affecting the main function.	It is easy to be detected and has a long pre-warning time.	No process lag.
2	The probability of occurrence is very small.	The effect is low, slight damage, affect the main function，take emergency measures cannot be dealt with.	It is not easy to be detected and has a long pre-warning time.	Process lag time ≤1hour
3	The probability of occurrence is medium.	Medium impact, general failure, must be troubleshooting.	It is difficult to be detected and the pre-warning time is short.	Process lag time ≤1day
4	It happens frequently.	Significant impact, serious damage, process stop.	It is difficult to be detected and there is no pre-warning time.	Process lag time ≥1 day

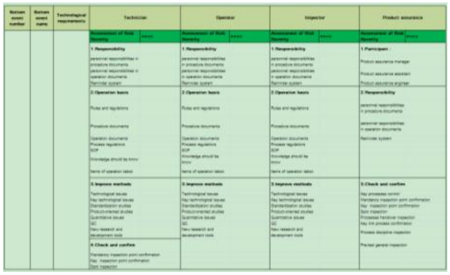
5 Risk Control Matrix Based on PFTA

Risk control is based on risk identification and assessment, and takes control measures to the identified and assessed bottom events. The goal of risk control is to establish a risk prevention control system and reduce the expected risk losses. The risk control measures mainly include risk avoidance, loss control, isolation of risk, diversification of risk, risk transfer, risk acceptance and so on. [9]

Different control measures should be taken according to different risk levels. Level I and Ⅱ risks must be monitored regularly and carefully, and various measures such as loss control, isolation of risk, diversification of risk, risk transfer should be taken jointly; Level Ⅲ risks need to be monitored regularly to ensure that they do not translate into Level I risks. Loss control, isolation of risk, diversification of risk, risk transfer can be taken to control Level I risks; Level Ⅳ risks need to be monitored regularly, and measures such as loss control, risk transfer can be taken.

Based on the risk control of PFTA, the matrix of control measures should be formulated to clarify the control methods and implementation measures for each bottom event of the sub-fault tree in the AIT development process of spacecraft.

The risk control matrix model is constructed from the two dimensions of the implementation steps of the bottom events, which involve job-related control uniforms and control activities, on the basis of risk assessment of the identified bottom events, and in view of the severity of the bottom events.



Bottom event number	Bottom event name	Technological requirements	Technician	Operator	Inspector	Product assurance
			Assessment of Risk Severity	Assessment of Risk Severity	Assessment of Risk Severity	Assessment of Risk Severity
			1 Responsibility personal responsibilities in procedure documents personal responsibilities in operation documents Reminder system	1 Responsibility personal responsibilities in procedure documents personal responsibilities in operation documents Reminder system	1 Responsibility personal responsibilities in procedure documents personal responsibilities in operation documents Reminder system	1 Participant Product assurance manager Product assurance assistant Product assurance engineer
			2 Operation basis Rules and regulations Procedure documents Operation documents Process regulations SOP Knowledge should be know Items of operation taboo	2 Operation basis Rules and regulations Procedure documents Operation documents Process regulations SOP Knowledge should be know Items of operation taboo	2 Operation basis Rules and regulations Procedure documents Operation documents Process regulations SOP Knowledge should be know Items of operation taboo	2 Responsibility personal responsibilities in procedure documents personal responsibilities in operation documents Reminder system
			3 Improve methods Technological issues Key technological issues Standardization studies Product-oriented studies Quantitative issues QC New research and development tools	3 Improve methods Technological issues Key technological issues Standardization studies Product-oriented studies Quantitative issues QC New research and development tools	3 Improve methods Technological issues Key technological issues Standardization studies Product-oriented studies Quantitative issues QC New research and development tools	3 Check and confirm Key processes control Mandatory inspection point confirmation Key inspection point confirmation Spot inspection Processes handover inspection Key link process confirmation Process discipline inspection Pre-test general inspection
			4 Check and confirm Mandatory inspection point confirmation Key inspection point confirmation Spot inspection			

Fig.4 Model of risk control matrix

The risk control matrix model based on PFTA, takes post control measures as horizontal, and takes control requirement and activities as vertical. It achieves risk control by carrying out research on process and quantitative subjects, tackling key problems in process, QC, etc. and applying the methods of implementing product assurance elements, compiling SOP, perfecting system document, combing knowledge and operation taboo items, etc, starting from various positions involved in AIT process, from the dimensions of responsibilities, tools, methods and monitor.

The risk control matrix is designed for each identified bottom event, and each control dimension of the matrix is in the form of a drop-down menu. According to the actual situation of each underlying event, one or more appropriate methods are selected to formulate measures, in the process of formulating control measures. The risk control system of the sub-fault system is constituted by combining the control matrix of each bottom event that constitutes the top event of the sub-fault tree, thus the risk control system covering the whole process of AIT is constructed.

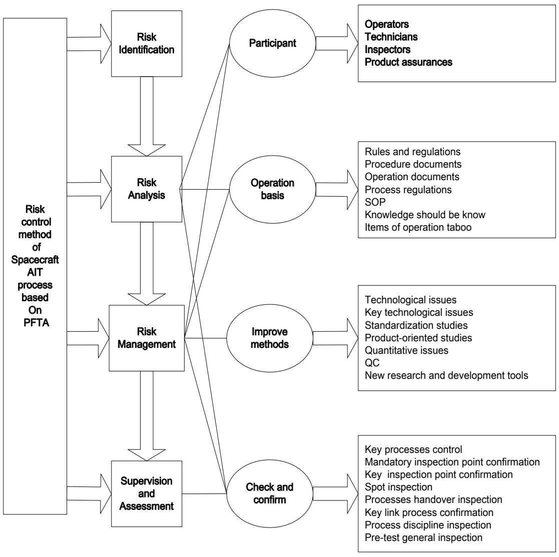


Fig.5 Relationship of risk control system

6 Monitor and Inspection

After determining the risk control measures, we should monitor and check the implementation of risk control measures, monitor the revision of system documents, the actual use of operation guidance documents, the development of improvement measure such as topics and tackling key problems, and the application in the development process. At the same time, for the confirmation items involved in the risk control matrix, the confirmation should be strictly carried out, and the quality records should be kept. To ensure that the bottom risk events are effectively controlled and the expected results are achieved, the development risk of the whole spacecraft AIT process is fundamentally reduced, and the product quality is improved.

7 Achievements Solidification

After the formulation of the risk control measures, the relevant rules and regulations, procedure documents, operation documents and process regulations should be revised to form standardized and quantified implementation requirements, the key technical issues, QC and other topics research should be completed and promoted. A communication platform should be established to promote mutual learning and sharing of achievements among different majors, so as to solidify the achievements of risk control, and improve management and technical level.

During the research of risk control method for spacecraft AIT based on PFTA, 39 sub-fault trees were drawn and 684 risk bottom events were identified, including 430 assembly risk bottom events, 42 professional testing risk bottom events and 212 environmental testing risk bottom events. And 684 risk control matrices are formulated according to the above bottom risk events. According to the risk measures formulated, 229 items of operation taboo, 99 knowledge should be know, 186 copies of SOP and 32 items of red line projects were compiled. Ten revision procedures documents, 56 operation documents, 8 new research and development tools, 4 standards at the institute level, and 7 technical and quantitative issues have been completed. The research results are compiled into a book, and the Guidelines for Risk Identification and Control of Spacecraft AIT Technology are compiled to form a set of tools and methodologies for AIT risk management and control.

8 Conclusion

In this paper, PFTA is used to study the risk control method of spacecraft AIT process. The identification methods of top and bottom risk events in spacecraft AIT process are introduced. Quantitative qualitative and assessment integrated code analysis methods are applied to analyze the risk severity of bottom events. The risk control system covering the whole process of AIT is constructed, through the establishment of risk control matrix, implementation of control measures and monitor and inspection,.

The quality problems and hidden dangers are effectively prevented and controlled, by applying the risk control method based on PFTA to the spacecraft AIT development process. In the past two years, the incidence of quality problems has been decreasing year after year, and the incidence of quality problems has decreased by 22.7%-33% compared with the same period last year, through the research and practice in the past two years. The low-level operational problems have been effectively controlled. The quality cost caused by abnormal quality has dropped dramatically, and the customer stabilized at more than 97%. This improves the business ability and management level of AIT process and ensures the successful completion of the development of high-density spacecraft AIT.

References

1. WANG Mei-zhi, Liu Yu-gang, Lv Jing-hui el al. Hazard analysis and safety process design for spacecraft general assembly [J]. Spacecraft Environment Engineering, 2014,31(5):568-570
2. XU Jin-hua, Sun De-qiang, FAN Ying el al. Accident risk probability for “Three Highs” gas field based on fault tree analysis [J]. System Engineering – Theory & Practice, 2012,32(4):877-883
3. PENG Mei-chun, ZHANG Zong-sheng. Process Quality Control Methods Based on Prevention[J]. INDUSTRIAL ENGINEERING JOURNAL, 2003 6(1):59-61
4. ECSS Secretariat. ECSS-M-ST-80C Space project management Risk management [s] The Netherlands: ESA-ESTEC Requirements & Standards Division. 2008
5. WANG Yun-hua, CHEN Li-ping. Discussion on Risk Analysis and Control for Space Technics Work

[J]. Aerospace Manufacturing Technology, 2014,(3):64-68

6. YUAN Xiao-bo, ZHANG Zhi-jie, WANG Jing-bin el al. Analysis of Failure Mode of Gun Stable Tracker Based on FTA [J]. Fire Control & Command Control, 2013,38(9):163-165
7. GB7829—87 Qualitative analysis for regular fault tree[s]．Beijing：Standards Press of China，2004
8. CUI Bao, ZHAO Ji-guang, CHEN Jing-peng el al.. Research of the Risk Analysis System of Space Launch Site [J]. Safety and Envbironmental Engineering, 2014, 21(4):152-158
9. CHENG Xiao, ZHU Yan-fang, Research on Risk Control of Aerospace Model Development [J]. Logistics Management,2011,34(11):1-4