Research on Risk Management in Weapon Equipment Identification Work

Jingjing Wang [a], Hailong Shi [b], Shanyang Liu [c], Xiaodong Jiang [d] and Zhao Li [e]

Baicheng ordnance test center of China 137001, China

[a]yayaya377@163.com, [b]robin_2003@126.com, [c]lsy19831234@163.com, [d]Xiaodong12jiang@163.com, [e]y869391235@qq.com

Abstract. According to the requirements of the military commission for the actual assessment of weapons and equipment, the identification of weapons and equipment is not only subject to the assessment of conventional projects such as reliability and safety, but also to the assessment of complex electromagnetic environment, complex geographical environment, and boundary conditions. The difficulty coefficient of the test is further increased. In addition, the unidentify weapon and equipment technology is unstable, the number of units, departments and personnel involved in the test is huge, and the risk of performance testing is further increased. It is a crucial issue How to reduce the test risk and ensure the evaluation work is completed smoothly. This paper introduces the connotation, significance and principles of risk management in weapon equipment identification work. On this basis, the whole process of risk identification, risk assessment, risk control and control effect evaluation in weapon equipment identification work is discussed, and weapon equipment is proposed. Several requirements were raised for the identification of work risk management.

Keywords: weapon equipment identification work, risk management, risk, identification, risk control.

1. The Concept and Significance of Risk Management in the Identification of Weapons and Equipment

There are many definitions of risk, and risks can be explained from different perspectives, but the usual definitions of risks cover factors such as randomness and uncertainty.With the development of society, people's awareness of risk has been further improved. People have begun to use some mathematical theories and tools (such as probability theory) to manage risks. The management of risks has gradually formed a subject, which is not only risk management.

The identification of weapons and equipment is an indispensable step in the finalization of weapons and equipment.Risk management in the identification of weapons and equipment refers to the scientific management methods for identifying, analyzing, and evaluating the risks faced during the testing and identification of weapons and equipment, and effectively disposing and controlling risks on this basis to achieve maximum security.

The risk management work in the identification of weapons and equipment has the following significant significance:

(1) It is conducive to the realization of quality objectives

(2) It is helpful to reduce the uncertain factors of evaluation decision.

(3) Ensure the safety of the test to the maximum extent.

2. Principles of Risk Management for Weapons and Equipment Identification Work

Risk management is a complex work, and, the risk management of weapon and equipment appraisal needs to meet the characteristics of weapon and equipment test and appraisal on the basis of comprehensive consideration, comprehensive system analysis, and make appropriate judgment and decision.In summary, the following principles should be followed in the risk management of the range.

(1) The principle of comprehensiveness, the risk management process should cover the whole process of the range test evaluation.

(2) the principle of adaptability, the risk management system should be compatible with the characteristics of the range test, in line with the principle of cost-effectiveness, and can be updated in a timely maimer according to changes in the internal and external environment.

(3) The principle of authority distribution, in the process of risk management, should clarify the responsibilities and authorities of each unit in each step of risk management.

(4) The principle of full communication, that is, the internal and external aspects of the risk management system should be fully exchanged and negotiated on relevant matters to avoid misjudgment and decision-making mistakes, and enhance the reality and operability of risk management decisions.

3. The Content of Weapons and Equipment Identification Work Risk Management

3.1 Risk Identification

Risk identification is the first step in risk management to identify sources of risk.Accurately identify the source of risk and manage the risk in a timely manner to reduce the probability of risk.Risk identification is generally carried out from multiple angles and in many aspects. By referring to historical data and work experience, it analyzes and summarizes the risk factors or the events that may occur.The risk identification of weapons and equipment identification work is based on the characteristics of the range test characteristics. From the receipt and release of test tasks to the release of test reports, the possible impacts on the range test progress, personnel safety, equipment integrity, etc. According to the reasons for the risk, the risks can be divided into: planned risk, management risk, technical risk, security risk and environmental risk.lt can also be divided according to the consequences of risk: personnel risk, equipment damage risk and schedule risk.In this paper, the risk of the test evaluation is divided into: planned risk, management risk, technical risk, security risk and environmental risk according to the cause of risk.

3.1.1 Test Plan Risk

The test plan risk refers to the situation where there is a flaw in the test documents such as the test implementation plan , resulting in risk of the test. The test implementation plan is the guiding documents for the test implementation, and is an important basis for the specific organization, management and execution of the test. For example, the test implementation plan does not completely cover the requirements of the test program, or the test implementation plan is beyond the scope of the test conditions, so that the test task can not achieve the expected goal. Factors such as test schedule, equipment state performance, weather and climate factors are the key factors affecting the normal operation of the test. If the advance information is insufficient or the uncertainties are not considered enough, the test may not be completed as planned. The risk of the test plan should also include the fact that the design of the test environment and the design of the test method cannot be close to the characteristics of modern warfare, resulting in the equipment, s combat performance and battlefield adaptability not meeting the actual combat conditions, which makes the national security threatened.

3.1.2 Test Management Risk

Test management risk refers to the risk arising from artificial management factors during the implementation of the test task. Management risks include both administrative risks and risks arising from the management of the test site. For example,the division of duties and powers is unclear, the test process is not organized, the testers are unreasonable, and an effective collaborative work mechanism is not established; there is no information communication between the units, or the communication is not timely or insufficient; resulting in untimely troubleshooting, delays in progress, and increased costs of participating units.

3.1.3 Test Technology Risk

Test technology risk refers to the test risk due to technical problems. For example, the technical parameters of the measurement and control equipment lag far behind the tactical technical index of

the tested product, and the test object cannot be tested; the risk brought by the accuracy of the test conclusion by using new technology, new equipment or new test method; The reliability and maintainability of the equipment are not enough to pay attention to the risks; the test data collection is incomplete, the data processing and evaluation methods are not scientific enough, the reliability of the equipment operational effectiveness evaluation results is not high.

3.1.4 Test Guarantee Risk

The test guarantee risk refers to the lack of guarantees in technical support, logistics, materials, communications, service, meteorology, network, military coordination, etc. during the test implementation, which affects the normal operation of the test tasks, and fails to achieve the expected goals.

3.2 Risk Assessment

After risk identification, the next step is to conduct a risk assessment.Risk assessment is to assess the probability of each risk occurring and the impact on the test results.The process of risk assessment is to quantify the risks that have been identified.Through the assessment, the risk level of each risk can be derived, so that different countermeasures can be taken according to different risk levels, thus providing a basis for risk control.There are two concepts : 1.risk impact,it refers to the impact of the risk on the project, which can be expressed by relative values; if the magnitude of the loss is not easy to estimate directly, the loss can be broken down into smaller parts for evaluation.2. Risk probability: It can be expressed as a percentage of the probability of occurrence of a risk, and is a subjective judgment based on certain historical data.After obtaining Risk impact and Risk probability , each risk level can be determined by the risk level matrix (see Table 1). Among them: the level of each risk probability probability is 1.0, 0.75, 0.5, 0.1 to indicate high, medium high, medium and low risk, respectively.The impact level of the risk is 100, 75, 50,10 to indicate high, medium, high, medium and low.Then, each risk is evaluated separately using this matrix to obtain different scores, and finally the level of each risk is obtained.

Table 1. Risk Level Determination Matrix

Risk impact / Risk probability	High (100)	medium high(75)	Medium(50)	Low (10)
High (1.0)	100	75	50	10
medium high(0.75)	75	56.25	37.5	7.5
Medium(0.5)	50	37.5	25	5
Low (0.1)	10	7.5	5	1

After the above methods are evaluated, we derive the risk level of the weapon equipment identification work.

Table 2. Risk I eve I of weapon equipment identification test.

Risk type	Risk level
Test plan risk	High
Test technology risk	medium high
Test management risk	Medium
Test guarantee risk	Low

After completing the above risk level determination, we can use Table 3to indicate the actions take when facing different levels of risk

Table 3. Comparison table of risk levels and measures

Risk level	Risk management requires action
high	communicate with the higher authorities and relevant departments in a timely manner to study solutions or measures to reduce risks. And record and record. If necessary, you can suspend testing and develop preventive measure.
medium high	It is necessary to communicate with the higher authorities and relevant departments in a timely manner to study solutions or measures to reduce risks. And record and record. Develop preventive measures when necessary.
Medium	It is necessary to communicate with the higher authorities and relevant departments in a timely manner to study solutions or measures to reduce risks. Supervise the implementation process of solutions and measures and make a record.
Low	Actively study solutions or measures to reduce risks. Communicate with the participants before the test and inform them of their risk items.

3.3 Risk Control

Based on the comprehensive identification and analysis of the risks faced by the system, scientific and reasonable risk control should be carried out. it includes prioritizing, evaluating, and implementing the security controls recommended during the risk assessment process. In fact, eliminating all risks is often impractical or even nearly impossible, so that with appropriate controls, the risk is reduced to an acceptable level, minimizing the negative impact on the range test. The process of risk control is actually a process of accepting, eliminating, reducing, and transferring. According to the goal of risk control, the basic idea of risk control strategy is formulated:

(1) Try to reduce the probability of a risk accident happening.

(2) Try to reduce the damage caused by a risk accident.

(3) Avoid risk strategies, especially if the probability of risk is not effectively reduced and the risk loss cannot be reduced.

Specifically, the risk control of the range test has the following strategies and methods:

3.3.1 Risk Avoidance

Avoid risks by eliminating the causes and consequences of risk. For any risk countermeasures, the first thing to consider is to avoid risks, especially for test implementation units such as weapons and equipment identification work. Avoiding risks is to avoid losses and reduce casualties. it is also an effective strategy It is also an effective strategy to voluntarily give up the project or change the project objectives to avoid risks for some risk potential threats to be too likely, the adverse consequences are too serious, and no other strategies are available. For example, for some new technologies and new methods in the range test, if it is considered that the direct use risk in the stereotype test task is large, it can be simulated in a trivial experiment or the risk can be avoided by suspending use.

3.3.2 Risk Limits.

Limiting risks by implementing safety controls that minimize the adverse effects of threats to the weaknesses of individual systems in the range test. When risk is unavoidable or when certain risks must be faced as a result of engaging in an activity, the first thing that should be thought of is how to control the time of occurrence of the risk, delay the occurrence of the risk as much as possible, reduce the occurrence of the risk, or how to reduce the risk. For example, the shooting range can be restricted by strengthening formalization and strengthening quality control. For some risks that are not avoided and limited, the risk can be limited by using other measures to compensate for the loss. For example, the technical parameters of a test equipment are not required by the tactical technical indicators of the test product, and the risk can be transferred by outsourcing this test to a qualified unit. Since the risk transfer will inevitably lead to the loss of benefits, In the appraisal of weapons and equipment, it is necessary to identify the magnitude of risks, weigh the gains and losses, and choose an appropriate way to transfer. weigh the gains and losses, and choose the appropriate way to transfer.

3.3.3 Risk Planning and Prevention

It is necessary to develop a risk mitigation plan to manage risks. In this plan, security control is prioritized, implemented and maintained. Once risks occur, effective measures can be taken immediately to minimize the risk. The core connotation of risk planning and prevention is to enhance risk prevention ability through system, culture, decision-making and organizational control.

3.3.4 Evaluation of Risk Control Effects

On the basis of completing the three stages of risk identification, risk assessment and risk control, the implementation of risk control decisions should also be checked and evaluated, and the plan should be revised and adjusted continuously. Because Whether the risk control decision conforms to the reality needs to be evaluated, discovered and corrected through practice. As the environment changes, new risk factors may arise and old risks may disappear. Therefore, the risk control effect must be evaluated regularly. The purpose of effect evaluation is to summarize the rules of risk control and strive to explore the law of risk occurrence and control to improve the scientific nature of risk control.

4. Requirements for Risk Management in Weapons and Equipment Identification Work

The risk management of the range test is still in the exploratory stage at present. In order to effectively control the risk and achieve the overall goal of risk management, in the risk management process, the following aspects should be grasped.

4.1 Enhance the Consciousness and Initiative to Control Risks

The essence of risk is uncertainty, so it takes a lot of effort to master the rules of risk accidents, and it is difficult to make up for it immediately in the event of an accident.

If it is passively controlled, it will pay a high price when it is temporarily dealt with after a risk loss has occurred. Therefore, we must take active control measures. The problem associated with this is to focus on pre-control and prevent problems before they happen. In the past, in the process of conducting tests in the shooting range, the system risk management was rarely implemented. Therefore, the first step in implementing the risk management of weapon test and equipment appraisal is to change the concept. Make the risk awareness into the mind of each employee, and regard risk management as the project. An indispensable stage in the scientificization of decision-making and project practice.

4.2 To Establish a Risk Management System and Management Organization

To prevent risks, we must establish a sound risk management system at first. The risk management thought of weapon and equipment test and appraisal should be straightened out, and the scientific decision-making procedure in line with the work of weapon and equipment test should be established to form a standard and good operating environment. Establish a specialized risk management organization, and have greater autonomy, maintain a high degree of independence, provide practical organizational assurance for risk management. At the same time standardize and strengthen the management of risks before, during and after the event, improve the overall anti-risk capability of the range test, enhancing the ability to adapt to changing and increasingly complex internal and external environments. Integrate risk management work into specific business activities, implement it in each department and individual, and implement risk management for all employees.

4.3 Handling the Relationship between Overall Control and Key Control

In the risk control process, various risk factors are complex, not only in terms of status and impact, but also in their own development. Therefore, we should focus on key links and risk accidents, and use the analysis tools such as correlation analysis and exception principle to carry out key control. Grasping the main contradictions in risk control can drive and promote the resolution of secondary

contradictions. Of course, the resolution of major contradictions is not the same as the resolution of secondary contradictions. Therefore, we should not neglect other secondary factors, but should focus on the overall situation, highlight key points, and take into account the general and coordinated.

4.4 Actions must be Timely

Risk control strategies are most important to translated into concrete actions and emphasize timeliness. Before the loss does not occur, it is necessary to take effective measures in time to eliminate or reduce the risk factors and their impacts. Once the losses occur, the consequences are unimaginable. Therefore, countermeasures should be formulated in a timely manner, information should be promptly reported, monitoring should be carried out in a timely manner, measures should be in place in time, and losses should be made up in time. Establishing a risk warning system is a necessary condition for timely control.

References

[1]. Chong Meng, Huawen Song, Research on analytical methods of total quality management of weapons and equipment. Industrial engineering and management. Vol. 17 (2012) No. 1, p. 52-57.

[2]. Yu Ma, Lei Gao:52-57, The role of six sigma in software project management. China Computer& Communication. Vol. 4 (2012) p. 42-45.

[3]. James H. Lambert. Identification, Ranking, and Management of Risks Ina Major System Acquisition. Reliability Engineering and System Safety, Vol. 72(2001) p. 315-325.

[4]. Xiaohui Li, Yurun He, Internal control and risk management China Renmin University Press 2016, p. 78-80.