



RISK MANAGEMENT IN INDUSTRIAL SECURITY IN THE FIELD OF PRODUCTION AND TRADE OF WEAPONS AND MILITARY EQUIPMENT

NENAD KOMAZEC

University of Defense Belgrade, Military Academy, nenadkomazec@yahoo.com

KATARINA JANKOVIĆ

Technical Test Center, Center for testing weapons and military equipment "Nikinci", jankovickatarina95@gmail.com

MILICA MLADENOVIĆ

S4 GloSec globalna bezbednost, Belgrade, mladenovicmilica21@yahoo.com

Abstract: *The production of weapons and military equipment represents an industrial sector that is advancing exceptionally quickly. Progress is being made in technological, personnel, and economic aspects. This rapid advancement is accompanied by technological processes, personnel selection, and results that, in many cases, exceed the real business conditions. Additionally, industrial capacities for the production of weapons and military equipment are an interesting "object" to various interested parties, in both positive and negative contexts. The risks generated in the process of producing weapons and military equipment are of a hybrid nature and can create opportunities or conditions for negative events. Industrial security recognizes the need for risk management in the production process of weapons and military equipment and materializes it through industrial security plans. Risk management in industrial security is a prerequisite for the effective prevention of events, from business disruptions to accidents with the most severe consequences. Industrial security based on risk management presupposes the production process of weapons and military equipment under conditions of acceptable risks.*

Keywords: *weapons and military equipment, risk management, industrial security.*

1. INTRODUCTION

The production and trade of weapons and military equipment represent complex and high-risk activities. These activities are classified as strategically significant for the state. Considering the importance of these activities and their profitability on a global scale, the risk of negative events with various consequences increases. States regulate the system of production and trade of weapons and military equipment through various legal solutions; however, the fact remains that these activities continue to be high-risk.

The production and trade of weapons and military equipment are monitored by intelligence services of other states as well as specific informal groups within and outside the country that engages in the production and trade of these items. An efficient system for the production and trade of weapons and military equipment involves the synchronization of numerous factors to ensure successful operation.

Technological solutions that enhance the production and trade processes of weapons and military equipment continually generate new risks. In most cases, these new risks are overshadowed by the required processes, posing a danger as they become apparent only when a problem arises.

2. PRODUCTION AND TRADE OF WEAPONS AND MILITARY EQUIPMENT

Considering its strategic significance for the state, the production and trade of weapons and military equipment are regulated by special laws. The legal framework for this area in the Republic of Serbia encompasses: research and development of weapons and military equipment; development and adoption of defense technologies; manufacturing, testing, overhaul, and upgrading of weapons and military equipment; demilitarization and disposal of weapons and military equipment; construction and equipping of capacities for the production of weapons and military equipment; and the creation of technical documentation [8].

The trade of weapons and military equipment within the country involves the conditions for purchasing and selling weapons and military equipment domestically, purchasing for the purpose of selling both domestically and internationally, and activities related to such purchasing and selling [8]. Thus, the overall portfolio of legal, technical, material, and spatial conditions for the sale and purchase of weapons and military equipment is defined.

As production is the process of converting raw materials or semi-finished products into finished products, namely

weapons and military equipment, it is concluded that this is a complex process involving numerous factors.

By definition, and according to legal provisions, weapons and military equipment are considered hazardous materials or products in terms of research, production, storage, maintenance, safeguarding, and use.

3. INDUSTRIAL SECURITY

Security, as a business function, attains high utility value in the activities of production and trade of weapons and military equipment. The need for high protection of data on processes and products, hazardous materials, and products that may be of interest to various informal groups, such as terrorist groups, makes security a priority among business functions.

Most legal frameworks define industrial security in the area of weapons and military equipment production as a system of security-protection measures and procedures that meet organizational and technical requirements for safeguarding technical documentation for the production of weapons and military equipment and other classified information. These measures also prevent the destruction or damage of production capacities, endangerment of human resources, destruction, damage, or theft of weapons and military equipment, and the disclosure of classified information about their production.

This approach, without delving into other aspects, indicates that industrial security in this area is complex and dependent on various factors. When viewed in this way, industrial security is essentially corporate security and includes all its elements. The foundation of the strategy and implementation of industrial security requirements is the industrial security plan. This plan regulates specific measures and approaches for all participants in the production and trade of weapons and military equipment.

The industrial security plan for the production of weapons and military equipment includes [8]:

1. An assessment of the vulnerability of production capacities to various external influences;
2. Security and protection measures for weapons and military equipment, production capacities, and technical documentation, and the methods of their implementation;
3. Measures and procedures to be undertaken in case of a breach of industrial security.

The basis of the industrial security plan is a variety of documents regulated by specific laws (Law on Occupational Safety and Health, Law on Fire Protection, Law on Disaster Risk Reduction and Emergency Management, Law on Environmental Protection, Law on Private Security, etc.). The essence of the industrial security plan is to define measures that ensure the safe process of production and trade of weapons and military equipment.

The core of the security philosophy is the concept of danger. Any phenomenon or interaction in the

environment that can generate a disturbance relative to the desired state of the system constitutes a danger. Lesser danger implies greater security, and vice versa. The essence is to act on the elements that constitute phenomena in the environment and thus mitigate their negative effects.

An effective way to influence system security is through risk management. Given that industrial security in the production and trade of weapons and military equipment possesses all the prerogatives of corporate security, it is possible to apply methods used in corporate security systems to manage risks.

4. RISK MANAGEMENT

Risk management is a complex process of identifying and assessing risks. In the area of production and trade of weapons and military equipment, risk management plays a key role in maintaining the desired level of security and control over risks. Effective risk management requires educated risk managers and resources dedicated to risk treatment. Integrating security areas enables the simplification of the risk management process.

Integrated risk management (Figure 1) allows for an overview of all factors affecting the security of protected values in the industrial security area of weapons and military equipment production and trade. It identifies potential hazards, determines the risk level for each hazard, and proposes the most efficient way to treat risks [5]. The risk assessment process (Figure 3) consists of the following phases:

1. Determining the context of risk management
2. Risk assessment
 - a. Risk identification
 - b. Risk analysis
 - c. Risk evaluation
 - d. Risk treatment
5. Monitoring and review
6. Consultation and communication:

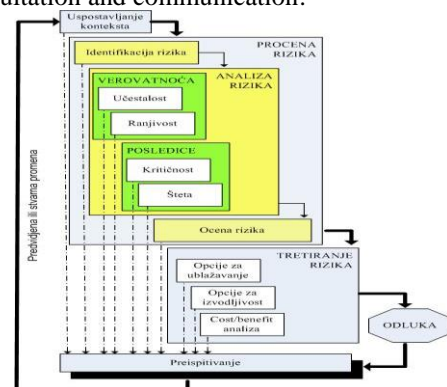


Figure 1: Risk Assessment Process According to SRPS A.L2.003 - Security and Resilience of Society - Risk Assessment

The risk management process is standardized and provides guidelines for handling the risk management process. Organizations are given the flexibility to adapt risk assessment to their needs in a real environment. In

practice, the templating of risk assessment is prevalent, leading to the creation of invisible risks.

Determining the Context of Risk Assessment

The context of risk assessment must be defined concerning external and internal factors. It needs to be set in relation to the organization's policy, culture, processes, and structure. Defining the context of risk assessment establishes the framework, scope, and criteria for the overall process [6]. In the area of protecting people, property, and operations, the main challenge is to ensure a comprehensive view of all factors that may pose potential threats to protected values.

Risk Assessment

Risk assessment is a comprehensive process of identifying, analyzing, and evaluating risks. It is the central process of risk management, in which a thorough examination and analysis of risks concerning identified hazards are conducted.

Risk Identification

The organization should ensure conditions for identifying potential hazards, i.e., sources of risk, events, or a series of circumstances, as well as their potential consequences. The primary goal of identification is to compile a realistic and comprehensive list of potential hazards based on those events and circumstances that may facilitate, hinder, or slow down the achievement of the organization's objectives. Any potential hazard not identified at this stage falls out of further analysis and remains a constant and hidden threat.

Risk Analysis

Risk analysis involves understanding the fundamental characteristics of risks [5]. It provides input information for risk evaluation and decisions on whether risks should be addressed and what the appropriate (most acceptable) strategies for risk treatment are. For a complete risk analysis, it is necessary to determine the likelihood of the potential hazard occurring and the consequences it may cause.

Likelihood is determined by the frequency of occurrence (exposure time) and the system's vulnerability, i.e., the existing level of protection, and is categorized as: impossible, unlikely, likely, almost certain, and certain.

Consequences are determined by the extent of possible damage and the system's criticality, i.e., the importance of individual protected values for the system, and are categorized as: minimal, minor, moderate, serious, and catastrophic. The level of risk is determined by the relationship between likelihood and consequences (Table

1)

Table 1: Risk matrix

Consequences \ Likelihood	Consequences				
	Minimal	Minor	Moderate	Serious	Catastrophic
Rare	1	2	3	4	5
Unlikely	2	4	6	8	10
Moderately Likely	3	6	9	12	15
Likely	4	8	12	16	20
Almost Certain	5	10	15	20	25

Risk is determined at the following levels: very low (negligible), low, moderately high, high, extremely high. Based on the risk level, risks can be classified into the following categories: first-very low, second-low, third-moderately high, fourth-high, and fifth-extremely high. By determining the risk level and category, the acceptability is assessed: risks in the first and second categories are considered acceptable, while those in the third, fourth, and fifth categories are deemed unacceptable.

Risk evaluation

The goal of risk evaluation is to assist in decision-making based on the results of risk analysis, and to determine which risks should be addressed and the priorities for risk treatment. Risk evaluation involves comparing the levels of risk identified during the analysis process with the risk criteria established while considering the entire context. The organization's objectives and the scope of potential circumstances should also be considered. In situations where choices need to be made between options, the decision will depend on the organization's context. Decisions should consider the broader risk context and include considerations of risk tolerance found by other organizations that the organization can benefit from. Decisions should also take legal constraints into account. If the risk level does not meet the criteria, that risk should be addressed (risk should be treated). Priority should be given to risks with the highest level.

Risk treatment

Risk treatment involves selecting one or more options to eliminate, reduce, or mitigate risks and implementing those options [6]. Risk treatment options do not necessarily exclude each other and may not be applicable in all circumstances. If resources for risk treatment are limited, the risk treatment plan should clearly identify the order of priority for applying individual risk treatment options. The full cost of taking and/or not taking action should be compared with budget savings. After risk treatment, decision-makers and stakeholders must be cautious about the nature and extent of the residual risk.

Residual risk should be documented and subject to control and review, and where appropriate, further treatment in line with new circumstances [2]. Risk treatment can be carried out by applying:

1. Risk mitigation options;
2. Feasibility options; and/or
3. Cost-benefit analysis.

Risk Mitigation Options [6] include the following:

1. Avoiding the risk by not starting or continuing the activity that would lead to the risk;
2. Seeking opportunities by starting or continuing the activity that may lead to or sustain the risk;
3. Influencing the likelihood;
4. Influencing the consequences;
5. Sharing the risk with one or more other parties; and
6. Retaining the risk, either by conscious choice or unconsciously.

Feasibility options

Each risk treatment option should be considered in stages of risk assessment. The analysis of each option must consider the cost of changing procedures or products (services) in accordance with risk treatment measures. Feasibility analysis should be conducted by competent financial bodies, and the results should be provided to the decision-maker.

Cost-Benefit Analysis

Cost-benefit analysis is the final step in conducting risk assessment concerning the undertaken risk treatment strategies. It is necessary to determine the actual cost of implementing the proposed risk treatment options and assess the financial and other costs resulting from the implementation of the proposed measures. The analysis should be conducted by competent financial bodies, and the results should be provided to the decision-maker.

Control and review

Control and review are integral parts of the risk management process [2]. Control and review should enable:

1. Adequate use of analysis results and lessons from analyzed disturbances or successes;
2. Detection of changes in the external and internal context, including changes in the risk itself, which may require reassessment of risk treatment options and priorities; and
3. Verification of whether risk control and treatment measures are effective in plans and implementation.

Actual progress in implementing risk treatment plans shows the achievement measure and can be integrated into the organization's operational management, measurement, and internal and external reporting activities. Control and review can include regular checks or controls of what is already present; it can be periodic or sudden, depending on management's assessment. Both aspects should be planned. It is not enough to rely only on occasional audits and controls.

Continuous improvement of the risk management process

Planning and implementing risk management should be one of the key competencies of every organization and its employees in the function of protecting protected values. Risk management methods and tools help each organization plan and implement specific actions and programs to raise their capabilities to the highest level and control threats [7]. Risk assessment can be applied partially or to the entire organization's operations. Horizontal integration is possible by applying specific risk management systems. All organizations should strive for the highest performance of their risk management framework relative to the importance of the decisions to be made. Continuous monitoring of activities and the state of internal and external factors, as well as the state and operations of the organization itself, is necessary. All employees and stakeholders should be involved in the risk management process. Based on control and review, decisions and conclusions should be made in the organization on how to improve the risk management framework, plan, and policy [7]. Such decisions should lead to improvements in the organization's risk management. This contributes to better management, flexibility, and accountability of the organization that applies the protection of people, property, and operations in any way.

5. CONCLUSION

Industrial security is a high-risk area of economic activity that requires a comprehensive approach to monitoring, identifying, and mitigating threats to protected values in the production and trade of weapons and military equipment. Neglecting any segment of impact on hazards in the environment itself poses a danger. A pragmatic method of influencing hazards and monitoring in conditions of uncertainty is risk assessment and management. The practical applicability of risk management methods allows the production and trade of weapons and military equipment to raise the level of security of their own capacities.

In the future, the number of risks in this area will increase. Some of the reasons are: the technologization of processes, which assumes less attention to the safety of technological systems; greater danger due to the application of various new technologies in the production of weapons and military equipment; an increasing number of interested parties in the environment; the need for

higher production, which implies less implementation of measures to maintain security, etc.

Today, risk management is not practiced, which is a precondition for the occurrence of negative events. Fulfilling legal obligations is of a template nature and aims to meet the minimum legal requirements. In terms of meeting legal requirements, this makes sense because there is no threat from inspections. In terms of the effectiveness of the security system, it does not make sense, as risks are generated in the own environment, and the question is not if they will happen, but when.

References

[1] Standard SRPS ISO 9001 - Sistemi menadžmenta kvalitetom – Osnove i rečnik

[2] Standard SRPS A.L2.001 – Društvena bezbednost – Privatno obezbeđenje - Rečnik

[3] Standard SRPS A.L2.002 - Društvena bezbednost – Privatno obezbeđenje - Zahtevi i uputstvo za ocenjivanje usaglašenosti

[4] Keković.Z., Komazec.N., Glišić.G.: Pristup metodologiji procene rizika, Žurnal za kriminalistiku i pravo, Beograd, 2009

[5] ISO TC 223/SC: Upravljanje rizicima - Uputstvo o principima i implementaciji upravljanja rizicima

[6] ASIS INTERNATIONAL: General security risk assessment guideline

[7] Drennan, L., McConnell, A, Risk and Crisis Management in the Public Sector, Routledge,

[8] Zakon o proizvodnji prometu naoružanja i vojne opreme (Sl Glasnik RS 36/2018)