

Anti-tampering Process for the Protection of Weapon Systems Technology in Korea

Ara Hur[1(✉)], Yeonseung Ryu[1], and Hyun Kyoo Park[2]

[1] Department of Security Management Engineering, Myongji University, Yongin, Gyeonggi-do, Korea
ara7494@gmail.com, ysryu@mju.ac.kr
[2] Defense Computing Information Agency, Seoul, Korea

Abstract. Korea's arms exports reached $17 billion in 2022, ranking fifth in the world. Further, Korea's defense science and technology level was ranked ninth in the world in 2020. Recently, cyberattacks targeting advanced weapon systems are on the rise, so the need to protect the technologies of defense companies while protecting the technologies of weapon systems for export is growing. In Korea, the Defense Industry Technology Protection Act, enacted in 2015, compels defense companies to build a defense technology protection system. However, the focus is only on the defense industry's technology protection system, and there is no system for protecting the weapon system technology, which is being exported, and the related research is insignificant. In this paper, we studied a weapon system anti-tampering process that can be applied to the weapon systems R&D procedure as a way to protect the defense critical technology of the weapon systems. The proposed method linked the anti-tampering process to the technical review meeting for each stage of systems engineering procedure. Also we defined the anti-tampering security level so that the target level to be implemented, and the process of determining the anti-tampering technology based on the identification of the defense critical technology and the risk assessment, and also the identification procedure for applicable anti-tampering technologies.

Keywords: Weapon Systems · Anti-tampering · System Engineering · Defense Technology Protection · Reverse-engineering

1 Introduction

Korea is independently developing advanced weapon systems and is considered the world's ninth-largest country with defense science and technology. North Korea and other hostile countries, which are directly confronting each other, are attempting to seize South Korea's defense technology, while exports of weapons systems are also increasing significantly, raising the risk of technology leakage through importing countries. In the event of an outflow to hostile countries, our weapons system may be neutralized, and if our defense technology is used by export competitors, it will be severely damaged by economic losses invested in development as well as weakened export competitiveness.

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2023
O. Gervasi et al. (Eds.): ICCSA 2023 Workshops, LNCS 14106, pp. 163–174, 2023.
https://doi.org/10.1007/978-3-031-37111-0_12

Developed countries of national defense systematically establish protection systems for personnel, facilities, and information to protect their own researchers and technical data, and operate anti-tampering systems to prevent technology leakage of weapons systems [3]. Anti-tampering is an engineering activity to protect the technology of the weapon systems, and is to prevent leakage of technology by blocking or delaying unauthorized access to important technologies implemented in the weapon systems.

The U.S. initiated an anti-tampering system to prevent leakage of secrets and technology of weapons systems after the incident in 2001 in which China seized EP-3 of its own reconnaissance plane that landed on Hainan Island, and leaked confidential information through reverse engineering [5]. The United States is evaluating risks by reviewing vulnerabilities, threats, etc. step by step at the entire life cycle of acquiring weapons systems, and performing system engineering procedures for anti-tampering applications [4]. In addition, there is an agency dedicated to anti-tampering, and research and development of related technologies are protected in secret.

In Korea, as exports of high-tech weapons systems have recently increased and the need to protect weapon systems technology has grown, the Defense Acquisition Program Administration will first mandate the application of anti-tampering to export weapons systems. However, there are no anti-tampering guidelines yet to be applied to the acquisition of weapons systems and R&D procedures, and research in related fields is insignificant [7, 8].

In this study, we propose a process for applying anti-tampering technology to the Korea's weapon system research and development procedure. The proposed method linked the anti-tampering process to the technical review meeting for each stage of systems engineering procedure. Also we defined the anti-tampering security level so that the target level to be implemented, and the process of determining the anti-tampering technology based on the identification of the defense critical technology and the risk assessment, and also the identification procedure for applicable anti-tampering technologies.

This paper is organized as follows. Section 2 briefly introduces procedure of weapon systems research and development in Korea. Section 3 proposes Korea's anti-tampering process and Sect. 4 describes the conclusions of the paper and policy suggestions.

2 R&D Procedure for Weapon Systems in Korea

The research and development procedure for weapon systems in Korea consists of prior reserach, exploratory development, system development, and mass production. This R&D procedure conduct technical review meetings at each major stage by system engineering methdology. System engineering is a methodology that develops a system economically and balanced to meet user requirements in consideration of the life cycle perspective in all stages from user requirements to requirement analysis, design and production, verification, verification, operation, and disposal [1]. The technical review meeting is a meeting to review the completeness by comparing and analyzing the current development progress according to the requirement analysis according to the step-by-step set-up criteria at the time of official technology review [2].

Figure 1 shows the weapon system research and Development process and technical review meetings in Korea. The system engineering-based technical review meetings

consist of system requirements review (SRR), system functional review (SFR), preliminary design review (PDR), critical design review (CDR), test readiness review (TRR), functional configuration audit (FCA), and physical configuration audit (PCA).

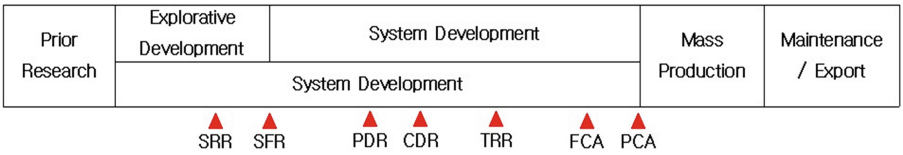

Fig. 1. Weapon Systems R&D Process and Technical Review Meetings [1]

During technical review, a baseline is set, and a baseline means a document, specification, or product baseline reviewed and agreed for shape management by development stage, and is divided into functional baseline, allocated baseline, and product baseline.

The functional baseline is a document that defines the performance, function, interoperability, and characteristics of the system/subsystem, including system specifications reflecting SFR results. The allocation baseline is a document that defines the characteristics of the development specification for the design of each feature item, such as a system/subsystem and interface reflecting the PDR results. The product baseline is a document defining the functional physical properties of a product completed as a system reflecting PCA results in the draft product specifications for prototype production reflecting CDR results [9, 10].

System Requirements Review (SRR) is performed at a time when an understanding of user requirements is completed and the results of developing major technologies and components verified through exploration and development can be reflected as weapon system requirements. Through SSR activities, all requirements included in user requirements, such as operating requirements (ORD), operational performance (ROC), and proposal requirements (RFP), should be properly converted to system/subsystem requirements, consistent and traceable by requirement.

System Functional Review (SFR) is a procedure for establishing a functional baseline for the system by ensuring that user requirements and system requirements are consistently and accurately reflected in the system standard. This procedure should be carried out before performing the initial basic design and can be performed simultaneously with SRR depending on business characteristics, but in this case, user requirements should be defined in detail and accurately as system function requirements.

Preliminary Design Review (PDR) is conducted when it is necessary to determine the completeness of the basic design and whether the Integrated Project Team (IPT) is ready to begin detailed design and testing procedures after the basic design of hardware and software products is completed.

Critical Design Review (CDR) is conducted when detailed design is completed up to detailed components/parts of the system, performance prediction is performed through M&S, and then it is necessary to determine whether prototype is ready to start.

Test Readiness Review (TRR) is a procedure to officially confirm that a test plan containing test purposes, methods, procedures, scope, manpower resources, and safety

considerations can enter the Development Test / Opeational Test (DT/OT) stage by verifying and verifying satisfaction with user requirements and system requirements.

Functional Configuration Audit (FCA) is a procedure for confirming whether the actual performance of a tangible product meets the requirements specified in the functional baseline and the allocation baseline. Physical Configuration Audit (PCA) is a procedure for determining whether the shape of the verified model matches the design document and confirming the product baseline [11–17].

3 Proposed Anti-tampering Process

3.1 Overview

The anti-tampering process is a series of activities conducted according to system engineering procedures through weapon system acquisition lifecycles, and is a risk management process for identifying, evaluating, and reviewing and implementing anti-tampering techniques.

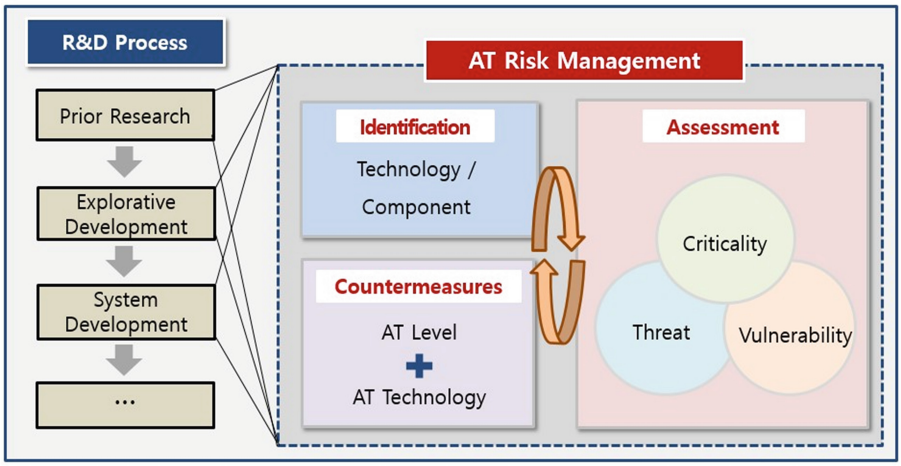

Fig. 2. Anti-Tampering Risk Management Model

Figure 2 schematically shows a proposed risk management model for anti-tampering of weapon systems. Proposed risk management should be repeatedly performed at each stage of prior research, exploration development, and system development in the acquisition life cycle. Risk management activities consist of identification of critical technologies and related components to be protected, risk assessment to analyze importance, threats, vulnerability, and review and implementation of protective measures to mitigate risk levels.

Figure 3 shows a simple schematic diagram of the entire anti-tampering process based on system engineering applied to the weapon system acquisition procedure.

The anti-tampering application process is also carried out in connection with the weapon system R&D process. The Integrated Project Team (IPT) is a control agency for

defense technology protection and must be managed from the beginning of the project. The need for protection requirement is identified from the prior research stage, and the anti-tampering protection requirements (target/grade) are clearly defined with the support of the security verification agency and provided to the R&D authority.

Based on the definition of anti-tampering requirements provided by the IPT, the R&D authority prepares the anti-tampering requirements in the anti-tampering plan (AT Plan) and reports/approves them in the Anti-Tampering Specification Review (ATSR).

For the application of anti-tampering procedures in the ATSR stage, the protection requirements (target/grade) are defined to identify the protection targets (technology/parts), update the protection level at the life cycle stage, reflect it in the AT Plan, and update the main products. After that, anti-tampering is developed and implemented, integrated into the system, and then the mass production system is integrated through a standardization process.

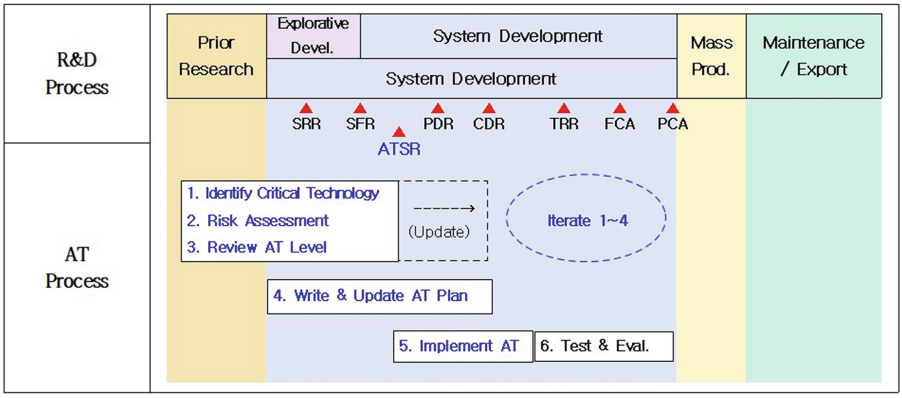

Fig. 3. Overview of anti-tampering process based on systematic engineering

In the system engineering procedures performed between weapon system R&D, the anti-tampering development procedures are system requirements review (SRR), system function review (SFR), AT requirement review (ATSR), basic design review (PDR), detailed design review (CDR), test readiness review (TRR), physical shape verification (FCA).

Among the R&D processes for each anti-tampering development stage, first, the anti-tampering requirements are analyzed in the System Requirement Review (SRR) stage. Identify the requirements for anti-tampering and devise the protection target and protection level. In the SRR phase, anti-tampering requirements are identified and an anti-tampering plan (draft) is conceived based on the anti-tampering requirements and anti-tampering requirements definitions for system performance.

In the step of Systematic Function Review (SFR), the protection targets for anti-tampering requirements are identified and the level of protection is reviewed. In the SFR stage, the anti-tampering requirements included in the system development requirement are prepared through the system function criteria, and the anti-tampering plan (draft) is

updated by reviewing the level of protection such as anti-tampering techniques based on the anti-tampering protection requirements.

The anti-tampering requirement review (ATSR) stage is proposed in this study, and based on the requirements of the anti-tampering protection level, such as anti-tampering techniques, testability, cost, and performance maintenance, etc. ATSR can be performed in combination with SFR or separately. The reason for performing ATSR separately was that it was proposed to hold an anti-tampering requirement review separately from the existing review meeting in consideration of the confidentiality of the anti-tampering design. In addition, this is because the definition of the requirements of the weapon system software can be performed separately between the system function review (SFR) and the basic design review (PDR). Anti-tampering protection consists of hardware and software and is primarily targeted at software, and software requirement analysis can be performed in the Software Specification Review (SSR) after SFR. Therefore, when defining software requirements, ATSR is performed to define and review anti-tampering requirements for software targets.

In the basic design review (PDR) stage, the HW/SW basic design for anti-tampering is reviewed. The effect on the update of anti-tampering requirements, anti-tampering design description (draft), and basic design is reviewed.

In the detailed design review (CDR) step, detailed design of H/W and S/W for anti-tampering is reviewed. Complete the final of the anti-tampering requirements, anti-tampering design techniques, anti-tampering implementation costs and problems, anti-tampering implementation activities, and AT Plan.

In the Test Preparation Status Review (TRR) stage, the test evaluation plan and preparation status are reviewed by verifying whether the anti-tampering requirements are met. In this step, the anti-tampering evaluation is planned and executed.

In the functional shape confirmation (FCA) and physical shape confirmation (PCA), the anti-tampering evaluation is supplemented and standardized by comparing the function of the shape item with the function/allocation (product) baseline.

3.2 Definition of Anti-tampering Requirements

3.2.1 Concepts and Procedures

The IPT should start activities to protect defense technology from the project preparation stage and manage anti-tampering requirements. To this end, from the stage of prior research, candidates for defense critical technology should be identified and risk assessment should be performed to define anti-tampering requirements. This definition of requirements is carried out with the support of a security verification agency (meaning a specialized institution in charge of anti-tampering of weapons systems).

The business management agency prepares the AT Requirement Definition with the support of the security verification agency. The AT requirement definition specifies defense technology candidates and AT level and is provided to R&D institutions of the project.

3.2.2 AT Level and Security Controls

When preparing an anti-tampering requirement definition, the business management agency performs a preliminary risk assessment and determines a preliminary anti-tampering level. The final anti-tampering level is determined when R&D institutions hold an anti-tampering requirement review meeting (ATSR). The anti-tampering level is repeatedly evaluated during the acquisition life cycle in consideration of the importance of the protected technology, the possibility and vulnerability of threats, and the project schedule/budget.

The anti-tampering (AT) level is consists of three levels as follows:

- A-level: Best protection
- B-level: Appropriate level of protection
- C-level: Minimum level of protection that must be applied

The anti-tampering requirements to be applied to the weapon systems consist of seven domains and security controls for each domain.

- Physical Security (PS)
- Component Security (CS)
- Cryptograph Management (CM)
- Side-channel attack Countermeasures (SC)
- Log management (LM)
- Integrity Assurance (IA)
- Account Management (AC)

Table 1 shows an overview of the anti-tampering level and requirements for each level. Required and selectively applied items are defined for each level, which means that they are recommended to be applied, but can be applied selectively in consideration of the schedule and cost of the project.

Table 1. AT requirement level and security controls

Level	Meaning	the number of security controls							
		PS	CS	CM	SC	LM	IA	AC	Total
A	Best	13	37	6	4	4	5	7	76
B	Appropriate	10	13	5	1	1	5	5	40
C	Minimum	7	-	1	-	-	-	-	8

Table 2 shows the security controls of Physical Security (PS) domain. There are thirteen security controls in PS domain. Security controls to be implemented for each AT level are defined. In the table, black circles are madatory security controls, white circles are optional, and dash is exampt for the level.

If the level A is required, eleven controls shall be implemented and two controls can be selectively implemented according to the cost and schedule of the project. However, if the level C is required, only seven out of thirteen security controls need to be implemented.

Table 2. Example: Security Controls of Physical Security (PS) Domain

Security Controls			Level		
Domain	ID	Description	A	B	C
Physical Security (PS)	PS-1	The system shall be protected with a rigid housing	●	●	●
	PS-2(1)	A pick-proof lock shall be installed on the cover or door of the cover	●	●	●
	PS-2(2)	Tamper-evidence functions, such as tampers' seals and coatings, shall be used for covers or doors of covers	●	●	●
	PS-3	A real-time detection method shall be provided when the cover or door of the unauthorized person's cover is opened. (e.g., mechanical sensors, illumination sensors, etc.)	●	●	–
	PS-4(1)	A role-based authentication method for opening the cover shall be provided. (e.g., controlling access by role by administrator, maintenance, etc.)	●	●	●
	PS-4(2)	Identity-based authentication method shall be provided for opening the cover. (e.g.,: passwords, biometric information, etc.)	●	●	●
	PS-4(3)	Multiple authentication methods shall be provided for opening the cover	○	–	–
	PS-4(4)	The authentication information for opening the cover shall be protected	●	●	●
	PS-4(5)	Authentication using the encryption module shall be provided	●	–	–
	PS-5	Physical access to external communication lines of the system shall be prevented. (prevention of eavesdropping, alteration, etc.)	●	○	–
	PS-6	Protection against electromagnetic pulse (EMP) attacks shall be provided	○	–	–
	PS-7	The tamper detection function shall be turned off when the lid of the accreditor is opened	●	●	–
	PS-8	Sensitive information (e.g., SW code, encryption key, etc.) on the system shall be erased when detecting unauthorized opening of the cover	●	●	●
	Count		13	10	7

3.3 Risk Assessment

Risk assessment analyzes the criticality, vulnerability, and threat of the protected object, and calculates the likelihood and severity of the outcome of the threat through the vulnerability.

The target of protection is defense technology and related components, and the importance of protection is evaluated by the level of mission failure in the event of technology infringement and the level of damage to national security. Vulnerability is evaluated as the severity of design weaknesses that components related to defense critical technology can be used by enemy threats (i.e., tampering attacks). Threats evaluate the likelihood of an enemy threat occurring and the likelihood of an enemy threat succeeding.

If the calculated risk level is high, protective measures to mitigate the risk should be established and implemented. In this study, protection measures were specified as AT level and requirements for each level so that R&D institutions could easily identify protection measures (Fig. 4).

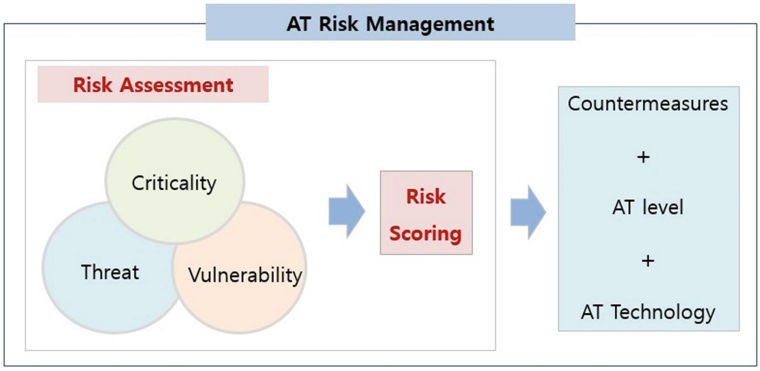

Fig. 4. AT Risk Assessment and Risk Management

Risk management starts from the prior research stage, which is the early stage of the R&D life cycle, and is updated by repeatedly identifying defense technology and implementing protection measures. The procedure for risk assessment performed by R&D institutions after the commencement of the project.

Risk evaluation is evaluated by scoring the risk level by synthesizing the results of importance analysis, vulnerability analysis, and threat analysis for defense technology and related components.

The importance analysis is analyzed by R&D agencies. Vulnerability analysis of related components is analyzed by a third professional security verification agency and also verifies that the vulnerability has been resolved when anti-tampering is applied later. Threat analysis of related components suggests a method of requesting an intelligence agency because it is necessary to analyze overseas threat information. The United States requests threat analysis to the Defense Intelligence Agency (DIA) to receive a threat analysis report. Since Korea does not have this role of intelligence agencies yet, there is a way to evaluate the threat level as high for the time being.

3.4 Determination of Anti-tampering

When the level of risk is determined to be "high (H)" for the identified defense critical technology, protection measures to lower the level of risk should be selected and implemented. In this study, anti-tampering is targeted as a protection measure. Figure 5 shows the procedure for selecting an anti-tampering technique.

The anti-tampering level required in the anti-tampering requirement definition is determined at the Anti-Tampering Requirement Review Meeting (ATSR). Anti-tampering technology that satisfies the requirements of the confirmed anti-tampering level should be designed and implemented. Mandatory requirements must be applied, and optional requirements are reviewed in consideration of costs, schedules, etc.

For the implementation of each anti-tampering requirements, the best technology should be selected by identifying anti-tampering technologies capable of various anti-tampering technologies and compromising analysis of cost, schedule, and system performance.

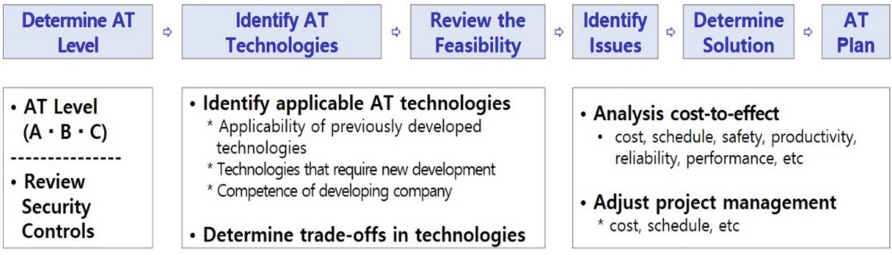

Fig. 5. Procedures for Selecting Anti-tampering Technology

The AT level and the respective security controls are reviewed. AT technology is selected by analyzing each technology by identifying applicable AT technology for each requirement and reviewing whether the applicable technology is negotiable.

4 Conclusion

This study proposed an anti-tampering process for weapons systems that can be applied to Korean defense R&D procedures. The proposed anti-tampering process is carried out in accordance with system engineering procedures, defining the work procedures and activities to be carried out at each technical review meeting, and defining the output. Major proposed anti-tampering activities include defining anti-tampering requirements, identifying defense critical technologies to be protected, risk assessment, and selection of anti-tampering techniques.

In the absence of anti-tampering systems and guidelines to be applied to weapons system R&D procedures in Korea, we propose policies for the development of the anti-tampering system as follows.

First, it is necessary to systematically establish a system through the designation or establishment of an agency dedicated to anti-tampering and support the development

of anti-tampering by defense companies. The U.S. has a dedicated agency under the Defense Ministry to support anti-tampering of defense companies. In addition, intelligence agencies such as the Defense Intelligence Agency (DIA) also analyze threat information about weapon system technology to support the decision to apply anti-tampering [16].

Second, the anti-tampering guidelines for weapons systems should be developed under the Defense Acquisition Program Administration Directive or regulations and provided to defense companies and defense science research institutes. Currently, the defense technology protection guidelines focus on protecting R&D data of defense companies [6], and there is no content for anti-tampering, so guidelines to be applied in weapons system R&D are urgently needed.

Third, it is necessary to establish a system in which defense companies and defense science research institutes build and share defense technology information as a database for consistent identification of defense technology. Anti-tampering is to protect the defense technology of weapons systems, and basically, consistent identification of defense technology should be preceded. However, it is currently difficult to apply consistent anti-tampering techniques due to different identification criteria for each defense company, so standard identification should be supported by sharing defense technology information.

The limitation of this study is that it was not applied to the actual weapons system development project and theoretical research was conducted. Therefore, it is necessary to establish a process by analyzing and researching in-depth anti-tampering process application cases or data not covered in this paper, and to apply them to actual weapons system R&D projects.

Acknowledgements. This research was supported by a research project awarded by Electronics and Telecommunications Research Institute.

References

1. Korea Defense Acquisition Program Administration: Systems Engineering Technical Review Guidebook (2017)
2. Korea Defense Acquisition Program Administration: Weapon Systems Software Development and Management Manual (Amendment Feb, 2020)
3. Huber, A.F., et al.: The Role and Nature of Anti-tamper Techniques in US Defense Acquisition. Acquisition Review Quarterly (1999)
4. USAF: Weapon System Program Protection / System Security Engineering Guidebook. Version 2.0 (2020)
5. MDA Directive 5200.05, Anti-Tamper Policy (2006)
6. Korea Defense Acquisition Program Administration: Defense Industry Technology Protection Guidelines (2020)
7. Min-Woo, L.: Risk management-based application of anti-tampering methods in weapon systems development. J. Korea Academia-Industrial Cooperation Soc. **19**(12), 99–100 (2018)
8. Min-Woo, L.: Development of life-cycle process model for technology protection of national defense systems. Ph.D Thesis, Department of Systems Engineering. Ajou University, Suwon, Korea (2019)

9. DoDD 5200.47E, Anti-Tamper (AT) (2015)
10. US General Accounting Office Report GAO-04–302, Defense acquisitions : DoD needs to better support program manager's implementation of anti-tamper protection (2004)
11. DoD: Program Protection Plan Outline & Guidance (2011)
12. DoDI 5200.39, Critical Program Information (CPI) Identification and Protection within Research, Development, Test, and Evaluation (RDT&E) (2015)
13. DoDI 5200.39, Required Use of Standardized Process for the Identification of Critical Program Information (CPI) in DON Acquisition Programs (2007)
14. DoDI 5200.44, Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN) (2012)
15. Malinda R.: System Security Engineering and Program Protection Integration into SE. In: 17th Annual NDIA Systems Engineering Conference (2014)
16. Malinda R.: Systems Engineering Requirements Analysis and Trade-off for Trusted Systems and Networks Tutorial (2013)
17. Raymond, S.: Identification and protection of critical program information (CPI). In: 18th Annual NDIA Systems Engineering Conference (2015)