Hindawi
Security and Communication Networks
Volume 2018, Article ID 6135845, 12 pages
https://doi.org/10.1155/2018/6135845

Research Article

Security Evaluation Framework for Military IoT Devices

Sungyong Cha, Seungsoo Baek, Sooyoung Kang, and Seungjoo Kim

Center for Information Security Technologies (CIST), Korea University, Seoul 02841, Republic of Korea

Correspondence should be addressed to Seungjoo Kim; skim71@korea.ac.kr

Received 6 March 2018; Revised 6 May 2018; Accepted 29 May 2018; Published 3 July 2018

Academic Editor: Ilsun You

IoT is gaining importance in our lives and in the military too. With the application of IoT paradigm in the military and the weapon system's connectivity to the network, this facilitates the commanders to make real-time decisions. However, cybersecurity threats to weapon systems intensify along with the growing of IoT's benefits. Coping with these cybersecurity threats nowadays, we require the implementation of "security by design" concept during weapon system development throughout the system lifecycle, but not traditional security solutions. Since only developed countries are capable of developing systems on their own, they adopt "security by design" when developing new weapon systems; another approach to acquire weapon systems is through import if a country cannot develop the whole weapon system. However, few studies have been done on the security evaluation framework that could be used upon purchase and integration of the developed weapon system. In this paper, we proposed a novel security evaluation framework that could be used to integrate IoT devices and components into the weapon system and a method to address cybersecurity requirements using international standard security control.

1. Introduction

With the advent of the IoT paradigm, all devices connected to the network began exchanging data among each other. The military is aware of the benefits of IoT and has continuously applied it to the weapon system, which ultimately becomes an essential to achieve military goals [1]. IoT technology connects and integrates into a myriad of devices and systems, but this will also increase attack surface. Until recently, cyber-attacks have been spreading beyond PCs to devices which of those have been connected to the Internet and smartphones [2]. But, the security threats of the network-centric weapon systems, including the IoT devices, are growing together with the advantages of IoT too [3]. What is more, the military domain is targeted by hackers. There is a recent experiment conducted in 2015 purported to hack into a Jeep Cherokee, the symbol of military mobility in the U.S., and it turned out to be a successful hacking later [4]. In fact, even if the network is far from another network physically, such as the Internet and Intranet, hacker attacks are still inexorable. According to [5], there is a possibility that the Trident system in partitioned network will be hacked through the air-gap from an external network, which will seriously affect operation and reliability. Therefore, some argue that the protection against cyber-attacks should be placed as the top priority. Simply, the usual way to enhance cybersecurity of the existing systems by introducing security solutions, e.g., firewall and cryptographic devices, is no longer effective. If a security vulnerability is found in a system, denoting that the cybersecurity factor has not been embedded in the system design at first, it would be difficult and costly to fix it; in some extreme cases, it would be impossible to handle the problem. In order to overcome these defects, researches are conducted by implementing 'security by design' concept as displayed in [6–8]. Representative examples are HACMS (High-Assurance Cyber Military Systems) project in DARPA (Defense Advanced Research Projects Agency) and the Defense Acquisition System in Department of Defense (DoD) which coordinately takes cybersecurity into account during weapon system acquisition [9, 10].

However, [9, 10] only confine the consideration for cybersecurity to weapon systems which are developed by the U.S.; in this manner when one country imports part or all of a weapon system from another country, its cybersecurity could not be checked. To remedy these drawbacks, a composite security evaluation method for assessing the cybersecurity

of the whole system in system integration has been studied [11, 12, 15]. Such composite security evaluation method is, yet, difficult to be applied to weapon systems because of the differences in the evaluation target and assurance levels for these composite security assessments. Therefore, according to [13], if the composite security evaluation cannot be implemented and the security of the system cannot be proved mathematically, the system should be developed along a well-structured process; hence we require a framework to evaluate cybersecurity when we buy parts from other countries and integrate them. To settle cybersecurity requirements, acquirer makes and utilizes security controls. For example, there are 253 security controls composed of 18 families being used in the United States and 5 families and 76 security controls utilized in Republic of Korea, respectively [16]. Nevertheless, security controls differ from country to country in terms of the criteria and description; on top of that, there are differences in interpretation between acquirer and provider, which may result in missing some security functions of the weapon system; hence, a universal security control is imperative.

In this paper, we propose a novel evaluation framework that could be used to evaluate cybersecurity requirements, not upon weapon system development, but the import of part or all of a weapon system from other countries. By using the international cybersecurity standards, security controls, as well as the understanding between acquirer and provider, are then unified in order to achieve mutual trust and strengthen cybersecurity along the arms import process.

The contents of this paper are as constructed as follows: we discuss the research about the background of this study in Section 2; in Section 3, we introduce the framework to improve the cybersecurity when purchasing weapon systems, in which our proposal also maps out domestic security controls with international cybersecurity standards. Following that, we examine how the proposed process can be applied in Section 4; we finalize the paper in Section 5.

2. Related Work

2.1. Cybersecurity Evaluation in Domestic and International. Reliability and security are verified through systems' cybersecurity evaluation. That is, system users can make use of evaluation certification methods to upgrade information protection level of an organization and their asset and contribute to credibility. Countries establish their standards to undergo cybersecurity evaluation and requirements based on their own circumstances. To name a few, BS 7799 part 2 [17] operated by United Kingdom and TCSEC (Trusted Computer System Evaluation Criteria) in the U.S. [18] are the representatives of domestic evaluation standards. NIST (National Institute of Standards and Technology) documents are also references to many countries, besides the U.S. government [19].

ISO / IEC 15408 [20], as known as the Common Criteria (CC), is an international standard established to coordinate different information protection system evaluation standards by country and to mutually certify the evaluation results. CC consists of 11 Security Functional Requirements (SFRs) which defines the required structure and content of security functional components; and 10 Security Assurance Requirements (SARs) define a scale for measuring assurance for component target of evaluations. However, the limited ability to evaluate a single product but not the whole system and disability to provide an evaluation of environments elements (physical, human, and operational security) discern the disadvantage of CC; to this end, the composite evaluation was introduced. Yet, composite ToE (Target of Evaluation) of CC-CAP (Composite Assurance Packages) is subjected to products only with CC certification. The highest evaluation level of CC-CAP, CAP-C, manifests a similar evaluation level of EAL (Evaluation Assurance Level) 4 in CC to which weapon systems requesting a level higher than EAL 5 are not applicable. CCDB-CPE (Common Criteria Development Board-Composite Product Evaluation) approach could be deployed to weapon systems demanding a level higher than EAL 5; still this approach is yet to be claimed ideal; design documents and other sensitive information are required to be disclosed; added to this disadvantage, it is not suitable for implementation in weapon systems as it was originally designed for smartcard evaluation. EURO-MILS (multiple independent levels of security), another evaluation approach appropriate for those security levels equivalent to EAL 5, is also limited to the use of designated platforms only. Table 1 concludes the characteristics of these composite security evaluation methods.

ISO/IEC 27001 [21], as known as the Information Security Management System (ISMS), consists of 114 controls in a total of 14 clauses. It also carries out verification for information security policy management, human resources security, physical environment security, communication and operation management, information system construction, and maintenance. The security controls of ISO/IEC 27001 could be indicators of whether the product (or information) is managed properly based on the established procedure. There is a shortcoming that the product security itself, still, could not been substantiated. Therefore, it is necessary to verify that the security of a product in general. Since the SFRs of ISO/IEC 15408 is initiated to confirm only the implemented security functions of the product but not the environment related to the development, the evaluation of functional and nonfunctional parts of the weapon system could be done by complementing ISO/IEC27001 mentioned previously.

2.2. Cybersecurity Evaluation in Defense. The evaluation of security functions and assurance of a to-be-imported system is of considerable importance. Despite that, to achieve high level of security and assurance of weapon systems as well as security functional evaluation, introducing formal verification is necessary. Nevertheless, a formal verification entails the combination of all the functions in the system to be proved mathematically to validate the logic. A framework should be followed by a well-defined development process if it cannot be proved on a mathematical basis [13]. Products are developed according to the System Development Life Cycle (SDLC); similarly, weapon systems are developed based on SDLC, considering whether they are suitable to the acquisition system of the respective country. However, these acquisition systems have traditionally focused on performance

Table 1: Composite security evaluation approach.

	CC-CAP [11]	CCDB-CPE [12]	EURO-MILS [13]
Operation area	CCRA Members (28 countries)	CCRA Members (28 countries)	European countries
key features	a composite Target of Evaluation (TOE) is composed of components that have already passed CC evaluation	enable installing applications onto an already passed CC evaluation platform	reuse component certificates
Evaluation subject	information product	smartcard	avionic and automotive
Assurance Level	CAP-(A, B, C) ∗ CAP-C is comparable to EAL4	EAL1 ~ EAL7	comparable to EAL 5

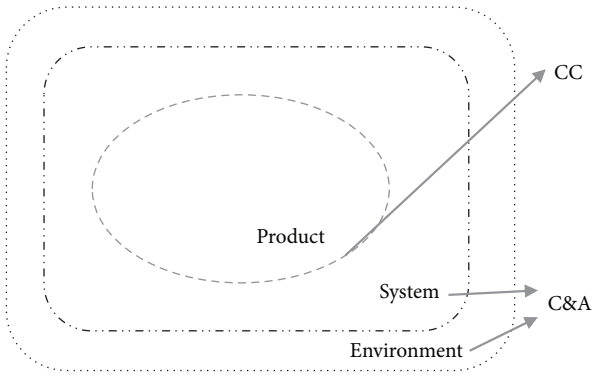

Figure 1: Scope of security evaluation by CC and C&A.

and operability rather than cybersecurity aspects of weapon systems. Instead of changing the acquisition system to reinforce cybersecurity, processes such as C&A (Certification and Accreditation) are blended into the existing systems to enhance cybersecurity level, of which this practice is shown in Figure 1.

The C&A process was introduced in the Trusted Computer System Evaluation Criteria (TCSEC) [18], known as the Orange Book, and was then recognized as an international standard under the name of Common Criteria (CC) [20]. However, as described in Section 2.1, there are drawbacks that make it difficult to apply these evaluation methods directly to weapon systems. Thus, the U.S. Department of Defense (DoD) created the Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP) in 1997 for environmental and system security evaluation as well as product security [23]. Later on, the DoD released Information Assurance Accreditation Process (DIACAP) [24] to overcome the drawbacks of DITSCAP and is currently operating Risk Management Framework (RMF) [25, 26]. At present, cybersecurity-enhanced defense acquisition system with RMF employed in the U.S. is shown in Figure 2 [22]. However, [22] focuses only on weapons systems development and, hence, is difficult to use when purchasing and integrating parts of weapons systems. It is not easy to apply the above-mentioned system in other countries because most countries would not develop weapons systems by themselves but import weapons systems from other countries. For example, some countries purchase critical parts, e.g., stealth functions, in developed countries; in essence, it is problematic to verify security by using different cyber security processes and standards for acquirers and providers. Besides, the provider developed the system of which its risk management was based on the assumption of an environment totally different from that of the acquirer. Therefore, it is not appropriate for the acquirer to assess risk based on the same environment in this respect. Therefore, we need a framework to design, verify, and test cyber security in the weapon system import process. Figure 3 is a general weapon system import process where we must combine some of the frameworks to enhance cybersecurity.

An analysis of the defense acquisition system shows that the Risk Management Framework and Cybersecurity Test & Evaluation are carried out throughout the lifecycle of weapon system development. In addition, it applies not only to risk management in functional part of the weapon system, but also to the nonfunctional aspects, such as the development environment and human resources. Therefore, it is essential to apply risk management in both functional and nonfunctional parts of the weapon system during the purchasing process shown in Figure 3.

2.3. Weaknesses in Current Evaluation Framework. To summarize the issues discussed earlier, first of all, among the existing import process for weapons systems, there is no framework to enhance cybersecurity. Secondly, there is a possibility of misinterpretation of weapon security requirements that arises from differences in security controls adopted in various countries. For that reason, the requirements for the weapon system import process are summarized as follows.

(i) To comprehensively evaluate both security and nonsecurity functions, processes for enhancing cybersecurity such as RMF and Cybersecurity T&E should be integrated into existing import processes.

(ii) Security controls of the provider and the acquirer should be matched so that they can be used in all instances, not limited to specific countries.

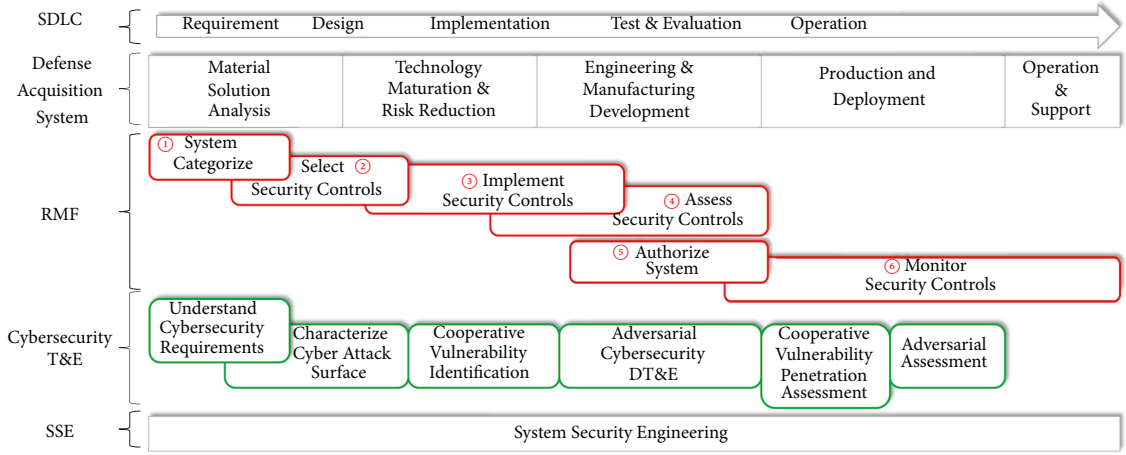

Figure 2: Defense Acquisition System in the U.S. for enhancing cybersecurity [22].

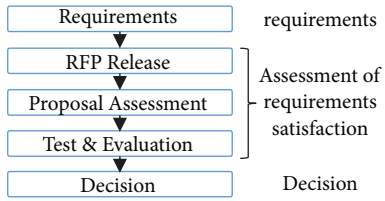

Figure 3: General weapon system purchasing process.

3. Proposed Security Evaluation Framework

3.1. Security Evaluation Framework. In this chapter, we propose a new security evaluation framework that combines RMF and Cybersecurity Test & Evaluation in the existing weapons import process with cybersecurity international standards. The framework for improving cybersecurity is shown in Figure 4: ① ~ ⑥ relate to each RMF step in Figure 2 and the blue boxes indicate the purchase process in Figure 3; the red and green boxes represent RMF and Cybersecurity T&E in Figure 2, respectively. Also, the indicators of italicized alphabets for flow of steps are illustrated in detail below.

(A) Defining Requirements with Risk Identification (System Categorization). At this stage, the same method as the first step in RMF [25, 26] is used to identify the risks for the product (or system) to be acquired. And the provisional impact value for each risk is calculated. Provisional impact values are classified into three levels: high, moderate, low for confidentiality, integrity, and availability. By defining the cybersecurity requirements for the product to be acquired with reference to the impact value of the identified risk, the unnecessary cost can be reduced and accurate security functions can be implemented. These cybersecurity requirements are then integrated with other functions, operating requirements and then passed on to the next step.

(B) Selecting Appropriate Security Controls from the Requirements. In this step, we choose security controls as a countermeasure to achieve the cybersecurity requirements defined in step (A). To select security controls for the product to be imported, we should review the security controls in the parent systems first and determine if there are any security controls that could be inherit from the system. Those are inherent in the system should be tailored out from the product list of security controls and the remaining list would be the security controls we should implement. At this point, the security control set made by the acquirer comes into effect. The reason is to reduce time to select security controls and to remove missing parts by using new sets of security controls that are not familiar with. If there is no set of security controls available from the acquirer, they may skip this step and the provider may bring up a set of security controls or a set of international standard security controls. Once the security controls have been selected, one can proceed to the next step following by review.

(C) Converting the Security Controls into the International Standards. The selected security controls are converted into international standard (ISO/IEC 15408, ISO/IEC 27001) security controls at this stage. The reason for this standardization is that it is difficult for the provider to clearly understand the security controls of the acquirer, so the misunderstanding ensued from such environmental differences can be reduced. However, the problem is to what extent the set of security controls of the acquirer and the provider can be converted and expressed under the set of international standard security controls. This will be covered in detail in Section 3.2, and briefly, the mapping table and definition of addition subjects are provided in Appendix H [16].

Concurrently, the part corresponding to the function of product security is converted into the Security Functional Requirements (SFR) of ISO/IEC 15408, and that of operation and environment is converted into ISO / IEC 27001. Nonetheless, there are real cases where ISO/IEC 15408 does not cover

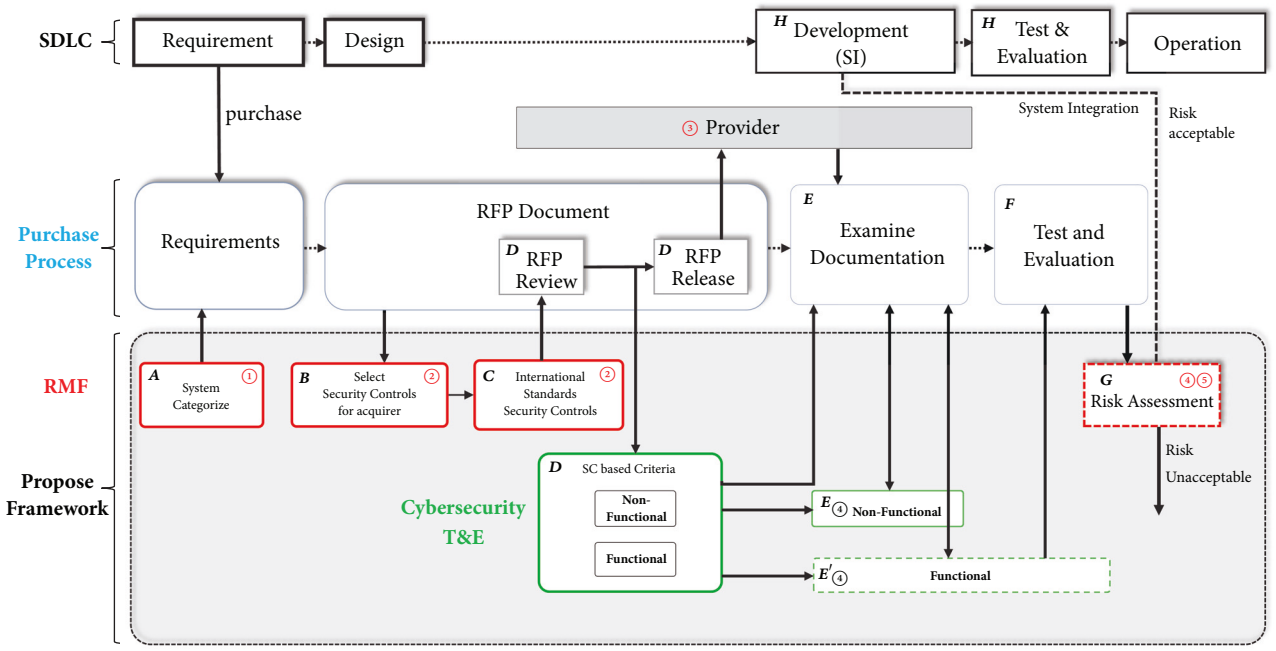

Figure 4: Proposed security evaluation framework.

all the conversions for product security function, then ISO / IEC 27001 is used for the conversion in such cases. Using international standard security controls in this construct, we can generate a set of security requirements similar to the Profile Protection used in the Common Criteria.

(D) Completion of RFP Evaluation Criteria and Preparation for Proposal Evaluation. It is a step for a comprehensive assessment of those security controls, functions, and operating requirements that has been converted into international standards which reflect cyber security requirements. The main objective at this stage is to gather all stakeholders and coordinate any conflicting interests in between, in particular, to adjust requirements that may be confined to funding. If resource constraints and other issues do not reflect all requirements, they should be broken down into mandatory requirements and optional requirements on the foundation of distinguished risk and impact values identified in the first step [27]. In other words, risk-based decisions are made so that risks can be handled according to priorities. Once everything is done consistently, it is followed by the announcement of RFP (Request for Proposal).

While the provider is in the middle of RFP release and proposal preparation, the acquirer constructs the evaluation list by dividing the nonsecurity functional part and the security functional part based on the cybersecurity requirements in Figure 4. The rationale behind this is to insure the evaluation of security-related means and environments for required security functions and product development.

(E) Evaluation of Submitted Proposals and Preverification. The provider submits the proposal of the announced RFP

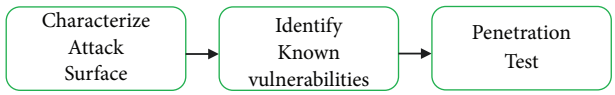

Figure 5: Security functional test flow.

to the acquirer based on the international standard security controls. Since the security nonfunctional parts are difficult to verify directly, it is advised to submit proposal results which has been verified by an authorized third party. Despite the fact that the nonfunctional parts could be compromised by certifications such as ISO/IEC 27001, it is only possible when the scope of evaluation is identical. The security functional parts are the main components to be verified in the next step "Real verification"; nevertheless, it should also engage in assessing whether the document evaluation comprises the functionality to confirm the satisfactory level of security functions. When examining the satisfactory level of security functions (for the security functional parts of the document evaluation), it is necessary to deploy advance preparation to shorten the evaluation time for "Real verification". Advance preparation refers to the identification of the attack surface and the identification of known vulnerabilities [28] which embody the penetration test, and Figure 5 is a detailed description of E′ in Figure 4.

(F) Functional Requirement Verification. Products that passed documentation undergo another test to gauge whether they can function exactly as what have been stated in the proposal. The focus of the verification is not only to validate the

Table 2: Number of security controls that do not provide mapping table in NIST 800-53.

Security Controls		Total	Not Provides
AC	Access Control	25	8
AT	Awareness and Training	5	1
AU	Audit and Accountability	12	4
CA	Security Assessment and Authorization	9	5
CM	Configuration Management	11	2
CP	Contingency Planning	13	1
IA	Identification and Authentication	11	4
IR	Incident Response	10	5
MA	Maintenance	6	3
MP	Media Protection	8	1
PE	Physical and Environmental Protection	20	2
PL	Planning	9	1
PS	Personnel Security	8	1
RA	Risk Assessment	6	1
SA	System and services Acquisition	22	8
SC	System and Communications Protection	44	31
SI	System and Information Integrity	16	11
PM	Program Management	9	5

Figure 6: Risk assessment flow.

described requirements, but also to confirm if cybersecurity is implemented properly by carrying out known vulnerabilities check and penetration test. The actual evaluation is based on a block-box test. However, if the acquirer is in agreement with the provider on white-box testing, the acquirer could verify the product in detail. In case of lack of time and cost, this might be an optional step for acquirers to follow.

(G) Risk Assessment. The product is cleared if it has passed through all the evaluations at "verification" stage; products that fail to meet the requirements criterion are directed to undergo risk assessment. The first risk assessment was a provisional impact value done under a proposed situation, whereas the risk assessment at this step, will be revealed using real data input. The risk assessment flow is shown in Figure 6, and this procedure is applied in accordance with the procedure in [29].

At this stage, an actual and reliable risk assessment is feasible as outcome is collected from real data. If the risk level result is acceptable, acquirer can advance to the next step; if not, the parts would be taken as inappropriate and acquirer may consult with provider.

(H) Secure System Integration and Operational Test and Evaluation. Products that survived "verification" ((F), (G) Step) are incorporated into the whole system and are, finally, reevaluated. After integrating into the system, similar evaluation on functionality of a single product goes through, except that the reevaluation for the time being concentrates on the product operability. The "Assurance" part that is designed to guarantee the function performance of the product is excluded from this paper.

3.2. Mapping Security Controls to ISO/IEC 15408 and 27001. The security controls of acquirer have to be revised to adapt to international standardized security requirements with a purpose to guarantee a successful flow of Stage (C) in Section 3.1. This section illustrates the amended international security controls with the most concrete and detailed NIST 800-53. According to the analyzing result from the conversion table provided in Appendix H, 73 out of 252 security controls in 18 categories are not provided with mapping as security controls of ISO/IEC 15408 and 27001 [Table 2].

Those security controls without mapping are analyzed and converted into international standard security controls of which the results are shown in Table 3.

The conversion of security controls demands considerable of technical controls; in view of this, it is recommended to proceed conversion using ISO/IEC 15408. The definition of the class regarding ISO/IEC 15408 Security Functional Requirements is listed in Table 4. Also, security controls that are not related to weapons purchasing, IR (Incident Response), AT (Awareness and Training), and PM (Program Management) are removed from conversion of security controls.

For example, the *IA-3 (Device Identification and Authentication)* relates to the identification and authentication of devices connected to the information system. This control can be converted into the UAU (User Authentication) and UID

Table 3: Security controls that are converted on component and family level.

NIST	Security Controls	ISO/IEC15408 Common Criteria Component or Family
AC-21	Information Sharing	FPT_TDC.1
AC-22	Publicly Accessible Content	FPT_TDC.1
AC-23	Data Mining Protection	FTA_LSA.1
AU-13	Monitoring for Information Disclosure	FAU_SAR.1, FDP_ETC.1
AU-16	Cross-Organizational Auditing	FAU_SAR.1
CM-2	Baseline Configuration	EAL package
IA-3	Device Identification and Authentication	FIA_UAU.1, FIA_UAU.2, FIA_UAU.1, FIA_UAU.2
IA-9	Service Identification and Authentication	FIA_UAU.1, FIA_UAU.2, FIA_UAU.1, FIA_UAU.2
IA-10	Adaptive Identification and Authentication	FIA_UAU.1, FIA_UAU.2, FIA_UAU.1, FIA_UAU.2
MP-8	Media Downgrading	ALC_CMC, ALC_CMS
PE-6	Monitoring Physical Access	FPT_PHP.1, FPT_PHP.2, FPT_PHP.3
PE-8	Visitor Access Records	ALC_DVS
PS-2	Position Risk Designation	FPT_PHP.1, FPT_PHP.2, FPT_PHP.3
RA-6	Technical Surveillance Countermeasures Survey	AVA_VAN
SA-2	Allocation of Resources	FRU_RSA
SA-13	Trustworthiness	EAL package
SA-16	Developer-Provided Training	ALC_DVS
SA-20	Customized Development of Critical Components	ALC_CMC, ALC_CMS
SC-2	Application Partitioning	FIA_ATD.1
SC-18	Mobile Code	FMT_MSA.1, FMT_MSA.2
SC-19	Voice Over Internet Protocol	FMT_MSA.1, FMT_MSA.2
SC-20	Secure Name/Address Resolution Service (Authoritative Source)	FMT_MSA.1, FMT_MSA.2
SC-21	Secure Name/Address Resolution Service (Recursive or Caching Resolver)	FMT_MSA.1, FMT_MSA.2
SC-22	Architecture and Provisioning for Name/Address Resolution Service	FMT_MSA.1, FMT_MSA.2
SC-29	Heterogeneity	FDP_IFF
SC-32	Information System Partitioning	ADV_ARC
SC-37	Out-of-Band Channels	FPT_PHP.1, FPT_PHP.2, FPT_PHP.3
SC-39	Process Isolation	ADV_ARC
SC-42	Sensor Capability and Data	FDP_ETC.1, FDP_ETC.2
SC-43	Usage Restrictions	FDP_IFF.3
SI-8	Spam Protection	FDP_ACC.1, FDP_ACC.2 FDP_IFC.1,FDP_IFC.2
SI-11	Error Handling	FDP_ACC.1, FDP_ACC.2, FIA_AFL.1
SI-15	Information Output Filtering	FDP_ACC.1, FDP_ACC.2 FDP_IFC.1,FDP_IFC.2
SI-16	Memory Protection	ADV_ARC
SI-17	Fail-Safe Procedures	FPT_RCV, ADV_ARC

(User Identification) families in Functional Identification and Authentication (FIA) class. The selected components are shown in Table 5.

The reason is that the FIA_UID and FIA_UAU families are related to user authentication and identification but can also be described equivalently under the condition that the user of the CC is conceived as the same subject as the device in the NIST security controls. However, as shown in Table 6, security controls of some specific technologies that are not directly converted to the component or family unit can be mapped at the class level and organizational security policy pursued by illustration.

3.3. Comparison Analysis. Different from other evaluation frameworks, our proposed framework is intended for the integration of imported systems. It is set up based on RMF and Cybersecurity T&E of which their properties are inherited. However, as shown in Table 2, RMF does not carry

Table 4: Families of security functional requirements in ISO/IEC15408.

Family	Description
FAU	Security Audit
FCO	Communication
FCS	Cryptographic Support
FDP	User Data Protection
FIA	Identification and Authentication
FMT	Security Management
FPR	Privacy
FPT	Protection of the TSF
FRU	Resource utilization
FTA	TOE access
FTP	Trusted path/channels

Table 5: Example of security control conversion into CC component.

Components	Description
FIA_UAU.1	Timing of authentication, allows a user to perform certain actions prior to the authentication of the user's identity.
FIA_UAU.2	User authentication before any action, requires that users authenticate themselves before any action will be allowed by the TSF.
FIA_UID.1	Timing of identification, allows users to perform certain actions before being identified by the TSF.
FIA_UID.1	User identification before any action, require that users identify themselves before any action will be allowed by the TSF.

Table 6: Security controls that are converted on class level.

NIST	Security Controls	ISO/IEC15408 Family
SA-22	Unsupported System Components	FMT
SC-25	Thin Nodes	FRU
SC-26	Honeypots	FDP
SC-27	Platform-Independent Applications	FDP, FIA
SC-30	Concealment and Misdirection	FDP
SC-34	Non-Modifiable Executable Programs	FMT
SC-35	Honey clients	FDP
SC-36	Distributed Processing and Storage	FMT
SC-40	Wireless Link Protection	FIA,, FPT, FTA FTP
SC-44	Detonation Chambers	FDP
SI-14	Non-Persistence	FDP

all the mapping tables required for international standard; therefore, we propose an addition conversion method in Section 3.2. Table 7 is the comparison table of our framework with RMF, Cybersecurity T&E, and CC-based approaches.

4. Use-Case: Adoption of the Inertial Navigation System Import for Unmanned Aerial Vehicle

A formal evaluation upon our framework would be an ideal proof of framework's novelty. The framework we proposed however would be difficult to be proved formally as such evaluation is out of scope of this proposal. In lieu of a formal proof, we demonstrate use-case to explain how our proposed framework in Section 3 is applied to the weapon system purchasing process, an example of an inertial navigation system(INS) built in an unmanned aerial vehicle (UAV). It is noted that owing to confidentiality issue the components of military UAV are not disclosed; hence we use a general UAV instead for illustration in the use-case. An inertial navigation system is a navigation aid that uses a computer, motion sensors (accelerometers), rotation sensors (gyroscopes), and occasionally magnetic sensors (magnetometers), to continuously calculate by dead reckoning the position, the orientation and the velocity (direction and speed of movement) of a moving object without the need for external references. The INS is a critical part of computing data from sensors in UAV; thus, security is assured.

(A) Defining Requirements with Risk Identification (System Categorization). As presented in [30], the risk of INS in UAV should be evaluated by the parameter, i.e., velocity, attitude,

Table 7: Comparison with other approaches.

	Our framework	RMF	Cybersecurity T&E	CC based approaches
Purpose	Integrated into arms import process	Integrated into acquisition system	Eliminate vulnerabilities	Security evaluation of information products
For international use	○	△	X	○
Functional test	○	○	○	○
Operational test	○	○	○	X
Risk management	○	○	X	X

Table 8: Example of system categorization of INS.

Elements	Confidentiality	Integrity	Availability
		Provisional Impact Value	
Velocity	M	H	H
Attitude	M	H	H
Horizontal position	M	H	H
Depth	M	H	H
Total	M	H	H

horizontal position, and depth, which factor out the system categorization. When the confidentiality of the parameters does not impact much on duty, the system is graded as low; when the values of parameters are vague and calculation of position becomes infeasible, availability is classified as high; and integrity is marked as high too where inaccurate values deter an anticipation of position. Table 8 shows the risk evaluation result of INS.

(B) Selecting Appropriate Security Controls from the Requirements. Based on the result from Stage (A), the security control of INS brings the focus on the assurance of integrity and availability. The security controls of INS are compared with that of UAV for analysis to derive the necessary security controls of INS for later integration. The security controls inherent in UAV should then be excluded from the INS security control list. Since INS is a part of UAV, physical and environmental security controls against direct approach and accident could be inherited from UAV together with the security controls of management and operation security. Table 9 lists out the potentially inheritable security controls from UAV.

After tailoring out these inheritable security controls, the remaining INS security controls are concluded in Table 10.

AC-17, 18 are chosen because they carry Ethernet port; IA-2 is used for the identification of user and authentication of device to notify UAV of the identity of INS; IA-3 is to verify the authenticity of signal if it comes from INS. After selecting the proper security controls, acquirer should proceed to the next step.

(C) Converting the Security Controls into the International Standards. We convert selected elements in the security control into the international standards with Table 2 and [25]. Table 11 shows that result of converting security controls to international standards.

(D) Completion of RFP Evaluation Criteria and Preparation for Proposal Evaluation. We review the result of conversion whether it is reasonable. If, due to certain reason, the chosen security control is found inapplicable amid the evaluation process, its property should be further distinguished from compulsory to optional. For example, in the manner where IA-3 cannot be enacted unless it executes along with GPS (Global Positioning System), it is considered as an optional security control whereas IA-3 becomes compulsory when it is to be implemented in the absence of assistive device. Then, we prepare security evaluation in cases of function elements and nonfunction elements.

(E) Evaluation of Submitted Proposals and Preverification. If the security evaluation is ready, acquirer verifies documents from provider whether the documents meet the criteria of the security evaluation on the international standards. Then, we prepare the functional test by using open vulnerabilities on Common Vulnerabilities Exposures (CVE) and Common Weakness Enumeration (CWE) in order to save evaluation time. For instance, because Ethernet is adhered to INS, potential attacks arising from Ethernet are predictable and hence, Ethernet contributes to one part of the attack surface in this regard. Table 12 shows some of the common vulnerabilities found on Ethernet, and given the fact that time is limited in most cases, acquirer should opt for the most likely and influential ones. In situations where provider has already attained the approved ISO/IEC 15408 or ISO/IEC 27001, it is at acquirer's discretion to adopt the system as embedded or not.

(F) Functional Requirement Verification. This part is highly reliant on external factors such as the test time and budget given. Because of the adequate availability of papers in the respect of test method, we will not discuss in detail here.

Table 9: Example of potentially inheritable security controls from UAV and above.

SC	Description	SC	Description
AC-1	Access Control Policy and Procedures	PE-9	Power Equipment and Cabling
AC-2	Account Management	SC-1	System and Communications Protection Policy and Procedures
AU-1	Audit and Accountability Policy and Procedures	SC-7	Boundary Protection
AU-2	Audit Events	SC-8	Transmission Confidentiality and Integrity
PE-1	Physical and Environmental Protection Policy and Procedures	SC-12	Cryptographic Key Establishment and Management
PE-2	Physical Access Authorizations	SC-13	Cryptographic Protection
PE-3	Physical Access Control	SC-20	Secure Name /Address Resolution Service
PE-6	Monitoring Physical Access	SC-38	Operations Security

Table 10: Example of selected INS security controls.

SC	Description	SC	Description
AC-17	Remote Access	IA-2	Identification and Authentication
AC-18	Wireless Access	IA-3	Device Identification and Authentication

Table 11: Example of converting the security controls to ISO/IEC 15408 and 27001.

NIST	Security Controls	ISO/IEC15408 or ISO/IEC 27001 Requirements
AC-17	Remote Access	A.6.2.1: Mobile device policy: A.6.2.2: Teleworking A.13.2.1: Information transfer policies and procedures
AC-18	Wireless Access	A.6.2.1: Mobile device policy: A.13.1.1 Network controls A.13.2.1: Information transfer policies and procedures
IA-2	Identification and Authentication	FIA_ATD.1: User Attribute Definition FIA_UAU.1: User Authentication (Timing of Authentication) FIA_UAU.2: User Authentication before any action) FIA_UID.1: Timing of identification FIA_UID.2: User Identification before any action
IA-3	Device Identification and Authentication	FIA_UAU.1: User Authentication (Timing of Authentication) FIA_UAU.2: User Authentication before any action) FIA_UID.1: Timing of identification FIA_UID.2: User Identification before any action

Table 12: Example of selected CVE on Ethernet vulnerabilities.

Name	Description
CVE-2017-9628	An Information Exposure issue
CVE-2017-9945	a Denial-of-Service condition could be induced by a specially crafted PROFINET DCP packet sent as a local Ethernet (Layer 2) broadcast.
CVE-2017-3726	a privilege escalation vulnerability
CVE-2016-8106	vulnerable to a denial of service in certain layer 2 network configurations.

Table 13: Example of assessment scale-level of risk [14].

Overall Likelihood	Impact Level of Risk				
	Very Low	**Low**	**Moderate**	**High**	**Very High**
Very High	Very Low	Low	Moderate	High	Very High
High	Very Low	Low	Moderate	High	Very High
Moderate	Very Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Low	Moderate
Very Low	Very Low	Very Low	Very Low	Low	Low

The requirement verification lies in the test method, which is decided by acquirer or settled between acquirer and provider.

(G) Risk Assessment. If the IA-3 security control failed in the functional test, we should reevaluate the impact level of the risk about IA-3 failure by referring to Table 13 [14]. As demonstrated in Table 12 the possibility of direct attacks to communication between INS and the rotation sensor is low, but the resulting damage can result in catastrophic consequences of UAV failing to fly properly (high). As a result, owing to the fact that the overall risk is low, acquirer still manages to continue the process even if IA-3 declines)

(H) Secure System Integration and Operational Test & Evaluation. If the whole evaluation ends successfully, acquirer could commence the integration of INS into UAV, after which the development and evaluation of UAV are to be deployed. The postintegration process follows the existing procedures of the acquirer.

5. Conclusion

Provided that the evaluation framework is system-specific, variations emerge in the midst of negotiations between countries; it is therefore difficult to employ the same approach to every scenario in reality. Notwithstanding, an existence of a well-established framework to guide, in part, is beneficial upon the trading of systems. We proposed the security-enhanced framework based on the Risk Management Framework and Cybersecurity Test & Evaluation, and this framework has been designed to be integrated into import process of weapon systems, but not developmental process. Also, we have raised the assurance level of the weapon system via a well-structured framework instead of mathematical (formal) verification. Within this framework, the cybersecurity of weapon systems is ensured throughout the lifecycle of weapon systems, from the development stage of the provider to the operation stage of the acquirer. In addition, by employing international standards rather than using domestic security controls under the proposed framework, it facilitates the weapon system acquisition communication between the acquirer and provider. We reinforced the construction of this framework with reference to NIST documents; however, we did not recommend an evaluation methodology relevant to this framework. Some nations might encounter difficulties in applying our framework into their weapon system acquire process. Therefore, future studies would require a more detailed evaluation method for this framework and for compositing security evaluation in order to address the assurance level of weapon systems.

Data Availability

The datasets generated during and/or analyzed during the current study are available from the corresponding author upon reasonable request.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This research was supported by the MSIT (Ministry of Science, ICT), Korea, under the ITRC (Information Technology Research Center) support program (IITP-2018-2015-0-00403) supervised by the IITP (Institute for Information & Communications Technology Promotion).

References

[1] L. Yushi, J. Fei, and Y. Hui, "Study on application modes of military internet of things (miot)," in *Proceedings of the IEEE International Conference*, vol. 3, pp. 630–634, Computer Science and Automation Engineering (CSAE), 2012.

[2] J. P. Farwell and R. Rohozinski, "Stuxnet and the future of cyber war," *Survival*, vol. 53, no. 1, pp. 23–40, 2011.

[3] A. Kim, B. Wampler, J. Goppert, I. Hwang, and H. Aldridge, "Cyber attack vulnerabilities analysis for unmanned aerial vehicles," in *Proceedings of the AIAA Infotech at Aerospace Conference and Exhibit 2012*, USA, June 2012.

[4] C. Miller and C. Valasek, "Remote exploitation of an unaltered passenger vehicle," in *Proceedings of the Black Hat Briefings*, USA, 2015.

[5] A. Futter, *The Politics of Nuclear Weapons*, SAGE Publications Ltd, 1 Oliver's Yard, 55 City Road London EC1Y 1SP , 2015.

[6] C. Dougherty, K. Sayre, R. C. Seacord, D. Svoboda, and K. Togashi, "Secure design patterns," Tech. Rep., Carnegie Mellon University, Pittsburgh, Pa, USA, Software Engineering Institute, 2009.

[7] N. Davis, "Secure software development life cycle processes: A technology scouting report," Tech. Rep., Carnegie-Mellon Univ Pittsburgh Pa Software Engineering Inst, A technology scouting report, 2005.

[8] C. Mundie, P. de Vries, P. Haynes, and M. Corwine, "Trustworthy computing," Technical Report, 2002.

[9] K. Fisher, "Using formal methods to enable more secure vehicles," *ACM SIGPLAN Notices*, vol. 49, no. 9, pp. 1-1, 2014.

[10] M. Schwartz, *Defense Acquisitions: How Dod Acquires Weapon Systems And Recent Efforts to Reform The Process*, Library of Congress Washington Dc Congressional Research Service, 2010.

[11] H.-G. Albertsen and F. Forge, "The modular approach: A composite product evaluation for smart cards," in *Proceedings of the 3rd International Common Criteria Conference-Common Criteria: Delivering Information Assurance Solutions*, 2002.

[12] K. Muller, M. Paulitsch, S. Tverdyshev, and H. Blasum, "MILS-related information flow control in the avionic domain: A view on security-enhancing software architectures," in *Proceedings of the 2012 IEEE/IFIP 42nd International Conference on Dependable Systems and Networks Workshops (DSN-W)*, pp. 1–6, Boston, Mass, USA, June 2012.

[13] B. S. Blanchard and W. J. Fabrycky, "System engineering and analysis," 5th ed. Upper Saddle River, N. J. : Pearson, Prentice-Hall international series in industrial and systems engineering, 2011.

[14] S. Ross Ronald, "Guide for conducting risk assessments," No. Special Publication (NIST SP)-800-30r1. September, 2012.

[15] A. B. Jeng and Y.-M. Yu, "Analysis of the composition problems in cc v3. 1 rev. 1 with some suggested solutions, ICCC, 2006".

[16] R. S. Ross, "Security and privacy controls for federal information systems and organizations," Tech. Rep., 2013.

[17] R. Von Solms, "Information security management (3): The Code of Practice for Information Security Management (BS 7799)," *Information Management & Computer Security*, vol. 6, no. 5, pp. 224-225, 1998.

[18] S. L. Brand, *Dod 5200.28-std Department of Defense Trusted Computer System Evaluation Criteria (orange book)*, National Computer Security Center, 1985.

[19] C. E. Landwehr, "Computer security," *International Journal of Information Security*, vol. 1, no. 1, pp. 3–13, 2001.

[20] I. ISO and I. Std, "Iso 15408-2: 2009, Information technology-Security techniques-Evaluation criteria for IT security-Part 2".

[21] G. Disterer, "ISO/IEC 27000, 27001 and 27002 for Information Security Management," *Journal of Information Security*, vol. 04, no. 02, pp. 92–100, 2013.

[22] R. Sandoval, "Information systems development (isd) and the national institute of standards and technology (nist) risk management framework," 2017.

[23] D. Instruction, "5200.40, dod information technology security certification and accreditation process (ditscap)," December, 1997.

[24] D. Instruction, "8510.01, dod information assurance certification and accreditation process (diacap), november 28, 2007".

[25] NIST, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, February, 2010.

[26] D. Instruction, 8510.01, Risk Management Framework (RMF) for DoD Information Technology (IT), 2014.

[27] K. F. Joiner, S. R. Atkinson, and E. Sitnikova, *AUSTRALIA'S FUTURE SUBMARINE: Cybersecurity Challenges and Processes*, 2017.

[28] D. Instruction, DoD Cybersecurity Test and Evaluation Guidebook, June 26, 2015.

[29] Y. Y. Haimes, *Risk Modeling, Assessment, and Management*, John Wiley & Sons, 2015.

[30] M. Kevin, R. L. Kissel, W. C. Barker et al., *Guide for Mapping Types of Information and Information Systems to Security Categories (2 Volume)*, NIST, 2008.