chapter 1

사이버 보안 표준 및 위협 분석 기법 동향

도성룡 ‖ 상명대학교 특임교수

최근 사물인터넷 혁명으로 인해 자동차, 철도, 의료 등의 모든 산업 시스템들과 외부의 연결이 급격히 증가하고 있다. 이로 인해, 오늘날 거의 모든 시스템들은 다양한 사이버 보안 위협에 노출되어 있으며, 기술이 발전됨에 따라 이러한 위협은 더욱 증가할 것이다. 본 고에서는 산업 시스템들이 사물인터넷 기반의 CPS(Cyber Physical System) 패러다임으로 전환되는 흐름을 반영하여, 사이버 보안 사고를 사전에 예방하기 위한 관련 국제 표준 및 위협 분석 기법 동향에 대해 살펴본다.

I. 서론

고도화된 ICT 인프라를 통해 생성, 수집, 축적된 데이터와 인공지능이 결합한 지능정보기술이 경제, 사회, 삶 모든 분야에 보편적으로 활용됨으로써 새로운 가치를 창출하고 발전하는 사회를 지능정보사회라고 부른다[1].

지능정보사회에서는 모든 사물들이 유/무선으로 연결됨에 따라, 사이버 보안에 대한 중요성이 높아지고 있다. 특히, 자동차, 철도, 의료 등과 같은 안전 필수 시스템(Safety Critical System)의 보안 취약점은 치명적인 사고로 이어질 수 있으며, 사회적 이슈가

* 본 내용은 도성룡 특임교수(☎ 02-781-7667, imdsr@smu.ac.kr))에게 문의하시기 바랍니다.
** 본 내용은 필자의 주관적인 의견이며 IITP의 공식적인 입장이 아님을 밝힙니다.

되고 있다. 예를 들어, 자동차, 의료 등 안전 필수 시스템이 갖고 있는 보안 취약점을 해커들이 의도적으로 공격하는 사례가 증가하고 있다. 대표적으로 2015년 7월 크라이슬러의 지프(Jeep) 체로키의 컨트롤 시스템에 접속하여 자동차의 펌웨어를 변경 후 제어권을 탈취한 사례, 2017년 5월 워너크라이(Wanna Cry) 랜섬웨어 공격으로 영국의 국민건강서비스 산하 40여개 병원의 PC가 감염되어 모든 의료 서비스가 중단된 사례 등이 있다.

오늘날 거의 모든 소프트웨어 시스템은 다양한 사이버 보안 위협에 노출되어 있으며, 기술이 발전됨에 따라 위협은 더욱 증가할 것이다. 포브스 자료에 의하면, 2018년 2분기에 소프트웨어 취약성을 악용하는 악성 코드가 151% 증가했으며, 사이버 범죄 피해 비용은 2021년까지 6조 달러에 이를 것으로 추정되고 있다[2].

본 고에서는 최근에 자동차, 철도, 의료 등의 모든 산업 시스템들이 사물인터넷 기반의 CPS(Cyber Physical System) 패러다임으로 전환되는 흐름을 반영하여, 사이버 보안 사고를 사전에 예방하기 위한 관련 국제 표준 및 위협 분석 기법 동향에 대해 살펴본다.

II. 사이버 보안 개념

사이버 보안이란 무엇일까? 사이버 보안은 사이버 환경에서 네트워크를 통해 연결된 조직/사용자 자산을 보호하기 위해 사용되는 기술적 수단, 보안 정책, 개념, 보안 안전장치, 가이드라인, 위기관리방법, 보안 행동, 교육/훈련, 모범사례, 보안 보증, 보안 기술들의 집합을 의미한다[3].

사이버 보안은 정보 보안과 마찬가지로는 [표 1]의 기밀성(Confidentiality), 무결성(Integrity), 가용성(Availability)을 목표로 한다[4].

[표 1] 사이버 보안의 목표

사이버 보안 목표	설명
기밀성(Confidentiality)	허락되지 않은 사용자 또는 객체가 정보의 내용을 알 수 없도록 함
무결성(Integrity)	허락되지 않은 사용자 또는 객체가 정보를 임의로 수정할 수 없도록 함
가용성(Availability)	허락된 사용자 또는 객체가 정보에 접근하려고 할 때 허용할 수 있도록 함

〈자료〉 Y. R. Hong & D. S. Kim., "Analysis of the Effects of Common Criteria Certification on the Information Security Solutions," Journal of Society for e-Business Studies, 17(4), 2013, pp.57-68.

하지만, 사이버 보안의 3가지 목표는 다양한 공격에 의해서 달성되지 않을 수 있다.

첫째, 기밀성(Confidentiality)은 위장(Impersonation), 스누핑(Snooping), 도청(Sniffing), 백도어(Backdoor), 트로이목마(Trojan Horse) 공격에 의해 위협받을 수 있다. 대표적으로 스누핑이란 네트워크 상의 중요 정보를 모르게 획득하는 행위를 의미하며, 백도어란 정상적인 인증 절차를 거치지 않고, 특정 시스템에 접근하는 행위를 의미한다.

둘째, 무결성(Integrity)은 변장(Masquerading), 스푸핑(Spoofing), 부인(Repudiation) 공격에 의해 위협받을 수 있다. 대표적으로 스푸핑이란 인터넷 프로토콜인 TCP/IP의 구조적 결함을 이용해 사용자의 시스템 권한을 획득한 뒤, 정보를 탈취하는 행위를 의미하고, 부인이란 메시지의 송수신자가 송수신 사실을 인정하지 않는 행위를 의미한다.

셋째, 가용성(Availability)은 서비스 거부(Denial of Service: DoS) 공격에 의해 위협받을 수 있다. 서비스 거부란 특정 시스템에 대량의 접속을 유발해 해당 시스템의 서비스를 마비시키는 행위를 의미한다.

사이버 보안의 목표를 위협하는 공격 유형은 기술이 발전함에 따라 계속해서 진화하고 있고, 우리 삶에 심각한 문제를 초래하고 있으며, 앞으로 더욱 큰 영향을 미칠 것이다. 이러한 문제를 해결하고자 사이버 보안 관련 국제 표준 개발 및 다양한 사이버 보안 위협 분석 기법 연구가 진행되고 있다. 본 고에서는 이와 관련하여 III장에서는 사이버 보안 국제 표준화 동향에 대해, IV장에서는 사이버 보안 위협 분석 기법에 대한 간략한 개요를 살펴본다.

III. 사이버 보안 국제 표준화 동향

사이버 보안 관련 국제 표준은 기존 정보 보안 관리 시스템(Information Security Management Systems)으로 알려진 ISO/IEC 27000 시리즈를 기반으로 사이버 보안에 특화하여 제정 중에 있다. 본 고에서는 [표 2]의 대표적인 사이버 보안 국제 표준에 대해서 살펴본다.

[표 2] 대표적인 사이버 보안 국제 표준 목록(표준 제정 현황은 2019년 8월 기준)

사이버 보안 국제 표준	표준 명칭	제정 현황
ISO/IEC 27100	Information technology -- Cybersecurity -- Overview and concepts	WD
ISO/IEC 27101	Information technology -- Security techniques - Cybersecurity -- Framework development guidelines	WD
ISO/IEC 27102	Information security management -- Guidelines for cyber-insurance	IS
ISO/IEC 27103	Information technology -- Security techniques -- Cybersecurity and ISO and IEC Standards	IS(TR)
ISO/IEC 27032	Information technology -- Security techniques -- Guidelines for cybersecurity	IS(개정 중)

* 국제 표준 제정 단계
  - WD: Working Draft의 약자, 국제표준 워킹그룹에서 초안을 준비하는 단계
  - CD: Committee Draft의 약자, 국제표준 위원회에서 초안을 검토하는 단계
  - DIS: Draft International Standard의 약자, 초안이 등록되어, 모든 위원들의 찬반 의견을 수렴하는 단계
  - FDIS: Final Draft International Standard의 약자, 모든 위원들의 2/3이상 찬성할 경우, FDIS가 됨
  - IS: International Standard의 약자, 최종적으로 국제 표준으로 채택됨
* TR은 Technical Report를 의미
〈자료〉 ISO/IEC 27100: Information technology -- Cybersecurity -- Overview and concepts
ISO/IEC 27101: Information technology -- Security techniques - Cybersecurity — Framework development guidelines
ISO/IEC 27102: Information security management -- Guidelines for cyber-insurance
ISO/IEC 27103: Information technology -- Security techniques -- Cybersecurity and ISO and IEC Standards
ISO/IEC 27032: Information technology -- Security techniques -- Guidelines for cybersecurity

1. ISO/IEC 27100

ISO/IEC 27100의 명칭은 Information technology -- Cybersecurity -- Overview and concepts이고[5], 2019년 8월 기준 WD(Working Draft) 상태이며, 2021년 제정을 목표로 하고 있다. 본 표준은 ISO/IEC JTC 1/SC 27 Information security, cybersecurity and privacy protection에서 담당하고 있다. 주요 내용은 사이버 보안에 관한 전반적인 개념과 시리즈 표준에서 사용되는 사이버 보안 관련 정의를 포함하고 있다.

2. ISO/IEC 27101

ISO/IEC 27101의 명칭은 Information technology -- Security techniques - Cybersecurity -- Framework development guidelines이고[6], 2019년 8월 기준 WD 상태이며, 2020년 제정을 목표로 하고 있다. 본 표준은 ISO/IEC JTC 1/SC 27 Information security, cybersecurity and privacy protection에서 담당하고 있다. 주요 내용은 조직에서 사이버 보안 프레임워크를 개발하고 구축하기 위한 가이드라인을

포함하고 있다. 사이버 보안 프레임워크를 Identify, Protect, Detect, Respond, Recover의 단계로 구분하고, 각 단계별 입력과 출력 그리고 세부 활동을 정의하고 있다. 또한, 국가별 사이버 보안 프레임워크를 소개하고 있다.

3. ISO/IEC 27102

ISO/IEC 27102의 명칭은 Information security management -- Guidelines for cyber-insurance이고[7], 2019년 8월 기준 IS(International Standard) 상태이다. 본 표준은 ISO/IEC JTC 1/SC 27 Information security, cybersecurity and privacy protection에서 담당하고 있다. 주요 내용은 조직 내 사이버 사고로 인한 영향을 관리하기 위한 방안으로서, 사이버 보험을 도입하기 위한 가이드라인을 포함하고 있다. 즉, 사이버 보험 개요, 사이버 보험 정책, 사이버 보험이 커버하는 사이버 사고의 유형, 사이버 보험 지원 측면에서 ISMS(Information Security Management System)의 역할 등의 내용을 담고 있다.

4. ISO/IEC 27103

ISO/IEC 27103의 명칭은 Information technology -- Security techniques -- Cybersecurity and ISO and IEC Standards이고[8], 2019년 8월 기준 IS 상태이다. 본 표준은 ISO/IEC JTC 1/SC 27 Information security, cybersecurity and privacy protection에서 담당하고 있다. 주요 내용은 조직이 정보 보안 표준을 기반으로 사이버 보안 프레임워크를 활용하여 체계적으로 사이버 보안을 관리하기 위한 방법에 대한 내용을 포함하고 있다. 즉, 위험 기반(Risk-based), 우선순위 지정(Prioritized), 성과 중심(Outcome-focused) 등의 속성을 기반으로 하는 사이버 보안 프레임워크의 목표와 활용 방법에 대해서 설명하며, 기존 표준들과의 매핑 정보를 제공한다.

5. ISO/IEC 27032

ISO/IEC 27032의 명칭은 Information technology -- Security techniques -- Guidelines for cybersecurity이고[9], 2019년 8월 기준 IS 상태이고, 개정 중이다. 본

표준은 ISO/IEC JTC 1/SC 27 Information security, cybersecurity and privacy protection에서 담당하고 있다. 주요 내용은 사이버 보안 개요, 사이버 보안과 다른 보안 유형 간의 관계, 이해 관계자의 정의와 사이버 보안에서의 역할, 일반적인 사이버 보안 문제를 해결하기 위한 지침에 대한 내용을 포함하고 있다. 또한, ISO/IEC 27001에 명시된 사이버 보안 프레임워크를 기반으로 맬웨어(Malware), 허가받지 않은 단체의 공격 준비, 공격 탐지 및 모니터링, 공격에 대응하는 모범 사례를 제공한다.

IV. 사이버 보안 위협 분석 기법

사이버 보안 위협 분석은 가상의 공격자 관점에서 시스템의 구조적 취약점과 같은 잠재적인 위협을 식별 및 분류하고, 영향도를 평가하며, 우선순위를 지정하는 프로세스로, 본고에서는 [표 3]의 대표적인 사이버 보안 위협 분석 기법에 대해서 설명한다.

[표 3] 대표적인 사이버 보안 위협 분석 기법 목록

사이버 보안 위협 분석 기법	개발기관/개발자
STRIDE	Microsoft
PASTA	Tony UcedaVelez, Marco M. Morana
OCTAVE	SEI
TVRA	ETSI
STPA-sec	Nancy Leveson, William Young

〈자료〉 Hernan, S., Lambert, S., Ostwald, T., & Shostack, A., "Threat modeling-uncover security design flaws using the stride approach," MSDN Magazine-Louisville, 2006. pp.68-75.
Tony U., & Marco M., "Risk Centric Threat Modeling: Process for Attack Simulation and Threat Analysis," John Wiley & Sons, 2015, pp.1-696.
Christopher A., Audrey D., James S., & Carol W., "Introduction to the OCTAVE Approach," SEI, 2003, pp.1-37.
"ETSI TS 102 165-1 v4.2.3 - Telecommunications and Internet converged Services and Protocols for Advanced Networking(TISPAN); Methods and protocols; Part 1: Method and proforma for Threat, Risk, Vulnerability Analysis," 2011, pp.1-79.
Young, W., & Leveson, N., "Systems thinking for safety and security," In Proceedings of the 29th Annual Computer Security Applications Conference, 2013, pp.1-8.

1. STRIDE

STRIDE(Spoofing identify, Tampering with data, Repudiation, Information

disclosure, Denial of service, Elevation of privilege)는 Microsoft사에서 1999년에 개발한 보안 위협 모델링 방법이다. STRIDE는 인증, 무결성, 부인 방지, 기밀성, 가용성, 권한 부여와 같은 보안 속성을 고려하고, DFD(Data Flow Diagram)의 개체, 프로세스 등에 존재하는 위협을 식별한다[10]. 예를 들어, 사용자란 개체에 Spoofing identify 키워드를 적용할 때, 해커가 사용자로 위장하여, 시스템 접근 권한을 획득한다와 같은 위협을 식별할 수 있다.

[표 4] STRIDE의 위협 분류 및 정의

STRIDE 위협	관련 보안 속성	위협 정의
Spoofing identify	인증(Authentication)	거짓된 계정 등을 이용하여 시스템 접근 권한 획득함
Tampering with data	무결성(Integrity)	불법적으로 데이터를 변경함
Repudiation	부인 방지 (Non-repudiation)	특정 서비스를 수행하지 않았다고 부인하거나 책임이 없다고 부인함
Information disclosure	기밀성(Confidentiality)	접근 권한이 없는 누군가에게 정보를 제공함
Denial of service	가용성(Availability)	서비스 또는 애플리케이션이 정상적으로 수행되지 않게 함
Elevation of privilege	권한 부여(Authorization)	누군가가 권한을 부여받아 권한이 없는 서비스를 수행함

〈자료〉 Hernan, S., Lambert, S., Ostwald, T., & Shostack, A., "Threat modeling-uncover security design flaws using the stride approach," MSDN Magazine-Louisville, 2006. pp.68-75.

2. PASTA

PASTA(The Process for Attack Simulation and Threat Analysis)는 Tony Uceda Velez와 Marco M. Morana가 2012년에 개발한 리스크 기반의 위협 모델링 프레임워크이다. PASTA의 목적은 방어자가 자산 중심의 완화 전략(Asset Centric Mitigation Strategy)을 개발할 수 있는 응용 프로그램 및 인프라에 대한 공격자 중심의 관점(Attacker Centric View)을 제공하는 것이다. PASTA는 동적인(Dynamic) 위협을 식별 및 열거하고, 스코어링(Scoring)하는 등의 7단계 프로세스를 정의하고 있다.

PASTA의 프로세스는 [그림 1]과 같이 비즈니스의 목적을 정의하는 단계(Step 1. Define Objectives), 위협 분석할 인프라, 애플리케이션 등의 범위를 정의하는 단계(Step 2. Define Technical Scope), Use Case, DFD(Data Flow Diagram)를 이용하여 애플리케이션을 분해하는 단계(Step 3. Application Decomposition), 공격 시나리오 분석

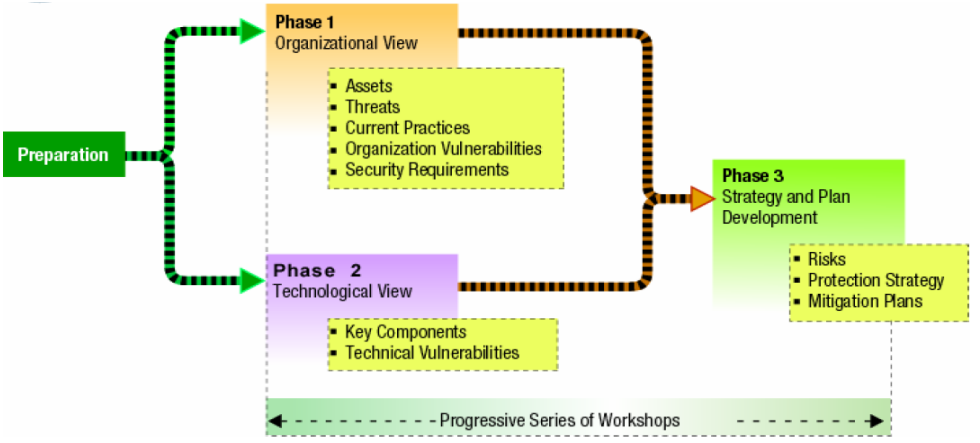
〈자료〉 Tony U., & Marco M., "Risk Centric Threat Modeling: Process for Attack Simulation and Threat Analysis," John Wiley & Sons, 2015, pp.1-696.

[그림 1] PASTA 적용 프로세스

등을 통해 위협을 분석하는 단계(Step 4. Threat Analysis), 취약점을 분석하는 단계(Step 5. Vulnerability & Weakness Analysis), 공격 트리 등을 개발하는 공격 모델링 단계(Step 6. Attack Modeling), 위협에 따른 정성적/정량적 리스크의 영향을 분석하는 단계(Step 7. Risk & Impact Analysis)로 구성되어 있다[11].

3. OCTAVE

OCTAVE(Operationally Critical Threat Asset and Vulnerability Evaluation)는 카네기멜론대학의 SEI(Software Engineering Institute)에서 2003년에 개발한 위협 분



〈자료〉 Christopher A., Audrey D., James S., & Carol W., "Introduction to the OCTAVE Approach," SEI, 2003, pp.1-37.

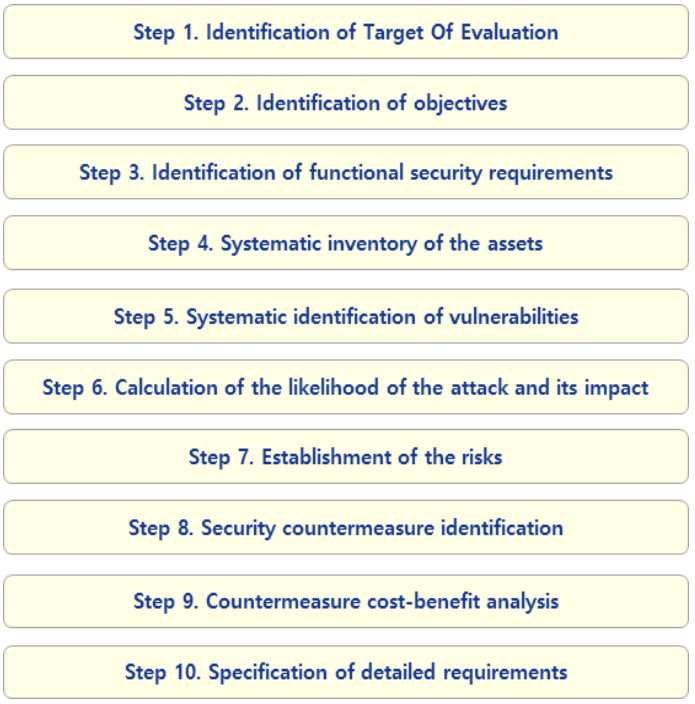
[그림 2] OCTAVE 적용 프로세스

석 및 리스크 평가 방법론이다. OCTAVE의 목적은 조직의 리스크 관리를 체계적으로 수행하기 위해 운영자 중심의 위협 모델링(Operations Centric Threat Modeling) 방법을 제공하는 것이다. OCTAVE는 조직 내부의 전문가들로 분석팀을 구성하여 정보의 수집 및 분석, 전략을 개발하는 등의 자가 진단(Self-Direction) 방식으로 추진한다는 특징이 있다. OCTAVE는 조직의 비즈니스 수행에 필요한 중요 자산과 자산에 대한 위협과 취약성을 식별하고, 리스크를 완화하기 위한 전략을 수립하는 프로세스를 정의하고 있다.

OCTAVE의 프로세스는 [그림 2]와 같이 조직 자산에 기초하여 위협 프로파일을 구축하는 단계(Phase 1. Organizational View), 인프라의 취약성을 정의하는 단계(Phase 2. Technological View), 보안전략 및 계획 개발 단계(Phase 3. Strategy and Plan Development)로 구성되어 있다[12].

4. TVRA

TVRA(Threat, Risk, Vulnerability Analysis)는 ETSI(European Telecommunications Standards Institute)에서 2011년에 통신 시스템의 위협 분석 및 리스크 평가를 위해 개발한 방법론이다. TVRA는 위협의 대상이 되는 주요 자산을 식별하고, 현장에서 개인의



〈자료〉 "ETSI TS 102 165-1 v4.2.3 - Telecommunications and Internet converged Services and Protocols for Advanced Networking(TISPAN); Methods and protocols; Part 1: Method and proforma for Threat, Risk, Vulnerability Analysis," 2011, pp.1-79.

[그림 3] TVRA 적용 프로세스

안전과 주요 인프라의 운영에 미치는 영향에 대해 평가하기 위한 시나리오를 도출한다. 시나리오는 식별된 위협, 해당 위협에 영향을 받는 개체 및 결과를 포함한 관련 조건으로 구성된 가상의 상황을 의미한다.

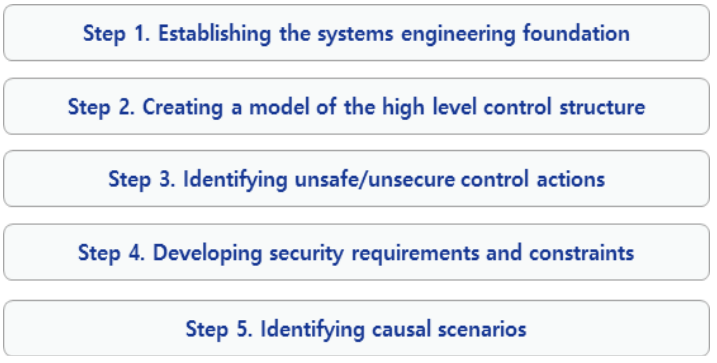
TVRA의 프로세스는 [그림 3]과 같이 평가 대상(Target Of Evaluation)을 식별하는 단계(Step 1. Identification of Target Of Evaluation), 해결해야 할 보안 목표를 식별하는 단계(Step 2. Identification of objectives), 기능적 보안 요구사항을 식별하는 단계(Step 3. Identification of functional security requirements), 자산을 물리적(Physical), 인적(Human), 논리적(Logical) 목록으로 분류하는 단계(Step 4. Systematic inventory of the assets), 취약점을 체계적으로 식별하는 단계(Step 5. Systematic identification of vulnerabilities), 공격 가능성과 영향도를 정량화하는 단계(Step 6. Calculation of the likelihood of the attack and its impact), 리스크(Risks)를 결정

하는 단계(Step 7. Establishment of the risks), 리스크를 완화하기 위한 보안 대책을 식별하는 단계(Step 8. Security countermeasure identification), 리스크 저감 보안 대책에 대해 비용과/이점을 분석하는 단계(Step 9. Countermeasure cost-benefit analysis), 상세한 보안 요구사항을 명세하는 단계(Step 10. Specification of detailed requirements)로 구성되어 있다[13].

5. STPA-sec

STPA-sec(System Theoretic Process Analysis for Security)은 MIT의 Nancy Leveson, William Young이 2013년에 개발한 시스템 이론 기반의 사이버 보안 분석 기법이다. Nancy Leveson 교수가 제안한 STAMP(System Theoretic Accident Model and Processes) 기반의 해저드 분석 기법인 STPA(System Theoretic Process Analysis)를 사이버 보안 분야에 적용한 방법이다.

STPA-sec의 프로세스는 [그림 4]와 같이 시스템이 최종적으로 로스(Loss)를 보는 상황을 식별하는 단계(Step 1. Establishing the systems engineering foundation), 상위 수준의 제어 구조도를 작성하는 단계(Step 2. Creating a model of the high level control structure), 제어 명령(Control Action)이 로스로 이어질 수 있는 잘못된 경우를 식별하는 단계(Step 3. Identifying unsafe/unsecure control actions), Unsafe/Unsecure한 제어 명령을 완화하거나 제거하기 위한 보안 요구사항과 제약사항을 개발하



〈자료〉 Young, W., & Leveson, N., "Systems thinking for safety and security," In Proceedings of the 29th Annual Computer Security Applications Conference, 2013, pp.1-8.

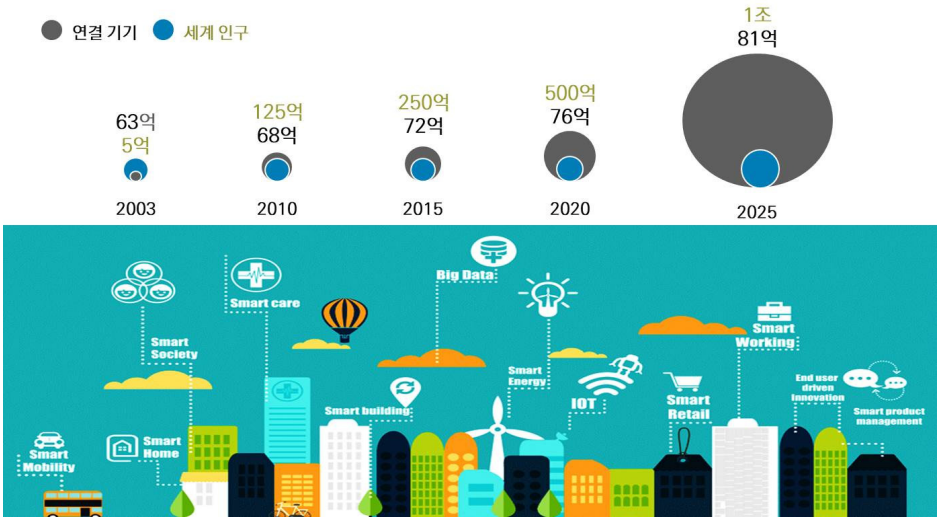
[그림 4] STPA-sec 적용 프로세스

는 단계(Step 4. Developing security requirements and constraints), 보안 요구사항과 제약사항을 위반할 수 있는 다양한 시나리오를 분석하는 단계(Step 5. Identifying causal scenarios)로 구성되어 있다[14].

이 외에도 LINDDUN(Linkability, Identifiability, Nonrepudiation, Detectability, Disclosure of Information, Unawareness, Noncompliance)[15], CVSS(Common Vulnerability Scoring System)[16], Attack Tree[17], Security Cards[18], HTMM (Hybrid Threat Modeling Method)[19], Trike[20], VAST(Visual, Agile, and Simple Threat) Modeling[21] 등 다양한 사이버 보안 위협 분석 기법이 활용되고 있다.

V. 맺음말

최근 전 세계를 대상으로 하는 사이버 보안 사고가 계속해서 증가하고 있다. 특히, 사물인터넷 혁명으로 인해 [그림 5]와 같이 자동차, 철도, 의료 등의 모든 산업 시스템들의 경우 외부와의 연결이 급격히 증가함에 따라[22], 이로 인한 사이버 보안 사고는 더욱 증가할 것이다.



〈자료〉 Evans, D., "The internet of things: How the next evolution of the internet is changing everything," CISCO white paper, 2011, pp.1-11.

[그림 5] 사물인터넷 혁명으로 인한 시스템의 연결성 증가

이에 미국과 영국 등 선진 국가를 중심으로 사이버 보안 전담 부처 또는 기관을 설립하여 대응 전략을 시행하는 등 정책적인 노력을 하고 있다. 또 한편으로는 사이버 보안 필수 시스템의 체계적인 개발을 위해 국제 표준 및 사이버 보안 위협 분석 기법에 관한 연구가 활발히 진행 중에 있다.

이의 일환으로 본 고에서는 사이버 보안 관련 국제 표준으로 ISO/IEC 27100, ISO/IEC 27101, ISO/IEC 27102, ISO/IEC 27103, ISO/IEC 27032에 대한 개요와 제정 현황을 소개하였다. 또한, STRIDE, PASTA, OCTAVE, TVRA, STPA-sec 등의 사이버 보안 위협 분석 기법의 소개와 프로세스를 살펴보았다.

본 고에서 살펴본 사이버 보안 관련 국제 표준이 제정되면, 시스템 개발에 반드시 적용하도록 요구할 것이다. 또한, 관련된 사이버 보안 위협 분석 기법에 대해서도 적용을 요구할 것이다. 이미 선진 조직들은 사이버 보안 표준에서 요구하는 내용과 위협 분석 기법을 적용한 연구들을 발표하고 있다. 하지만 국내 조직들은 이러한 흐름에 많이 뒤쳐진 것이 현실이다.

국내 조직들은 시스템의 안전성 확보를 위해 관련 표준과 해저드 분석 기법 적용에 집중해 왔다. 이제는 사이버 보안과 안전성을 통합하는 연구로 흐름이 변화하고 있다. 국내 조직들이 이러한 흐름을 이해하고, 적용할 수 있도록 관련 역량을 확보하기 위한 다양한 연구와 국가적 지원이 필요하다.

[참고문헌]

[1] 최양희, “지능정보사회 중장기 종합대책 추진방향”, 관계부처 합동, 2016, pp.1-72.
[2] Chuck Brooks, “A Scoville Heat Scale For Measuring Cybersecurity,” Forbes, 2018.
[3] 심현보, “정보 보안에서 사이버 보안까지”, 한국과학기술정보연구원, 2014. pp.1-5.
[4] Y. R. Hong & D. S. Kim., “Analysis of the Effects of Common Criteria Certification on the Information Security Solutions,” Journal of Society for e-Business Studies, 17(4), 2013, pp.57-68.
[5] ISO/IEC 27100: Information technology -- Cybersecurity -- Overview and concepts.
[6] ISO/IEC 27101: Information technology -- Security techniques - Cybersecurity -- Framework development guidelines.
[7] ISO/IEC 27102: Information security management -- Guidelines for cyber-insurance.
[8] ISO/IEC 27103: Information technology -- Security techniques -- Cybersecurity and ISO and IEC Standards.

[9] ISO/IEC 27032: Information technology -- Security techniques -- Guidelines for cybersecurity.
[10] Hernan, S., Lambert, S., Ostwald, T., & Shostack, A., "Threat modeling-uncover security design flaws using the stride approach," MSDN Magazine-Louisville, 2006. pp.68-75.
[11] Tony U., & Marco M., "Risk Centric Threat Modeling: Process for Attack Simulation and Threat Analysis," John Wiley & Sons, 2015, pp.1-696.
[12] Christopher A., Audrey D., James S., & Carol W., "Introduction to the OCTAVE Approach," SEI, 2003, pp.1-37.
[13] "ETSI TS 102 165-1 v4.2.3 - Telecommunications and Internet converged Services and Protocols for Advanced Networking(TISPAN); Methods and protocols; Part 1: Method and proforma for Threat, Risk, Vulnerability Analysis," 2011, pp.1-79.
[14] Young, W., & Leveson, N., "Systems thinking for safety and security," In Proceedings of the 29th Annual Computer Security Applications Conference, 2013, pp.1-8.
[15] Wuyts, K., & Joosen, W., "LINDDUN privacy threat modeling: a tutorial," 2015, pp.1-38.
[16] Mell, P., Scarfone, K., & Romanosky, S., "Common vulnerability scoring system," IEEE Security & Privacy, 4(6), 2006, pp.85-89.
[17] Potteiger, B., Martins, G., & Koutsoukos, X., "Software and attack centric integrated threat modeling for quantitative risk assessment," In Proceedings of the Symposium and Bootcamp on the Science of Security, 2016, pp.99-108.
[18] Tamara D., Batya F., Tadayoshi K,, "Poster - the security cards: a security threat brainstorming toolkit," University of Washington, 2013.
[19] Mead, N., Shull, F., Vemuru, K., & Villadsen, O., "A Hybrid Threat Modeling Method," Carnegie Mellon University - Software Engineering Institute, 2018, pp.1-53.
[20] Saitta, P., Larcom, B., & Eddington, M., "Trike v1 methodology document," 2005, pp.1-17.
[21] Agarwal, A., "Vast methodology: Visual, agile, and simple threat modeling," Prescott Valley, 2016.
[22] Evans, D., "The internet of things: How the next evolution of the internet is changing everything," CISCO white paper, 2011, pp.1-11.