

제어시스템 인증평가 동향 및 검증방안

植田 修*

*情報セキュリティ大学院大学
e-mail : mgs145101@iisec.ac.jp

Trend and verification measures of certification evaluation in control system

Osamu Ueda*

*Institute of Information Security

요약

최근 중요 인프라 업계에서 주로 다뤄지는 제어시스템을 표적으로 한 사이버 공격으로 Stuxnet에 이어 Havex RAT, BlackEnergy2 라고 하는 멀웨어(Malware)를 이용한 사건이 많이 증가하고 있다. 제어시스템의 새로운 공격 방법에 대한 대책으로 시스템 입구와 내부조직에 대한 대책을 강화하기 위한 필요성이 요구되어 왔지만 그러한 대책은 한정되어 있다. 본 논문에서는 보안 대책에 필요한 인증 취득에 있어서 기준이 되는 국제 표준인 ISASecure®EDSA 인증제도에 착목했다. 인증평가는 요구사항이 중복되는 불필요한 인증평가 작업을 최소화 하는 것으로 인증 취득 시 발생되는 코스트를 절감할 수 있으며 기존의 정보 보안 관리체계(ISMS)의 인증을 취득하고 있는 기업이나 조직이면 제어시스템의 인증 기준으로 추가된 차분 요건만으로 취득이 가능 할 수 있을 것으로 상정된다. 이러한 제어시스템의 보안을 구현하기 위해 IACS(Industrial Automation and Control System)에서 표준화로 제정한 IEC62443 시리즈를 참조하여 세계각국에서 사용되는 제어시스템을 대상으로 인증(EDSA) 요구사항의 차분을 도출하는 수법을 제안하고자 한다

Keywords :IACS, EDSA, CSMS, Certification Assessment

1. 서론

최근 중요 인프라 업계에서 주로 다루어지는 제어시스템을 대상으로 한 사이버 공격으로 Stuxnet에 이어 Havex RAT, BlackEnergy2 같은 악성 코드에 의한 사고가 증가하고 있다. 이러한 사이버 공격의 위협에 의해 IACS (Industrial Automation and Control System) 가 정지 할 경우 사회 인프라 및 비즈니스 연속성에 영향을 미칠뿐만 아니라 HSE (Health, Safety , Environment)에 대해 심각한 영향을 줄 가능성성이 높다[1].

2014년 12월 2일 일본 경찰청에서는 산업 제어 시스템에 사용되는 특정 PLC 의 소프트웨어에서 원격으로 임의의 코드를 실행하는 위협이 취약점으로 공개되었다. 이와같이 해당 취약점을 표적으로 한 액세스를 관측하여 볼때 고난도에 공격이 이루어지고 있음을 추측할 수 있다.

이러한 제어 시스템의 새로운 공격에 입구 대책이나 내부 대책의 필요성이 요구되어 왔지만 그 대책은 한정되어 있었다. 한편 증가하는 취약점과 위협에 대한 기술적, 관리적, 물리적 및 정책 조치의 보안대책은 외부 기관에 의해 보안 평가를 하는 것이 중요시되어 지면서 많은 보안 표준이 책정되었다.

따라서 개별 보안인증 취득에 관해서도 보안대책 요구항목에 대한 망라성의 문제나 표준에 관한 전문 지식을 요구하는 문제가 있어 통합적으로 취급하는 환경은 아직 갖추어지지 않고 있다. 아울러 보안 인증이라고 해도 종류가 매우 많아 각각의 인증을 취득하는 것이 용이하다 라고는 말하기 어렵다.

본 연구는 보안 인증 취득에 있어서 다양한 문제를 고찰하고 인증시 기준이 되는 국제 표준 ISASecure®EDSA 인증 제도에 착목했다. 인증 평가는 요구사항이 중복 된 불필요한 인증 평가 작업을 최소화 하는 것이 인증 비용을 절감할 수 있다.

이에 따라 기존의 정보 보안 관리 체계 (ISMS) 인증을 취득하고 있는 기업이나 조직이라면 제어 시스템에서 추가 된 차분의 요구 사항만으로 취득이 가능 할 수 있을 것으로 상정된다. 이러한 제어 시스템 보안을 구현하기 위해 IACS 가 표준화로 제정한 IEC62443 시리즈를 참조하여 세계각국에서 사용되는 제어 시스템을 대상으로 인증 (EDSA) 요구사항의 차분을 도출하는 수법을 제안하고자 한다.

2. 제어시스템의 보안표준화

2.1 국제 표준의 IEC62443 채용

제어 시스템의 보안 표준은 실로 다양하며 산업 분야별로 국제 표준, 업계 표준으로 책정되어 있다. 그 중에서도 일반적인 표준으로 주목 받고 있는 것이 IEC62443이다. 이미 해외 사업자의 조달 요구 사항으로 포함되는 경향이 있다. 지금까지 선행으로 업계에서 평가인증을 해온 ISCI (ISA Security Compliance Institute)의 WIB 기준도 IEC62443 시리즈에 통합되는 움직임이 보여지고 있다. 현재 CSMS 인증은 일본에서 선행되고 있으며 반면 EDSA 인증은 미국이 선행하여 제어 시스템의 보안 향상을 위한 표준화 제정을 진행하고 있다. Fig.1은 제어 시스템 분야의 표준 규격 관계 및 분야별 명칭을 나타낸다[2].

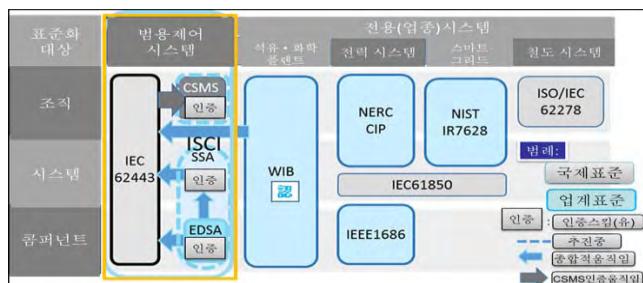


Fig.1. Standard relationship and the name of the sector control systems

2.2 IEC62443 구성

국제표준 제정까지 도달하여 있는 조직은 ISA 의 ISA99 이다 .ISA99 는 ISA62443 시리즈로 표준화 안을 작성하고 IEC TC 65 / WG 10 에서 각국의 심의를 거쳐 IEC 62443 문서 시리즈로서의 국제표준이 된다. 현재 IEC62443 시리즈는 Table 1 와 같이 13 권으로 구성 되어 있으며 이중에 IEC62443-1-1, IEC62443-2-1, IEC62443-3-1, IEC62443-3-3 은 표준이 개발 제정되어 있는 상태이며 최근 2015 년 12 월 1 일 IEC62443-2-2, IEC62443-2-3 을 제정하여 발표했다[3].

Table.1 Standardization and evaluation of the ISA / IEC 62443 Certification status

File Reference	IEC Reference	Date	Type	Work Group	Task Group	Status	Comments
ISA-TR62443-6-3		N/A	Draft environment of ANSI/ISA-TR62443-6-3	WIB	WG2	Published	This is an internal committee working document, prepared for use in assessing gaps in existing work products in light of industry developments.
ISA-62443-1-1	IEC62443-1-1	IEC/TR 62443-1-1	Needs and concepts	Draft	WG1	N/A	This was originally published as an IEC standard, IEC TR 62443-1-1:2007, as part of the IEC 62443 series. It is currently being revised to make it current with other documents in the series, and to clarify normative content.
ISA-TR62443-1-2	IEC62443-1-2	IEC/TR 62443-1-2	Handy glossary of terms and abbreviations	Draft	WG1	Under Development	This is a technical report, which will be published as an IEC standard. It is available on the IEC website. This report will likely be the last in the series to be finalized.
ISA-62443-1-3	IEC 62443-1-3	IEC 62443-1-3	System security competence maturity	Draft	WG12	N/A	A second committee draft for comment will soon be circulated. This standard will be submitted to IEC for approval and revision as an IEC standard.
ISA-TR62443-1-4	IEC62443-1-4	IEC62443-1-4	Security life cycle and use	Draft	TBD	TBD	Proposed
ISA-62443-2-1	IEC 62443-2-1	IEC 62443-2-1	Requirements for an IACS security management system	Draft	WG12	N/A	CSMS
ISA-TR62443-2-2	IEC62443-2-2	IEC62443-2-2	Implementation guidance for IACS security management system	Draft	WG12	N/A	This standard was initially published as IEC TR 62443-2-2. It has been updated and revised to include new and comments. Comments received are addressed to the work group.
ISA-TR62443-2-3	IEC62443-2-3	IEC62443-2-3	Patch management in the IACS environment	Draft	WG12	N/A	This proposed standard will build on the content of IEC 62443-2-2, focusing on patch management in the IACS environment. The two cases have will be strong alignment with the ISO 27000 series of standards.
ISA-62443-2-4	IEC 62443-2-4	IEC 62443-2-4	Requirements for IACS solution	Draft	TC65/SC10/IG01	N/A	The USA version of this document (ISA-TR62443-2-4) has been approved and published as an IEC standard. The equivalent IEC version (IEC TR62443-2-3) is also available.
ISA-TR62443-3-1	IEC62443-3-1	IEC62443-3-1	Security techniques for IACS	Draft	WG1	N/A	This technical report was previously issued as ANSI/ISA-TR 62443-3-1. It is updating the content to reflect currently available IEC committee draft for vote.
ISA-62443-3-2	IEC 62443-3-2	IEC 62443-3-2	Security risk assessment and systems design	Draft	WG12	Comments Draft	SSA
ISA-62443-3-3	IEC 62443-3-3	IEC 62443-3-3	System security requirements and security levels	Draft	WG12	TBD	Published
SA-62443-4-1	IEC 62443-4-1	IEC 62443-4-1	Product development	Draft	WG12	TBD	The USA version of this standard has been approved and published as an IEC standard. The next revision will be submitted for approval to the committee voting members.
SA-62443-4-2	IEC 62443-4-2	IEC 62443-4-2	Toolbox security assessments	Draft	WG12	TBD	A second committee draft for comment has been circulated and the comments received are addressed to the work group.

Source: <http://isa99.isa.org>

2.3 IEC62443 개요

IEC62443 표준을 사용하여 보안평가, 인증을 진행하기 위하여 ISCI 가 설립 되었으며 평가용 표준인증 프레임워크를 마련 하였다. 현재 제어기기 평가인증 프레임워크를 사용하여 제어시스템 인증을 부분적으로 시작했다[4].

IEC62443 시리즈은 4 개의 시리즈로 구성되어 있으며 1,2,3,4)에서 상세하게 설명하고 있다.

1) 시리즈 1

IEC62443-1 은 개념 모델, 용어 등 일반적인 사항을 규정하고 있다.

2) 시리즈 2

IEC62443-2 는 제어 시스템을 보유하는 조직에 대한 보안, 즉 보안정책과 관리 시스템에 대해 규정하고 있다. 특히 IEC62443-2-1 에 대해서는 CSMS (Cyber Security Management System for Industrial Automation and Control System)로서 제어 시스템의 제조나 운영 프로그램을 실시 하고 있는 기업의 보안 관리시스템의 인증이 시작되고 있다. 또한 IEC 62443-2-4 는 공급 업체, 시스템 통합 업체의 의견을 받아 들여 다른 IEC 62443 시리즈와의 요구요건 중복을 해소하고, 심사자의 암묵지에 의한 판단이 문서화되도록 IEC TC65 / WG 10 에서 진보적 심의가 계속되어 곧 표준으로 공개 되어질 예정이다.

3) 시리즈 3

IEC62443-3 은 시스템 통합을 위한 제어 시스템에 대한 보안 기능 요구 사항을 규정하고 있다. 요구 사항으로는 식별, 인증 (FR1) 사용 제어 (FR2) 시스템 무결성 (FR3) 데이터 기밀성 (FR4) 데이터 제한 성 (FR5) 응답성 (FR6), 자원 가용성 (FR7))의 7 개의 항목이 있고, 제어 시스템의 위험을 줄이기 위해 필요한 강도를 가진 기능 요구 사항 (FR1 ~ FR7)을 선택하여 설계, 구현을 실시하게 된다.

4) 시리즈 4

IEC62443-4 는 제어 시스템을 구성하는 제어기기, 장비, 애플리케이션의 보안을 취급하는 장비 업체를 위한 보증 요구 사항과 기능 요구 사항이 규정 될 예정이며 현재 표준화가 진행되고 있다. 이에 앞서 ISCI 는 IEC62443 의 프레임워크를 사용하여 임베디드 디바이스의 보안에 초점을 맞춘 ISA Secure® EDSA 인증을 시작했다.

3. 제어시스템의 인증동향

3.1 보안 인증

제어 시스템을 구성하는 각 제품이나 시스템 전체가 업계와 표준 단체에 의해 규정 된 보안기준을 충족하고 있는지를 제삼자 기관이 인증하는 주요 인증 프로그램은 이미 Table2 와 같이 존재한다. 그 중에서도 유력한 것이 국제계측제어학회 (ISA)의 회원을 중심으로 한 비영리단체 ISCI (ISA Security Compliance Institute)가 제공하는 인증프로그램 EDSA (Embedded Device Security Assurance)이다.

Table.2 System security main certification program

인증 프로그램	ISASecure	Achilles	WIB
대상	Component System	Component	Control System
표준	업계 표준(ISA/ISCI)	업계 표준	업계 표준
형태	국제 학회 주도	Worldtech 사(Canada)	민간 단체(Oleanda shell) 등
제공 방법	표준 평가+Tool 제작형	Tool 제공형	표준 평가형+Tool 제작형
내용	미국 ISCI가 작성한 Component System에 관한 System(SSA) 인증 프로그램	Worldtech사가 제작하고 있는 Component System vendor에 보안 조달 요청을 규정한 Worldtech사의 Achilles Test Platform을 표준 인증 사용	유럽 석유 Major가 중심이 되어 Component System vendor에 보안 조달 요청을 규정한 Worldtech사의 Achilles Test Platform을 표준 인증 사용
특징	IEC62443에 Capture 필 전망	원격으로 부터 remote test 가능	IEC62443-2-4 규격으로 국제 표준화 되어질 전망

3.2 EDSA 평가기준

ISASecure®EDSA은 3 가지 인증으로 구성되어 있으며 소프트웨어 개발 보안 평가인 (SDSA), ICS 구성장치에 대한 기능성 보안평가(FSA), 기기의 통신 장인도 테스트(CRT)평가에 있어 상정 위협 요소를 충분히 카バー 할수 있는지에 대한 범위를 검증한다. Fig.2은 도큐먼트 체계를 나타내며 평가 등급체계 Fig.3은 LEVEL1,2,3으로 구성되어 있으나 각각에 평가 항목수가 있다.

level1(SDSA(136),FSA(19)),level2(SDSA(155),FSA(48),FSA(48)),level3(SDSA(174),FSA(82))로 평가 항목이 있고 CRT(78)은 LEVEL에 관계없이 항목수는 동일하다[5].

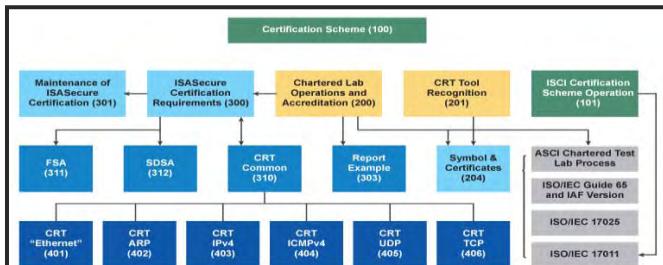


Fig.2. ISASecure EDSA Certification Scheme Document Systems Source: <http://isasecure.org>

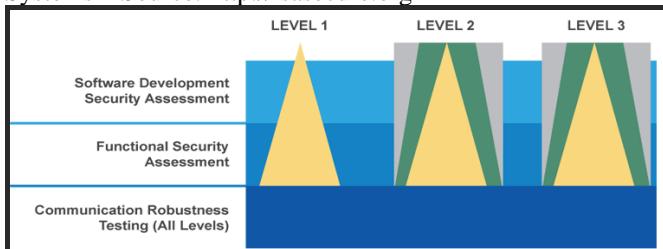


Fig.3. Safety Integrity Level' Certification (ISO/IEC 61508)
Source: <http://isasecure.org>

3.3 국제 상호승인의 인증 FRAMEWORK

EDSA 인증은 미국 ANSI/ACLASS가 실시하고 그 결과를 Scheme owner에게 보고함으로서 인증기관으로 등록하게 된다. 현재는 미국 주체의 스키ーム이 되어 있다. 아울러 일본에서는 2013년 8월 경제산업성 주도로 CSSC에 독립적인 CSSC 인증 연구소(laboratory)를 설립하고 ISASecure EDSA 인증을 추진하여 국제적 상호인정의 목적으로 2014년 1월부터 일본 국내에서 일본어로 세계공통의 인증 취득을 실시하고 있다[6].

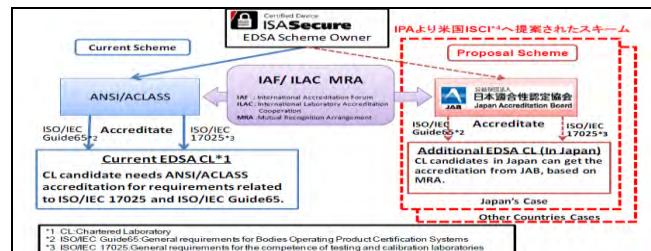


Fig.4. Safety Integrity Level' Certification (ISO/IEC 61508)
Source: <http://www.ipa.go.jp>

4. 제안 평가 방법

4.1 개요

IEC(62443) 시리즈를 데이터로 사용하여 제어 시스템을 대상으로 한 인증(EDSA) 요구사항의 차분을 도출할 수 있는 수법을 Fig.5에서 나타내고 있으나 현재까지의 조사로서는 인증취득 실적이 없다.

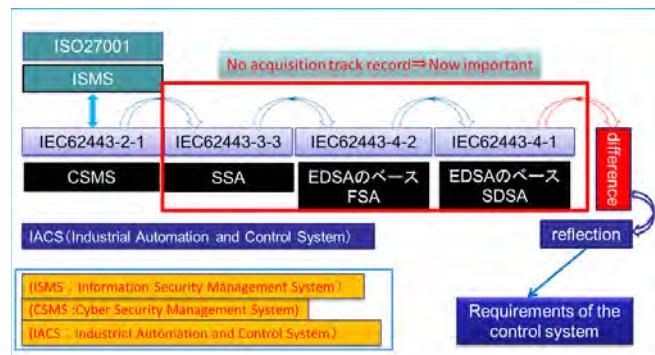


Fig.5. Procedure of detection method of EDSA of request

4.2 CSMS 와 ISMS 관계

IACS(Industrial Automation and Control System)의 구축, 운용을 담당하는 조직에서 보안의 근본적인 향상을 위해 보안 관리시스템의 구조가 필요하다. IEC 62443 시리즈는 제어시스템 보안 구현에 활용할 수 있는 기준의 하나인 IACS 보안 관리시스템으로 IEC 62443-2-1가 규격화 되어 있다. 또한 ISMS(ISO/IEC 27001) 및 CSMS(62443-2-1) 규격을 평가인증 대상으로 사용하여 ISMS에 포함되지 않은 CSMS 고유 요구사항을 차분으로 두고 ISMS와 병행하여 인증 평가를 실시한다. IEC 62443-2-1은 IACS 분야의 보안 관리시스템 인증으로 CSMS(Cyber Security Management System) 인증 기준(IEC 62443-2-1:2010)이 책정되었다[7].

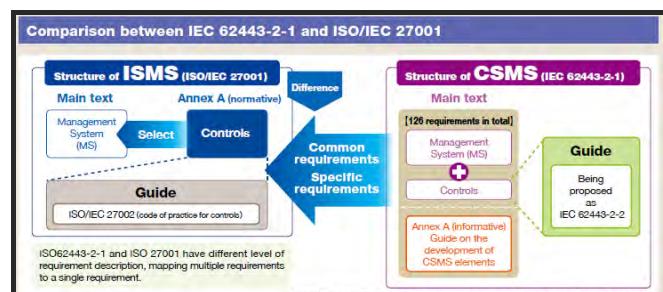


Fig.6. Comparison between IEC62443-2-1 and ISO/IEC 27001

4.3 IEC62443-2-1 와 IEC62443-3-3 대응 관계

IEC62443-2-1 의 보안 관리시스템 구축을 실현하는데 있어 기술적 요건을 어떻게 구현할 수 있는지가 중요한 과제다. IEC62443-3-3 은 시스템의 보안 요구 사항을 규정하고 있으므로 요건을 준수하여 시스템의 보안 구현이 가능하면 기준간의 연계 및 정합성을 포함해 일관성으로 취할 수 있다. 따라서 본절에서는 IEC62443-2-1 에 있어서 기술요건이 IEC62443-3-3 의 기술요건에 어느 정도 커버 할 수 있는지를 검증한다. IEC62443-2-1 에서 기재되어 있는 요건 중 기술요건으로 ISA-62443-3-3 에 대응요건이 기재되어 있는 주요한 요건대응 관계의 예를 Table.3 에서 일부 나타내고 있다[8].

Table.3 IEC62443-2-1 correspondence ISA62443-3-3

또한 IEC62443-2-1의 보안 대처안, 장치구현이 카테고리내에 기술적인 요구사항이 ISA-62443-3-3의 요구사항에 따라 서포트 가능한지 검증결과를 정리하면 Table4에 나타낸 바와 같이 70% ~ 90%의 요구사항이 포함되어 있는 것을 알 수 있다.

따라서 IEC62443-2-1에 기술 요구사항의 실현에 임해 대부분은 IEC62443-3-3 대응 부분의 보안 요구사항을 참조하면 된다. 대응 요구사항이 없는 항목에 대해서는 시스템에 따라 다른 기존의 기준안을 인용할 필요가 있다.

Table.4 IEC62443-2-1 and ISA62443-3-3 of relationship

Category ⁽²⁾	요건분류 ⁽²⁾	IEC62443-2-1 요건수 ⁽²⁾	IEC62443-3-3 요건수 ⁽²⁾	비율 ⁽²⁾
사업상의근거 ⁽²⁾	운영 ⁽²⁾	1 ⁽²⁾	0 ⁽²⁾	0% ⁽²⁾
리스크식별 ⁽²⁾	운영 ⁽²⁾	14 ⁽²⁾	0 ⁽²⁾	0% ⁽²⁾
보안정책 ⁽²⁾	운영 ⁽²⁾	27 ⁽²⁾	0 ⁽²⁾	0% ⁽²⁾
보안대향안 ⁽²⁾	기술 ⁽²⁾	19 ⁽²⁾	17 ⁽²⁾	89% ⁽²⁾
	운영 ⁽²⁾	22 ⁽²⁾	0 ⁽²⁾	0% ⁽²⁾
장치구현 ⁽²⁾	기술 ⁽²⁾	10 ⁽²⁾	7 ⁽²⁾	70% ⁽²⁾
	운영 ⁽²⁾	19 ⁽²⁾	0 ⁽²⁾	0% ⁽²⁾

4.4 IEC62443 의 대응관계 FLOW

IEC62443-2-1 및 IEC62443-3-3 의 관계에 대해 분석을 실시했다. 그 결과 IEC62443-2-1 의 요구 사항 중 기술적인 대책이 요구 조건에서 IEC62443-3-3 에 준거 한 시스템을 도입하는 효과가 밝혀졌다. 시스템의 보안 요구 사항인 IEC62443-3-3 와 향후 공개되는 장

비, 장치의 보안 요구 사항인 IEC62443-4-2 와 대응을 분석해 보면 Fig.7 과 같이 기준 간의 연계와 일관성이 명확하여 현재 집필중에 있는 IEC62443-4-1 도 포함하여 고찰하면 전체적인 보안의 실현에 활성화가 될 것으로 보여진다.

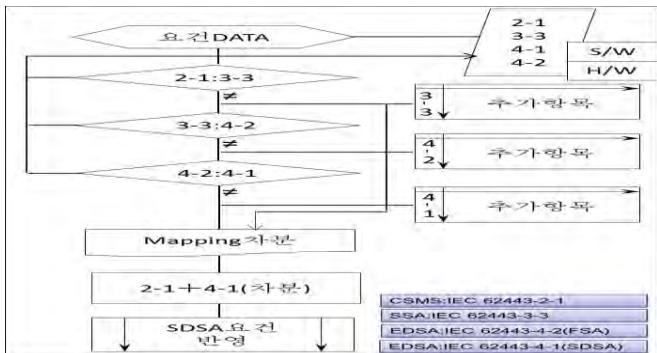


Fig.7. Certification Evaluation Flow

5. 결론

본 논문에서는 인증 평가에 대하여 중복되는 불필요한 인증 평가 작업을 최소화하는 것으로 인증 취득 시 발생되는 코스트를 절감하는 방법에 대해 논하였다. 아울러 기존의 정보보안 관리체계(ISMS) 인증을 취득하고 있는 기업이나 조직이면 제어 시스템의 인증 기준으로 추가 된 차분 요건만으로 취득이 가능할 수있을 것으로 상정된다. 이러한 제어 시스템의 보안을 구현하기 위해 IACS(Industrial Automation and Control System)에서 표준화로 제정 한 IEC62443 시리즈를 참조하여 세계각국에서 사용되는 제어 시스템을 대상으로 인증(CSMS,EDSA,SSA)평가를 하는데 있어서 요구 사항의 차분을 도출하는 방법에 대해 관계 증명과 함께 제안 하였다.

References

- [1] Japan Computer Emergency Response Team. Coordination Center Mar.,2015
 - [2] Hideaki KOBAYASHI, "Increasing Number of Cyber Attacks against Social Infrastructure," Information Processing , Vol.55 No.7,pp660-665,Jul.,2014
 - [3] http://isa99.isa.org/ISA99%20Wiki/WP_List.aspx
 - [4] Tatsuaki Takebe, "Trends in Industry Standards and International Standards for Industrial Automation Control System Security , Yokogawa Technical Report Vo 1.57 No.2(2014)
 - [5] <http://isasecure.org/en-US/Certification/IEC-62443-4-2-EDSA-Certification>
 - [6] <http://www.ipa.go.jp/files/000026445.pdf>
 - [7] <http://www.isms.jipdec.or.jp/csms/doc/JIP-CSMS120E-10.pdf>
 - [8] <https://www.ipa.go.jp/files/000014265.pdf>
 - [9] Satoru Ota, et al. " Proposal and implementation of related information creation method of international standard in the security assessment platform, " Information Processing , the 76th National Convention of 4 (2014): 5. pp555-556
 - [10] <https://www.ipa.go.jp/files/000026445.pdf>