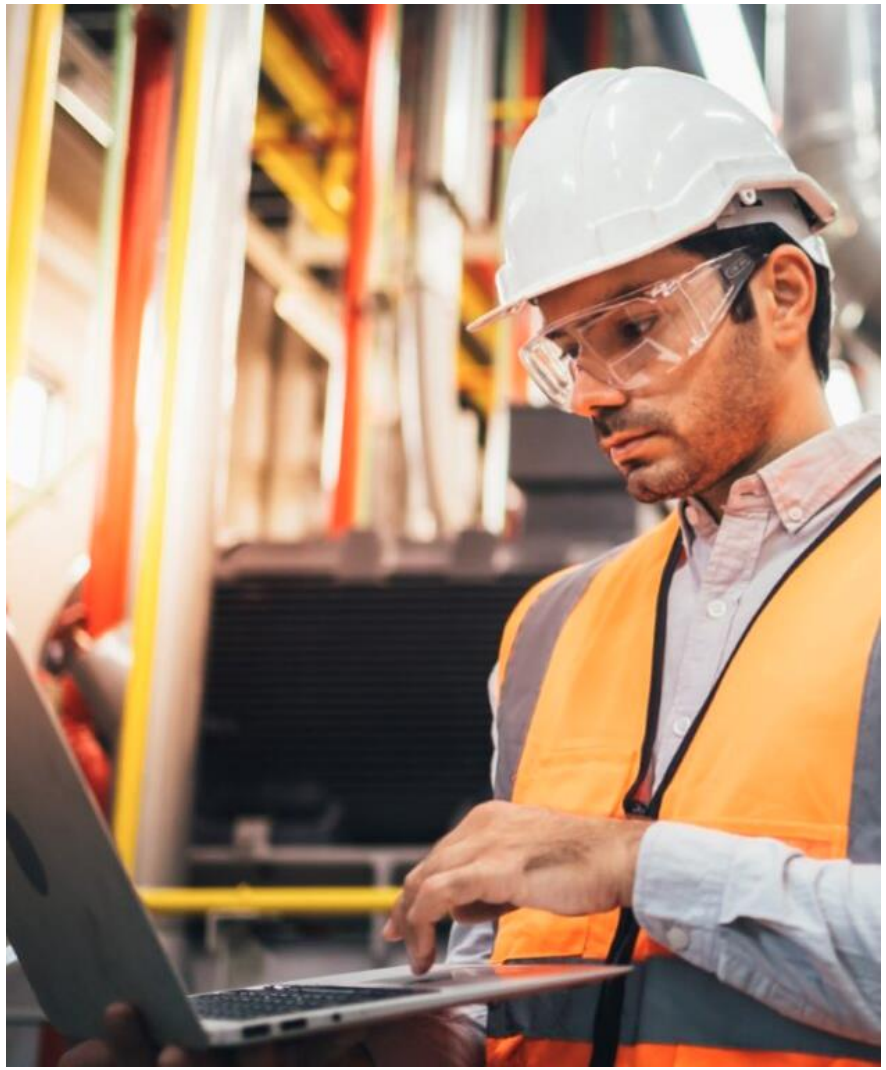
사이버보안 동향 및 협동로봇 인증 대응위한 고려사항

IEC 62443 Series Assessment and Certification

SGS KOREA | 박소연 사이버보안 팀장 | 2023/10/19

WHEN YOU NEED TO BE SURE SGS



Content

- SGS/ SGS Brightsight 소개
- 사이버보안의 현재
- IEC 62443란?
- SGS 서비스 소개

SGS IS THE WORLD'S LEADING INSPECTION, VERIFICATION, TESTING AND CERTIFICATION COMPANY

140

YEARS OF ADDING VALUE TO SOCIETY

97,000

EMPLOYEES AROUND THE WORLD

2,600

OFFICES AND LABORATORIES

SGS Brightsight

SGS Brightsight Introduction

SGS, 2021년 네덜란드 독립 사이버보안 평가 연구소 브라이트사이트 인수.

1 최고 수준의 독립 보안 평가 연구소

11 전세계 11개의 연구소

10+ 공통평가인증(CC) 연구소 인가

35+ 다년간의 보안 평가 경험

170+ 보안 평가 전문가

700+ 매년 보안 프로젝트 수행

Payment	Telcom	Government (ID)	IC multi-purpose	Industrial	IoT	Automotive	Space	Medtech	Tools

Robot Industry
사이버보안의 현재

로봇 활용의 확대

제조업

교육/서비스업

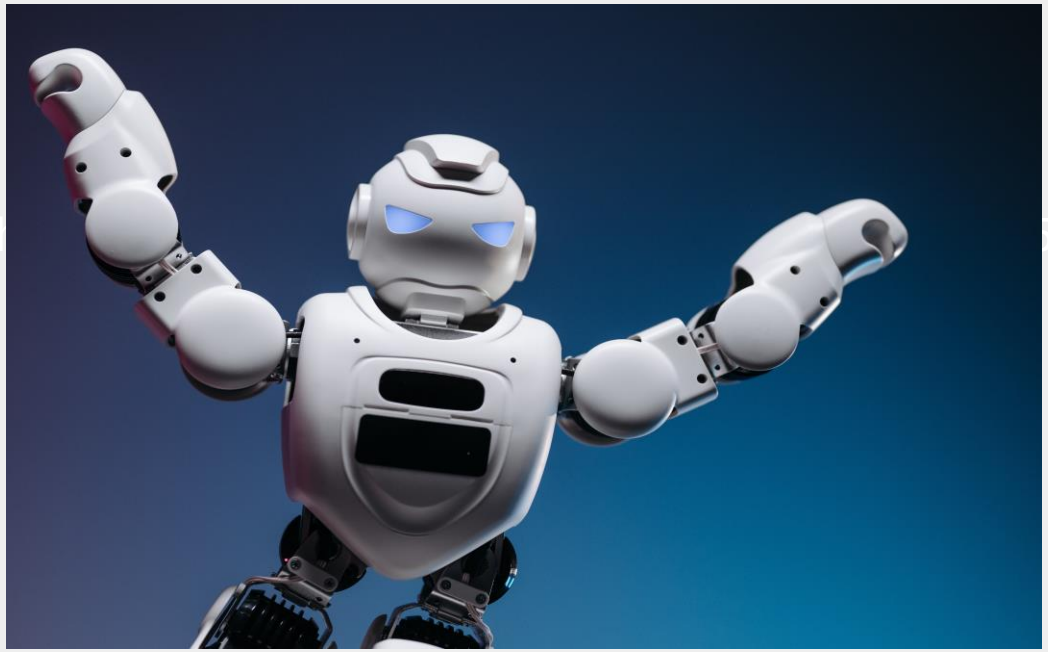
의료업

물류/유통업

로봇 사이버보안의 중요성

- **로봇 해킹 시연**

로봇이 흉기가 된다?..."해킹 당하면 사람 공격"
(2017.08.26/YTN)



https://youtu.be/RX_aLJ2QsVQ?si=1hAOaDzuIn5rOnsQ

- **체스 게임 사건**

체스 시합하던 로봇, 7살 어린이 손가락 '뚝'
(2022.07.26/뉴스투데이/MBC)

https://youtu.be/ekl8L42QBjQ?si=S8pexRuLNkUBQxMA

사이버보안 관련 정책 및 표준

EU 선언

- **EHSR**(**E**ssential **H**ealth and **S**afety **R**equirements) 사이버보안 항목 신설

참고: https://eur-lex.Europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0881#d1e3275-15-1

- **CE Machinery Directive** 2006/42/EC 사이버보안 항목 추가 예정

참고 표준

- **ISO 10218-1,-2** (사이버보안 항목 추가 논의 진행 중)

- **IEC 62443 시리즈** (산업 자동화 사이버보안 표준)

MD 사이버보안 요구사항

- 사이버보안 요구사항 EHSR 1.1.9

1.1.9. Protection against corruption

The machinery product shall be designed and constructed so that the connection to it of another device, via any feature of the connected device itself or via any remote device that communicates with the machinery product does not lead to a hazardous situation.

A hardware component for connection that is critical for the compliance of the machinery product with the relevant health and safety requirements shall be designed so that it is adequately protected against accidental or intentional corruption. The machinery product shall collect evidence of a legitimate or illegitimate intervention in the hardware component.

Software and data that are critical for the compliance of the machinery product with the relevant health and safety requirements shall be identified as such and shall be adequately protected against accidental or intentional corruption.

The machinery product shall identify the software installed on it that is necessary for it to operate safely, and shall be able to provide that information at all times in an easily accessible form.

The machinery product shall collect evidence of a legitimate or illegitimate intervention in the software or a modification of the software installed on the machinery product or its configuration.

기계 자체 또는 원격 연결된 기계가
다른 장치와 연결 시 안전하도록 설계
=> **안전한 연결(통신)**

중요한 하드웨어 구성 요소는 보건 및 안전 요구사항을 준수하기 위해 우발적 또는 의도적 손상(예: 잠재적인 사이버 공격)으로부터 적절하게 보호되도록 설계
=> **공격 대응**

모든 수정이나 소프트웨어 업데이트에 대해서도 구성에 대한 개입의 적법성이 입증
=> **안전한 업데이트**

MD 사이버보안 요구사항

- 강화된 안전성, 신뢰성 관련 요구사항 EHSR 1.2.1

1.2.1. Safety and reliability of control systems

Control systems shall be designed and constructed in such a way as to prevent hazardous situations from arising.

Control systems shall be designed and constructed in such a way that:

(a) they can withstand, where appropriate to the circumstances and the risks, the intended operating stresses and intended and unintended external influences, including malicious attempts from third parties to create a hazardous situation;

(b) a fault in the hardware or the logic of the control system shall not lead to hazardous situations;

제어 시스템은 위험을 방지하는 방식으로 제조

(A) 상황과 위험에 적절한 경우, 의도된 운영 스트레스와 의도했거나 의도하지 않은 외부 영향(위험한 상황을 조성하려는 제3자의 악의적인 시도 포함)을 견딜 수 있습니다.
(B) 하드웨어 또는 제어 시스템 논리의 결함이 위험한 상황으로 이어져서는 안 됩니다.

=> **다양한 보안 기능 또는 환경을 구현**

인력 부족 해결 및 생산성 증대 목표로 로봇 및 산업 자동화 수요 ↑, IOT 및 AI 기술 접목으로 Connectivity 확대

로봇 디바이스 + 작업 환경 시스템 + 리스크 관리의 사이버보안 확대 적용

Robot Industry

IEC 62443이란?

Industrial Automation and Control Systems

Industrial Automation and Control System(s) (IACS) Introduction

- Industrial Automation and Control Systems (IACS)는 자산의 자동화 또는 원격 제어 또는 모니터링을 사용하는 시스템을 의미하며, 공장 및 설비의 제조 및 가공, 건설, 유틸리티, 파이프라인, 배전설비 등 지리적으로 분산된 운영 및 기타 산업 및 응용 분야에 대한 제어 시스템을 포함합니다. IACS 정보보안 개념은 IEC 62443 시리즈 표준에서 널리 사용되고 있으며, IEC 62443 시리즈는 모든 산업, 플랜트, 설비, 시스템 및 필수 인프라에 대한 모든 유형의 구성요소를 다루고 있습니다.
- IACS 에는 아래 다음이 포함되지만 이에 국한되지는 않습니다.

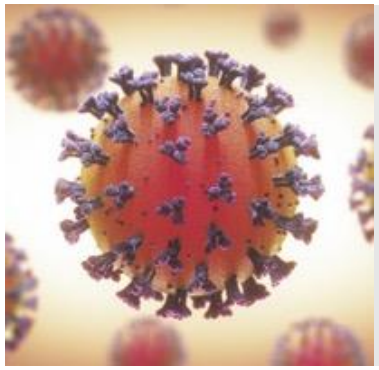
- ✓ Hardware and software systems such as Distributed Control Systems (DCS), Programmable Logic Controllers (PLCs), Supervisory Control and Data Acquisition (SCADA) systems, networked electronic sensing systems, and monitoring, diagnostic and evaluation systems.
- ✓ Internal, human, network or machine interface logging, diagnostics, security, monitoring, maintenance, quality assurance, regulatory compliance, auditing and other types of operational functions, whether continuous, batch, discrete and combinatorial processes, used to provide control, data.

Why IACS Information Security is Essential?

Why Information Security is Essential?

- 최근 몇 년 동안 비즈니스 및 개인용 컴퓨터 시스템에 대한 악성 코드 공격이 크게 증가했습니다.

- 자동화된 공격 도구는 인터넷에서 흔히 볼 수 있습니다. 사이버 범죄자들은 산업 자동화 및 제어 시스템을 공격할 자원이 더 많을 수 있습니다.



- IACS는 COTS 운영 체제/프로토콜로 이동하여 비즈니스 네트워크와 상호 연결하므로 상용 장치에서 발견되는 동일한 공격에 취약합니다.

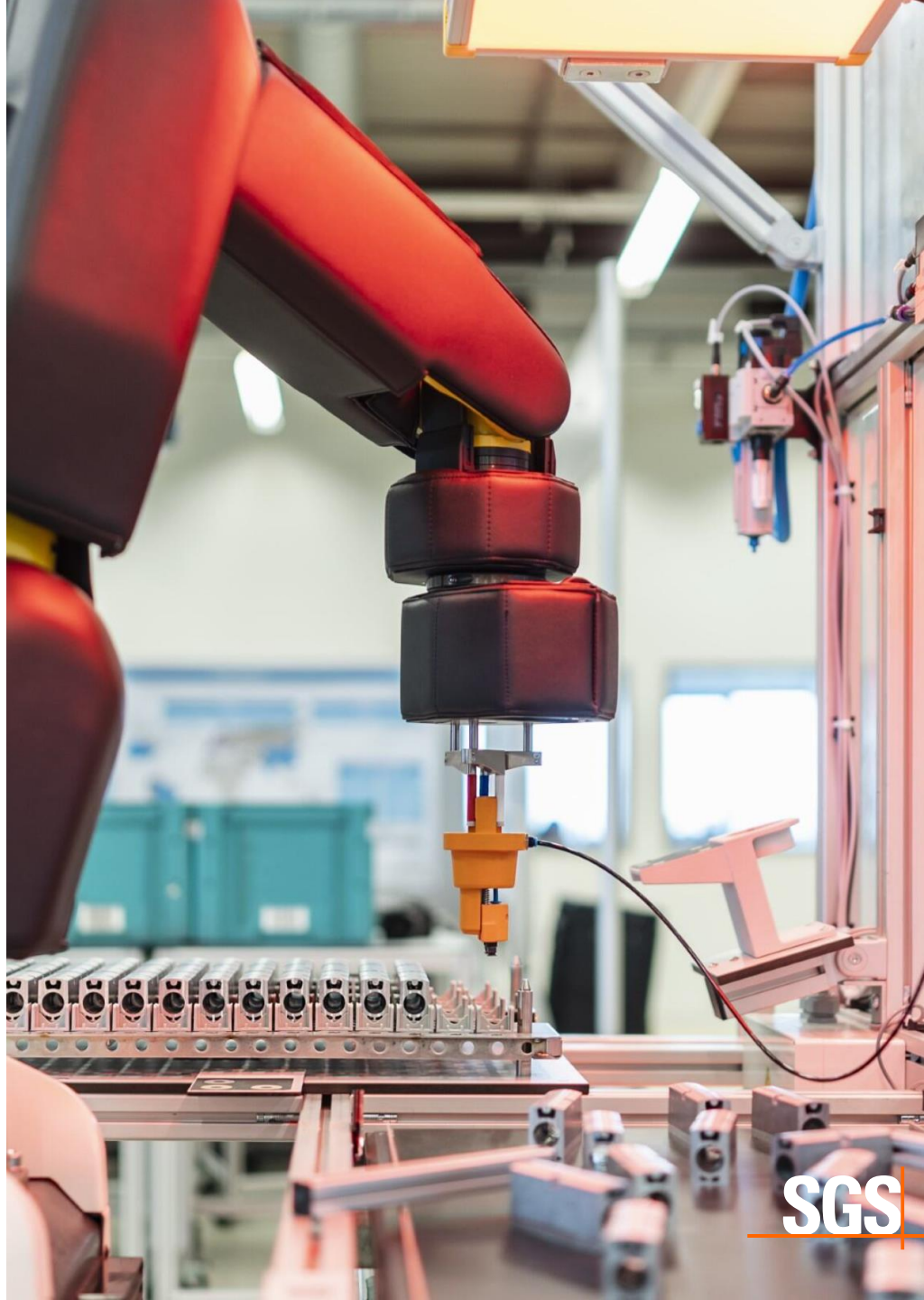
- IACS와 현장 장치 간의 통신을 위해 IP와 같은 산업 문서 프로토콜을 사용하면 네트워크 계층 시스템과 동일한 취약성에 노출될 수 있습니다.

IEC 62443 Series Introduction

- IEC 62443 시리즈 표준은 ISA(International Society of Automation)가 개발하고 IEC(International Electrotechnical Commission)가 검토하여 채택한 것으로, 시스템 통합업체, 제품 공급업체 및 서비스 공급업체가 제품 및 서비스의 보안을 평가하도록 안내하고 IACS의 배치 및 운영에 따른 위험을 최소화하기 위한 산업 자동화 및 산업 보안을 위한 일련의 표준입니다.

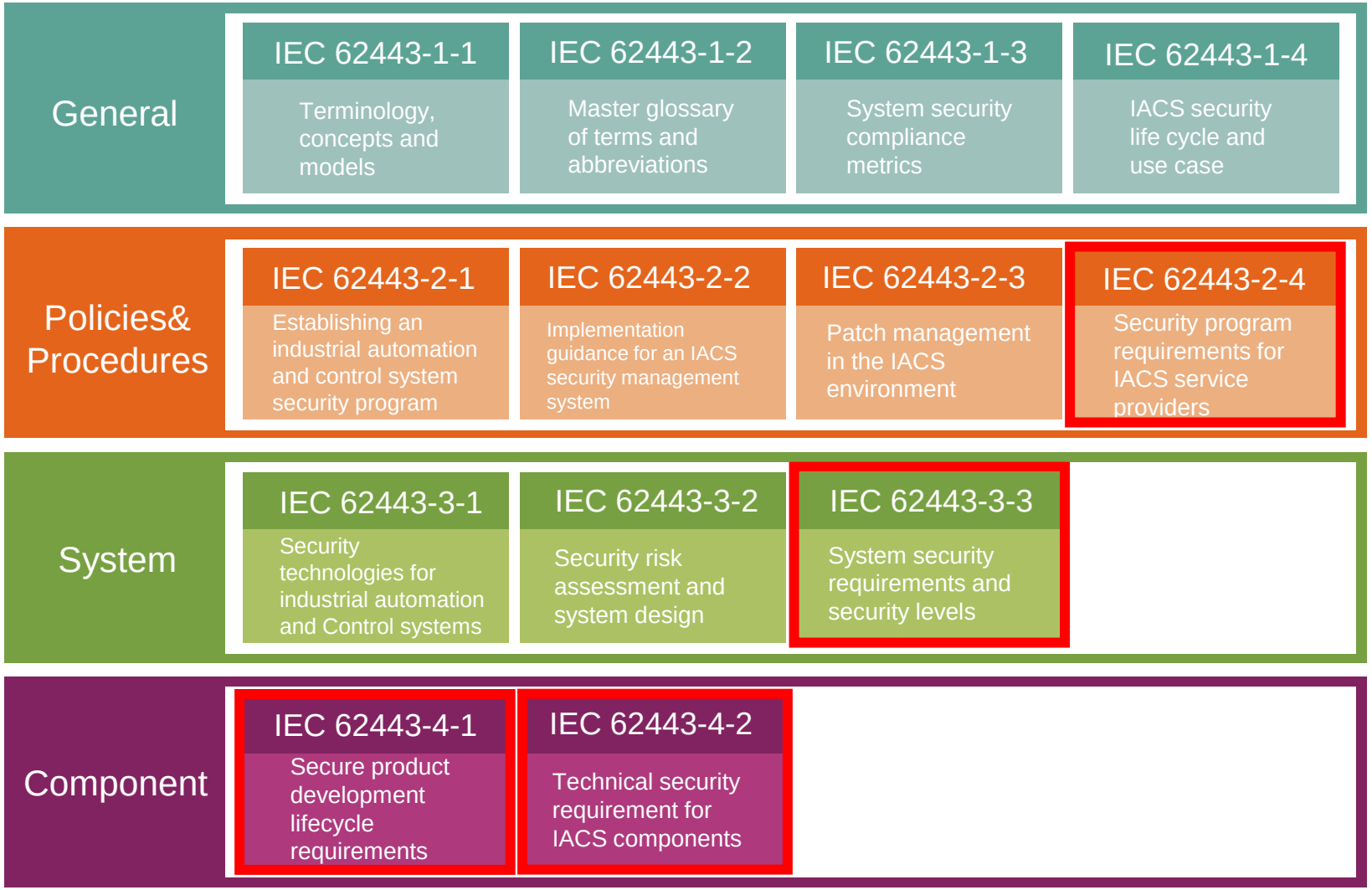
- IEC 62443은 다양한 관점에서 산업 정보 보안에 대한 지침을 제공하는 기타 표준 (ISO 27001, IEC 62351, NIST SP800)을 고려하여 제품, 시스템, 관리, 기술 및 프로세스를 포함한 산업 정보 보안을 다양한 역할, 다양한 수준에서 체계적으로 분류하여 정의하고 있습니다.

IEC 62443 시리즈는 최근 10년간의 가장 중요한 산업정보보안 연구와 우수사례를 정리한 세계적인 표준으로 많은 정부기관과 바이어들의 정보보안 요구사항 가이드라인이 되고 있습니다.



IEC 62443 Series Content

IEC 62443 Series Content



- ✓ 일반에서는 안전 프로세스를 소개하며, 다른 챕터에서 다뤄지는 개념과 기초를 소개한다.
- ✓ 정책 및 절차에서는 보안 시스템, 보안 정책 및 리스크 관리에 대한 지침을 제공한다.
- ✓ 시스템에서는 사이버보안 및 프로세스 방법론을 통합한 보안 IACS 시스템의 설계 및 구현에 중점을 둔다.
- ✓ 구성요소에서는 산업 네트워크에 필요한 제품의 수명주기와 기술적 기능 수준을 설명한다.

IEC 62443 Series Certification Serviceability

IEC 62443 Series Standard Certification Serviceability

Standard	Brief	Application Roles	Applications
IEC 62443-2-4	IACS 서비스 제공자를 위한 보안 프로그램(관리 시스템) 요구사항	자산 소유자(예: IACS의 실제 운영자인 IACS를 담당하는 개인 또는 조직)에게 적용.	제품생산자동화라인, 지하철신호제어시스템, 상수도시스템, 스마트그리드 등 산업시설의 소유자 또는 운영자.
IEC 62443-3-3	시스템 보안 요구사항 및 수준	시스템 통합업체(예: 구성요소 또는 서브시스템을 전체로 통합하고 서브시스템이 기능적으로 작동하도록 보장하는 전문업체)에 적용.	다양한 IACS 계약자 및 운영자
IEC 62443-4-1 IEC 62443-4-2	4-1: 제품개발 수명주기에 따른 보안 요구사항 4-2: IACS 구성요소 보안 기술 요구사항	부품 제조업체, IACS 계약업체에 적용.	네트워크 장치, 임베디드 장치, 센서 등과 같은 IACS 시스템 구성 요소의 설계자 및 제조자

IEC 62443-2-4/4-1Maturity Level

IEC 62443-2-4/-4-1 Maturity Level (ML) Concept Introduction

Level 1

Initial

- Ad-hoc process.

Level 2

Managed

- 문서화된 프로세스로 반드시 반복 가능한 프로세스는 아님

Level 3

Practiced

- Maturity Level 2
- 반복 가능하고 일관성 있게 수행되는 문서화된 프로세스

Level 4

Improving

- Maturity Level 3
- 반복 가능하고 일관성 있게 수행되는 문서화된 지속적으로 보완가능 한 프로세스

IEC 62443-3-3/-4-2 Security Requirements

IEC 62443-3-3/-4-2 Fundamental Security Requirements

IAC

Identification and authentication control
(식별 및 인증관리)

UC

Use control
(사용 제어)

DI

Data Integrity
(데이터 무결성)

DC

Data Confidentiality
(데이터 기밀성)

RDF

Restrict Data Flow
(데이터 흐름 제한)

TRE

Timely Response to Event (시의적절한 이벤트 대응)

RA

Resource Availability
(리소스 가용성)

IEC 62443-3-3/4-2 Security Level Introduction

IEC 62443-3-3/-4-2 Security Level (SL) Concept Introduction

SL1

도청 또는 일상적인 노출을 통해 정보가 무단으로 공개되는 것을 방지.

SL2

부족한 리소스, 일반적인 기술, 소극적인 동기를 가진 단순한 수단을 사용하여 적극적으로 정보를 검색하는 기업에 무단으로 정보가 공개되는 것을 방지.

SL3

적당한 리소스, IACS 특정 기술 및 적절한 동기를 가진 정교한 수단을 사용하여 정보를 적극적으로 검색하는 단체에 정보가 무단으로 공개되는 것을 방지.

SL4

광범위한 리소스와 고도의 IACS 기술, 적극적인 동기를 가지고 정보를 적극적으로 검색하는 단체에 정보를 무단으로 정보가 공개되는 것을 방지.

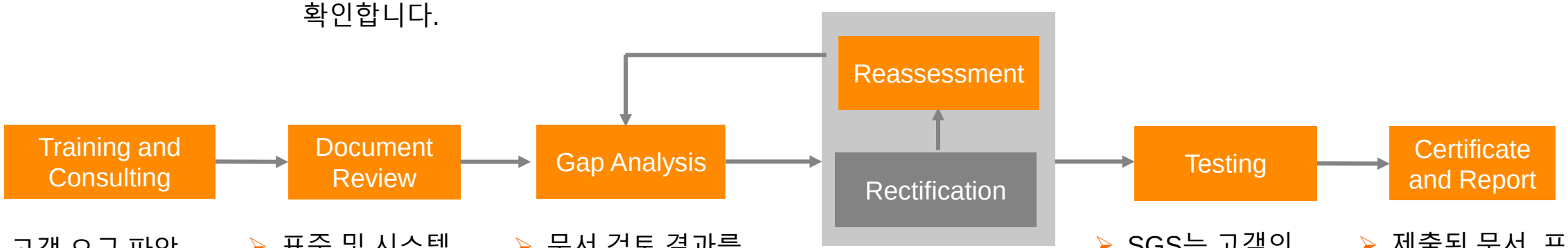
Robot Industry

SGS 서비스 소개

IEC 62443 Series Certification Process

IEC 62443 Standard Certification Process

- 문서 및 보안 기능을 재평가합니다.
- 모든 문제가 종결될 때까지 표준 및 인증 프로그램의 요구사항을 충족하는지 확인합니다.



- 고객 요구 파악
- 인증서비스, 프로젝트 프로그램 및 평가 계획에 대한 소개
- 표준 교육

- 표준 및 시스템 보안 수준 또는 성숙도 요구사항에 따라 고객 문서를 검토

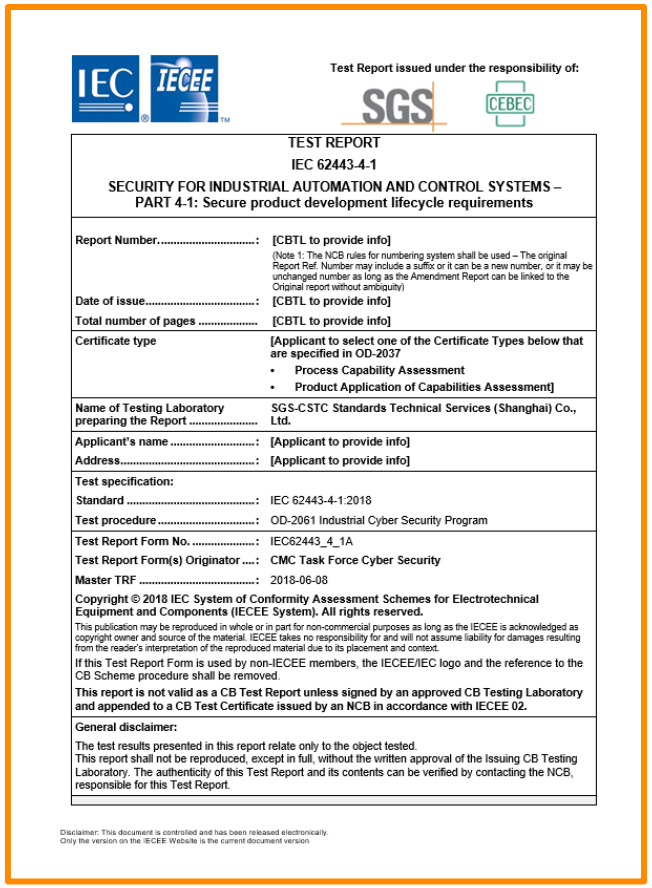
- 문서 검토 결과를 바탕으로 고객이 보완해야 할 부분을 파악하고 이해할 수 있도록 지원
- Gap analysis reports

- 고객은 Gap analysis report에 따라 문서 및 기술 조치사항을 수정 및 업데이트
- SGS는 문서 수정 및 기술 업데이트를 완료하는 데 도움이 되는 기술 컨설팅을 제공

- SGS는 고객의 실험실 또는 공장에서 FAT를 수행하고 필요에 따라 설치 장소에서 SAT를 수행
- 문서수정 및 보완이 올바르게 구현되었는지 확인

- 제출된 문서, 프로젝트 기록, 평가 결과 등을 토대로 보고서 및 인증서 초안 작성
- SGS는 최종 보고서와 CB 인증서를 발행

IEC 62443 Certificate & Report



Test Report issued under the responsibility of:

TEST REPORT

IEC 62443-4-1

SECURITY FOR INDUSTRIAL AUTOMATION AND CONTROL SYSTEMS – PART 4-1: Secure product development lifecycle requirements

Report Number..... :	[CBTL to provide info]
	(Note 1: The NCB rules for numbering system shall be used – The original Report Ref. Number may include a suffix or it can be a new number, or it may be unchanged number as long as the Amendment Report can be linked to the Original report without ambiguity)
Date of issue..... :	[CBTL to provide info]
Total number of pages	[CBTL to provide info]
Certificate type	[Applicant to select one of the Certificate Types below that are specified in OD-2037 • Process Capability Assessment • Product Application of Capabilities Assessment]
Name of Testing Laboratory preparing the Report	SGS-CSTC Standards Technical Services (Shanghai) Co., Ltd.
Applicant's name ..... :	[Applicant to provide info]
Address..... :	[Applicant to provide info]
Test specification:	
Standard ..... :	IEC 62443-4-1:2018
Test procedure ..... :	OD-2061 Industrial Cyber Security Program
Test Report Form No. ..... :	IEC62443_4_1A
Test Report Form(s) Originator ....:	CMC Task Force Cyber Security
Master TRF ..... :	2018-06-08

Copyright © 2018 IEC System of Conformity Assessment Schemes for Electrotechnical Equipment and Components (IECEE System). All rights reserved.

This publication may be reproduced in whole or in part for non-commercial purposes as long as the IECEE is acknowledged as copyright owner and source of the material. IECEE takes no responsibility for and will not assume liability for damages resulting from the reader's interpretation of the reproduced material due to its placement and context.

If this Test Report Form is used by non-IECEE members, the IECEE/IEC logo and the reference to the CB Scheme procedure shall be removed.

This report is not valid as a CB Test Report unless signed by an approved CB Testing Laboratory and appended to a CB Test Certificate issued by an NCB in accordance with IECEE 02.

General disclaimer:

The test results presented in this report relate only to the object tested.
This report shall not be reproduced, except in full, without the written approval of the Issuing CB Testing Laboratory. The authenticity of this Test Report and its contents can be verified by contacting the NCB, responsible for this Test Report.

Disclaimer: This document is controlled and has been released electronically.
Only the version on the IECEE Website is the current document version

IEC 62443 Assessment Report

Ref. Certif. No.

CertificateNo

IEC SYSTEM FOR MUTUAL RECOGNITION OF TEST CERTIFICATES FOR ELECTRICAL EQUIPMENT (IECEE) CB SCHEME

CB TEST CERTIFICATE

Product	Subgroup
Name and address of the applicant	CertificateHolderName CertificateHolderAddress
Name and address of the manufacturer	ManufacturerName ManufacturerAddress
Name and address of the factory Note: When more than one factory, please report on page 2	NewFactoryName NewFactoryAddress ☐ Additional Information on page 2
Ratings and principal characteristics	CharacteristicValue
Trademark (if any)	XXXXXXX
Customer's Testing Facility (CTF) Stage used	TestingType
Model / Type Ref.	Order_ProductModel_Type
Additional information (if necessary may also be reported on page 2)	Remark ☐ Additional Information on page 2
A sample of the product was tested and found to be in conformity with	Order_Standards National Differences: Order_Standards_ExtraText
As shown in the Test Report Ref. No. which forms part of this Certificate	TestReportNo

This CB Test Certificate is issued by the National Certification Body

SGS Belgium NV - Division SGS CEBEC
Riverside Business Park
Bld Internationalelaan 55, Building A
B-1070 Brussels, Belgium

Date: CertificateIssueDate

Signature: Name

1/1

This certificate is issued by the company under its General Conditions for Certification Services accessible at http://www.sgs.com/en/Terms-and-Conditions.aspx
Attention is drawn to the limitations of liability defined therein and in the Test Report here above mentioned which findings are reflected in this certificate. Any unauthorized alteration, forgery or falsification of the content or appearance of this document is unlawful and offenders may be prosecuted to the fullest extent of the law.

IEC 62443 CB Certificate

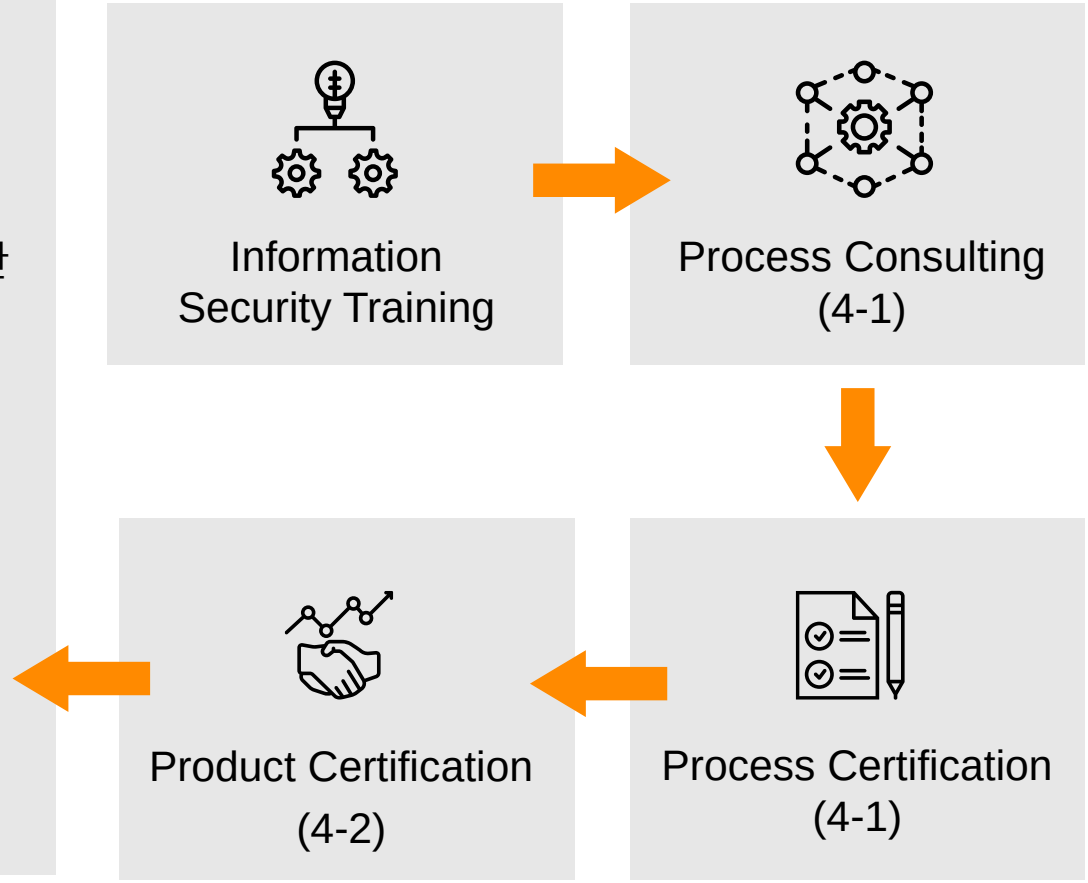
REQUIREMENTS ASSESSED

Security management (12/13),
Security requirements (5/5),
Secure by design (4/4),
Secure implementation (2/2),
Security verification and validation testing (5/5),
Management of security-related issues (6/6),
Security update qualification (5/5),
Security guidelines (6/7)

IEC 62443-4-2 Certification Process

IEC 62443-4-2 Standard Certification Bullets

- SGS는 평가 및 시험을 수행하고, 고객은 시험 요구사항에 따라 시험 샘플 및 관련 기술문서를 제공하며, 시험 환경을 정비하는 데 도움을 줍니다.
- 샘플이 데이터 보호와 사이버 보안 측면에서 요구되는 보안 수준을 충족하는지 확인합니다. 핵심 요구 사항은 다음과 같습니다 :
  - a) Identification and authentication control (IAC),
  - b) Use control (UC),
  - c) System integrity (SI),
  - d) Data confidentiality (DC),
  - e) Restricted data flow (RDF),
  - f) Timely response to events (TRE)
  - g) Resource availability (RA).



IEC 62443 Training and Consulting Service

SGS Provides IEC 62443 Training and Process Consulting Service

- **IEC 62443 Standard Training Service**

IEC 62443 Standard Training Service	
Purpose	기업(정보보안부서)의 정보보안 대응력 향상
Content	IEC62443 Series 기반 IACS 정보보안 교육 실시
Workflow	1. 교육 요구사항 논의 및 교육내용 최종화 2. 현장교육 및 검사(선택사항) 3. 유자격자 교육 수료증 발급 (선택사항)

- **IEC 62443-4-1 Process Consulting Service**

- 고객이 기존 개발 시스템(예: CMMI)을 IEC 62443-4-1의 개발 프로세스로 업그레이드할 수 있도록 도와줍니다.

- SGS팀은 IEC 62443-4-1의 요구사항을 고객이 기존 프로세스에 적용하는 것을 안내하기 위해 고객의 기존 개발 프로세스를 기반으로 작업을 할당하여 다음을 수립합니다 :
  - ✓ 정보보안 조직구조의 적합성
  - ✓ 정보보안 개발의 주요 프로세스
  - ✓ 하위 프로세스 및 상세 기술 등

- SGS팀은 프로세스 정의, 운영 지침, 전형적인 작업 결과, 구현 현황 및 제품 보안 개발 라이프사이클 관리 관련 증빙 서류를 확인합니다.

SGS Service

Why Choose SGS Service for your Cybersecurity needs?

Team of Technical Experts

- ✓ ISA/IEC 62443 Cybersecurity Fundamentals Specialist
- ✓ IECEE ETF expert
- ✓ IECEE Technical Auditor
- ✓ CISP/CISSP/OSCP Certificate

Sufficient Lab Accreditation

SGS is the CBTL for：

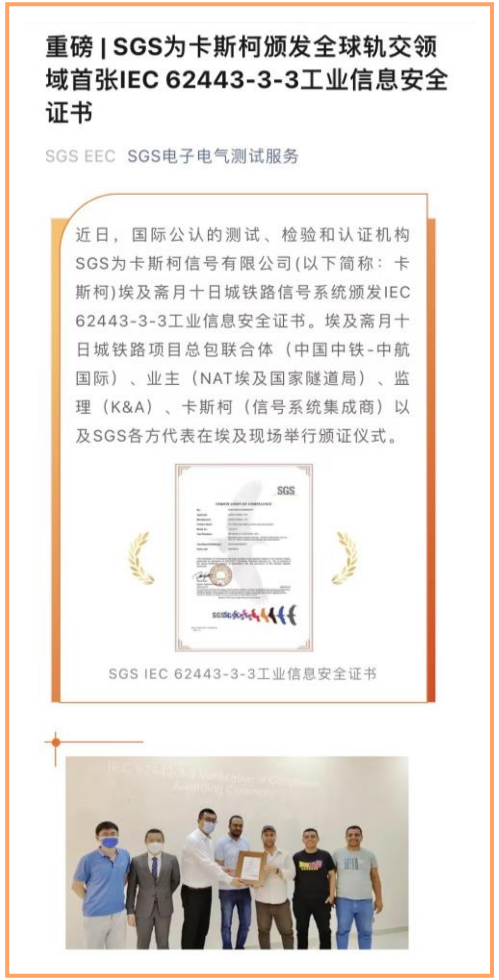
- ✓ IEC 62443-2-4
- ✓ IEC 62443-3-3
- ✓ IEC 62443-4-1
- ✓ IEC 62443-4-2

Promotion Support

SGS는 마케팅 행사 공동 개최, 홍보 영상 촬영, 뉴스 기사 작성 등으로 고객과 함께 인증 홍보에 더욱 힘써, 인증 시장에 대한 영향력을 더욱 확대해 나갈 예정입니다.

One-stop CYBR Service

다중 표준 및 규정, 취약점 및 침투 테스트 등을 활용한 사이버 보안 평가 원스톱 서비스로 더 많은 인증을 합리적인 가격과 짧은 기간으로 수행할 수 있습니다.



Thank you!

Do you have any questions?

한국 SGS 사이버보안팀

kr_cybersecurity@sgs.com