Headline

비즈니스를 위한 제조사 OT 보안 동향

OT 사업팀 강서일 수석

■ OT(Operational Technology) 보안의 동향

OT(Operational Technology)보안은 IT 보안과 접근 방식이 본질적으로 다르다. IT 는 기업 운영에 필요한 정보(데이터)를 중심으로 보안 통제가 설계되며, 표준화된 기술과 프레임워크를 기반으로 최신 보안 트렌드에 맞춰 도입·고도화를 검토하는 방식이 일반적이다.

반면 OT 보안은 ICS(Industrial Control Systems) 환경에서의 보호가 핵심이다. 동일한 보안 요구사항이라도 산업별 제어 환경, 시스템 구성에 따라 적용 가능한 보안 기술과 운영 방식이 달라진다. 즉, OT 보안은 표준 기술을 그대로 적용하기보다 현장의 제어 구조(SCADA/DCS/PLC 등)와 운영 조건을 전제로 보안 대안을 설계해야 하며, 이 때문에 기술 검토·적용 난이도가 상대적으로 높다.

최근에는 CPS(Cyber-Physical Systems Security) 보안이 부각되면서 OT 보안과 유사한 맥락에서 함께 논의되기도 한다. 다만 적용 대상과 범위는 구분될 필요가 있다. OT 보안이 전통적으로 주요 기반시설과 제조 현장에서 활용되는 SCADA, DCS, PLC 등 제어 시스템 중심의 보호를 다룬다면, CPS 보안은 컴퓨팅·통신·물리 프로세스가 통합된 스마트 인프라, 로봇 및 자율 시스템 등 보다 확장된 사이버-물리 융합 환경을 포괄한다.

본 보고서 '비즈니스를 위한 제조사 OT 보안 동향'은 제품을 제조해 공급하는 기업을 대상으로, 제조 환경 전반에서 OT 보안을 강화하기 위한 필수 요소와 고려사항을 정리하는 데 초점을 둔다.

■ 제조사 SW 및 서비스 업체의 사이버보안 동향

최근 발생한 보안 사고를 살펴보면, 협력 업체 및 공급망을 경유한 사이버 공격으로 정보 유출이나 생산 중단이 발생하는 사례가 지속적으로 증가하고 있다. 특히 랜섬웨어 등 악성코드 공격으로 인해 제조 설비는 물론 가스·전력과 같은 주요 인프라의 운영이 중단되는 사례도 보고되고 있다. 이러한 위협 확산으로 인해 국가 핵심 기반시설의 OT 보안뿐 아니라, 공급되는 소프트웨어(SW)와 제품 자체에 대한 사이버보안 요구도 함께 강화되는 추세다.

공급망 보안을 실질적으로 확보하기 위해서는 공급사의 IT 보안 관리만으로는 충분하지 않다. 제조사가 제공하는 제품(HW + SW)에 대해 개발 환경 단계부터 사이버보안이 내재화돼야 하며, 제품 생산·개발 전 과정에서 보안이 고려돼야 한다는 요구가 강화되고 있다.

공급망 보안에서는 제조사의 위치가 특히 중요하다. 특정 제조사는 자신의 공급자[1] 이자 자산 관리자[2] 가 되는 구조에 놓인다.

그림 1. 제조사의 위치에 따른 역할

이와 같이 공급자와 자산 관리자 역할을 동시에 수행해야 하는 제조사는 관련 사이버보안 요구사항을 폭넓게 고려해야 한다. 이는 ISO((nternational Organization for Standardization)/IEC 27001 을 준수하는 업체라 하더라도 제품 안전성을 확보하기 위해 추가적인 OT 보안 요구사항을 검토해야 하는 상황이 발생할 수 있음을 의미한다. 반대로 기존에 사이버보안 체계가 미흡했던 업체는 공급망 보안 요구로 인해 제품 보안을 고려하는 과정에서 IT 보안부터 새롭게 도입해야 하는 상황까지 발생할 수 있다.

이 지점에서 OT 보안은 두 가지 관점으로 구분해 이해할 필요가 있다. 첫째는 자산 관리자 관점에서 운영 중인 제어 시스템의 안전성을 확보하는 것으로, 공정·생산 과정 전반을 보호하는 공정(운영) 보안이다. 둘째는 제조사가 생산·공급하는 제품 자체의 안전성을 확보하는 것으로, 개발 단계에서 사이버보안이 고려됐는지와 제품이 필요한 보안 기능을 제공할 수 있는지를 확인하는 제품 보안이다. 두 영역은 목적과 적용 대상이 다르므로 혼동해서는 안 되며, 별도로 구분해 접근해야 한다.

특히 OT 보안 표준은 공정·생산망 보안과 제품 보안 요구사항을 모두 포함하는 경우가 많다. 따라서 표준을 참고할 때에는 해당 기준이 공정 및 생산망 보안을 대상으로 하는지, 또는 제품 단위 사이버보안을 요구하는지 구분해 확인해야 한다.

예를 들어 선박 보안 기준인 UR E27 은 선박 운항 장비 각각에 적용되는 제품 단위 사이버보안 요구사항으로, 장비별 사이버보안 요구 기준을 준수해야 한다. 반면 UR E26 은 선박 전체, 즉 장비들이 결합돼 운영되는 OT/IT 시스템에 대한 운영 환경(시스템) 사이버보안 요구사항으로, 제조 관점에서는 공정과 생산 과정의 보안을 요구하는 것과 유사하다고 볼 수 있다.

[1] 공급자 : 제품을 고객에게 제공하는 업체

[2] 자산 관리자 : 공급자가 납품한 제품으로 생산하여 소비자에게 제공하는 최종 산물을 만드는 업체

이로 인해 UR E27 이 적용되는 제조사는 요구사항을 검토하는 과정에서, 해당 항목들이 IEC 62443-4-1 및 IEC 62443-3-3 에서 요구하는 사이버보안 기능과 연계돼 구성돼 있음을 확인하게 된다. 결과적으로 제조사는 IEC 62443 준수 필요성을 주요 검토 대상으로 삼게 된다.

한편 선박 운영사는 UR E26 요구사항에 따라 선박 내 IT 와 OT 전반의 사이버보안을 고려해야 하며, 이에 따라 IEC 62443 뿐 아니라 NIST(National Institute of Standards and Technology)의 CSF(Cybersecurity Framework) 등 운영 환경 중심의 보안 기준을 함께 검토하게 된다.

■ OT 보안의 정책 및 규제

OT 보안 정책과 규제는 사이버보안 관련 법·지침의 일부로 포함되기도 하고, 제어시스템 보안 또는 에너지·헬스케어 등 도메인별 정부 기관이 별도의 보안 가이드 형태로 제정하는 경우도 있다. 다만 대부분의 가이드는 국제 표준인 IEC 62443 을 기반으로 하거나, 미국 NIST 의 SP 800-82 등 기존에 검증된 프레임워크를 차용해 구성되는 경우가 많다.

그러나 OT 보안은 산업 도메인별로 비즈니스 구조와 운영 환경의 차이가 뚜렷하기 때문에, 단순히 국제 표준을 이해하는 것만으로는 충분하지 않다. 각 도메인별 규제 기관이 제시하는 사이버보안 가이드의 적용 범위와 의도를 정확히 해석하는 것이 무엇보다 중요하다. 이를 위해 제조사와 운영 기관은 국제 표준을 기본 지식으로 숙지하되, 국내외 정책과 규제가 요구하는 구체적인 준비 사항을 도메인 관점에서 이해할 필요가 있다.

1. 국내

최근 국내에서도 OT 보안에 대한 관심이 높아지면서, 제어시스템 사이버보안을 위한 가이드와 요구사항이 주요 기반시설 및 공공기관을 중심으로 확대되고 있다. 특히 에너지 도메인에서는 신재생에너지 설비를 대상으로 한 보안 가이드라인이 새롭게 마련돼 발표를 앞두고 있으며, 기존 주요정보통신기반시설로 지정된 기관을 중심으로 취약점 평가와 제어시스템 모니터링 요구가 강화되는 추세다.

「국가정보보안기본지침」에서는 국가·공공기관이 운영하는 제어시스템에 대해 '국가/공공기관 제어시스템 보안 가이드라인'을 준수하도록 명시하고 있다. 이에 따라 에너지, 항만 등 주요 기반시설을 운영하는 기관을 대상으로 운영·제어시스템의 취약점 분석 및 평가 방법도 점차 고도화되고 있다. 이러한 정책 방향은 앞서 살펴본 공정 및 생산 과정에 대한 OT 보안 강화 흐름과 궤를 같이한다. 과거에는 물리적 보안을 중심으로 출입 통제나 설비 보호에 초점이 맞춰졌다면, 현재는 모니터링 및 제어시스템 구성 요소에 보안 솔루션을 적용해 악성코드 탐지·완화·대응까지 고려해야 하는 단계로 진입하고 있다.

한편 제품 보안 측면에서는 공급망 보안 강화의 일환으로 발표된 「SW 공급망 보안 가이드」를 통해, 미국과 유럽이 요구하는 소프트웨어 구성요소 명세서(SBOM) 제출 의무에 대응할 수 있는 방향이 제시되고 있다.

SBOM 작성과 제출 자체도 중요하지만, 그 이전 단계로 해당 소프트웨어가 안전한 개발 환경에서 사이버보안을 고려해 개발됐는지에 대한 정책과 프로세스를 요구하는 것이 핵심이다. 특히 이러한 요구는 SW 전문 개발사를 중심으로 논의되고 있으나, 해외 정책의 경우 제품에 포함된 모든 소프트웨어 하드웨어와 연동되는 모니터링 SW, 설정·운영용 SW 등 까지 포함하고 있어, 제조사 역시 향후 SW 제공 방식 전반에 대한 검토와 대응이 필요하다.

2. 국외

미국과 유럽을 중심으로 사이버보안 관련 법·규제가 강화되면서, 수입 제품에 대한 사이버보안 요구 수준 역시 빠르게 높아지고 있다. 각 산업 도메인별로 별도의 사이버보안 규정이 제정되는 추세이며, 에너지, 선박, 자동차, 의료 등 산업 특성에 따라 요구사항이 세분화되고 있다. 이러한 대표적인 규정과 가이드를 살펴보는 것은 향후 글로벌 시장을 대상으로 비즈니스를 추진하는 제조사에게 중요한 참고 지점이 된다.

가. 미국

OT 및 ICS 보안을 논의할 때 IEC 62443 와 함께 가장 많이 언급되는 문서가 NIST SP 800-82 다. 이 문서는 OT 및 ICS 환경 전반의 사이버보안을 다루며, 공정 및 생산 과정의 안전성을 확보하기 위한 보안 통제 방안을 중심으로 구성돼 있다. 또한 제어 환경에 도입되는 장비를 보호하기 위한 기본적인 보안 요구사항도 함께 제시하고 있어, 중요 인프라 보안 구축 시 기초 가이드로 활용하기에 적합하다.

NIST SP 800-82 가 주요 인프라 및 공정 중심의 OT 보안 가이드라면, 스마트팩토리 등 IT·OT 융합 환경을 운영하는 제조사는 NIST CSF 2.0(최신 버전)을 함께 참고할 필요가 있다. 제조사의 공정과 설비는 SP 800-82 를 기반으로 보호하되, IT 와 OT 를 포괄하는 사이버보안 리스크 관리와 거버넌스 체계 수립을 위해서는 CSF 를 병행 적용하는 것이 효과적이다. 두 문서를 함께 활용할 경우, OT 정책 및 보안 가이드 방향을 보다 체계적으로 수립할 수 있다.

에너지 도메인에서는 규제 강화에 따라 NERC(North American Electric Reliability Corporation)의 CIP(Critical Infrastructure Protection) 규정을 통해 전력망에 대한 사이버 공격과 물리적 위협을 동시에 방지하고 있다. 해당 규정은 발전소에 납품되는 장비의 시스템 보안뿐 아니라 공급망 전반의 사이버보안 관리까지 요구하고 있어, 북미 발전소에 제품을 공급하는 제조사는 이에 대한 대응 방안을 마련해야 한다. 또한 미국 에너지부는 전력망뿐 아니라 풍력·태양광 등 재생에너지 운영 환경에서도 사이버보안을 의무화하는 가이드라인을 발표하고 이를 적용하고 있다.

해당 내용을 정리하면 다음 표와 같다.

문서명	NIST 800-82 Rev.3	NIST CSF2.0	NERC CIP
목적	ICS/OT 구성 환경 보안 가이드	범용 사이버보안 위험 관리 및 거버넌스	북미 전력망(BES)보호를 위한 법적 규제
적용 범위	SCADA, DCS, PLC, 빌딩, 자동화 등 ICS/OT 시스템	모든 산업 조직 (IT/OT 포함)	발전/송전/제어 시스템 등 대량 전력 시스템(BES)
구성 요소	아키텍처, 위협모델, 보안 대책, 사고 대응 등 사이버보안의 요구 사항 별 가이드	6 대 기능 : 거버넌스, 식별, 보호, 탐지, 대응, 복구 (공급망 보안을 세분화 함)	CIP 문서로 최근까지 업데이트 중(자산부터 공급망 보안, 네트워크 보안 및 제어 등)
중점 요소	ICS/OT 의 가용성, 안전성 등의 보안 특화	리스크 관리, 공급망 보안, 조직 거버넌스	법적 규제 준수, 전력망 안전성, 사이버 및 물리적 보안
법적 강제성	해당 없음	해당 없음	있음(FERC 승인 및 미 준수 시 벌금), 연간 감사 및 주기적 보고
활용 사례	미국 내 중요 인프라 보안 참고 가이드	기업 사이버보안 전략, ISO 27001, ISMS 와 비교 가능	북미 전력망 운영자, 유틸리티, 공급사 등의 준수 필수

이와 같은 규제 환경을 고려할 때, 전력망 관련 비즈니스를 수행하는 제조사는 자사 제품과 서비스가 NERC CIP 의 사이버보안 적용 대상에 해당하는지 여부를 필수적으로 검토해야 한다.

이 과정에서 NERC CIP 요구사항을 직접적으로 해석하는 데 그치지 않고, 자연스럽게 NIST SP 800-82, NIST CSF 등 관련 참조 문서를 함께 분석하게 된다. 특히 최근에는 이러한 규제 검토 과정에서 공급망 보안이 핵심 이슈로 부각되고 있다.

나. 유럽

유럽의 사이버보안 규제는 유럽연합(EU) 차원의 공통 규제와 각 회원국의 국가별 법령으로 구분해 살펴볼 필요가 있다. 본 문서에서는 국가별 차이에 대한 상세 논의는 제외하고, 제조사에 직접적인 영향을 미치는 EU 차원의 대표 규제인 NIS2 와 CRA 를 중심으로 살펴본다.

NIS2 는 Directive (EU) 2022/255 on measures for a high common level of cybersecurity across the Union 으로, 유럽연합 전반의 사이버보안 수준을 공통적으로 강화하기 위해 제정된 지침이다. 기존 NIS 대비 적용 대상이 확대됐으며, 벌금 체계, 사고 신고 의무, 관리 책임 등을 보다 구체적으로 규정한 것이 특징이다.

NIS2 에 따라 EU 회원국은 2024 년 10 월 17 일까지 해당 지침을 각국의 국내법으로 전환해야 한다. 다만 현재 회원국별로 준비 상황과 적용 범위는 상이하게 진행되고 있다. 따라서 유럽 내 공장이나 지사를 운영하거나, 유럽에서 제품·서비스를 생산·제공하는 기업의 경우, 해당 국가의 NIS2 기반 사이버보안 법령을 반드시 확인할 필요가 있다.

NIS2 는 공장의 안전한 운영과 제공되는 서비스가 사이버 위협으로부터 충분한 보호 수준을 갖출 것을 요구한다. 특히 사고 발생 시 24 시간 이내 초기 보고, 72 시간 이내 상세 보고 의무를 준수하기 위해서는, 사전에 이를 지원할 수 있는 시스템 구성과 운영 프로세스가 마련돼 있어야 한다.

한편, CRA(Cyber Resilience Act)는 Regulation (EU) 2024/2847 로, 유럽 시장에 출시 혹은 수입하는 디지털 요소가 포함된 제품에 대한 사이버보안 요구 사항을 법적으로 강제하는 규정이다. CRA 는 하드웨어·소프트웨어 제조사를 대상으로 보안 설계, 취약점 관리, 보안 업데이트 제공 의무 등을 명시하고 있으며, 국내 제조사가 제품을 유럽 시장에 판매하기 위해서는 해당 법령의 적용 여부를 판단하고 요구사항을 충족하는 것이 필수적이다.

특히 중소 제조사의 경우 CRA 요구사항을 충족하기 위한 준비 과정에 상당한 시간과 노력이 필요할 것으로 예상된다. 공식 적용 시점은 2027 년 12 월로, 약 2 년의 준비 기간이 남아 있으나, 유럽 수출 제품 전반에 영향을 미칠 가능성이 크다. CRA 요구사항을 충족하기 위해서는 소프트웨어 개발 환경, 개발 프로세스, 취약점 관리 체계 등 다양한 요소를 정비해야 하며, 실무적으로는 IEC 62443-4-1, 4-2, 3-3 의 준수를 기준으로 대응 전략을 수립하는 것이 현실적인 접근으로 평가된다.

CRA 는 CE 인증 체계에 포함되는 규정이기 때문에, 명시적인 예외 대상이 아닌 이상 해당 사이버보안 요구사항을 회피하기는 어려울 것으로 보인다.

법령	NIS 2 Directive (EU 2022/2555)	Cyber Resilience Act (CRA, EU 2024/2847)
적용 특징	EU 지침으로 회원국이 국내법으로 전환 해야 함 유럽 국가별 사이버보안 법 참조 필요	EU 규정으로 모든 회원국에 직접 적용
목적	중요 인프라 및 서비스 제공자의 사이버보안 위험 관리 보고 의무 강화	EU 시장에 출시되는 디지털 제품의 보안 내제화 및 취약점 관리 의무
적용 대상	에너지, 운송, 금융, 보건, 공공 등 유럽내 기업으로 50 명 이상 직원 및 매출 1 천만 유로 이상	디지털 요소 포함 제품 (법령내 예외 대상 정의) 제품 단위로 적용, 제조사, 수입업자, 유통업자 모두
주요 사항	위험 분석 및 보안 정책, 사고 대응 및 보고, 공급망 보안 등 국가별 감독 기관 및 감사 수행	보안 설계, 취약점 관리, 취약점 신고 및 대응 절차 CE 인증서 발행으로 적합성 증명
벌금 및 제재	최대 1,000 만 유로 또는 매출 2% 각 국가별 감독기관이 수행	최대 1,500 만 유로 또는 매출 2.5% 제품 판매 및 시장 진입 통제

비즈니스 관점에서 보면, NIS2 는 국내 기업이 유럽의 공장 및 지사 등의 제품 생산 공정과 운영에 대한 보안 검토를 요구하는 규정이며, CRA 는 유럽 시장에 출시되는 제품에 대한 사이버보안과 안전성을 확보하는 규정으로 보면 된다.

3. 국제

OT/ICS 보안과 관련된 국제 표준은 크게 ISO 계열 표준과 ISA/IEC 62443 계열 표준으로 구분할 수 있다. 이들 표준은 각국의 법령과 산업별 보안 가이드의 기반이 되는 문서로, 규제나 요구사항을 검토할 때 가장 기본적으로 참조되는 국제 기준이다. 선박 분야의 경우 국제 표준 인증 체계와는 다소 차이가 있으나, 글로벌 선박 산업 전반에서 사실상 표준처럼 적용되고 있어 본 문서에서는 국제 항목으로 함께 다룬다.

가. ISO/IEC 27019 : 전력 에너지 분야

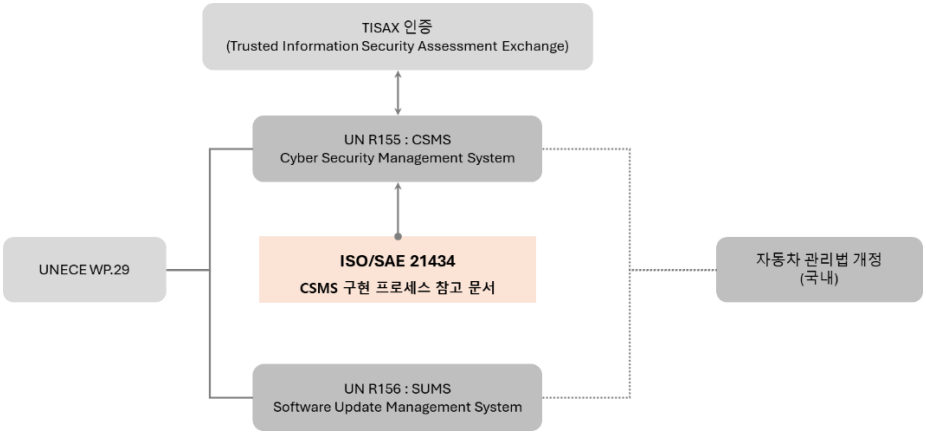
ISO/IEC 27019 는 비교적 생소할 수 있으나, ISO/IEC 27000 시리즈를 이해하는 과정에서 자연스럽게 접하게 되는 표준이다. ISO/IEC 27001 을 기반으로 산업 제어 환경에 특화된 보안 요구사항을 정의했던 ISO/IEC 27009 가 과거에 존재했으나, 현재는 폐기돼 더 이상 사용되지 않는다.

ISO/IEC 27019 는 에너지 산업의 사업 프로세스 제어 환경을 대상으로 한 보안 표준으로, 전력 등 에너지 분야에 특화된 사이버보안 요구사항을 포함하고 있다. 미국 에너지부(DoE)가 태양광, 수력 등 전력 공급 분야의 보안 표준을 수립하는 과정에서 참조한 항목들도 반영돼 있으며, ISO/IEC 27002 의 정보보안 통제 지침을 기반으로 에너지 제어 시스템에 추가로 필요한 보안 요구사항을 정의하고 있다. 따라서 전력·에너지 도메인에서 OT 보안을 검토할 경우 핵심적으로 참고해야 할 표준이다.

나. ISO/SAE 21434 : 차량 분야

차량 도메인의 사이버보안을 강화를 위한 국제 표준으로, 유럽 및 해외 자동차를 판매하는 제조사가 OT 보안 관점에서 반드시 참고해야 할 문서이다. 실제 UNECE(United Nations Economic Commission for Europe) WP.29 에서는 글로벌 차량 산업에 대한 사이버보안 국제 규제를 만들어 제공하고 있다.

그 결과물이 UN R155 와 UN R156 이다. 제조의 사이버보안 관리 및 차량 제공 소프트웨어 관리 내용이 포함되어 있으며 UN R155 은 차량 인증 TISAX 에 활용되고 있다. 해당 내용을 기반으로 국내 자동차 관리법 개정을 진행중이다. 이와 같은 규제의 기반이 되는 참고 문서가 ISO/SAE 21434 이다.



다. ISA/IEC 62443 : OT 표준 분야(산업 분야 공통 참조)

ISA/IEC 62443 은 OT 사이버보안을 다룰 때 가장 핵심적으로 참조되는 표준 체계다. 이론적으로는 전체 문서를 포괄적으로 이해하는 것이 이상적이지만, 실제 정책·규제 검토나 실무 적용 과정에서는 특정 문서들이 반복적으로 활용된다.

대표적으로 가장 많이 참조되는 문서는 다음 세 가지다.

ISA/IEC 62443 3-3 은 시스템 보안 요구 사항 및 보안 레벨을 정의한 문서다. 여러 장비와 제품이 결합된 시스템 환경에서 요구되는 사이버보안 요구사항을 제시한다. 선박 분야의 UR E27 요구사항과 연계되며, 공정 및 생산 설비에 적용되는 보안 요구사항을 정의할 때도 폭넓게 활용된다.

ISA/IEC 62443 4-1 는 제품 개발 라이프사이클 전반에 적용되는 보안 요구 사항을 규정한 문서다. 제품 개발 단계에서 사이버보안 고려 사항, 개발 환경의 안전성 확보 그리고 취약점 관리까지 전반적인 개발 보안을 요구한다. 대부분의 글로벌 규제와 공급망 보안 요구에서 이 문서의 내용을 기반으로 제품 개발 보안을 요구하고 있으며, 제조사가 안전한 제품 공급을 입증하기 위한 핵심 인증 기준으로 활용된다.

ISA/IEC 62443 4-2 는 제품을 구성하는 컴포넌트 단위의 사이버보안 요구 사항을 정리한 문서다. 개체 요소에서 보안 기능 제공 제공에 어려움이 있는 경우, 시스템적인 보안으로 제공할 수 있다. 그러므로 본 내용에는 3-3 의 항목과 해당 내용이 포함되어 기술되어 있는 경우가 존재한다.

IEC 62443 계열 문서는 상호 참조 구조로 구성돼 있어, 제품 개발 단계부터 안전한 운영 환경 구축까지 전 과정을 통합적으로 고려하도록 설계돼 있다는 점이 특징이다.

라. UR E26/ UR E27 : 선박 분야

UR E26 은 선박 전체를 대상으로 한 사이버보안 요구사항으로, 선박 내 모든 IT·OT 시스템을 통합적으로 고려해 보안을 구축하도록 요구한다. 이는 기업 관점에서 공정 및 운영 환경 전반의 OT 보안을 요구하는 것과 유사하다. 반면 UR E27 은 선박에 탑재되는 개별 장비 및 제품을 대상으로 한 사이버보안 요구사항이다. 선박에 제품을 납품하는 제조사는 UR E27 인증을 획득해야 하며, 이를 준비하는 과정에서 IEC 62443-4-1 과 3-3 을 기준으로 대응할 경우 상당 부분의 요구사항을 충족할 수 있다.

제조업은 전력, 선박, 차량, 의료기기, AI 시스템 등 다양한 도메인으로 세분화되며, 각 분야마다 별도의 규제와 OT 보안 가이드가 존재한다. 다만 이러한 문서들이 완전히 새로운 요구사항으로 구성돼 있는 것은 아니다. 대부분 기밀성, 무결성, 가용성(CIA)을 기본 원칙으로 하며, 자산 식별, 사고 대응, 인증·접근제어·암호화·네트워크 보호 등 공통적인 보안 기능을 요구한다.

따라서 하나의 핵심 표준을 충분히 이해하고 나면, 다른 도메인 표준을 해석하는 데에도 큰 어려움은 없다. 다만 각 산업별 제품의 목적과 운영 환경이 다르기 때문에, 이에 따라 요구되는 보안 수준과 적용 방식의 차이를 면밀히 검토하는 것이 중요하다.

■ 비즈니스를 위한 OT 보안 준비

앞서 살펴본 국내외 규제와 산업 동향을 종합하면, 2026년 이후 제조사가 글로벌 시장에서 제품을 판매·공급하기 위해 사이버보안 준수는 선택이 아닌 필수 요건으로 자리 잡을 가능성이 높다. 특히 공급망 보안 요구가 강화되면서, 자산 관리자(고객사)는 납품 제품의 사이버보안 안전성 확보 여부를 보다 엄격하게 확인하고, 침해사고 발생 시 신속한 보고·알림 체계를 통해 피해를 최소화하려는 노력을 지속할 것이다. 이러한 환경 변화에 대응하기 위해 제조사는 제품 보안과 공정(운영) 보안을 포괄하는 관점에서 체계적인 대응 전략을 수립해야 한다.

① **도메인별 적용 규제 식별**: 생산·공급하는 제품과 사업 범위에 적용될 수 있는 국내외 규제를 식별하고 목록화

② **규제 요구 사항 분석**: 규제가 제품 사이버보안을 요구하는지, 공정·운영 안전성을 요구하는지, 또는 두 영역을 동시에 요구하는지 구분하고, 구체적으로 요구하는 항목을 정리

③ **규제 내 참조 문서 확인**: 규제가 모든 구현 방법을 상세히 제시하지 않는 경우가 많으므로, 규제에서 참조하는 표준 문서(ISO/IEC 등)를 확인해 요구사항의 세부 해석 기준으로 활용

④ **현 수준 진단 및 차이 분석**: ①~③에서 정리한 요구사항·체크리스트를 기준으로 조직의 현재 프로세스, 운영 체계, 제품 보안 수준을 비교·점검하고 차이를 분석. 차이가 크다면 원인을 식별하고, 실제 운영 현실과의 정합성을 함께 검토

⑤ **보완 및 신규 정책 수립**: 분석 결과 확인된 차이를 기반으로 기존 정책·프로세스를 보완하고, 필요한 경우 신규 정책과 운영 절차를 수립해 규제 요구사항을 충족할 수 있도록 개선

⑥ **신뢰 기관을 통한 검증**: 대응 체계가 정비되면, 내부 확인에 그치지 않고 신뢰 가능한 외부 기관을 통해 검증을 수행함으로써 객관성 확보

이와 같은 절차를 체계적으로 수행할 경우, 제품 판매 과정에서 발생할 수 있는 규제 리스크와 비즈니스 제약을 사전에 완화할 수 있다.

■ 맺음말

최근 글로벌 규제와 산업 동향을 종합하면, 국내 산업 업체가 글로벌 시장에서 제품을 판매하기 위해 IT 및 OT 보안 역량은 사실상 필수 요건으로 자리 잡고 있다. 특히 공급망 보안 요구가 강화되면서, 신뢰할 수 있는 기관의 인증서 보유 여부가 거래 조건 또는 시장 진입 요건으로 인식되는 사례가 증가하는 추세다. 따라서 제조 기업은 공정(운영) 보안과 제품 보안을 함께 고려한 규제 대응 체계를 조기에 수립할 필요가 있다.

SK 쉴더스는 이러한 규제·요구사항 변화에 대응할 수 있도록 제조 고객을 대상으로 OT 보안 진단 및 컨설팅 조직을 운영하고 있다. SK 쉴더스는 규제 요구사항 매핑, 현 수준 진단 및 차이(Gap) 분석, OT 보안 로드맵 수립에 필요한 체크 체계를 구축·운영하고 있으며, 이를 기반으로 고객사의 대응 전략을 신속하게 도출한다.

또한 OT 공정 환경은 물론 제품 생산 과정과 제품 자체의 안전성까지 포괄하는 관점에서 보안 강화 활동을 지원한다. 아울러 신규 도메인 산업의 경우에도 축적된 노하우를 기반으로 관련 규제를 신속히 탐색·분석·검토해, 산업 특성에 최적화된 OT 보안 대응 체계를 수립할 수 있도록 지원한다.

■ 참고 문헌 및 자료

[1] “국가정보보안 기본 지침”, 국가시업 보안 센터,

https://www.ncsc.go.kr:4018/main/cop/bbs/selectBoardArticle.do?bbsId=InstructionGuide_main&nttId=18588&pageIndex=1

[2] “SW 공급망 보안 가이드”, 한국인터넷 진흥원,

https://www.kisa.or.kr/2060204/form?postSeq=15&page=1

[3] “NIST 800-82”, NIST, https://csrc.nist.gov/pubs/sp/800/82/r3/ipd

[4] “NIST CSF 2.0”, NIST, https://www.nist.gov/cyberframework

[5] “NERC CIP”, NERC, https://www.nerc.com/standards/reliability-standards/cip

[6] “NIS 2”. European Union, https://eur-lex.europa.eu/eli/dir/2022/2555

[7] “CRA”, European Union,

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R2847

[8] “ISO/IEC 27001”, ISO, https://www.iso.org/standard/27001

[9] “ISO/IEC 27019”, ISO, https://www.iso.org/standard/85056.html

[10] “ISO/SAE 21434”, ISO, https://www.iso.org/standard/70918.html

[11] “ISA/IEC 62443 시리즈”, IEC,

https://webstore.iec.ch/en/iec-search/result?q=62443&p=1&f=eyJkYXRlUmFuZ2VzIjp7fSwidGVybXMiOnt9LCJ2YWxpZE9ubHkiOnRydWUsInB1YmxpY2F0aW9uSWRzIjpudWxsLCJzaG93VHJmIjpmYWxzZSwiZGlzcGxheU1vZGUiOiJsaXN0In0=

[12] “UR E26 and UR E27”, IACS, https://iacs.org.uk/resolutions/unified-requirements/ur-e