SDGs 달성에 기여하는 보안 제품 개발에 대한 Yokogawa의 약속

호시노 히로시 (Hiroshi Hoshino) [*1] *츠지 히로타카 (Hirotaka Tsuji)* [*1]

플랜트와 핵심 인프라는 사회의 기초이기 때문에, 운영 설비 가용성을 극대화하고 고객에게 제품과 서비스를 지속적으로 제공하려면 이에 대한 장기적 안정적 운영이 보장되어야 합니다. 이를 위해서는 사이버 공격으로부터 시설을 보호할 수 있는 안전한 제품과 장비를 도입해야 합니다.

이 비전(Commitment)은 또한 SDGs (SDGs9)에 정의된 회복 탄력적인 사회 인프라를 달성하는데 도움이 됩니다.

취약성 해결은 보안 제품 개발의 기초입니다. 그러나 취약성 해결이 개발 효율성과 제품 기능 (사용성)의 향상으로 직접 연결되는 것은 아니기 때문에 개발 프로세스에서 종종 우선 순위가 낮아집니다.

이러한 문제는 단일 사업부에선 해결할 수 없습니다. 사회 인프라를 담당하는 회사로써 Yokogawa는 이를 지원하는 시스템, 거버넌스, 개발에 대한 전사적 접근 방식을 채택하여 이 문제를 해결하고 있습니다. 이 문서는 보안 제품 개발에 대한 Yokogawa의 약속과 노력을 설명합니다. 구체적으로는 회사의 정책, 조직 구조, 보안 시스템 제품 개발 프로세스 (Secure Development Life Cycle (보안개발 수명주기): SDLC) 및 관련 국제 인증을 획득을 포함하고 있습니다.

도입

사이버 보안 위협은 그 대상이 사회 인프라로 확산됨에 따라 심각한 사회 문제가 되고 있습니다.

악명 높은 예는 2015년과 2016년 우크라이나에서 발생한 사이버 공격으로 전기 변전소의 차단기를 셧다운이 발생했습니다. 이 사건으로 대규모 정전이 발생해서 6시간 동안 22만 가구에 영향을 미쳤습니다. 또한 사우디 아라비아 석유 공장의 안전 계측 시스템을 겨냥한 2017년 사이버 공격으로 인해 제어 컨트롤 프로그램이 중단되어 공장이 중단되었습니다. 만약 시스템이 완전히 탈취당했다면 안전, 환경 및 인명 손상도 있었을 것입니다.

사회 인프라를 담당하는 회사는 지속적으로 사이버 보안을 위한 조치를 취해야 한다는 것이 분명해졌습니다.

*1 IA 시스템 및 서비스 사업 본부
라이프 사이클 서비스 사업부의 사이버 보안 관리부

시설의 장기 안정적인 운영을 위한 보안 조치

플랜트 및 핵심 인프라의 자산 소유자는 시설의 가용성을 극대화하고 고객과 사용자에게 가치를 제공하기 위해 장기 안정적 운영을 목표로 하므로 안전한 제품을 도입하고 사이버 보안 위협으로부터 보호해야 합니다. 이는 SDG9 “회복 탄력성 있는 인프라 구축” 달성과 관련이 있습니다. 이 섹션에서는 안전한 제품을 개발하고 장기 안정적 시설 운영을 보장하기 위한 Yokogawa의 노력에 대해 설명합니다.

일반 보안 조치 및 관련 문제

플랜트 및 중요 인프라를 운영하는데 사용되는 주요 구성 요소인 제어 시스템에 대한 다양한 보안 조치가 있습니다. Yokogawa는 오랫동안 제어 시스템에 대한 보안 조치를 개발해 왔습니다. 먼저, 제어 시스템이 안정적으로 작동할 수 있도록 운영 체제 (OS) 업데이트 프로그램을 제공합니다. 또한 제어 시스템와 함께 사용할 수 있는 바이러스 백신 소프트웨어도 제공합니다. 제어 시스템을 안전하게 관리하고 유지하기 위한 이러한 지원은 보안 사고 및 셧다운 (shutdown) 위험을 줄이고 장비가 장기간 안정적으로 작동할 수 있도록 합니다.

OS 업데이트 프로그램 및 안티 바이러스 소프트웨어는 제어 시스템에 대한 효과적인 보안 조치이지만 제어 시스템 소프트웨어의 취약성 (vulnerability)에 대한 공격을 방지하지는 못합니다. 취약성 (vulnerability)은 공격자가 불법적으로 정보를 얻거나 시스템을 탈취하는 데 사용할 수 있는 소프트웨어의 보안 취약점입니다. 제어 시스템의 장기 안정적 운영을 위해서는 이러한 취약점을 제거하는 것이 필수적입니다.

취약성은 모든 프로세스에서 그리고 심지어 제품 출하 후에도 주의 깊게 감지되고 해결되어야 합니다. 그러나 이 작업이 일반적으로 제품 기능 직접적 향상이나 개발 효율성 향상과 직접 연결되지 않으므로 개발 프로세스에서 우선 순위를 얻지 못할 수 있습니다. 이러한 딜레마는 SDGs 달성의 어려움과 유사합니다. 경제적 이익만 추구하면 의도하지 않은 부작용이 발생하여 사회의 건강을 위협할 수 있는 취약성이 발생할 수 있습니다. 이 문제를 극복하기 위해 SDGs가 작성되었습니다. 두 가지 방법 모두 편리함과 효율성만을 추구하지 않으려고 합니다.

도전에 대한 해결책으로서의 거버넌스 및 개발 프로세스

개별 사업부는 스스로 취약점을 해결할 수 없습니다. 경제적 이익을 추구하면서 이러한 문제를 해결하기 위해 사회 인프라에 관련된 회사는 적절한 기업 지배 구조 및 개발 프로세스와 이를 지원할 수 있는 시스템이 필요합니다.

다음 섹션에서는 보안 제품 개발을 위한 규칙 및 시스템, 보안 시스템 제품 개발 프로세스 및 인증 획득 노력에 초점을 맞춘 보안 제품 개발을 위한 Yokogawa의 노력을 설명합니다.

제품에 대한 사이버 보안 위협에 대한 조치

Yokogawa는 회복 탄력적 사회 인프라 구축에 도움이 되는 제품과 서비스를 제공합니다. 이 섹션에서는 제품에 대한 사이버 보안 위험을 관리하는 방법, 보안 제품을 개발하는 방법 및 취약성을 적절히 해결하는 방법 및 이를 위한 Yokogawa의 기업 지배 구조에 대해 설명합니다.

제품에 대한 사이버 보안 위험 관리

장기적으로 안정적인 플랜트 운영을 하려면 고객은 보안 시스템을 도입하고 보안 수준을 유지해야 합니다.

이러한 고객을 지원하기 위해 Yokogawa는 안전한 제품 제공은 물론이고 납품 후 취약성 완화, 운영 환경 보호 솔루션과 같은 플랜트 라이프 사이클 전반에 걸친 대책도 제공합니다. 이 문제는 개별 비즈니스 조직에서 해결할 수 없습니다.

따라서 Yokogawa는 2015년에 전사적 차원에서 비즈니스 조직이 동일한 접근 방식으로 협력할 수 있도록 기본 정책을 마련했습니다. 현재 각 비즈니스 조직은 기본 정책을 공유하고 고객 사이트에서 동등한수준의 시스템 보안을 유지합니다.

〈〈기본 방침〉〉

Yokogawa Group 은 고객이 안전하게 비즈니스를 계속할 수 있도록 자산에 대한 사이버 위협에 대해 고객과 협력 및 노력을 계속 할 것입니다.

제품에 대한 사이버 보안 위험 관리 시스템

Yokogawa 제품에 대한 사이버 공격은 고객에게 사업 손실을 초래할 수 있으므로 Yokogawa는 이러한 종류의 위험을 관리적 위험으로 간주합니다. 사이버 보안 리스크 관리 시스템 (그림1)에서는 리스크 관리 담당자와 리스크 관리 조직이 제품 관련 사이버 보안 리스크를 모니터링하고 검토합니다. 검토 결과는 그룹 규정에 반영되어 대응 정책 및 기준으로 설정됩니다. 관리자의 감독하에 제품 기획 및 개발 담당자와 서비스 담당자는 그룹 규정을 자체 관리 절차에 반영하고 그들의 작업을 수행합니다. 따라서 각 비즈니스 조직은 고객에게 안전한 제품과 서비스를 제공합니다.

사이버 보안 리스크 관리 활동은 감사 기관의 감사를 받고 그 결과는 이사회 및 관리자 회의에 보고됩니다.

위에서 언급했듯이 제품의 사이버 보안 위험과 관련된 활동은 Yokogawa의 경영진이 감독합니다. Yokogawa그룹은 고객의 플랜트의 장기 안정적 운영의 중요성을 인식하고 이를 달성하기 위해 열심히 노력하고 있습니다.

사이버 보안 대응 개선 노력

고객 시스템의 보안 수준을 유지하려면 각 사업부가 협력해야 합니다. 내부 정보 및 관련 인프라 관리도 마찬가지입니다.

제품에 대한 기밀 정보가 누출될 경우, 우리는 그 영향과 위험을 관련 인원에게 즉시 알려야 합니다. 이를 위해 다음 조직이 협력해야 합니다: 정보관리를 제어하는 ISMS Office (정보보안관리 시스템 사무소: Information Security Management System Office); 정보 인프라에 대한 사이버사고를 처리하는 CSIRT (Computer Security Incident Response Team: 컴퓨터 보안사고 대응 팀); 제품에 대한 사이버 사고에 대응하는 PSIRT (Product Security Incident Response Team: 제품 보안사고 대응 팀); 고객에게 솔루션을 제공하는 보안 사업 담당자

Yokogawa는 사이버 보안 정보를 공유하기 위해 ‘조직 간 정보

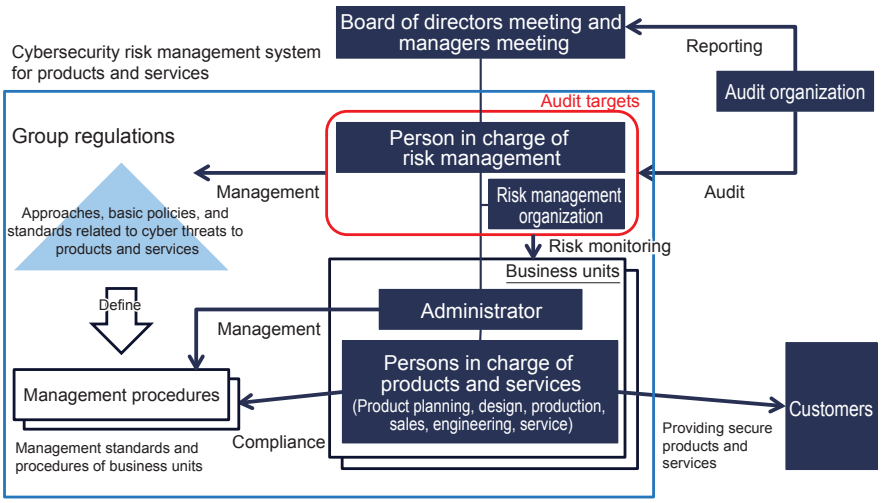


그림1 사이버 보안 위험 관리 시스템

보안위원회 (cross-organizational information security committee)'를 운영하고 있습니다 (그림2).

정보 보호위원회는 보안 담당관 아래 ISMS실, CSIRT, 제품 보안 담당 부서, 정보를 조사하는 마케팅 담당 부서, 솔루션을 제공하는 보안 업무 담당 부서로 구성됩니다. 이 위원회는 사이버 보안의 최신 동향을 파악하고 정보를 공유하여 사이버 보안 위협에 대한 그룹의 대응책을 개선하고 있습니다.

안전한 제품 개발을 위한 노력

산업 인프라를 담당하는 회사인 Yokogawa는 고객 플랜트의 안정적 운영을 보장하기 위해 제품의 취약점 해결에 노력하고 있습니다.

취약점이 없는 안전한 제품을 개발하기 위해 Yokogawa 그룹 설계 표준 (Yokogawa Group Design Standards)에 관리 표준 및 절차를 정의했습니다. 각 개발 프로세스에 대해 품질 경영 시스템에서 보안 설계 기준을 충족하는지 확인합니다.

진화하는 사이버 위협에 대응하기 위해 조직 간 정보 보안위원회 (cross-organizational information security committee)'에서 엔지니어링 표준을 정기적으로 검토합니다. 또한 보안 제품에 대한 지침 및 도구 개발을 주도하고 개발 담당 부서를 지원합니다.

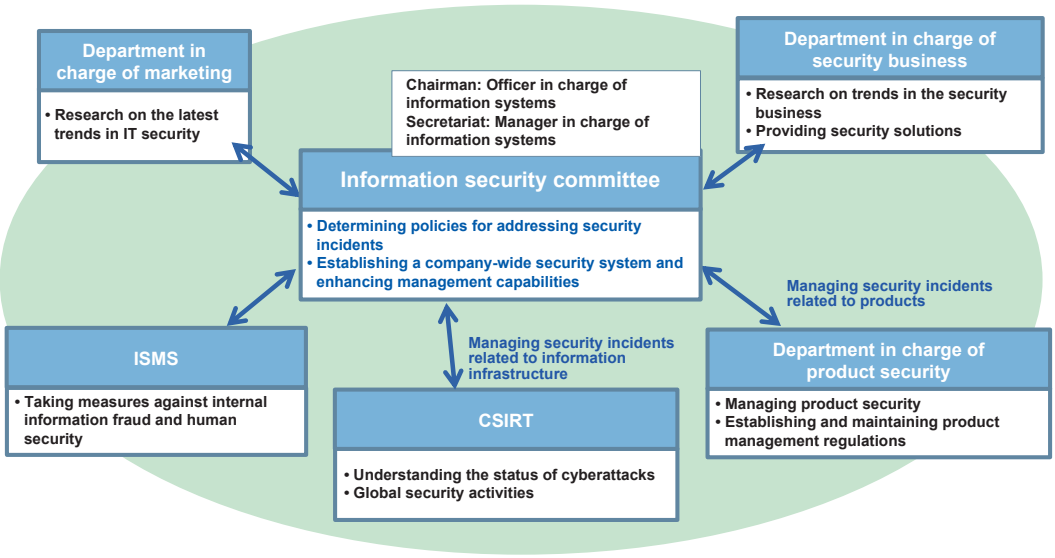


그림2 정보 공유 시스템

이러한 노력을 바탕으로 각 제품이 고객의 엄격한 보안 요구 사항을 충족하는지 확인합니다.

제어 시스템 제품과 관련하여 우리는 “보안 제어 시스템 제품을 개발하기 위한 노력” 섹션에 설명된 대로 보안 인증을 적극적으로 획득하고 있습니다.

제품 취약성을 처리하는 방법

고객은 공장 운영을 강화하고 안정화하기 위해 사이버 보안 위험을 관리해야 합니다. 이를 위해서는 플랜트에 설치된 장비의 취약점을 파악하고 대응하는 것이 필수적입니다. Yokogawa는 고객이 사이버 보안 위험을 관리할 수 있도록 관련 정보를 공개합니다. 적절한 정보를 얻고 공개하려면 내부 및 외부 당사자 (정보 제공 업체, 제품 및 서비스 담당자 등)와의 협력이 필요합니다. 다음 섹션에서는 정보 획득에서 공개에 이르기까지 취약성 정보를 처리하는 프로세스 및 시스템에 대해 설명합니다.

취약점 처리 프로세스 및 시스템

Yokogawa는 제품 취약성을 처리하는 조직인 Yokogawa PSIRT를 설립하고 ISO/ IEC30111 국제 표준 기반 취약성 처리 프로세스에 따라 고객에게 관련 정보를 공개합니다 (그림3).

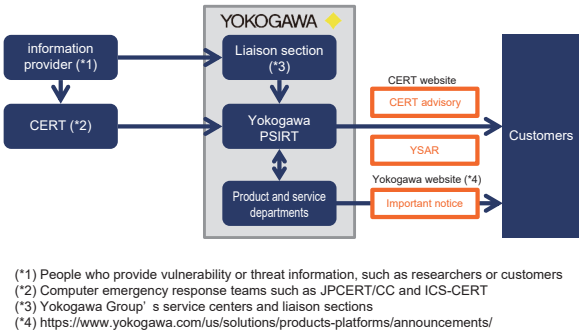
Yokogawa PSIRT는 JPCERT/CC 및 ICS-CERT와 협력하여 Yokogawa 내부 및 외부에서 정보를 적극적으로 수집합니다. 검증 과정에서 획득한 정보는 개발 및 서비스 담당자에게 전달되어 영향을 받는 제품이 있는지 확인합니다.

심각도 평가 프로세스에서 Yokogawa PSIRT는 관련 제품의 개발 및 서비스 담당자와 협력하여 취약성의 중요성 정도를 평가합

그림3 취약성 처리 프로세스

니다. 공개 과정에서 Yokogawa PSIRT는 외부 정보 제공자, ICS-CERT 및 개발 및 서비스 담당자와 공개 시점 및 내용을 논의합니다. 그 결과를 바탕으로 Yokogawa PSIRT는 개발 및 서비스 담당자와 협력하여 YSAR (Yokogawa Security Advisory Report: Yokogawa 보안 자문 보고서)를 작성하고 Yokogawa의 웹 사이트 및 기타 미디어를 통해 고객에게 정보를 공개합니다. 내부 및 외부 이해 관계자와의 조정을 위해 조직은 JPCERT 조정 센터 (JPCERT/CC)와 정보기술 진흥기관 (Information-technology Promotion Agency: IPA)에서 제정한 정보 보안 조기 경보 파트너십 지침 (Information Security Early Warning Partnership Guidelines)을 따릅니다. 둘 다 일본에 있는 취약점 정보를 조정하는 조직입니다. 그림4는 Yokogawa PSIRT의 활동을 요약한 것입니다.

Yokogawa PSIRT는 취약점 처리에 대한 국제 표준 및 지침을 따르고 고객이 위험을 관리하는 데 도움이 되는 유용한 정보를 제공합니다. Yokogawa PSIRT는 증가하는 취약성 정보에 대응하기 위해 프로세스를 체계화하고 있습니다. 이러한 노력은 그룹의 효율성을 개선하고 적시에 고객에게 정보를 제공합니다.



(*1) People who provide vulnerability or threat information, such as researchers or customers
(*2) Computer emergency response teams such as JPCERT/CC and ICS-CERT
(*3) Yokogawa Group’ s service centers and liaison sections
(*4) https://www.yokogawa.com/us/solutions/products-platforms/announcements/

그림4 Yokogawa PSIRT의 활동

취약성 정보 제공

Yokogawa는 고객이 위험을 관리할 수 있도록 제품 취약성 정보를 광범위하게 공개합니다. 조사 및 평가된 취약성 정보와 함께 개발 직원이 준비한 대응책을 일본 국내외 고객에게 공개합니다. 이 정보는 당사 웹 사이트[1], JPCERT/CC 및 IPA에서 편집한 일본 취약성 정보 (JVN)[2], 제어 시스템 제품의 취약성 정보를 조정하는 글로벌 조직인 ICS-CERT의 취약성 데이터베이스[3]에서 확인할 수 있습니다.

또한 Yokogawa 웹 사이트에 취약성 처리에 대한 기본 정책[4]을 공개하여 고객과 사회가 취약성에 대한 Yokogawa의 입장을 이해할 수 있도록 하고 위험 관리를 할 수 있도록 도움을 제공합니다.

Yokogawa는 2015년에 JPCERT/CC로부터 취약점 처리에 대한 감사장 (certificate of appreciation)을 받았습니다[5]. 사유는 사이버 보안 조치에 대한 탁월한 기여와 제어 시스템 공급업체로서 선구적인 역할이었습니다.

보안 제어 시스템 제품 개발을 위한 노력

"보안 제품 개발 노력" 섹션에 설명된 보안 제품 개발을 위한 Yokogawa 그룹 설계 표준 (Yokogawa Group Design Standards)에 따라 각 개발 부서에는 자체 프로세스가 있습니다. 이 섹션에서는 IEC 62443-4-1 국제 표준[6]을 소개합니다. 이 표준은 제품 및 관련 예에 대한 프로세스를 개발할 때 참조합니다.

IEC 62443-4-1 국제 표준

제어 시스템 보안을 위한 국제 표준인 IEC 62443은 산업 제어 시스템과 관련된 다양한 플레이어(자산 소유자, 서비스 제공 업체 및 제어장비 제품 공급업체)에 대한 요구 사항을 규정합니다. IEC 62443-4-1은 제어장비 제품 공급업체가 설계 단계에서 보안 조치를 취할 수 있도록 개발 프로세스에서 다 계층 방어 심층 프레임워크 (multi-layered defense-in-depth framework)를 제공하도록 요구합니다. 표1에 나열된 관행은 제어장비 공급업체가 개발 프로세스에서 수행해야 하는 작업입니다.

표 1 개발 프로세스에 대해 IEC 62443-4-1에 규정된 보안 요구 사항

관행 (약어)	주요 목적
보안 관리 (SM)	보안 제품 개발을 위한 시스템 구축
보안 요구 사항 (SR) 사양	보안 요구 사항 및 사용 조건 정의
설계 단계의 보안(SD)	심층 방어 전략에 기반한 보안 설계
보안 구현 (SI)	보안 코딩
보안 검증 및 검증 테스트 (SVV)	보안 관련 테스트의 문서화 및 구현
보안 관련 문제 (DM) 관리	식별된 취약점 처리
보안 업데이트 관리 (SUM)	보안 업데이트 제공
보안 지침 (SG)	사용자에게 통합에 필요한 정보 제공

SDLC (Secure Development Life Cycle: 보안 개발 수명주기) 조정

SDLC는 IEC 62443-4-1에 따라 보안 시스템 제품을 개발하기 위한 Yokogawa의 프로세스입니다. 그 목적은 취약점이 없는 제품을 개발하는 것입니다. SDLC는 그림5에 설명된 6단계로 구성됩니다. 우리는 각 단계의 출력에서 취약성을 최소화하고 개발 단계 초기에 취약성을 식별하여 안전한 제품을 개발합니다. 각 단계는 다음 섹션에서 설명합니다.

필수 사양 단계

필수 사양 단계의 주요 목적은 제품의 요구 사항 및 사용 조건을 이해하고 보안 개발 시스템 및 실행 계획을 개발하며 보안 요구 사항 및 외부 사양을 정의하는 것입니다. 이러한 활동을 지원하기 위해 보안 관련 활동을 실행하고 검토하는 보안 전문가가 제품별로 지정됩니다. 또한 각 개발 부서는 미래 보안 전문가 양성을 위해 IEC 62443-4-1 표준에 대한 교육 및 교육 프로그램을 제공합니다.

그림5 SDLC (보안 개발 수명주기)

설계 단계

설계 단계의 주요 목적은 생성될 수 있는 가능한 많은 취약점을 설계 프로세스 중에 제거하는 것입니다. 이 단계에서는 외부 사양을 기반으로 보안 요구 사항을 충족하는 특정 기능을 설계하고 보안 측면에서 소프트웨어의 전체 구조를 확인합니다. 또한 위협 분석을 수행하여 보호할 자산, 자산 간 상호 인터페이스 및 가능한 위협을 식별합니다.

이러한 활동을 지원하기 위해 위협 분석 및 설계 중에 고려해야 할 사항을 요약한 보안 제품 개발 지침을 마련했습니다.

구현 단계

구현 단계의 주요 목적은 구현 프로세스 중에 발생할 수 있는 가능한 많은 취약점을 제거하는 것입니다. 설계 문서를 기반으로 소프트웨어를 구현할 때 버퍼 오버플로 (buffer overflows)와 같은 보안 문제를 일으킬 수 있는 코드를 식별하고 해결해야 합니다. 이를 지원하기 위해 우리는 사람이 검토할 때 간과될 수 있는 소스 코드 문제를 식별할 수 있는 정적 코드 분석 도구 (static code analysis tool)를 사용합니다.

검증 단계

검증 단계의 주요 목적은 제품에 알려진 취약점이 없고 보안 기능이 효과적으로 구현되었는지 확인하는 것입니다. 이 단계에서는 보안 요구 사항을 충족하기 위해 구현된 보안 기능의 유효성을 확인하는 것은 물론 잠재적 대상 영역 식별, 오픈 소스 소프트웨어 문제 확인, 통신 퍼징 (fuzzing) 테스트 등 다양한 기술로 보안 테스트를 수행합니다. 이를 지원하기 위해 상용 테스트 도구를 사용하고 테스트의 효율성을 개선합니다.

출시 단계

출시 단계의 주요 목적은 개발 프로세스 전반에 걸쳐 필요한 노력이 수행되었는지 확인하고 제품 배송 시 바이러스가 없는지 확인하는 것입니다. 이를 지원하기 위해 보안 전문가는 체크리스트를 사용하여 최종 확인을 수행합니다.

유지보수 관리 단계

유지 보수 관리 단계의 주요 목적은 배송 후 취약점을 해결하는 것입니다. 앞서 언급한 취약성 처리 조직과 협력하고 보고된 취약성을 분류하며 개발 중에 발견된 취약성을 보고합니다. Microsoft Windows 운영 체제 (당사 제품의 플랫폼)에 취약점이 발생할 경우 보안 패치를 적용해야 할 수 있습니다.

이 경우 당사는 각 상품에 필요한 정보를 유료 서비스로 제공합니다.

보안 인증서 획득을 위한 노력

2014년에 Yokogawa는 CENTUM VP 통합 생산 제어 시스템 및 ProSafe-RS 안전 계장 시스템에 대해 ISCI[7]로부터 EDSA (ISASecure Embedded Device Security Assurance) 보안 인증을 받았습니다. 둘 다 Yokogawa의 OpreX 제어 및 안전 시스템 제품입니다. 2020 년 1 월 제어 시스템 개발을 담당하는 Yokogawa의 부서는 보안 개발 수명주기에 대해 ISCI로부터 ISASecure SDLA (Security Development Lifecycle Assurance: ISA 보안 임베디드 장치 보안 보증) 인증을 획득했습니다. 이러한 최근의 인증 획득은 개별 제어 시스템 제품은 물론 Yokogawa의 개발 프로세스도 국제 표준 IEC 62443-4-1을 준수한다는 증거입니다.

결론

사회 인프라에 관련된 회사는 제품 시스템이 장기 안정적으로 작동하도록 할 책임이 있습니다. 이를 위해 지속적으로 사이버 보안 조치를 취하고 이러한 노력에 대한 책임을 져야합니다. Yokogawa는

제품에 대한 사이버 보안 위협을 해결하고 책임을 지는 시스템을 구축했습니다. 또한 보안 제품 개발 노력이 객관적으로 뒷받침될 수 있도록 각 개발 시스템에 대한 외부 평가 및 인증을 획득했습니다. 이러한 보안 제품의 개발을 통해 Yokogawa는 회복 탄력적 사회 인프라(SDG9)를 구축하고 2050년을 향한 Yokogawa의 3가지 목표 중 하나인 순환 경제(Circular Economy)를 달성하는 데 기여할 것입니다.

참고문헌

(1) Yokogawa Electric Corporation, "Yokogawa Security Advisory Report List," https://www.yokogawa.com/library/resources/whitepapers/yokogawa-security-advisory-report-list/ (accessed on September 15, 2020)
(2) JPCERT/CC, IPA, Japan Vulnerability Notes (JVN), https://jvn.jp/ (accessed on September 15, 2020)
(3) ICS-CERT website, https://www.us-cert.gov/ics/ (accessed on September 15, 2020)
(4) Yokogawa Electric Corporation, Yokogawa Group Vulnerability Handling Policy, https://www.yokogawa.com/solutions/productsplatforms/announcements/vulpolicy/ (accessed on September 15, 2020)
(5) "JPCERT Coordination Center presents a certificate of appreciation to collaborators for cybersecurity activities," (in Japanese) https://www.jpcert.or.jp/press/priz/2015/PR20150820-priz.html (accessed on September 15, 2020)
(6) IEC, IEC 62443-4-1 "Security for industrial automation and control systems–Part 4-1: Secure product development lifecycle requirements," 2018
(7) ISA Security Compliance Institute (ISCI), https://www.isasecure.org/en-US/Certification (accessed on October 4, 2020)