

ITIL 우수 사례를 통해 개선된 Managed Service

라이콩 추 (Chooi LaiKong)^{*1}

현장 생산 작업의 운영 유연성과 효율성을 개선하기 위해 제조업체들은 자사의 산업 자동화 및 프로세스 제어 시스템에 개방형 표준 네트워크(open-standard networks)를 도입했습니다. 이러한 네트워크를 통해 플랜트 관리자는 시스템에 원격으로 액세스하고 엔지니어링 인력 및 외부 파트너들과 플랜트 데이터, 애플리케이션 및 리소스를 공유할 수 있습니다. 숙련된 근로자의 수가 줄어들면서 플랜트 내 문제점에 대한 정보 공유와 신속한 대응이 어렵기 때문에 자동화 공급 업체의 원격 지원 서비스가 점점 더 요구되고 있습니다. 이에 대한 대응으로 Yokogawa는 정보 기술 인프라 라이브러리(information technology infrastructure library, ITIL) 접근 방식의 우수 사례를 기반으로 한 Managed Service를 출범시켰습니다. 본 글에서는 Managed Service가 운영 효율을 어떻게 개선하는지에 대해 소개합니다.

도입

현장 생산 작업의 유연성과 효율성을 높이기 위해, 제조업체들은 산업 자동화(IA) 및 제어 시스템에 개방형 네트워크 표준(open network standards)을 도입했습니다.

개방형 네트워크는 플랜트 관리자가 물리적 위치에 관계없이 제어 시스템에 원격으로 액세스하고, 플랜트 운영에 대한 정확한 정보, 애플리케이션 및 리소스를 엔지니어 및 그 밖의 플랜트 인력과 공유할 수 있도록 해주는 장점이 있습니다. 반면에, 플랜트 제어 시스템과 장비가 서로 다른 공급 업체로부터 제공되기 때문에 보안 관리가 어렵고 복잡한 경향이 있습니다. 따라서 통합된 보안 관리 시스템을 확립하고 운영하는 것이 필요합니다.

아울러, 인구 고령화 및 그 밖의 요인들로 인해 숙련된 근로자가

감소하여 플랜트 장비를 관리하고 비상시 신속하게 대응하는 것이 점점 더 어려워지고 있습니다. 플랜트 관리자는 공급 업체가 원격 접속 및 기타 수단을 통해 제어 시스템의 안정적인 운영을 보장할 수 있도록 운영 기술(OT) 분야의 지원을 제공할 것을 기대하고 있습니다. 관리자가 개방형 네트워크의 보안 관리를 포함해서 IT 지원도 공급 업체에 맡길 수 있다면, 이들은 자사의 주된 생산 업무에 집중할 수 있게 됩니다. 이에 따라, 도입에서부터 관리 및 운영까지 IT와 OT의 통합 서비스를 위한 관리 서비스의 필요성이 높아지고 있습니다.

IA 산업에서는 현재 IT/OT 융합 개념이 널리 받아들여지고 있습니다. 2013년, 업계 내에서조차 아직 그 용어가 생소할 때, Yokogawa는 이러한 서비스를 제공할 기회가 있었습니다. 영국의 다국적 석유 및 가스 회사인 Shell은 전 세계에 걸친 자사의 플랜트에 Shell SecurePlant 솔루션 프로젝트를 수행할 계획을 세웠고, IT 업계 솔루션 선두 주자인 Cisco Systems와 Yokogawa를 파트너로 선택했습니다. Yokogawa는 이미 Shell과 오랜 파트너십이 확립되어 있었으며, 프로세스 제어 분야에서 상위 솔루션을 제공했습니다. 또한

^{*1} 디지털 솔루션 본부 산하 라이프사이클 서비스 사업부 서비스 Coe 부서

Yokogawa는 IA 분야에서 OT 용 제어 시스템 구축에 광범위한 경험을 가지고 있었습니다. 이 세 회사가 공동으로 종합 사이버 보안 관리 솔루션을 개발했으며, Yokogawa는 운영 서비스를 제공했습니다. 개발 배경에 대해서는 다음 섹션에서 설명합니다.

본 글에서는 Yokogawa가 SecurePlant 프로젝트를 통해 얻은 경험 및 전문 지식과 정보 기술 인프라 라이브러리(information technology infrastructure library, ITIL)의 다양한 우수 사례를 최대한 활용하여 Opnex Managed Service의 기반을 마련하고 새로운 서비스를 개발한 운영 구조를 어떻게 구축했는지 설명합니다.

또한 이 프로젝트에서 위임받은 조직의 설립, 프로젝트에 필요한 내부 제어 시스템, 그리고 이 새로운 서비스 조직이 어떻게 새로운 비즈니스로 이어지게 되는지에 관해 설명합니다.

본 글은 다음과 같이 구성되어 있습니다.

- (1) Shell SecurePlant 개발의 배경
- (2) 솔루션 및 서비스 고안
- (3) SSAE16에 따른 내부 제어
- (4) 새로운 서비스에 의한 이점 및 향후 과제
- (5) 향후 개발

SHELL SECUREPLANT 개발의 배경

Shell이 SecurePlant 솔루션의 개발 및 구현을 결정한 다양한 이유 중에는 사이버 공격의 위협에 대응하기 위해 철저한 보안 관리 확립에 대한 긴급한 필요가 있었습니다.

당시 Shell의 각 지역 사무실 및 플랜트는 제어 시스템 및 그 구성 요소 PC에 대해 각자의 재량에 따라 OS 보안 업데이트 및 바이러스 백신 소프트웨어를 선택했습니다. 플랜트에서도 바이러스 정의 파일의 업데이트를 독립적으로 관리하는 경우가 많았습니다. 그 결과 보안 운영 및 관리가 각기 달랐고, 보안 조치가 적시에 시행되었는지 여부는 아무도 알지 못했습니다.

Shell은 자체 IT 서비스 데스크에 그 관리를 위임했습니다. 그러나 각 지역 및 장비마다 서로 다른 공급 업체의 제어 시스템이 있었기 때문에 한 부서가 그 복잡한 보안 관리를 다루는 것이 쉽지 않았습니다. 그래서 설치, 관리 및 운영을 포함하여 보안과 관련된 모든 사항을 지원할 수 있는 서비스 공급 사업자가 필요했습니다.

이에 따라 Shell, Cisco, Yokogawa는 제어 시스템의 보안 관리를 강화하고 표준화하는 종합적인 사이버 보안 관리 솔루션인 SecurePlant를 설계, 개발, 운영하기 위해 함께 노력했습니다.

세 회사가 공동으로 설계하고 개발한 솔루션은 전용 Shell 플랜트에서 출시되었습니다. 이 솔루션은 대상 제어 시스템에 대한 보안 업데이트와 바이러스 백신 소프트웨어에 대한 정의 파일을 하나의 패키지로 제공합니다. Yokogawa는 서비스 데스크 운영을 담당하여, 이 솔루션의 작동 및 건전성 상태를 모니터링하고 중앙 집중 방식으로 플랜트를 관리했습니다. 이를 통해 각 현장에 전달된 장비에 대한 정보를 실시간으로 파악할 수 있었고, 보안 업데이트 프로그램 및 바이러스 정의 파일의 전달 및 애플리케이션 상태를 주기적으로 점검할 수 있었습니다. Yokogawa의 서비스 데스크는 전 세계에 있는 Shell의 모든 현장에서 발생하는 모든 사건에 즉각적으로 대응하기 위해 24시간 연중무휴로 운영했습니다. 그림 1은 SecurePlant 솔루션의 아키텍처 및 운영 흐름을 보여줍니다.

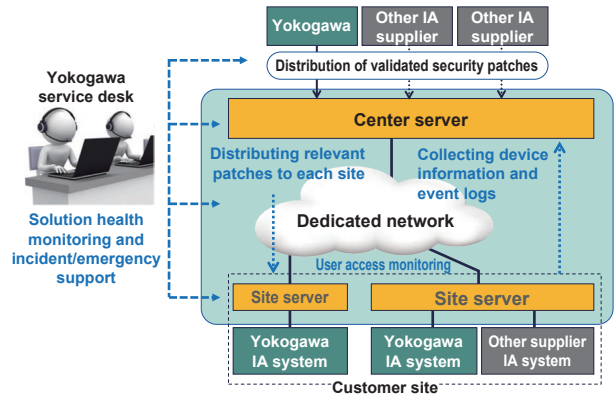


그림1 SecurePlant 솔루션의 아키텍처 및 운영 흐름

솔루션 및 서비스 고안

Shell의 각 현장에 SecurePlant 솔루션을 신속하게 배치하기 위해 Shell은 Yokogawa에 엔지니어 교육과 지원 시스템 구축을 요청했습니다. 이 경우에 엔지니어는 각 현장에서 시스템 납품 및 시운전을 관리하는 엔지니어와 서비스 데스크에서 일하는 엔지니어의 두 그룹으로 분류되었습니다. 이에 대한 대응으로, 프로젝트에 참여한 Yokogawa의 모든 직원들이 함께 일했습니다. 특히, 우리는 다양한 ITIL 우수 사례를 활용하여 IT 서비스 관리 프레임워크를 충족하는 조직을 효율적으로 구축하고 각 엔지니어가 자신의 기술을 연마할 수 있도록 지원했습니다. 결과적으로 우리는 Shell의 모든 플랜트에 고급 서비스를 제공하는 운영 체제를 확립할 수 있었습니다.

IT 서비스 관리 분야에서 IT 솔루션 관리의 성숙도는 인력, 프로세스, 기술이라는 세 가지 요소의 균형에 의해 결정됩니다. 그림 2에서 보는 바와 같이 이 세 가지 요소를 잘 균형 잡힌 방식으로 결합하는 것이 중요합니다.

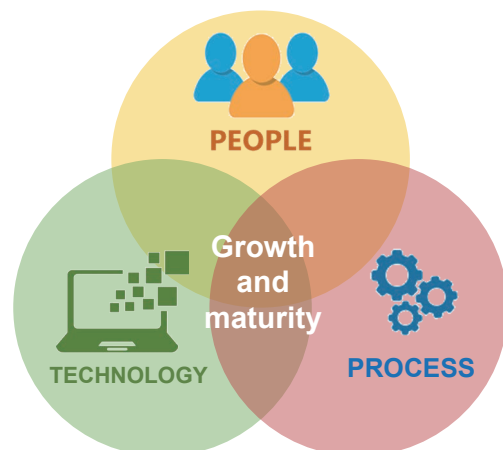


그림2 인력, 프로세스, 기술 간 균형이 잘 잡힌 모습

먼저, 인력 관점에서 역할과 책임이 명확하게 정의된 시스템을 구축합니다.

프로세스의 관점에서는, 작업을 수행하기 위한 프로세스와 문서를 명확히 합니다. 그런 다음 기술의 관점에서 조직을 관리하고 업무를 수행하는 데 필요한 도구 및 시스템을 도입합니다.

SecurePlant 프로젝트를 시작할 때 우리는 각 그룹에 필요한 인력 규모 및 다양한 기술을 판단하여 그림 3에서 보는 바와 같이 3개의 실무 그룹을 설치했습니다.

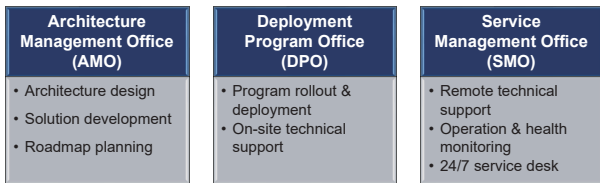


그림3 SecurePlant프로젝트 실행을 위한 3가지 그룹

아키텍처 관리 그룹(Architecture Management Office, AMO)은 SecurePlant 솔루션의 아키텍처 설계 및 개발, 배포관리 및 로드맵 작성을 담당합니다. AMO는 또한 효과적인 운영을 위한 도구를 개발하는 등 솔루션을 배치하고 서비스 운영을 개선하는 데에도 관여합니다.

배치 프로그램 그룹(Deployment Program Office, DPO)에는 두 가지 역할이 있습니다. 하나는 각 Shell플랜트에 솔루션을 배포할 때 표준화된 롤 아웃 프로세스를 결정하고, 각 현장과 협력하여 프로세스를 기반으로 실행 계획을 작성하며, 계획에 따라 솔루션을 배치하기 위해 엔지니어를 교육하여 각 현장에 배치하는 것입니다. 다른 하나는 시스템 납품 후 Shell의 각 현장에서 고객을 위한 교육을 제공하는 것입니다. 네덜란드에 있는 Yokogawa Europe B.V.(YEF)는 필요한 기술 및 관련 자료 준비 작업을 담당했습니다. 이와 더불어 Yokogawa는 Shell의 주요 현장 서비스를 담당하는 직원들을 교육하고 배치가 원활하게 이루어지도록 했습니다.

서비스 관리 그룹(Service Management Office, SMO)은 실시간으로 Shell의 각 현장에 있는 솔루션의 건전성 상태를 모니터링하고, ITIL에 정의된 프로세스를 따르면서 각 현장에서 보고되는 제반 사고를 처리하는 24시간 서비스 데스크를 갖추고 있습니다. Yokogawa는 24시간 연중무휴 서비스 데스크를 루마니아 YEF에 설치했습니다. 우리는 또한 네덜란드 YEF에 단계적 확대를 위한 전문가 조직(Center of Excellence, COE)팀을 설치하여 필요한 프로세스를 정의하고, 매뉴얼을 작성했습니다. 이와 더불어, 수작업을 줄이고 작업을 효율적이고 효과적으로 수행하기 위해 시스템화에 필요한 도구를 만들었습니다. 이를 통해 필요한 기술을 갖춘 인력의 확보, 명확한 프로세스 확립, 효율성 향상을 위한 기술과 도구 활용이라는 세 가지 요소의 균형을 잘 맞췄습니다.

Shell과 Cisco와의 좋은 관계를 유지하면서, 우리는 참여 모델이라는 관리방식 체계를 사용하여 솔루션 및 서비스 제공에 문제가 없도록 고위 경영진과의 정기적인 검토 및 논의를 수행했습니다. 그림 4는 이 체계를 보여줍니다.

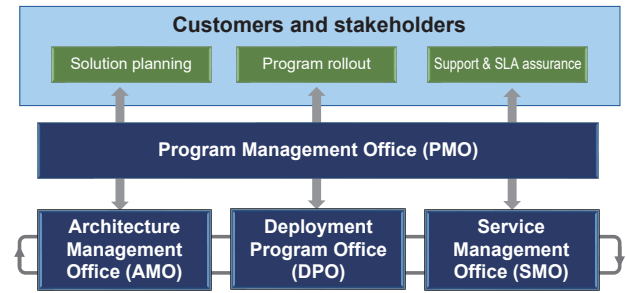


그림4 솔루션 및 서비스 구현을 위한 거버넌스 체계

그림 4는 조직 간 수평적 및 수직적 협력을 보여줍니다. 수평적으로 볼 때, AMO는 솔루션을 개발하고 배포하며, DPO는 각 현장에 이를 배치하고, SMO는 그 운영을 관리하고 지원합니다. 일상적 지원을 통해 SMO의 서비스 데스크는 피드백을 받아 AMO에 제공합니다. 이러한 협업은 다음 단계의 개발로 이어집니다.

수직적으로 볼 때, 프로젝트 관리 그룹(Project Management Office, PMO)은 AMO, DPO, SMO의 활동을 관리하고, 고객과의 정기적인 검토를 수행하며, 현장에서의 의견과 피드백을 점검하고, 고객의 요구 사항을 AMO, DPO, SMO의 활동에 반영합니다.

이러한 참여 모델을 기반으로, 커뮤니케이션이 잘 확립되고 모든 조직과 팀 간에 정보가 수직적 수평적으로 공유되어 모든 직원의 역량이 향상됩니다.

SSAE16에 따른 내부 제어

Shell과 Cisco에 의해 서비스 데스크 운영을 위임 받은 Yokogawa는 계약에 있어서 SAS 인증 보고서를 제출해야 합니다. 이는 Yokogawa가 서비스와 관련된 내부 제어 및 프로세스에 대해 독립 감사 법인의 감사를 받아야 하며, 또한 SSAE16(후에 SSAE18로 개정됨)의 요구 사항을 충족해야 한다는 것을 의미합니다. SSAE16⁽¹⁾은 미국 공인 회계사 협회(American Institute of Certified Public Accountants, AICPA)가 발행하는 감사 표준 세트인 "Statement on Standards for Attestation Engagements No. 16"을 의미합니다. 감사 인들은 SSAE16을 지침으로 사용하여 아웃소싱 서비스를 수행하는 회사의 내부 통제에 대한 효과성을 검증합니다. 감사는 두 가지 특정 보고서로 마무리됩니다.

유형 1: 서비스 제공 사업자의 내부 제어 프레임워크(규칙 및 업무 흐름)가 명확하게 정의되었음을 확인함.

유형 2: 유형 1에 곁하여, 6개월에서 1년의 기간 동안 제어의 실행 및 효과성에 대해 확인함.

보안성(Security), 가용성(availability), 처리 무결성(processing integrity), 기밀 유지성(confidentiality), 개인 정보 보호(privacy)가 다섯 가지 기준이며, 이 중 하나 이상을 선택하여 확인합니다.

Yokogawa는 네덜란드의 감사 기관의 확인을 받았으며, 루마니아 YEF와 네덜란드 YEF의 서비스 데스크 운영에 대해 유형 1 및 유형 2 인증 보고서를 받았습니다.

또한 Yokogawa는 운영 중인 시스템 및 프로세스의 증빙을 기술하는 정기 보고서를 Cisco 및 Shell에 제출했습니다.

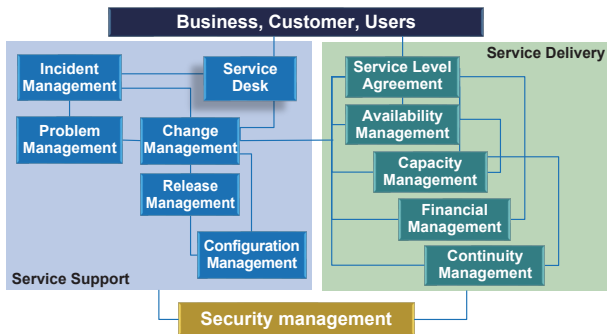


그림5 감사의 범위

그림 5는 감사의 범위를 보여줍니다. 본 운영에는 ITIL에서 정의된 두 가지 측면(서비스 지원 및 서비스 제공)이 있습니다. 서비스 지원(Service support)은 서비스 데스크가 운영 정보 시스템에서 수행하는 일상적인 업무(사고, 문제, 기타 관리)를 가리킵니다. 이러한 작업은 고객인 Shell이 서비스 데스크의 IT 서비스에 쉽게 액세스하고 사용할 수 있도록 보장합니다. 서비스 지원은 ITIL 운영 기준에 따라 체계적으로 관리되고 있는지에 대해 평가됩니다. 한편 서비스 제공(service delivery)은 다섯 가지 관리 프로세스, 즉 서비스 수준 협약(service level agreement, SLA), 재무 관리, 가용성 관리, 연속성 관리, 용량 관리 측면에서 평가됩니다.

내부 제어에 대한 감사를 받고 인증을 보고하는 것은 아웃소싱 업체와 서비스 제공 업체에게 모두 이득이 됩니다. Shell과 Cisco는 Yokogawa가 법과 규정을 준수하고 있다는 확신을 가질 수 있으며, Yokogawa는 고객의 개인정보 및 보안을 보호하며, 보고서를 다른 이해관계자에게 제공하기 위해 효과적인 내부 통제를 수립하고 운영할 수 있습니다. 이러한 통제를 통해 Yokogawa는 명확한 규칙을 따라 조직 운영을 수행할 수 있었습니다.

새로운 서비스에 의한 이점 및 향후 과제

Shell의 핵심 비즈니스가 아니었기 때문에 Shell 단독으로 IT/OT 솔루션을 표준화하고 이를 Shell SecurePlant 솔루션으로 출시하는 것은 쉽지 않았습니 다. 따라서 Shell은 각 분야에서 강점이 있는 두 기업과 협력하기로 결정했던 것입니다. Cisco는 IT 업계에서 솔루션 선두 주자이며, Yokogawa는 IA 분야에서 OT 제어 시스템의 구축 및 운영에 폭넓은 지식을 보유하고 있습니다. 그 결과, 이 세 기업은 IT 및 OT 영역 모두 보안 조치에 사용될 수 있는 표준화된 하드웨어 및 소프트웨어를 갖춘 솔루션을 설계할 수 있었고, Cisco와 Yokogawa가 설치한 서비스 데스크는 Shell사이트에 모든 IT 및 OT 지원을 제공했습니다.

또한 Yokogawa는 IT와 OT 지식을 모두 갖춘 엔지니어를 Shell의 현장에 파견했습니다. 이들은 Cisco 지원팀과 협력하여 시스템 배치 및 문제 해결 시 현장에 있는 직원들을 안심시켰고, Shell의 안정적인 운영에 큰 도움이 되었습니다.

SecurePlant프로젝트에서 이러한 조직을 설립하고 운영하면서, Yokogawa의 서비스 비즈니스 담당자는 인력, 프로세스, 기술의 세 가지 요소를 신중하고 균형 있게 결합하고 각 요소를 지속적으로 개선하는 것이 중요하다는 것을 알게 되었습니다. “인력” 측면에서, 서비스 데스크에 적합한 직원을 유지해야 합니다. 이를 위해 IT 엔지니어가 OT 지식을 습득하고 OT 엔지니어는 IT 지식을 받아들일 수 있도록 교육이 필요합니다. 최근 수년 동안 IT와 OT 지식 두 가지 모두를 최대한 활용할 수 있는 엔지니어의 필요성이 커지고 있습니다. 이들에 대한 채용과 교육을 반드시 고려해야 합니다.

아울러, 프로세스와 기술의 지속적인 개선이 필수적입니다. 근로자 개개인의 기술에만 의존하지 않고 운영의 효율성을 증대시키는 프로세스, 문서 및 유용한 도구를 적극적으로 도입할 필요가 있습니다. 또한 인력, 프로세스, 기술의 균형 잡힌 조합을 기반으로 운영 모델을 개발해야 합니다.

향후 개발

Shell SecurePlant프로젝트를 통해, Yokogawa는 ITIL의 다양한 우수 사례를 최대한 활용하여 그 서비스를 새로운 관리 서비스 분야로 전환할 수 있었습니다. 이것이 바로 OpreX Managed Service의 기반입니다.

OpreX Managed Service는 2030년을 향해 지속적으로 발전하고 성장할 것입니다. 운영 모델은 Shell SecurePlant프로젝트를 통해 개발된 인력, 그리고 확보된 지식과 경험을 계승할 뿐만 아니라, IA 산업 고객의 시장 요구를 충족시키기 위해 진화할 것입니다. 이는 Yokogawa의 서비스 비즈니스가 새로운 도약을 하기 위한 중요한 요소입니다.

결론

Shell의 결정에 따라, Cisco와 Yokogawa는 2021년 9월에 SecurePlant서비스를 종료하고 Shell에게 이양했습니다. 이 프로젝트를 시작한 이후, Yokogawa는 수 년에 걸쳐 귀중한 경험을 축적할 수 있었습니다. 우리는 이 프로젝트의 출범에 참여한 선구적인 직원 및 그 후임자들을 포함하여 관련된 모든 분들에게 감사를 표현하고 싶습니다.

참고문헌

(1) SSAE-16 website, <https://www.ssaе-16.com>

* OpreX is a registered trademark of Yokogawa Electric Corporation.

* All other company names, organization names, product names and logos that appear in this paper are either registered trademarks or trademarks of their respective holders.