

프로젝트 실행 및 사회 공헌에 대한 “Remote Engineering 및 FAT”의 효과

오자와 타케시 (Takeshi Ozawa)*¹ 타케다 나오타 (Naoya Takeda)*¹ 구보타 히데키 (Hideki Kubota)*¹

Yokogawa는 통합 제어 및 안전 시스템 (ICSS) 프로젝트에서 탄탄한 실적을 보유하고 있습니다. 최근에는 원격 Engineering 및 FAT (Factory Acceptance Test)가 가능한 환경 개발에 주력하여 성공적으로 애플리케이션을 개발하고 테스트를 수행했습니다. 이 환경은 CENTUM VP 통합 생산 제어 시스템 (integrated production control system)과 ProSafe-RS 안전 계장 시스템 (safety instrumented system) 및 네트워크 기술의 시뮬레이션 및 가상 I/O 기능을 기반으로 합니다. 이 기능을 사용하면 프로젝트에 관련된 모든 사람이 언제 어디서나 이 환경에 액세스 할 수 있습니다. 또한 이 기능은 COVID-19 대유행에 따른 사회적 거리두기의 필요성이 강하게 대두되면서 오늘날 주목을 받고 있습니다.

이 환경은 SDGs 달성, 특히 전염병 퇴치 (No. 3.3), 기후 변화 완화를 위한 에너지 절감 (No. 7.3 및 13.3)을 지원합니다. 생산 측면에서 새로운 라이프 스타일 달성을 위한 수단을 제공함으로써 지속 가능성도 향상될 것으로 예상됩니다 (No. 9.4 및 12.6).

이 백서에서는 이 환경의 구성과 성과를 설명하고 프로젝트를 보다 효율적으로 실행하는 방법과 해결해야 할 과제에 대해 설명합니다.

도입

최 근 몇 년 동안 Amazon의 AWS 및 Microsoft의 Azure와 같은 퍼블릭 클라우드를 사용하는 기업이 증가하고 있습니다. 이러

한 Cloud는 웹 서비스를 넘어 기업의 핵심 시스템을 포함하도록 확장되고 있습니다. 또한 수십억 개의 사물 인터넷 (IoT) 장치가 도시의 건물, 병원, 교통 시설, 플랜트 및 유전과 같은 생산 시설에서도 정보를 수집하기 위해 확산되었습니다. 데이터 분석 및 사용에서 운영 효율성 향상에 이르기까지 다양한 방식으로 사용됩니다. 이러한 인터넷 기반 서비스와 시간과 장소에 구애받지 않는 비즈니스 스타일이 확산될 것으로 예상됩니다.

그러나 이러한 서비스는 바이러스 및 정보 유출과 같은 보안

*1 IA 시스템 및 서비스 사업 본부

글로벌 프로젝트 납품 사업부의 Engineering 생산 기술부

위험이 증가할 수 있습니다. 정보기술진흥원의 조사에 따르면 일본의 타겟 메일 관련 사고 건수는 2012년 201건에서 2019년 401건으로 두 배가 증가했습니다⁽¹⁾. 따라서 인터넷에 연결된 시설의 보안 위험에 대처하는 방법에 대한 관심도 증가하고 있습니다. Yokogawa는 이미 시간과 장소에 구애받지 않는 통합 제어 및 안전 시스템 Engineering에 대한 많은 프로젝트를 실행했습니다. 이것은 CENTUM VP의 제어 스테이션, ProSafe-RS의 안전 제어 스테이션의 시뮬레이터 기능, 테스트 절차 및 통신 네트워크 기술을 결합함으로써 가능하게 되었습니다. 또한 가상 머신 (virtual machines) 및 TCP/IP 통신과 같은 공통 부분을 특정 회사 또는 산업에서 사용되는 부분과 분리하여 ICSS Engineering에 적합한 환경을 구축해야 합니다.

이 백서에서는 안전한 Remote Engineering 및 FAT를 위해 Yokogawa에서 개발한 Engineering 환경인 CEE (Cloud Enabled Execution)에 대해 설명합니다. 또한 구성, 과제 및 향후 계획에 대해서도 설명합니다.

Yokogawa의 요구 사항

Yokogawa의 엔지니어는 고객이 계획대로 시운전을 완료하고 플랜트를 가동할 수 있도록 프로젝트 실행의 효율성을 개선하기 위해 노력하고 있습니다. 최근 몇 년 동안 글로벌화되는 프로젝트가 급속히 늘어남에 따라 이러한 프로젝트를 전 세계 어디에서나 수행할 수 있는 Remote Engineering 환경에 대한 수요가 높습니다. 이 요구 사항을 충족하려면 관련된 사람들이 현장에 모여 직접 회의를 하지 않고도 가상 머신을 사용하여 애플리케이션을 개발, 테스트 및 검토하고 프로젝트를 실행할 수 있습니다.

FAT에는 더 많은 고객, 특히 수준 높은 전문성을 갖춘 전문가와 숙련된 운영자의 참여가 필요하고 초기 단계에서 부적합 사항을 판단하고 적절히 대응하여 품질을 유지할 수 있어야 합니다. 그러나 많은 사람들이 현장에 모이는 것이 어렵기 때문에 Remote로 FAT에 참여할 수 있는 시스템이 필요합니다.

또한 많은 기업들이 다양한 사회 활동, 특히 SDGs에 기여할 것으로 기대됩니다. SDGs는 더 좋고 지속 가능한 세상을 만들기 위해 모든 국가가 참여하는 보편적 비즈니스 활동 목표입니다. 구체적인 목표에는 에너지 소비 감소와 COVID-19 및 기타 전염병 근절이 포함될 수 있습니다.

Yokogawa는 고객의 요구에 대응하기 위해 CEE를 구성하였습니다. CEE는 가상 머신 및 다양한 Remote 액세스 장비 및 최신 기술을 사용하여 프로젝트를 원활하게 실행하는 데 도움이 되는 Engineering 환경입니다 (그림1).

CEE는 Remote Engineering, Remote FAT, Remote 액세스 및 화상 회의를 위한 장비로 구성됩니다. 구성 및 성취는 “CEE 구성” 및 “CEE 성취” 섹션에 설명되어 있습니다.

CEE는 확립된 솔루션이지만 안전 계장 시스템 Engineering의 효율성과 하위 시스템과의 통합 테스트의 효율성을 개선해야 합니다.

이 두 가지 개선 사항과 관련하여 “CEE의 진화 (Evolution of CEE)” 섹션에서는 그 배경을 설명하고 Yokogawa가 구상하고 있는 아키텍처를 중심으로 솔루션을 제안합니다.

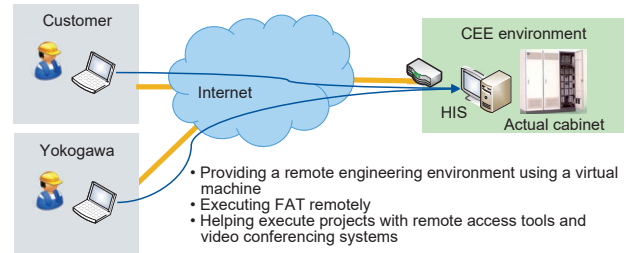


그림1 CEE 구성의 예

Yokogawa의 CEE는 SDGs를 통해 어떻게 사회에 기여하는가?

CEE를 사용하여 사용자는 글로벌 프로젝트를 실행하고 원격 FAT를 수행할 수 있습니다. Yokogawa는 프로젝트 실행의 효율성을 향상시키기 위해 원격 Engineering을 위한 가상 머신과 원격 FAT를 위한 IT 환경을 제공합니다. 이러한 기술은 초기 단계의 기본 설계 작업에서, 시스템 출하 직전 최종 검사 단계의 FAT에 이르기까지 프로젝트 단계 전반에 걸쳐 사용됩니다.

가상 머신을 사용함으로써 사용자는 대상 시스템의 Engineering 및 HIS (Human Machine Interface Station) 용 머신 구매를 미룰 수 있으며, 이는 또한 유지보수 작업을 줄이고 최신 기술을 도입할 수 있도록 합니다. 또한 기존 플랜트 자산을 효과적으로 사용하고 공유할 수 있어 에너지를 절약하고 기후 변화를 완화할 수 있습니다 (SDG7.3 및 13.3).

원격 Engineering 및 FAT를 사용하면 직원이 현장을 방문할 필요가 없으므로 출장 비용이 절감됩니다. 또한 인간의 이동에 따른 전염병을 예방하고 (SDG3.3) 운송을 위한 에너지 소비를 줄여 기후 변화를 완화하는 데 기여합니다 (SDG7.3 및 13.3). 이 새롭고 생산적인 라이프 스타일은 또한 직업 만족도와 경제 성장 (SDG8) 사이의 균형을 맞추고 지속 가능성을 개선하는 데 도움이 됩니다 (SDG9.4 및 12.6).

CEE의 구성 (Configuration of CEE)

CEE는 원격 Engineering을 위한 가상 머신과 원격 FAT를 위한 환경을 제공합니다. 원격 실행에 대한 요구 사항은 일반 IT 환경과 다릅니다. Engineering 관련 요구 사항과 보안을 모두 고려해야 합니다. 이 섹션에서는 보안 요구 사항 및 플랜트 네트워크를 간략하게 설명하고 원격 Engineering 및 FAT에 대한 세부 정보를 설명합니다.

보안 요구 사항 (Security Requirements)

인터넷으로 구현되는 서비스 (Internet-enabled services)는 독립 실행형 네트워크 (stand-alone network)보다는 훨씬 더 엄격한 보안 요구 사항을 충족해야 합니다. 이 섹션에서는 CEE에서 사용할 장치 및 응용 프로그램을 선택하기 위한 기본 요구 사항을 설명합니다. 그림2는 CEE와 관련된 보안 요구 사항을 보여줍니다.

고객 정보의 유출과 바이러스로 인한 피해를 방지하는 것이 최우선입니다. 따라서 CEE 환경에 대한 무제한 연결 및 인바운드 통신

은 금지되어야 합니다. 그러나 원격 실행을 위해 고객은 인터넷을 통해 외부에서 시스템에 액세스해야 하며 HIS를 운영하고 확인해야 합니다.

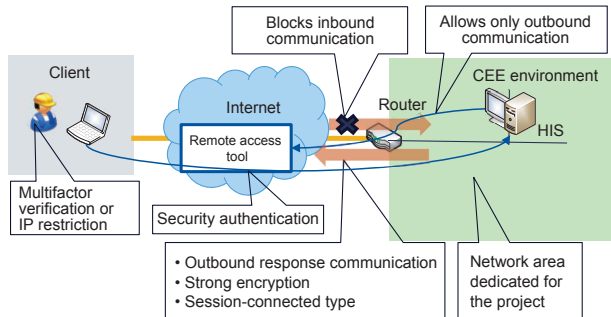


그림2 보안 요구 사항

이 문제를 해결하기 위해 인터넷에서 원격 액세스 장치를 사용하는 특정 통신 방법을 채택했습니다. 이 방법에서 CEE 환경은 주기적으로 원격 액세스 장치에 신호를 보냅니다. 장치가 액세스 권한을 얻고자 하는 권한이 부여된 사람을 인식하면 응답 신호를 보냅니다. 응답을 받으면 CEE 환경은 HIS 화면을 공유하기 위한 세션을 설정합니다. 외부로부터의 다른 모든 인바운드 통신은 차단되어 외부로부터의 무단 액세스를 차단합니다.

또한 이 방법은 다음 보안 요구 사항을 충족합니다.

- 세션 연결 유형
- 최소 256 비트 AES (advanced encryption standard: 고급 암호화 표준) 암호화
- 세션 별 인증 (authentication)
- 일회성 암호로 보호
- 다중 요소 인증이 가능하거나 소스 IP 주소를 제한할 수 있습니다.
- ISO27017 및 SOC (service organization control: 서비스 조직 제어)와 같은 여러 주요 보안 인증을 획득했습니다.
- 정보 유출과 같은 보안 사고를 유발하지 않아야 합니다.
- 해당 네트워크는 Yokogawa의 사무실 네트워크 및 기타 프로젝트와 분리되어 바이러스 감염 및 무단 액세스 위험을 줄입니다.

플랜트 네트워크 개요

플랜트 네트워크는 필드 네트워크 (field network), 제어 네트워크 (control network) 및 제어 정보 네트워크 (control information network)의 세 계층으로 구성됩니다. 필드 네트워크는 필드 장치와 측정 기기를 컨트롤러에 연결하고 산업 및 제조업체가 다양한 표준을 설정합니다. Vnet/IP 제어 네트워크는 국제 표준을 준수하는 중복 고속 네트워크 (redundant, high-speed network)입니다.

통신 경로의 상태는 지속적으로 모니터링됩니다. 한 경로에서 오류가 발생하면 통신이 자동으로 다른 경로로 빠르게 전환되어 제어 통신을 계속합니다. 제어 정보 네트워크는 인터넷 및 인트라넷에서 사용되고 있는 일반 TCP/IP 네트워크와 유사합니다.

CEE는 가상 머신 또는 HIS에서 시뮬레이션된 제어 스테이션 (Control Station)의 기능을 사용합니다. 이 기능을 사용하면 프로젝트 초기에 Engineering 환경을 사용할 수 있습니다.

가상 머신은 네트워크의 동작을 시뮬레이션하므로 실제 제어 및 필드 네트워크를 설정할 필요가 없습니다. Engineering은 TCP/IP 네트워크에서만 수행할 수 있습니다 (그림3).

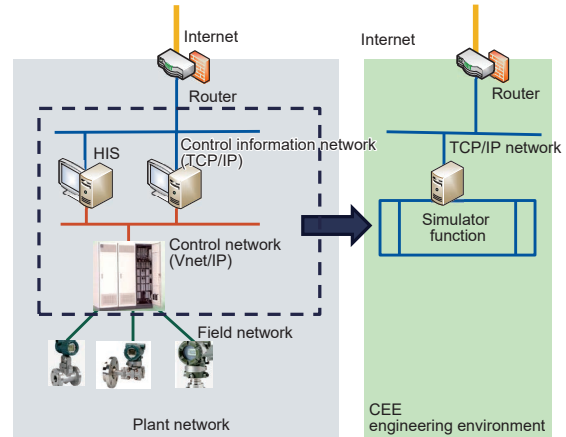


그림3 플랜트 네트워크 및 시뮬레이터 기능

Remote Engineering

CEE로 Remote Engineering을 진행하려면 다음 요구 사항이 충족되어야 합니다.

- HIS 화면은 원격으로 액세스 할 때도 시인성이 확보되어야 하고 플랜트 운영에 적합해야 합니다.
- 가상 머신 환경 (OS, Microsoft Office 등 포함)은 Engineering에 적합해야 합니다. CEE는 회사의 자체 장비 기반으로 (on premises) 또는 퍼블릭 클라우드에서 사용할 수 있는 클라우드 서비스로 제공됩니다. 퍼블릭 클라우드의 경우, 일반적으로 서버용으로 설계되었습니다. 따라서 CENTUM VP, ProSafe-RS, 개발 도구, 원장 출력 기능과의 호환성 확인이 필요합니다.
- “보안 요구 사항”섹션에 설명된 보안 요구 사항이 충족되어야 합니다.

이를 충족하기 위해 CEE는 그림4에 표시된 Engineering 환경을 제공합니다.

- 외부 네트워크 (Yokogawa 사무실 포함)와의 통신을 제한하기 위해 방화벽이 설치됩니다.
- 서버는 데스크톱 화면 데이터만 전송하는 게이트웨이로 설정됩니다. 방화벽은 CEE에 사용되지 않는 포트에서 통신을 차단합니다. 바이러스가 화면 데이터를 감염시키는 것은 거의 불가능합니다. 이 설정은 모든 통신을 허용하는 VPN (virtual private network)보다 더 안전합니다.
- 응용 프로그램 데이터베이스 내보내기 및 같은 파일 전송은 바이러스를 확산시킬 수 있으므로 안전하게 설계된 파일 서버를 통해

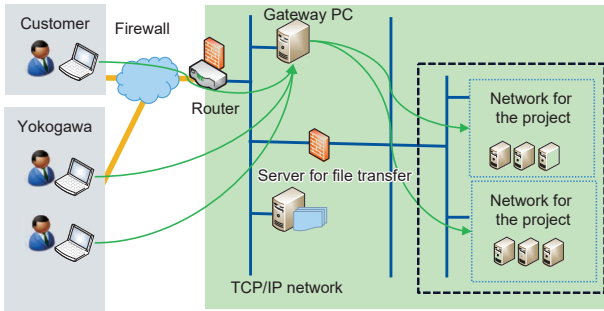


그림4 CEE Engineering 환경 개요

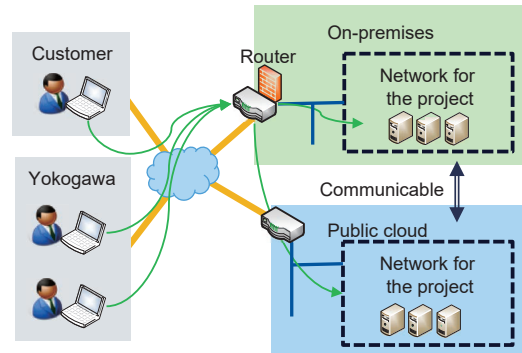


그림5 하이브리드 환경

수행해야 합니다.

- 네트워크를 분리하고 고객 프로젝트별로 접근을 통제함으로써 정보 유출 위험을 최소화합니다.

이러한 요구 사항은 Engineering 환경에 언제든지 액세스하고 실제 프로젝트에서 사용할 수 있도록 보장합니다. 구성의 유연성을 유지하면서 가상 머신 수를 늘리기 위해 퍼블릭 클라우드와 자체 장비 기반 (on premises) 설정으로 구성된 하이브리드 환경을 구성할 수 있습니다 (그림5). 퍼블릭 클라우드의 높은 확장성 (가상 머신 수에 제한 없음)과 자체 장비 기반 (on premises) 설정의 높은 유연성 (가상 머신 수는 제한되지만 OS 종류 및 구성에 대한 제한은 Yokogawa의 재량에 따라 변경할 수 있음)이 함께 제공됩니다.

Remote Engineering에서 Remote FAT로

소프트웨어 FAT 및 하드웨어 FAT를 Remote로 수행하려면 Yokogawa와 고객이 Remote Engineering 환경 및 대상 시스템에 액

세스 할 수 있는 환경이 필요합니다 (그림6).

요구 사항은 다음과 같습니다.

- 고객이 인터넷을 통해 HIS를 운영하고 테스트할 수 있습니다. Engineering 환경과 마찬가지로 FAT 환경은 화면을 공유할 수 있어야 하며 이러한 공유가 플랜트 운영을 방해해서는 안 됩니다.
- I/O 모듈과 같은 하드웨어의 외부보기 (비디오 이미지)와 HIS 화면에서 내부 상태 (파라미터)를 비교합니다.
- 전체 프로젝트 팀이 펀치 항목 (punch items: FAT 실행 중에 발생하는 변경 및 부적합)을 공유할 수 있습니다.
- 원격 사이트 간에 적절한 통신 수단을 제공합니다.
- “보안 요구 사항” 섹션에 설명된 보안 요구 사항을 충족합니다.

스푸핑 (spoofing) 및 무단 액세스를 방지하기 위해 원격 연결 도구에는 “보안 요구 사항” 섹션에 설명된 기능 (사용자 인증, 각 프로젝트에 대한 사용자 권한 부여 및 다중 요소 인증)이 있습니다.

프로젝트에는 고정 카메라와 헤드 마운트 카메라가 사용됩니다.

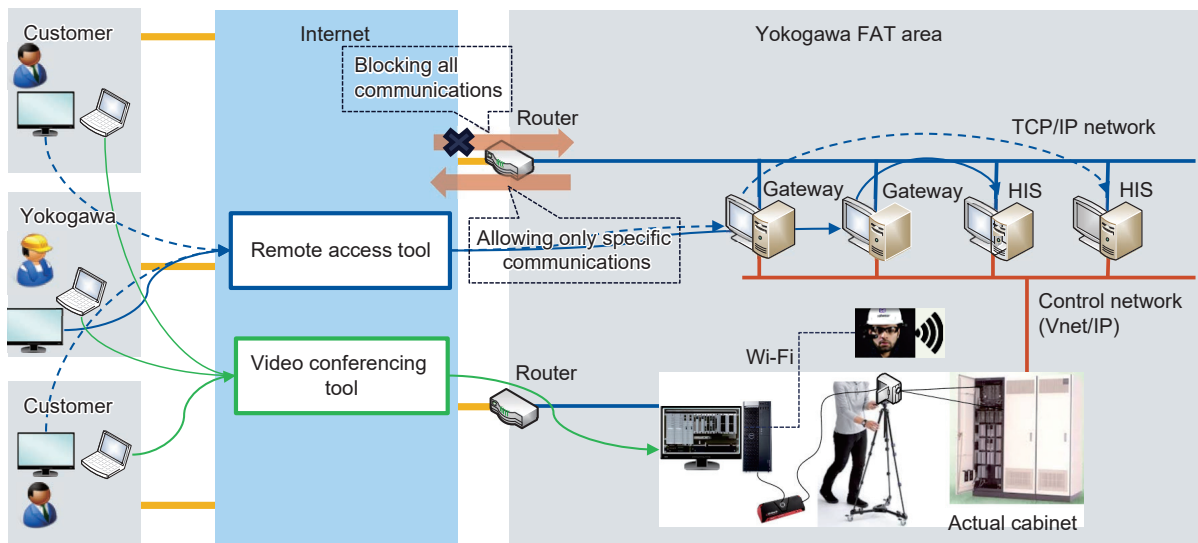


그림6 원격 FAT

둘 다 인터넷을 통해 캐비닛 및 기타 하드웨어의 영상을 실시간으로 원활하게 배포할 수 있음을 확인했습니다.

통신 및 정보 공유를 위해 Cisco의 Webex 또는 Microsoft의 Teams가 사용됩니다. 둘 다 인기있는 화상 회의 도구입니다. Yokogawa의 독점 웹 기반 펀치 항목 관리 시스템인 온라인 PLMS (Online Punchlist Management System)는 펀치 항목을 관리하는 데 사용됩니다.

PLMS를 통해 사용자는 프로젝트에 관련된 사람들과 온라인으로 펀치 항목의 내용을 공유할 수 있습니다. 이러한 여러 응용 프로그램은 원격 FAT를 안전하고 효과적으로 구현하는 데 사용됩니다.

CEE의 효과

CEE는 가상 머신과 Remote FAT를 적극적으로 사용하여 프로젝트 실행의 효율성을 향상시킵니다. 여러 가상 머신을 사용하면 플랜트 자산의 평균 활용률이 증가하여 리소스를 보다 효율적으로 사용할 수 있습니다.

Remote FAT는 또한 사람들의 업무 이동 필요성을 줄여주고 온라인 커뮤니케이션을 강화합니다. 이러한 이점으로 인해 CEE는 점점 인기를 얻고 있습니다. 2020년 상반기에 CEE는 100개 이상의 프로젝트에 사용되었으며 이는 전년 대비 3배입니다.

CEE는 COVID-19의 확산으로 인해 더 널리 도입될 것으로 예상됩니다.

CEE의 발전 방향

“Yokogawa에 대한 요구사항”섹션에서 언급했듯이 CEE에는 두 가지 개선해야 할 점이 있습니다.

- 방향-1: 안전 계장 시스템의 Engineering 간소화
- 방향-2: 서버 시스템과의 통합 테스트의 효율성 향상

방향-1은 애플리케이션을 개발하고 테스트를 수행하기 위해 CEE 가상 머신을 실제 안전 제어 스테이션에 연결하는 것이며, 이는 아직 달성되지 않은 것입니다. 이러한 개선은 인간과 환경을 보호하기 위한 안전한 플랜트 운영을 보장하는 ProSafe-RS 안전 계장 시스템의 Engineering에 필요합니다.

안전 제어 스테이션의 시뮬레이터 기능은 안전 계장 시스템을 테스트하는 데 사용되지 않습니다. 대신 실제 머신의 I/O 모듈에서 실제 신호의 입출력을 확인해야 합니다. 이러한 테스트 설정 (그림7)을 통해 CEE는 초기 단계에서 안전 기능 로직의 유효성을 보다 유연하게 테스트할 수 있습니다.

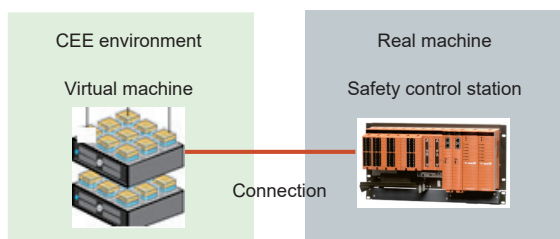


그림7 개선1

가상 머신과 제어 스테이션은 Vnet/IP를 통해 통신하므로 TCP/IP가 아닌 특수 프로토콜을 지원하는 전용 네트워크 카드가 필요합니다. Vnet/IP 지원 가상 네트워크 카드는 이미 개발되었으며 현재 가상 머신과의 호환성을 확인하고 있습니다.

Vnet/IP에는 높은 안정성이 필요합니다. Engineering 환경과 실제 머신이 같은 위치에 설치되면 문제가 없지만 그렇지 않다면 주의가 필요합니다. 특히 멀리 떨어져 있을 때는 거리에 따른 지연이 불가피합니다. 이 문제를 해결하기 위해 전 세계에 데이터 센터가 있는 퍼블릭 클라우드의 사용을 연구하고 있습니다. 실제 머신과 지리적으로 가까운 데이터 센터를 선택할 수 있습니다.

방향-2는 인터넷을 통해 실제 머신의 제어 스테이션 또는 안전 제어 스테이션을 타사 하위 시스템과 연결하는 것입니다. 최근에는 다른 회사의 컨트롤러가 시스템에 통합되는 경우가 많으며 통합 테스트 시기 결정 문제가 이슈가 되어 왔습니다. 현재 통합 테스트는 실제 머신을 반입하거나 현장에서 대체 머신을 사용하여 수행됩니다. 인터넷을 통한 연결이 허용되면 현장에 설치된 하위 시스템으로 테스트를 수행할 수 있으므로 안전 계장 시스템의 실제 머신을 운송할 필요가 없으므로 FAT 프로세스가 가속화됩니다 (그림8).

타사 하위 시스템과 통신하기 위한 I/O 모듈 및 스테이션은 이러한 하위 시스템을 통합, 작동 및 모니터링하는데 사용됩니다. 원격

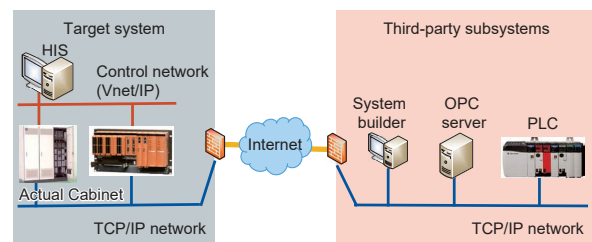


그림8 개선2

으로 통합 테스트를 수행하려면 인터넷 전송 속도와 대상 하위 시스템을 지정하고 기능 테스트를 수행하며 전체 조건에 대한 지침을 결정해야 합니다. 가상 머신에서 시뮬레이션된 컨트롤러가 하위 시스템과 통신할 수 있는 경우 실제 컨트롤러가 제공될 때까지 기다릴 필요가 없으며 통합 테스트를 보다 유연하게 예약할 수 있습니다. 이러한 가능성은 미래에도 고려해야 합니다.

두 가지 개선 사항은 프로젝트 실행에 중점을 둡니다. 또한 엔지니어가 Engineering 환경을 보다 쉽게 설정할 수 있게 해 주는 자동화 도구와 사용자가 Azure 또는 기타 클라우드 서비스와 통합된 콘솔을 사용할 수 있는 웹 사용자 인터페이스를 도입할 계획입니다. 프로젝트의 효율성을 높이기 위해 다양한 방법을 연구하고 있습니다.

결론

Remote로 Engineering 및 FAT를 수행하려면 ICSS Engineering 요구 사항을 충족하고 인터넷을 통한 통신 보안 조치를 구현해야 합니다. 그 해결 방안으로 이 백서는 Yokogawa의 Cloud Engineering

환경인 CEE를 제시했습니다. 이 환경은 이미 많은 프로젝트에서 도입되어 프로젝트 실행 성과를 크게 향상시키고 SDGs, 특히 전염병 대응에 기여했습니다.

이 백서에 제시된 두 가지 개선 사항 외에도 Yokogawa는 프로젝트 실행의 효율성을 높이고 고객, SDG 및 기타 사회적 목표에 기여하기 위해 CEE를 계속 개발할 것입니다.

참고문헌

- (1) Information-Technology Promotion Agency Security Center, Cyber Information Sharing Initiative (J-CSIP), <https://www.ipa.go.jp/security/J-CSIP/index.html> (in Japanese) (accessed on September 11, 2020)

* CENTUM VP, Vnet/IP, and ProSafe-RS are registered trademarks of Yokogawa Electric Corporation.

* All other company names, organization names, product names, and logos that appear in this paper are registered trademarks or trademark