변전소 보안 네트워크의 설계 및 구성

Andreas Klien[1], Yann Gosteli[2], Stefan Mattmann[3]

[1]OMICRON electronics GmbH, Klaus, Austria (andreas.klien@omicronenergy.com)
[2]Centralschweizer Kraftwerke (CKW) AG, Luzern, Switzerland (yann.gosteli@ckw.ch)
[3]Centralschweizer Kraftwerke (CKW) AG, Luzern, Switzerland (stefan.mattmann@ckw.ch)

키워드 : 사이버 보안, IEC 61850, 간섭 감지, 변전소 자동화

개요

공공 사업자와 사이버 보안 감사원은 변전소도 사이버 공격의 잠재적 진입점으로 간주하고 있습니다. 중요한 보호 요소는 프로세스, 보호 및 제어 시스템의 커미셔닝 방법, 원격 유지보수 액세스 구현 방법입니다. 따라서 보안성을 위해 보호 및 제어 시스템의 아키텍처를 검토해야 합니다. 이를 위해 스위스 발전 및 유통 유틸리티 회사는 2016/2017 년 보호 시스템을 위한 새로운 참조 아키텍처를 개발하기 시작했습니다. 이들의 설계는 이러한 공격에 대응책을 제시하면서 유지성과 보안 사이의 합리적인 균형을 제공합니다. 또한 침입 방지 시스템(IDS)이 적용됩니다. 변전소에 적합한 IDS 를 선택하는 것은 많은 IDS 가 변전소 네트워크의 요구사항을 지원하지 않기 때문에 어려운 것으로 판명되었습니다. 본 논문은 변전소에 가장 중요한 공격 벡터를 열거한 다음, CKW 에 의한 새로운 그린필드 110kV 변전소에서 처음으로 구현된 보안 아키텍처에 대해 설명합니다. 그 후에 변전소에 적합한 IDS 를 선정하는 경험과 공장 검수 테스트에서 배운 교훈으로 끝을 맺습니다.

1. 소개

1.1. 변전소 공격 벡터

우리는 이 기사의 나머지 부분들에 대한 사이버 공격이 하나의 변전소 내 보호, 자동화 또는 제어장치의 변경, 축소 또는 비활성화하는 사건이라고 가정합니다. 이를 달성하기 위해 공격자는 그림 1[1]에 표시된 공격 경로 중 하나를 사용합니다.

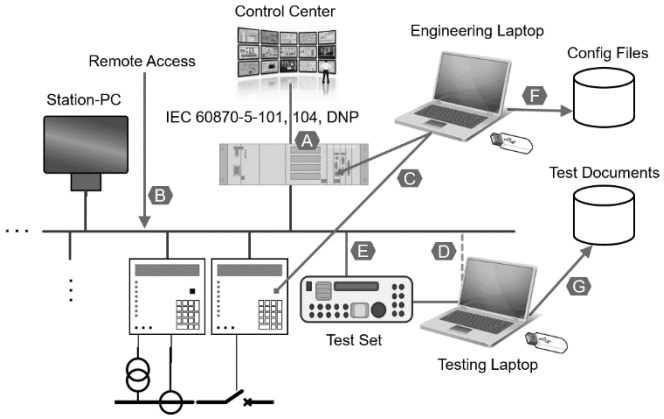

그림 1 변전소의 공격 벡터 [1]

공격자는 제어센터 연결부(A)를 통해 진입할 수 있습니다. 우크라이나 전력망에서의 첫 사이버 공격처럼, 게이트웨이 장치의 펌웨어가 수정된 경우 파괴의 원인이 됩니다. 2016 년 제 2 차 우크라이나 사이버 공격은 원격 액세스 연결 (B)를 통해 발생했고, 중요 인프라 PLC 에 대한 'TRITON' 사이버 공격이 일어났습니다.

또 다른 진입점은 변전소 장비나 네트워크에 직접 연결된 엔지니어의 PC 를 통해서 입니다. 보호 엔지니어가 자신의 PC 를 릴레이에 연결하여 보호 설정을 수정할 때, PC 의 'Stuxnet' 악성 코드는 릴레이에 악성코드를 설치할 수 있습니다. [5] (2010 년의 PLC 사례)
IEC 61850 시스템(D) 테스트에 사용되는 PC 는 종종 스테이션 버스와 직접 연결되며, 이는 IED 를 감염시킬 수 있습니다. 이러한 이유로 새로운 IEC 61850 도구는 테스트 PC 와 변전소 네트워크 사이에서 사이버 보안으로 분리되어야 합니다. 이로써 시험 기기(E)는 잠재적 진입 경로가 될 수 있으며, 이 때문에 테스트 세트를 강화하는데 투자하는 것이 중요합니다.
설정(F)과 시험문서(G)의 보관 위치도 감염원이 될 수 있습니다. 따라서 서버 또는 저장 위치도 중요한 경계에 속하며 사무실 IT 영역에 위치해서는 안됩니다. 따라서 이러한 데이터를 분리하고 격리 보호되는 별도의 데이터 관리 솔루션을 도입하는 것이 타당합니다.

2. 새로운 변전소 아키텍처 제안

2.1. OT 사이버 보안 기술 현황

스위스 전력 산업협회는 OT(Operational Technology)의 보안에 관한 실무그룹을 구성했으며, 이후 업계 추천서인 '전력시스템에서의 운전기술 및 보호에 관한 핸드북' 을 발간했습니다. 본 핸드북은 국가 표준원(NIST)[7]의 '중요 인프라에 대한 사이버 보안 프레임워크'를 참조하고 있으며 이 프레임워크는 2018 년 최신 버전으로 업데이트 되었습니다. NIST 프레임워크는 사이버 공격에 대한 100% 보호가 없다는

가정에 기초합니다. 충분한 지식과 노력으로 모든 보안 수단을 뚫을 수 있습니다. 이를 바탕으로 NIST 프레임워크는 '식별, 보호, 검출, 응답, 복구'의 5 단계로 구성된 프로세스를 권장합니다. 따라서 첫번째 단계는 공격 벡터의 식별입니다. 그 후 다음 단계(보호)에 대한 대책을 실시할 수 있습니다. 공격자가 여전히 이러한 장벽을 뚫을 수 있는 경우, 공격을 탐지해야 하며, 즉시 행동(반응)하여 가능한 빨리 정상 상태를 회복해야 합니다.(복원) 검출과 대응에서 배운 교훈으로 새로운 공격 벡터를 식별할 수 있고, 새로운 대응책을 구현할 수 있으며, 프로세스가 반복됩니다.

스위스 산업계의 권고사항은 조직 내의 인력, 기술 및 프로세스의 상호작용을 강조합니다. 예를 들어, 지속적인 모니터링이나 침입 탐지는 경보 메세지가 적절하게 반응하는 경우에만 의미가 있습니다. 따라서 경보 메세지는 OT 엔지니어 및 IT 보안 전문가 등 대응 프로세스에 관련된 모든 사람이 이해할 수 있어야 합니다. 그렇지 않으면 대응 과정이 비효율적으로 될 것입니다. 또한 IDS 가 너무 많은 거짓 정보를 전송하면 결국 모든 경보가 무시됩니다.

2.2. CKW 의 OT 사이버 보안 개시 [6]

OT 보안, 특히 제어 및 보호 시스템에 대한 주제는 최근 몇 년동안 CKW 에서 점점 더 중요해졌습니다. 이는 스위스에서 언급된 업계 권장사항에 의해 발생했지만, 무엇보다도 최근 CKW 가 수행한 OT 보안평가 때문이기도 합니다. 이러한 평가는 변전소에 사용되는 네트워크와 브로드캐스트 제어 기술 모두에서 약점을 보여주었습니다. 예를 들어 안전하지 않은 구역 전환과 스테이션 제어 컴퓨터의 몇가지 중요한 원격 액세스 방법이 발견되었습니다. 또 현재 변전망에서 공격이 발생하고 있는지, 또는 임박한 공격을 나타낼 수 있는 의심스러운 활동이 네트워크상에서 이루어지고 있는지를 평가할 수 없었습니다.
이러한 발견에 기초하여 CKW 는 본질적인 약점들을 제거하고 그들의 미래 변전소 아키텍처에 대한 요건을 강화한다는 목표를 정했고, 이러한 발견들은 CKW 의 새로운 변전소 설계 표준에 통합되었습니다.
이 설계 표준에 대한 작업 외에도, CKW 는 언급된 OT 보안 핸드북의 스위스 워킹 그룹에 참여할 수 있었습니다. 이 정보를 바탕으로 CKW 는 작업 그룹의 조사 결과를 자체 설계 표준에 일관되게 통합하였습니다.

2016/2017 년, CKW 프로젝트 팀은 2020 년에 가동될 새로운 그린필드 변전소 'US 로텐버그'를 계획 시작했습니다. 이 프로젝트에서는 CKW 의 새로운 보안 아키텍처 표준이 적용되었고 스위스 OT 보안 핸드북의 최신 권장사항이 뒤따랐습니다. 이러한 정교한 보안 대책을 구현할 수 있도록, CKW 는 스스로 네트워크 아키텍처를 구현하고 스위치 구성을 전환하기로 결정했습니다.

2.3. 네트워크 설계

미국 로텐부르크의 네트워크 설계는, 가능한 공격을 어렵게 하기 위해 모든 영역에 장애물이 내장되었습니다. 그림 2 는 로텐버그 변전소의 네트워크를 보여줍니다.

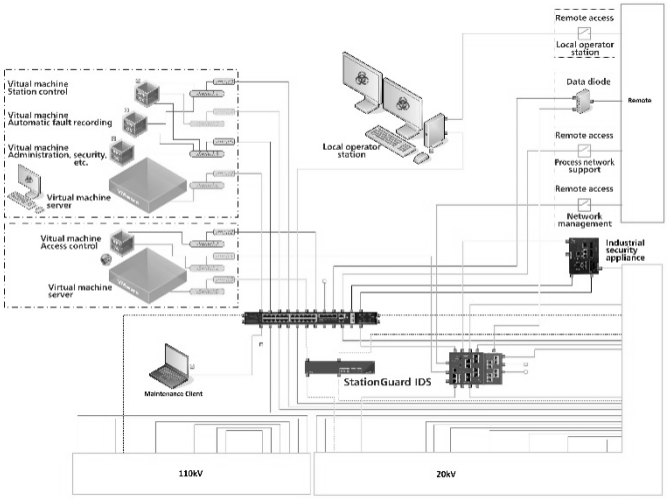

그림 2 미국 로텐버그 네트워크 아키텍처 [6]

이 아키텍처에서, 본 문서의 1.1 절에 기술된 모든 공격 벡터는 전체 범위의 보안 대책을 사용하여 다루어집니다. 발전소의 원격 연결은 최우선적으로 다루어 졌습니다. 이러한 원격 연결은 방화벽과 터널 솔루션을 사용하여 보호될 뿐만 아니라 기본적으로 비활성화 됩니다. 원격 액세스를 위한 연결은 필요할 때만 활성화 됩니다. 이는 2 단계 인증 프로세스와 유사하게 원격 액세스를 가능하게 하기 위해 여러 사람이 참여한다는 것을 의미합니다.
Supervisory Control and Data Acquisition (SCADA) 통신은 IEC60870-5-101 시리얼 프로토콜을 사용하여 이루어집니다. 유지보수를 위한 변전소 장치에 대한 모든 접근은 적절히 고정된 특수 작업대를 통해서만 이루어집니다. 이러한 워크스테이션은 가상화되고 중앙 위치에 있습니다. 이 유지관리 원격 액세스도 원격으로 활성화해야 합니다.
SCADA 시스템, 고장 기록 장치 및 보안 시스템 서버는 가상화하고 변전소의 로컬 호스트 시스템에서 운영됩니다. 심지어 로컬 HMI 스테이션도 추가 로컬 방화벽을 통해 원격 데스크탑을 사용하여 이러한 시스템에 액세스합니다. 역할 기반 액세스 제거(RBAC)가 사용됩니다. 기기당 암호가 아니라 사용자당 암호가 하나씩 있다는 뜻입니다. 이것은 엔지니어가 모든 변전소에서 자신의 암호를 사용할 수 있다는 장점을 가지고 있습니다. 직원이 회사를 관두면 쉽게 제거되므로 비밀번호를 변경할 필요가 없습니다. 이 사용자 관리는 변전소의 로컬 RADIUS 서버와 중앙 AD(Active Directory) 서버를 사용하여 구현됩니다. 사용자는 필요한 권한을 할당하는 AD 를 사용하여 로그인해야 합니다. 필요한 경우 중앙 AD 에 대한 액세스가 중앙 위치에서 활성화될 수 있습니다. 또한

사용자는 개별 사용자 이름과 암호를 사용하여 각 IED 에 로그온해야 합니다.
여기서 IED 는 로컬 RADIUS 서버를 사용하여 사용자와 암호의 인증을 확인하고 이 사용자에게 할당된 사용 권한을 검색합니다. 이는 엔지니어링 도구를 사용하는 기기에 대한 접근과 IED 디스플레이에서의 작동 모두에 적용됩니다. 표준 암호는 사용되지 않습니다.
변전소 네트워크에 연결된 모든 PC 가 강화됩니다. 이는 무엇보다도 변전소의 통신 매트릭스에 따라 윈도우 방화벽을 구성하고, 그 클라이언트의 역할에 따라 필요 없는 운영체제의 기능을 차단함으로써 이루어집니다.
추가 보안 대책으로서 MAC 인증 바이패스를 통해 네트워크 접속 제어를 실시하는데, 이는 등록된 기기만 네트워크 스위치에 연결할 수 있다는 것을 의미합니다.
오작동이 발생할 경우 스위치도 예비 장치를 재고로부터 인식하고 수용해야 합니다. 변전소 네트워크 스위치와 방화벽에서 접속 제어 목록은 사용된 프로토콜과 스위치 포트를 포함한 다른 네트워크 참여자가 통신할 수 있는 장치를 시행하도록 구성됩니다.
스테이션 버스 네트워크와 구성 및 유지보수를 위한 네트워크는 논리적(VLAN), 물리적으로 분리되어 있습니다. 즉, 각 IED 에서 IEC 61850 통신 MMS 및 GOOSE 는 유지보수 액세스와는 다른 인터페이스에서 실행됩니다. 또한 전체 스테이션 버스 네트워크는 분할되며, 그 중에서도 방화벽을 통해 다음과 같은 세그먼트가 분리됩니다.

- 110kV (GOOSE 및 MMS)
- 20kV (GOOSE 및 MMS)
- 로컬 HMI
- 프로토콜 게이트웨이
- 보조 시스템
- IED 및 클라이언트용 유지관리 네트워크
- 관리 네트워크, VM, RADIUS

변전소로부터 상위 네트워크 영역으로의 통신은 데이터 다이오드에 의해 추가로 확보됩니다. 이 데이터 다이오드는 발신 통신 세션만 개시할 수 있도록 하고 또 다른 보안 계층을 제공합니다.
침입 탐지 시스템(IDS)은 화이트리스트 접근방식을 사용하여 시스템의 전체 네트워크 트래픽을 모니터링합니다. 즉, 화이트리스트에 없는 모든 알 수 없는 트래픽은 기본적으로 경보를 생성합니다. IDS 는 RTU 를 통해 제어센터와 경보 로깅을 위한 특수 프로토콜을 통해 보안 운영 센터에 경보를 보고합니다.

3. 침입 탐지

CKW 의 보안 아키텍처는 각각 방화벽에 의해 분리된 네트워크 세그먼트의 설정에 기초합니다. 방화벽의 구성은 정확히 세그먼트 간의 통신에 사용될 수 있는 프로토콜을 지정합니다. 단, IEC 61850 에서 사용하는 MMS/GOOSE 와 같은 방화벽이 허용하는 프로토콜과 벤더별 엔지니어링 프로토콜을 사용하여 기기를 공격하고 감염시킬 수도 있습니다. 그러한 시나리오에서 CKW 는 초기 단계에서 허가되지 않은 활동을 감지할 수 있기를 원했습니다. 이러한 목적을 위해, IDS 는 CKW 의 기준 아키텍처에서 사용되어야 한다고 결정되었습니다.
가장 중요한 트래픽을 분석하려면, 게이트웨이와 IED 사이의 통신, 적어도 게이트웨이의 모든 트래픽은 IDS 에 미러링되어야 합니다. 베이 레벨 스위치는 일반적으로 GOOSE 또는 Sampled Values 와 같은 멀티캐스트 트래픽만 그곳에서 발생하므로 커버할 필요가 없습니다. 또한 모든 네트워크는 분기의 모든 유니캐스트 트래픽을 분석할 수 있도록 모든 스위치를 IDS 에 미러링하는 것이 바람직합니다.
CKW 아키텍처에서 IDS 는 모든 네트워크 스위치의 미러 포트에 연결됩니다. 이는 IDS 가 방화벽을 통과하기 전과 후에 원격에서 들어오는 트래픽뿐만 아니라 스테이션 버스의 트래픽도 분석한다는 것을 의미합니다.

3.1. 변전소 IDS 에 대한 요구사항

변전소에 적합한 IDS 를 선택하는 것은 어려운 것으로 판명되었습니다. 중요한 요건은 모든 IED 와 네트워크 장비를 담당하는 보호, 제어 및 네트워크 엔지니어가 IDS 를 쉽게 작동할 수 있어야 한다는 것입니다. 경보 대응 프로세스를 지원하기 위해서는 IDS 경보를 HMI 의 변전소 및 이벤트 로그에 있는 이벤트와 쉽게 연결할 수 있어야 합니다. 따라서 IDS 는 IT 보안 용어 대신 변전소에 대한 특정 보기를 허용해야 합니다.
서명 기반 접근법은 표준 PC 바이러스 스캐너와 같은 블랙리스트와 함께 작동합니다. 이것은 알려진 바이러스와 악성코드의 패턴을 검사합니다. 문제는 변전소로 알려진 사이버 공격은 극소수에 불과하지만 새로운 공격이 처음 발생하더라도 심각한 결과를 초래할 수 있다는 점입니다. 변전소 IDS 는 공격이 어떻게 보일지에 대한 사전 지식 없이 공격을 탐지할 수 있어야 합니다.
따라서 더 많은 IDS 시스템이 “학습 기반” 접근 방식을 사용합니다. IDS 는 각 매개변수의 평균값과 주파수를 학습하기 위해 서로 다른 프로토콜의 일반 프로토콜 매개변수를 살펴봅니다. 그 후, 정상운전 중 네트워크 통신이 학습된 평균으로부터 현저히 벗어날 때마다 알람이 발생됩니다. 그 결과 학습 단계에서 발생하지 않은 모든 이벤트에 대해 거짓 경보가 트리거됩니다. 여기에는 예를 들어 트립과 스위칭 작업 또는 정기적인 보호 시험이 포함됩니다. 시스템이 네트워크상의 전보의 의미를 모르기 때문에, 경보 메세지는 ‘MMS 확정-쓰기-응답 실패’와 같은 일반적인 프로토콜 매개변수를 가리킵니다. 따라서 IT 전문가와 IEC 61850 전문가가 각각 확인해야 하는 허위 경보가 많이 발생합니다. 대응 과정에서 그러한 노력은 CKW 에 받아들여지지 않았습니다.

3.2. IDS 접근법 사용

IEC 61850 변전소의 경우, 모든 IED, 그 데이터 모델 및 이들의 통신 패턴은 표준화된 형식 – SCL 로 기술됩니다. 이 정보는 침입 탐지를 위해 다른 접근법을 사용할 수 있도록 허용합니다. 모니터링 시스템은 변전소 자동화

시스템의 시스템 모델을 생성할 수 있으며, 네트워크 각 패킷을 이 모델과 비교할 수 있습니다. 전달된 (GOOSE, MMS, SV) 메세지에 포함된 변수들도 시스템 모델에서 도출된 기대에 대해 평가할 수 있습니다. 따라서 이 시스템 모델은 시스템 모델과 일치하지 않는 모든 패킷이 경보를 트리거하기 때문에 화이트리스트로 구성됩니다. CKW 는 이 접근법(OMICRON StationGuard)에 기초한 IDS 를 선택했습니다.
이 접근법의 장점은 잘못된 형식의 패킷과 금지된 MMS 제어 조치와 같은 사이버 보안 위협뿐만 아니라 통신 장애, 시간 동기화 문제, 그리고 결과적으로 특정 장비 고장이 감지되고 경보된다는 것입니다.
SCL 파일의 변전소 섹션을 사용하여 변전소의 개요 다이어그램을 자동으로 만들 수 있으며, 이 다이어그램에서 알람을 표시할 수 있습니다. 이러한 표시 장치는 경보를 트리거한 조치가 의도적으로 수행되었는지 여부를 식별하는 데 도움이 될 수 있습니다. 예를 들어, 이 사건은 테스트 상황에서 엔지니어에 의해 발생했을 수도 있고 감염된 테스트 PC 에 의한 악성 활동에 해당할 수도 있습니다.

이 논문의 작성 당시, 미국 로텐부르크의 공장 인수 시험(FAT)이 실시되어 커미셔닝이 진행되고 있었습니다. FAT 의 경우 설계가 제대로 작동하는지 테스트하기 위해 거의 모든 네트워크 구성이 완료되어야 했습니다. 우리는 또한 IDS 가 여러 단계의 방화벽에 의해 수행되는 라우팅에 대한 지원이 필요하다는 것을 알게 되었습니다. 방화벽 전후의 트래픽이 중복되어 IDS 디스플레이를 혼동시킬 수 있습니다. 그러나 선택한 IDS 가 이 시나리오를 올바르게 지원했습니다. 또한 방화벽 구성을 위한 통신 매트릭스를 작성하는 것은 상당한 노력이며, 이 작업은 수동으로 수행해야 하기 때문입니다. IDS 는 이미 SCL 의 화이트리스트를 보유하고 있기 때문에 이 프로세스도 향후 자동화할 수 있습니다.

4. 결론과 전망

공격자가 하나 이상의 변전소에 영향을 미칠 수 있는 경우, 이는 그리드에 심각한 결과를 초래합니다. 또한 방화벽을 우회할 수 있는 몇가지 공격 벡터를 가질 수 있습니다. CKW 의 안전한 변전소 네트워크 아키텍처는 본 논문에서 식별된 공격 벡터에 대한 수많은 대책을 제공합니다. 보안 대책은 높은 수준의 보안을 제공하는 동시에 원격 액세스를 이용한 효율적인 유지보수 및 엔지니어링 절차를 가능하게 합니다. 이 아키텍처는 네트워크 코어의 침입 감지에 의존합니다. IEC 61850 변전소의 경우 SCL 을 사용하여 허용된 모든 네트워크 트래픽의 화이트리스트를 자동으로 구축하는 IDS 접근방식을 사용할 수 있습니다. 이를 통해 탐지된 이벤트를 보호, 자동화 및 제어 엔지니어의 언어로 표시하여 보안 엔지니어와 협력하여 사건의 원인을 효율적으로 결정할 수 있습니다.
각 설계가 개선될 수 있는 것은 사이버 보안의 속성입니다. 개선사항 중에 현재 사용되는 MAC 기반 접근법 대신 802.1X[8]에 따른 인증서 기반 네트워크 액세스 제어를 예로 들 수 있습니다. 그러나 이를 위해서는 현재와 다른 802.1X 표준을 지원해야 하는 IED 가 더 많습니다. 후속 문서는 본 프로젝트의 커미셔닝에서 얻은 결과를 수집하고 본 변전소에서 수행한 향후 보안 평가 및 침입 테스트 결과를 문서화 할 것입니다.

5. 참조 문서

[1] Klien, A.: ‘New approach for detecting cyber intrusions in IEC 61850 substations’, PAC World Conference Europe, Glasgow, 2019
[2] ‘Analysis of the Cyber Attack on the Ukrainian Power Grid’, SANS, E-ISAC, https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf, accessed November 2019
[3] ‘WIN32/INDUSTROYER - A new threat for industrial control systems’, https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf, accessed November 2019
[4] ‘Threat Research - Attackers Deploy New ICS Attack Framework “TRITON” and Cause Operational Disruption to Critical Infrastructure’, https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html, accessed November 2019
[5] D. Kushner: ‘The Real Story of Stuxnet
How Kaspersky Lab tracked down the malware that stymied Iran’s nuclear-fuel enrichment program’, IEEE Spectrum, February 2013
[6] Gosteli, Y., Klien A.: ‘Sichere Stationsleittechnik – Neue Cyber Security Architektur mit Intrusion Detection in der US Rothenburg’, bulletin.ch, 2019, 6, pp 50-52
[7] NIST: ‘Framework for improving critical infrastructure cybersecurity, version 1.1, National Institute of Standards and Technology, April 2018
[8] IEEE: ‘802.1X-2010 - IEEE Standard for Local and metropolitan area networks--Port-Based Network Access Control’, International Standard, February 2010

OMICRON 은 혁신적인 테스트 및 진단 솔루션으로 전력 산업에 서비스를 제공하는 국제 기업입니다. OMICRON 제품의 적용으로 사용자는 시스템에 있는 고전압/저전압 설비의 상태를 완벽하게 평가할 수 있습니다. 컨설팅, 커미셔닝, 테스트, 진단 및 교육분야에서 제공되는 서비스는 제품을 보다 완벽하게 만듭니다.

160여 개국의 고객들은 이미 OMICRON의 우수한 품질과 첨단 기술 제품을 선택하였습니다. 모든 대륙에 있는 서비스 센터는 폭넓은 지식 기반과 함께 고객 지원을 제공합니다. 이 모든 것들이 OMICRON을 전력 산업에서 시장 선두주자로 만들었습니다.

자세한 정보, 추가 자료 및 전 세계 사무실의
연락처 정보는 당사 웹사이트를 방문하십시오.

www.omicronenergy.com