TeSys Active

TeSys Tera Motor Management System

사이버 보안 가이드

TeSys는 연결성을 갖춘 혁신적인 모터 스타터 솔루션을 제공합니다

DOCA0260KO-00
11/2025

법률 정보

이 문서에서 제공하는 정보에는 제품/솔루션과 관련된 일반적인 설명, 기술적 특징 및/또는 권장 사항이 포함되어 있습니다.

이 문서는 상세 연구 또는 운영 관련 및 현장 관련 개발 또는 개략적인 계획을 대체하기 위한 것이 아닙니다. 이 문서는 특정 사용자 애플리케이션에 대한 제품/솔루션의 적합성 또는 신뢰성을 판단하기 위해 사용되지 않아야 합니다. 해당 특정 애플리케이션과 관련하여 제품/솔루션에 대한 적절하고 포괄적인 위험 분석, 평가 및 테스트를 직접 수행하거나 자신이 선택한 전문가(통합자, 지정자 등)를 통해 수행하도록 하는 것은 해당 사용자의 의무입니다.

이 문서에서 언급되는 Schneider Electric 브랜드 및 Schneider Electric SE와 그 자회사의 모든 상표는 Schneider Electric SE 또는 그 자회사의 자산입니다. 기타 모든 브랜드는 각 소유자의 상표일 수 있습니다.

목차

안전 정보

중요 정보

이 설명서를 주의 깊게 읽고, 장치를 설치, 작동, 서비스 또는 유지보수하기 전에 장치에 익숙해지기 위해 장비를 살펴보십시오. 다음의 특정 메시지는 잠재적 위험을 경고하거나 절차를 명확하고 간소화하는 정보를 알려주기 위해 이 문서 전반에 또는 장비에 표시될 수 있습니다.

"위험" 또는 "경고" 라벨에 이 기호가 추가되어 있는 경우 감전의 위험성이 있으며, 지시에 따르지 않는 경우 인적 상해가 발생할 가능성이 있다는 것을 나타냅니다.

안전 경고 기호입니다. 인적 상해의 위험성이 있다는 것을 경고합니다. 이 기호의 뒤에 기재된 안전에 관한 정보에 따라 인적 상해나 사망의 위험에 대해 방지 대책을 마련하십시오.

⚠ 위험

위험 이 표시는 지시에 따르지 않으면, 사망 또는 중**상을 입을 상황이 되는 것**을 나타냅니다.

⚠ 경고

경고 이 표시는 지시에 따르지 않으면, 사망 또는 중상을 **입을 가능성이 있다는 것을**나타냅니다.

⚠ 주의

주의 이 표시는 지시에 따르지 않으면,경상 또는 중급의 상해를 **입을 가능성이 있다는 것을**나타냅니다.

주기

이 표시는 지시에 따르지 않으면, 물적 손해를 입을 가능성이 있다는 것을 나타냅니다.

주의하십시오

전기 장비는 자격을 갖춘 기사만 설치, 작동, 서비스, 유지관리해야 합니다. 이 자료를 사용하지 않고 일어난 결과에 대해서는 Schneider Electric에서 책임을 지지 않습니다.

전문 인력이란 전기 장비 구축, 작동, 설치에 관한 기술 및 지식을 갖추고 있고, 관련 위험을 인지하고 방지하기 위한 안전 교육을 받은 인력입니다.

문서에 관하여

문서 적용범위

본 가이드는 TeSys™ Tera 시스템의 사이버 보안 측면에 대한 정보를 제공하여 시스템 설계자와 운영자가 제품의 안전한 운영 환경을 조성하는 데 도움을 주기 위한 것입니다.

이 가이드는 운영 기술 네트워크 또는 회사 네트워크를 보호하는 방법을 다룹니다. Ethernet 네트워크를 보호하는 방법을 다룹니다.

주의: 이 가이드에서 **보안** 는 사이버보안을 의미합니다.

유효성 정보

이 문서는 다음과 같은 공인 TeSys Tera system구성 요소에 대해 유효합니다.

- LTMTEFM: LTMT main unit with EtherNet/IP 또는 Modbus TCP/IP 프로토콜, 100–240 Vac/Vdc
- LTMTEBD: LTMT main unit with EtherNet/IP 또는 Modbus TCP/IP 프로토콜, 24 Vdc
- LTMTMFM: LTMT main unit(Modbus RTU 프로토콜 포함), 100~240Vac/Vdc
- LTMTMBD: LTMT main unit(Modbus RTU 프로토콜 포함), 24Vdc
- LTMTPFM: LTMT main unit(PROFIBUS DP 프로토콜 포함), 100~240Vac/Vdc
- LTMTPBD: LTMT main unit(PROFIBUS DP 프로토콜 포함), 24Vdc

일반 사이버 보안 정보

최근 몇 년 사이에 네트워크화한 기계와 생산 공장의 수가 증가함에 따라 무단 액세스, 데이터 유출, 운영 중단 등 사이버 위협의 잠재성도 그에 상응하여 증가했습니다. 따라서 자산과 시스템을 이러한 위협에서 보호하는 데 도움이 되는 가능한 모든 사이버 보안 조치를 반드시 고려하셔야 합니다.

Schneider Electric 제품을 안전하게 보호하는 데 도움이 되려면 Cybersecurity Best Practices 문서에 설명된 사이버 보안 모범 사례를 시행하시는 것이 가장 좋습니다.

Schneider Electric은 다음과 같은 정보와 지원을 추가로 제공합니다.

- Schneider Electric 보안 뉴스레터 구독.
- 다음이 가능한 Cybersecurity Support Portal 웹 페이지
  - 보안 통지 사항 찾기
  - 취약점 및 사건 보고
- 다음이 가능한 Schneider Electric Cybersecurity and Data Protection Posture 웹 페이지
  - 사이버 보안 태세 액세스
  - 사이버 보안 아카데미에서 사이버 보안 자세히 알아보기
  - Schneider Electric의 사이버 보안 서비스 검색

환경 데이터

제품 규정 준수 및 환경 정보는 Schneider Electric Environmental Data Program을 참조하십시오.

이 문서의 번역 언어

이 문서는 다음 언어로 제공됩니다.

- 영어
- 중국어
- 프랑스어
- 독일어
- 이탈리아어
- 한국어
- 스페인어

관련 문서

문서 제목	설명	참조 번호
TeSys Tera Motor Management System 카탈로그	카탈로그: • TeSys Tera system에 대해 설명합니다. • TeSys Tera의 기술 특성을 포함합니다.	LVCATENTER
TeSys Tera Motor Management System 사용자 가이드	전체 TeSys Tera system에 대해 소개하는 기본 사용자 가이드입니다. LTMT main units, LTMTCT/LTMTCTV Sensor Module, LTMT expansion modules및 LTMTCUF control operator unit의 주요 기능을 설명합니다.	DOCA0257EN
TeSys Tera Motor Management System 설치 가이드	이 가이드에서는 LTMT main unit, LTMTCT/LTMTCTV Sensor Module, LTMT expansion modules및 LTMTCUF control operator unit의 설치, 시운전 및 유지보수에 대해 설명합니다.	DOCA0356EN
TeSys Tera Motor Management System DTM library Online Help Guide	이 가이드에서는 TeSys Tera DTM의 제어 기능을 사용자 정의하는 데 사용할 수 있는 TeSys Tera Motor Management SystemLibrary에 대해 설명합니다.	DOCA0275EN
TeSys Tera Motor Management System Modbus RTU 통신 안내서	이 가이드는 Modbus의 LTMT main unit네트워크 프로토콜 통신에 대해 설명합니다.	DOCA0355EN
TeSys Tera Motor Management System PROFIBUS DP 통신 안내서	이 안내서는 PROFIBUS DP의 LTMT main unit네트워크 프로토콜 통신에 대해 설명합니다.	DOCA0256EN
TeSys Tera Motor Management System EtherNet/IP 통신 안내서	이 안내서는 EtherNet/IP의 LTMT main unit네트워크 프로토콜 통신에 대해 설명합니다.	DOCA0258EN
TeSys Tera Motor Management System LTMTCUF control operator unit 사용자 가이드	이 가이드에서는 LTMTCUF control operator unit의 설치, 구성 및 사용 방법에 대해 설명합니다.	DOCA0233EN
TeSys Tera Motor Management System DTM library 소프트웨어 릴리스 노트	이 문서에서는 TeSys Tera DTM Library software에 대한 중요한 정보를 제공하며, 새로운 기능 및 향상된 기능에 대한 요약을 제공합니다.	DOCA0279EN
TeSys Tera Motor Management System Firmware Release Note	이 문서에서는 TeSys Tera system의 펌웨어 버전에 대한 정보와 새로운 기능 및 향상된 기능에 대한 요약을 제공합니다.	DOCA0276EN
사이버 공격에 대한 취약성을 어떻게 줄일 수 있나요?	이 가이드는 제어 시스템 및 자동화 분야의 사이버 보안 위험과 완화 전략을 설명합니다.	사이버 공격에 대한 취약성을 어떻게 줄일 수 있나요?

문서를 온라인으로 찾으시려면 Schneider Electric 다운로드 센터 (www.se.com/ww/en/download/)를 방문하십시오.

비포용적이거나 몰지각한 용어에 관한 정보

책임감 있고 포용적인 기업으로서 Schneider Electric은 비포용적이거나 몰지각한 용어가 포함된 홍보물과 제품을 지속적으로 업데이트하고 있습니다. 그러나 이 같은 노력에

도 불구하고 당사 콘텐츠에는 일부 고객에게 부적절하다고 여겨지는 용어가 들어 있을 수 있습니다.

상표

QR 코드는 일본 및 그 외 국가에서 DENSO WAVE INCORPORATED의 등록 상표입니다.

예방 조치

이 가이드에서 절차를 수행하기 전에 다음 주의 사항을 읽고 숙지해야 합니다.

⚠⚠위험

감전, 폭발 또는 아크 플래시 위험

- 이 장비는 자격을 갖춘 전기 기술자만 설치 및 정비해야 합니다.
- 이 장비의 작동 또는 내부 작업을 하기 전에 이 장비에 공급되는 모든 전원을 차단하십시오.
- 이 장비와 모든 관련 제품을 작동할 때는 지정된 전압만 사용하십시오.
- 전력이 꺼진 것을 확인하려면 항상 적절한 정격 전압 감지 장치를 사용하십시오.
- 인체 및/또는 장비 위험이 존재하는 경우 적절한 인터록을 사용하십시오.
- 전력선 회로는 현지 및 국가의 규정 요구 사항을 준수하여 배선 및 보호해야 합니다.
- 적절한 개인 보호 장비(PPE)를 착용하고 NFPA 70E, NOM-029-STPS 또는 CSA Z462 또는 해당 지역에 상응하는 전기 작업 방식을 따르십시오.

이러한 지침을 따르지 않을 경우 심각한 부상 또는 사망으로 이어질 수 있습니다.

⚠경고

의도하지 않은 장비 작동

- 이 장비를 분해, 수리 또는 개조하지 마십시오. 사용자가 정비할 수 있는 부품은 없습니다.
- 이 장비를 의도한 적용 환경에 맞게 적절한 등급을 받은 인클로저에 설치하고 작동하십시오.
- 이 장비의 각 구현은 서비스에 배치하기 전에 적절한 작동 여부를 개별적으로 철저하게 테스트해야 합니다.

이러한 지침을 따르지 않을 경우 심각한 부상 또는 사망으로 이어지거나 장비가 손상될 수 있습니다.

자격을 갖춘 직원

본 가이드 및 기타 관련 제품 문서의 내용을 숙지하고 이해하는 적절히 훈련된 인원만이 본 제품의 작업 및 사용을 수행할 수 있습니다.

자격 있는 담당자는 매개변수 값 변경 및 일반적으로 기계적, 전기적 또는 전자 장비에서 발생할 수 있는 잠재적 위험을 식별할 수 있어야 합니다. 자격 있는 담당자는 산업재해 예방을 위한 기준, 규정 및 규칙을 숙지해야 하며, 시스템을 설계하고 구현할 때 이를 준수해야 한다.

이 가이드에 포함된 정보를 사용하고 적용하려면 자동 제어 시스템의 설계 및 프로그래밍에 대한 전문 지식이 필요합니다. 사용자, 패널 제조업체 또는 설치업체만이 공정 플랜트 또는 기계의 설치, 설정, 작동 및 유지보수 중에 존재하는 모든 조건과 요인을 알 수 있으므로 특정 애플리케이션에 대한 자동화 및 제어 장비와 기타 관련 장비 또는 소프트웨어를 선택할 때 효과적이고 적절하게 사용할 수 있는 자동화 및 관련 장비와 관련 안전 장치 및 인터록을 결정할 수 있습니다. 해당 지역, 지역 또는 국가의 표준 및/또는 규정도 고려해야 합니다.

이 장비를 사용할 때 공정 플랜트 또는 기계에 적용되는 안전 정보, 전기 요구 사항 및 규범적 표준을 준수하는 데 특히 주의하십시오.

사용 목적

이 가이드에 설명된 제품은 소프트웨어, 액세서리 및 옵션과 함께 저압 전기 부하용 스타터를 구성하며, 본 문서 및 기타 지원 문서에 포함된 지침, 지시, 예 및 안전 정보에 따라 산업용으로 사용하도록 만들어졌습니다.

이 제품은 모든 해당 안전 규정 및 지침, 지정된 요구 사항 및 기술 데이터를 준수하여 사용해야 합니다.

제품을 사용하기 전에 계획된 애플리케이션에 대한 위험 평가를 수행해야 합니다. 그 결과에 따라 안전 관련 조치를 적절히 집행해야 합니다.

해당 제품은 공정 플랜트 또는 기계의 구성 요소로 사용되므로, 전체 시스템 설계를 통해 인원의 안전을 보장해야 합니다.

지정된 케이블 및 액세서리로만 제품을 작동하십시오. 정품 액세서리와 예비 부품만 사용하십시오.

명시적으로 허용된 사용 이외의 모든 사용은 금지되며 예기치 않은 위험을 초래할 수 있습니다.

사이버 보안 안전 공지

⚠경고

잠재적인 시스템 가용성, 무결성 및 신뢰성의 약화

- 기기 설정, 제어 기능 및 정보에 대한 무단 접근을 방지하기 위해 최초 사용 시 기본 비밀번호를 변경하십시오.
- 사용하지 않는 포트/서비스를 비활성화하여 악의적인 공격자의 침투 경로를 최소화하십시오.
- 네트워크 연결 장치를 방화벽, 네트워크 분할, 네트워크 침입 탐지 및 방어 시스템과 같은 다중 계층의 사이버 방어 체계 뒤에 배치하십시오.
- 사이버 보안 모범 사례(예: 최소 권한 원칙, 업무 분리)를 활용하여 데이터 및 로그의 무단 노출, 손실, 변경 또는 서비스 중단을 방지하십시오.

이러한 지침을 따르지 않을 경우 심각한 부상 또는 사망으로 이어지거나 장비가 손상될 수 있습니다.

사이버 보안 개론

이 파트의 내용

개요

사이버 보안은 프로세스, 도구 및 기술, 규정 준수, 거버넌스의 일부로서, 운영 중단(가용성), 정보 변조(무결성), 기밀 데이터 노출(기밀성)을 초래할 수 있는 공격으로부터 통신 네트워크 및 모든 연결된 장치를 보호하는 것을 목표로 합니다.

사이버 보안의 목적은 정보 및 물리적 자산이 도난, 손상, 오용 또는 사고로부터 보호 수준을 높이는 동시에 해당 자산을 사용하도록 의도된 사용자들의 접근성을 유지하는 데 있습니다. 사이버 보안에는 안전한 시스템 설계, 물리적 및 디지털 방법을 통한 접근 제한, 사용자 식별, 보안 통제/측정 절차 및 모범 사례 정책 구현 등 다양한 측면이 포함됩니다.

Schneider Electric 가이드라인

이 가이드에 제공된 권장 사항 외에도 TeSys Tera system사이버 보안에 대한 Schneider Electric 사이버 보안에 대한 다층 방어 접근법을 적용해야 합니다.

이 접근 방식은 권장 사이버 보안 모범 사례.

또한, 다음에서 유용한 자료와 최신 정보를 확인하실 수 있습니다. 슈나이더 일렉트릭 사이버 보안 지원 포털에서, 44 페이지.

Schneider Electric의 사이버 보안 접근법

Schneider Electric은 제어 시스템의 개발 및 구현에서 업계 모범 절차를 준수하고 있습니다. 여기엔 업계 제어 시스템을 보호하기 위한 심층적 방어 접근법이 포함됩니다. 이 접근법은 하나 또는 그 이상의 방화벽 뒤에 컨트롤러를 배치해 오직 인가된 직원 및 프로토콜로만 접속을 제한합니다.

⚠경고

인가되지 않은 접속 및 그에 따른 인가되지 않은 작동

- 장비 또는 전체 환경이 주요 인프라에 연결되어 있는지 평가합니다. 그렇다면 자동화 시스템을 네트워크에 연결하기 전에 심층적 방어에 따라 예방 측면에서 적절한 단계를 수행하십시오.
- 회사 내부 네트워크에 연결된 장치의 수를 제한하십시오.
- 귀하의 산업 네트워크를 회사 내부의 타 네트워크로부터 격리하십시오.
- 방화벽, VPN 또는 기타 입증된 보안 방식을 사용해 의도되지 않은 접속에 대해 어떠한 네트워크든 보호하십시오.
- 시스템 내 활동을 모니터링하십시오.
- 대상 장치가 인가되지 않은 당사자 또는 인증되지 않은 활동으로부터 직접 접속 또는 직접 링크되지 않도록 하십시오.
- 시스템 및 프로세스 정보의 백업을 포함해, 복구 계획을 준비하십시오.

이러한 지침을 따르지 않을 경우 심각한 부상 또는 사망으로 이어지거나 장비가 손상될 수 있습니다.

보안 위협

사이버 위협은 PC 및 PC 네트워크의 정상적 작동에 지장을 줄 수 있는 계획된 행동이거나 사고입니다. 이러한 행동은 물리적 시설 안에서 또는 외부 장소에서 시작될 수 있습니다. 제어 환경에 대한 보안 과제는 다음과 같습니다:

- 다양한 물리 및 논리적 경계
- 다수 위치 및 큰 지리적 범위
- 프로세스 가용성에 대한 보안 구현의 부작용
- 비즈니스 커뮤니케이션이 점점 더 개방됨에 따라 비즈니스 시스템으로부터 제어 시스템으로 이주되는 웜 및 바이러스에의 노출 증가
- USB 장치, 벤더 및 서비스 테크니션 랩탑 및 엔터프라이즈 네트워크로부터의 악성 소프트웨어에 대한 노출 증가
- 물리 및 기계 시스템에 대한 제어 시스템의 직접적 영향

정책 및 규정

Schneider Electric은 SDL(Secure Development Lifecycle) 프로세스를 보유하고 있으며, 이는 제품이 전체 수명 주기의 모든 단계에서 보안 설계 프로세스를 따르도록 지원하는 핵심 제품 개발 기반 프레임워크입니다. 슈나이더 일렉트릭 SDL 프로세스는 IEC 62443-4.1 표준을 준수합니다.

SDL 프로세스에는 다음이 포함됩니다:

- 공급망 전반에 걸친 내부 개발 활동에 적용된 SDL 관행.
- 프로젝트 출시를 위한 최종 보안 검토가 필요합니다.
- 제품 개발에 참여하는 인원을 위한 보안 교육.

보안 강화 지침

소개

PC에서 다양한 애플리케이션을 실행하여 제어 환경의 보안을 강화할 수 있습니다. 시스템에는 심층적 방어 접근법에 대한 Schneider Electric의 장치 강화 권장 사항과의 일관성을 위해 재구성을 요구하는 공장 기본 설정이 있습니다.

다음 지침은 Windows 운영 체제에서의 절차를 설명합니다. 이들은 단지 예시로만 제공됩니다. 귀하의 운영 체제 및 애플리케이션이 다른 요구 사항 또는 절차를 가질 수도 있습니다.

원격 데스크탑 프로토콜 비활성화하기

Schneider Electric의 심층 방어 접근 방식 권장 사항에는 애플리케이션에서 원격 데스크탑 프로토콜(RDP)을 요구하지 않는 경우RDP의 비활성화가 포함됩니다.

Windows 11에서 원격 데스크톱 프로토콜(RDP)을 비활성화하려면 **설정 > 시스템 > 원격 데스크톱 > 원격 데스크톱 사용**(**꺼짐**으로 전환)을 사용합니다.

보안 정책 업데이트하기

명령창에 `gpupdate`를 입력하여 시스템에서 PC의 보안 정책을 업데이트합니다. 자세한 내용은 Microsoft에 대한 `gpupdate` 설명서를 참조하십시오.

업데이트 관리하기

배포에 앞서, Microsoft의 **Windows 업데이트** 웹 페이지에서 유틸리티를 사용하여 모든 PC 운영 체제를 업데이트하십시오. Windows에서 이 툴에 접속하려면, **시작 > 모든 프로그램 > Windows 업데이트**를 선택하십시오.

워크스테이션 보호

엔지니어링 워크스테이션과 관련된 보안 위험을 줄이기 위해 DEP(Data Execution Prevention) 및 ASLR(Address Space Layout Randomization)과 같은 메모리 취약성 보호 설정을 활성화하십시오. 이러한 보안 설정은 Windows 11 운영 체제에서 시스템 취약성 보호 설정을 사용하여 활성화할 수 있습니다. 자세한 내용은 Microsoft 보안 기능 웹페이지를 참조하십시오.

안전한 비밀번호 적용

대문자, 소문자, 숫자 및 특수문자 등 필수 요소를 충족하는 강력한 비밀번호를 사용하십시오. 이 기능을 활성화하면 취약한 비밀번호로 인한 위험을 줄여 무단 접근을 방지하는 데 도움이 됩니다.

기본이 아닌 포트 사용

HTTPS, DWPS, Modbus TCP와 같은 프로토콜의 기본 통신 포트를 변경하면 추가적인 보안 계층이 적용됩니다.

허용 IP 목록

IP 허용 목록 기능은 지정된 IP 주소만 허용함으로써 시스템 접근을 제한합니다. 이는 무단 장치의 시스템 연결을 방지하고 신뢰할 수 있는 출처만이 통신할 수 있도록 보장합니다. TeSys Tera system. IP 허용 목록 기능에 접근하려면 **보안 > IP 허용 목록 > 표시됩니다.** 표준 웹 서버에서

TeSys Tera 시스템 정보

이 파트의 내용

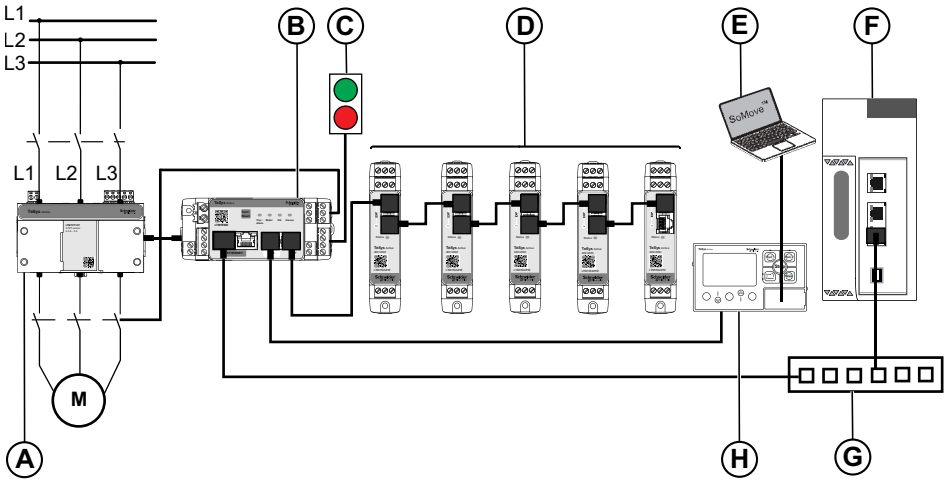
개요

그 TeSys Tera Motor Management System (또는 TeSys Tera system)는 TeSys 지능형 릴레이 및 모터 스타터의 액티브 제품군에 속합니다. 이 제품은 TeSys Tera system는 단상 또는 삼상 교류 유도 모터에 대한 완벽한 보호, 계량, 제어 및 모니터링 기능을 제공하기 위해 지능형 모터 제어 센터(iMCC)의 신뢰할 수 있는 구성 요소로 설계되었습니다.

TeSys Tera system은 저압 개폐기 시스템에 설치되며 Fieldbus 네트워크와 모터 피더를 통해 더 높은 수준의 자동화 시스템을 연결합니다.

TeSys Tera system:

- 기존 및 고급 모터 보호, 계량, 모니터링 기능을 iMCC 피더에 적용하여 독립형 HMI 장치가 포함된 단일, 구성 용이한 소형 통신 모듈로 통합합니다.
- 저압 접촉기 제어 모터 스타터 피더를 위한 보호 컨트롤러를 제공합니다.
- 저압 애플리케이션에서 일정한 속도로 작동하는 모터를 위한 유연한 모듈형 모터 관리 시스템을 제공합니다.



A LTMTCT/LTMTCTV sensor module

B LTMT main unit

C 시작/정지 명령

D LTMT expansion modules

E SoMove 설치된 TeSys Tera DTM FDT 컨테이너 소프트웨어를 실행 중인 PC

F 프로그래밍 가능한 로직 컨트롤러(PLC) 또는 분산형 제어 시스템(DCS)

G Ethernet 스위치

H LTMTCUF control operator unit

통신 인터페이스

TeSys Tera system 다음 인터페이스 유형을 통해 통신합니다:

LTMT main unit	레퍼런스	포트
Modbus RTU 	• LTMTMFM (100–240 Vac/ Vdc) • LTMTMBD (24 Vdc)	• Modbus RTU 터미널 커넥터가 있는 통신 포트 • HMI 포트와 Modbus RTU 구성용 통신 기능
PROFIBUS DP 	• LTMTPFM (100–240 Vac/Vdc) • LTMTPBD (24 Vdc)	• PROFIBUS DP 서브 D9 커넥터가 장착된 • Profibus 터미널 커넥터가 있는 포트 • HMI 포트와 Modbus RTU 통신

LTMT main unit	**레퍼런스**	**포트**
Modbus TCP/IP 	• LTMTEFM (100–240 Vac/Vdc) • LTMTEBD (24 Vdc)	• 두 Ethernet 포트가 Modbus TCP/IP • HMI 포트와 Modbus RTU 통신
EtherNet/IP 	• LTMTEFM (100–240 Vac/Vdc) • LTMTEBD (24 Vdc)	• 두 Ethernet 포트가 EtherNet/IP • HMI 포트와 Modbus RTU 통신

지원되는 프로토콜

직렬 통신 장치

그 Modbus RTU 그리고 PROFIBUS DP 모듈의 TeSys Tera system 지원 Modbus RTU 및 PROFIBUS 필드버스 장치와의 통신을 위한 프로토콜을 지원합니다.

통신 프로토콜 및 관련 상업적 참조 사항에 대해서는 통신 인터페이스, 22 페이지.

이더넷 통신 장치

그 Modbus TCP/IP 그리고 EtherNet/IP 모듈은 TeSys Tera system 다음 프로토콜을 지원합니다:

- 구성 도구 및 내장 웹페이지를 통한 HTTPS
- Modbus TCP/IP 그리고 EtherNet/IP 필드버스 장치와의 통신을 위해
- 네트워크 IP 주소 할당을 위한 DHCP
- 네트워크 이름 해상도를 위한 DNS
- 시간 동기화를 위한 NTP
- DPWS(Device Discovery)

통신 프로토콜 및 관련 상업적 참조 사항에 대해서는 통신 인터페이스, 22 페이지.

보안 기능

는 TeSys Tera system다음 기능을 지원합니다:

- 펌웨어는 디지털 서명된 Schneider Electric 다음에 설치할 수 있습니다. TeSys Tera system.
- 부팅 시마다 펌웨어의 디지털 서명이 실행 전에 검증됩니다.
- 사용자 비밀번호는 안전하게 저장됩니다(적용 대상: Ethernet 인터페이스 모듈에 적용됨).

  암호 정책에 대한 자세한 내용은 다음을 참조하십시오. *TeSys Tera Motor Management System EtherNet/IP Communication Guide - DOCA0258EN*
- 공장 초기화를 수행할 수 있습니다. TeSys Tera system 사용하여 **공장 초기화** 설정을 사용하여 TeSys Tera DTM 또는 **테스트 / 재설정** 버튼을 사용하여 LTMT main unit.

  자세한 내용은 **테스트 / 재설정** 버튼에 대한 자세한 내용은 *TeSys Tera Motor Management System User Guide – DOCA0257EN*.
- 해당 TeSys Tera system 내장 시계가 장착되어 있어 전원이 꺼진 상태에서도 12 시간 동안 날짜와 시간을 기억합니다(유효 기간: Modbus RTU 및 PROFIBUS DP 변형에 적용되며 Ethernet 모듈에는 적용되지 않음).
- 사용 TeSys Tera DTM선택적 핀 관리 기능을 사용하면 다음의 구성을 활성화하거나 비활성화할 수 있습니다. TeSys Tera system. 핀 관리 기능을 사용하여 TeSys Tera DTM PIN 관리 기능을 사용하여 PIN을 재설정할 수도 있습니다.

  핀 관리 기능에 대한 자세한 내용은 다음을 참조하십시오. *TeSys Tera Motor Management System DTM Library Online Help Guide – DOCA0275EN*.
- 확보하기 위해 TeSys Tera system, LTMTCUF control operator unit 핀 기능이 포함되어 있습니다. 해당 서비스에 접근하려면 6자리 PIN이 필요합니다. LTMTCUF control operator unit.

  핀 기능에 대한 자세한 내용은 다음을 참조하십시오. *TeSys Tera Motor Management System User Guide – DOCA0257EN*.

통신 프로토콜 및 해당 상업적 참조에 대해서는 통신 인터페이스, 22 페이지.

TeSys Tera 시스템 기능

이 파트의 내용

펌웨어 업데이트

최신 펌웨어 버전으로 업데이트하여 TeSys Tera system 최신 펌웨어 버전으로 업데이트하여 최신 기능을 확보하고 보안 패치를 최신 상태로 유지하십시오. 해당 장치를 위해 설계된 모든 펌웨어는 TeSys Tera system Schneider Electric 공개 키 기반 구조(PKI)를 사용하여 서명되어, 에서 실행되는 펌웨어의 무결성과 진위성을 보장하는 데 도움을 줍니다. TeSys Tera system.

펌웨어 업데이트에 대한 자세한 내용은 TeSys Tera DTM에 대한 자세한 내용은 다음을 참조하십시오. *TeSys Tera Motor Management System DTM Library Online Help Guide – DOCA0275EN*.

표준 웹 서버를 통한 펌웨어 업데이트에 대한 자세한 내용은 (적용 대상: Ethernet 인터페이스 모듈에 적용됨)에 대한 자세한 내용은 다음을 참조하십시오. *TeSys Tera Motor Management System EtherNet/IP Communication Guide - DOCA0258EN*.

보안 업데이트에 대한 자세한 내용은 *Security Notifications* 슈나이더 일렉트릭 사이버 보안 지원 포털에 등록하십시오.

날짜 및 시간

오류를 방지하려면 날짜와 시간을 동기화하는 것이 중요합니다.

다음 절차는 표준 웹 서버 또는 를 사용하여 인터페이스 모듈의 날짜 및 시간 설정을 업데이트하는 방법을 Ethernet 보여줍니다 TeSys Tera DTM:

1. 설정으로 이동 **Settings > General > Date & Time**.
2. 사용하는 **날짜 및 시간 선택** 드롭다운 목록에서 다음 옵션 중 하나를 선택하십시오:
   - **매뉴얼**

     주의:

     - 날짜와 시간을 수동으로 설정하면 LTMT main unit 재부팅 시 공장 설정으로 초기화됩니다.
     - 날짜 및 시간 설정은 수동으로 업데이트할 수 있습니다. TeSys Tera DTM 또는 LTMTCUF control operator unit.
   - **NTP**

     주의: NTP 프로토콜은 Ethernet 버전에서만 사용할 수 있습니다. LTMT main unit.

사용하지 않는 포트/인터페이스 비활성화

사용하지 않는 포트/인터페이스를 비활성화하면 적극적으로 사용되지 않는 통신 포트와 인터페이스를 꺼서 시스템의 공격 표면을 줄이는 데 도움이 됩니다.

다음 설정은 TeSys Tera system 표준 웹 서버를 사용하여 비활성화할 수 있습니다:

- **Modbus TCP**
- **장치 검색**
- **Modbus RTU**

주의: 자세한 내용은 *TeSys Tera Motor Management System EtherNet/IP Communication Guide - DOCA0258EN*를 참조하십시오

포트

그 Modbus TCP/IP 그리고 EtherNet/IP 의 모듈들은 TeSys Tera system 기본적으로 통신을 위해 다음 포트를 사용합니다:

포트 유형	EtherNet/IP	Modbus TCP/IP
TCP Port 443 (HTTPS)	✓	✓
TCP Port 502 (Modbus TCP/IP)	✓	✓
TCP Port 5357 (DPWS)	✓	✓
TCP Port 44814 (EtherNet/IP)	✓	X
UDP Port 2222 (EtherNet/IP)	✓	X
SNTP UDP Port 123 (EtherNet/IP)	✓	✓
DNS Port 53 (EtherNet/IP)	✓	✓
DHCP Port 68 (EtherNet/IP)	✓	✓

Syslog

해당 TeSys Tera system 시스템 로그를 생성하여 무효 로그인 시도 및 펌웨어 업데이트와 같은 이벤트를 기록합니다. 로그에는 어떠한 개인정보도 포함되어 있지 않습니다.

예상치 못한 동작(예: 빈번한 재부팅, 잘못된 펌웨어 업데이트 또는 무효한 로그인 시도)을 감지하려면 로그를 정기적으로 모니터링하는 것이 좋습니다.

로그에 대한 자세한 내용은 다음을 참조하십시오. *TeSys Tera Motor Management System DTM Library Online Help Guide – DOCA0275EN* 및 *TeSys Tera Motor Management System EtherNet/IP Communication Guide - DOCA0258EN*.

폐기

이 TeSys Tera system 시운전 중에 설정된 기밀 정보, 최근 데이터 값 및 로그를 포함합니다.

예를 들어, 이 정보에는 다음이 포함될 수 있습니다. Modbus LTMT main unit 토폴로지 또는 측정된 전력 소비량 등이 포함될 수 있습니다.

폐기 전에 공장 초기화를 수행해야 합니다. TeSys Tera system.

다음과 같은 방법으로 재설정할 수 있습니다. TeSys Tera system:

- **테스트 / 재설정** 버튼 LTMT main unit: 누르고 있으면 **테스트 / 리셋** 버튼을 LTMT main unit 10초간 누르고 있습니다.
- TeSys Tera DTM Library자세한 내용은 섹션 공장 초기화 을 참조하십시오. *TeSys Tera Motor Management System DTM Library Online Help Guide – DOCA0275EN*
- LTMTCUF control operator unit자세한 내용은 섹션 명령 메뉴 을 참조하십시오. *TeSys Tera Motor Management System LTMTCUF Control Operator Unit User Guide – DOCA0233EN*

네트워크 보안

이 파트의 내용

주의: 이 부분은 의 및 모듈에만 Modbus TCP/IP 및 EtherNet/IP 유효합니다 TeSys Tera system.

개요

이것은 TeSys Tera system 는 공개 인터넷에 직접 노출되는 것을 견디도록 설계되지 않았습니다. 최소한 네트워크 주소 변환(NAT) 뒤에 설치해야 하며, 바람직하게는 여러 방화벽 뒤에 설치해야 합니다. 자세한 내용은 다음 웹페이지를 참조하십시오:

- 슈나이더 일렉트릭 사이버 보안 컨설팅 서비스
- 국립표준기술연구소*(NIST)*
- 유럽연합 사이버보안청*(ENISA)*

네트워크 세그멘테이션

The TeSys Tera system 는 서로 다른 네트워크 간에 연결 고리를 형성하는 관문입니다. 네트워크 분할은 사이버 방어 체계를 강화하는 데 도움이 됩니다. 네트워크 세분화를 강화하기 위해, TeSys Tera system EtherNet/IP 버전 LTMT main unit 두 개의 Ethernet 포트를 사용 가능한 Ethernet 사용 가능한 포트는 정보 기술(IT) 및 운영 기술(OT)에 활용될 수 있습니다.

HTTPS 및 Modbus 사용 가능합니다 TeSys Tera system Ethernet 인터페이스에서 사용할 수 있습니다(ETH1, ETH2).

해당 서비스가 사용되지 않는 네트워크에서는 Modbus TCP/IP 사용하지 않는 네트워크에서는 해당 서비스를 비활성화하는 것이 좋습니다.

제품 웹 서버 인증서

안전한 HTTPS 통신을 지원하기 위해, TeSys Tera system 기본적으로 X.509v3 기본적으로 인증서가 제공됩니다. 이 인증서는 HTTPS 통신을 설정할 때 무결성과 기밀성을 보장하는 데 도움이 됩니다.

웹 브라우저는 제3자 인증 기관(CA)이 서명한 인증서만 인식합니다. 자체 서명된 인증서는 안전하지 않습니다. 타사 CA 서명 인증서를 TeSys Tera system 또한 날짜와 시간을 동기화해야 합니다.

다음 인증서 형식이 지원됩니다. TeSys Tera system:

형식	헤더/푸터	키 유형
PKCS#1	–––––RSA 개인 키 시작–––––	RSA 전용
PKCS#8	–––––개인 키 시작–––––	RSA, EC, DSA 등
암호화된 PKCS#8	–––––암호화된 개인 키 시작–––––	모두

주의: 수정된 시험 증명서는 인정되지 않습니다.

제3자 인증서에 대한 자세한 내용은 다음을 참조하십시오. *TeSys Tera Motor Management System EtherNet/IP Communication Guide - DOCA0258EN*.

연결된 장치에 관한 안전 정보

의 네트워크에 연결된 장치 목록을 정기적으로 확인할 것을 Ethernet권장합니다 TeSys Tera system. 알 수 없는 연결된 장치가 있는 경우, 해당 장치를 찾아 제거하십시오. 네트워크를 재구축하고 식별된 장치만 다시 연결할 수도 있습니다.

물리적 보안

설치

시스템의 물리적 보안을 보호하기 위해 다음 설치를 권장합니다:

- 설치하십시오. TeSys Tera system 설치 위험 수준에 적합한 방식으로 고정된 인클로저(예: 자물쇠나 열쇠가 있는 인클로저)에 설치하십시오.
- 만약 TeSys Tera system 이 스위치보드에 장착된 경우, 스위치보드를 보안이 유지되는 공간(예: 잠금 장치된 문이나 카메라가 설치된 공간)에 설치하십시오.

유지보수 중 보안 권고사항

이 파트의 내용

유지보수 작업

해당 제품의 수명 동안 TeSys Tera system다음과 같은 작업을 정기적으로 수행하는 것이 권장됩니다:

- 장치가 최신 펌웨어 버전을 실행 중인지 확인하십시오.
- 모든 네트워크 및 보안 패치가 최신 상태인지 확인하십시오.
- 권장되는 사이버 보안 모범 사례를 따르십시오.
- 예상치 못한 동작(예: 무효한 로그인 시도 또는 빈번한 재부팅)의 경우 다음을 확인하십시오. Syslog, 31 페이지.
- 현재 날짜에서 벗어나지 않도록 하려면 다음을 확인하십시오. 날짜 및 시간, 28 페이지.
- 장치에 대해 Schneider Electric이 권장하는 보안 표준을 준수하십시오.

보안 기능 검증

이 장의 내용

웹 인증

주의: 이 항목은 의 Modbus TCP/IP 및 EtherNet/IP 모듈에만 적용됩니. TeSys Tera system.

웹 인증 기능을 확인하려면 다음 단계를 따르십시오:

1. 표준 웹 서버에 로그인해 보십시오. TeSys Tera system 비밀번호 없이 로그인하거나 잘못된 비밀번호를 입력하십시오.

   결과: 해당 항목은 TeSys Tera system 표준 웹 서버에 대한 접근 권한을 부여하지 않습니다.

2. 세 개의 인스턴스에 대해 잘못된 자격 증명을 입력하십시오.

   결과: 잠금 장치는 TeSys Tera system 잠금 상태가 15분 동안 유지된 후 네 번째 시도를 할 수 있습니다.

웹 인증

주의: 이 항목은 Modbus TCP/IP 및 EtherNet/IP 모듈에만 적용됩니다. TeSys Tera system.

웹 인증 기능을 확인하려면 다음 단계를 따르십시오:

1. 표준 웹 서버에 로그인하십시오. TeSys Tera system 표준 웹 서버에 로그인하십시오.

   결과: 로그인 후 데이터와 기능에 대한 전체 접근 권한을 갖게 됩니다.

2. 웹페이지를 북마크에 추가하기 (예를 들어, **설정**).
3. 브라우저에서 새 창을 열고, 북마크된 웹페이지를 열어주세요.

   결과: 당 웹페이지에 접근할 수 없지만, 로그인 페이지로 자동 연결됩니다.

Syslog

Syslog 기능을 확인하려면 다음 단계를 따르십시오:

1. 일부 또는 모든 선행 테스트 후, TeSys Tera DTM 또는 표준 웹 서버를 사용하여 **로그**.
2. 로그 파일을 다운로드하십시오.
3. 실행된 테스트 또는 실패한 시도가 로그에 존재하는지 확인하십시오.

펌웨어 업데이트

펌웨어 업데이트 기능을 확인하려면 다음 단계를 따르십시오:

1. 다음으로 이동하십시오 **펌웨어 업데이트** 기능으로 이동하십시오. TeSys Tera DTM 또는 표준 웹 서버에서
2. 인증된 펌웨어 업데이트 파일을 업로드하십시오.
3. 펌웨어가 검증될 때까지 기다리십시오.

   결과: 시스템 재부팅은 해당 장치의 펌웨어가 업데이트되고 새로운 펌웨어 정보가 업데이트될 때만 발생합니다. LTMT main unit 이 업데이트되고 새 펌웨어 정보가 TeSys Tera DTM.

서비스 비활성화

주의: 이 항목은 의 Modbus TCP/IP 및 EtherNet/IP모듈에만 유효합니다 TeSys Tera system.

서비스 비활성화 기능을 확인하려면 다음 단계를 따르십시오:

1. 이동 **보안 > IP 네트워크 목록 > 장치 검색** 표준 웹 서버를 사용하여.
2. 장치 검색을 비활성화하십시오.
3. 동일한 네트워크에 Windows 동일한 네트워크에 연결하십시오.
4. 클릭 **네트워크** 에서 **파일 탐색기**.

   결과: 해당 TeSys Tera system 이 발견되지 않았으므로 네트워크의 장치 목록에 나타나지 않습니다.

다음으로 이동 **보안 > IP 네트워크 목록** 으로 이동하여 위 절차를 따라 다음 비활성화 방법을 확인하십시오:

- Modbus TCP
- Modbus RTU

슈나이더 일렉트릭 사이버 보안 지원 포털

이 파트의 내용

개요

The Schneider Electric *Cybersecurity support portal* 다음과 같이 Schneider Electric 취약점 관리 정책을 설명합니다.

취약점 관리 정책의 목적은 Schneider Electric 취약점 관리 정책의 목적은 설치된 솔루션, 고객 및 환경을 보호하기 위해 Schneider Electric 설치된 솔루션, 고객 및 환경을 보호하기 위함입니다.

Schneider Electric 연구자, 사이버 비상 대응팀(CERT), 자산 소유자와 협력하여 정확한 정보가 적시에 제공되어 그들의 설비를 적절히 보호할 수 있도록 합니다.

Schneider Electric기업 제품 보안 대응팀(CPCERT)은 제품 및 솔루션에 영향을 미치는 취약점과 완화 조치에 대한 경보를 관리하고 발행하는 책임을 맡고 있습니다.

CPCERT는 관련 CERT, 독립 연구자, 제품 관리자 및 모든 영향을 받은 고객 간의 의사소통을 조정합니다.

사이버 보안 지원 포털

는 Schneider Electric Cybersecurity support portal 다음 정보를 제공합니다:

- 제품의 사이버 보안 취약점에 관하여
- 사이버 보안 사고에 관하여
- 사이버 보안 사고 또는 취약점을 신고할 수 있도록 하는 인터페이스에 관하여

취약점 보고 및 관리

사이버 보안 사고 및 잠재적 취약점은 슈나이더 일렉트릭 웹사이트를 통해 신고할 수 있습니다: 취약점 신고하기.

Schneider Electric Industries SAS
35 rue Joseph Monier
92500 Rueil Malmaison
France

www.se.com

DOCA0260KO-00