자율성의 새로운 구심점: MCP와 자산 관리 쉘의 통합을 통한 스마트 제조의 재정의

Executive Summary

제조 산업은 전례 없는 복잡성과 압박에 직면해 있습니다. 노동력 부족, 비용 상승, 지정학적 변동, 그리고 탈탄소화 목표는 기업들로 하여금 운영 방식을 근본적으로 혁신하도록 요구하고 있습니다.[1] 이러한 변혁의 중심에는 인공지능(AI), 특히 자율적으로 작업을 수행할 수 있는 AI 에이전트가 있습니다. 그러나 AI 에이전트의 잠재력을 완전히 실현하기 위해서는 단편화된 시스템, 레거시 인프라, 그리고 표준화되지 않은 데이터라는 근본적인 장벽을 넘어야 합니다.[2]

본 기술 분석 보고서는 이러한 문제를 해결하고 자율 제조의 새로운 시대를 열 수 있는 두 가지 핵심 기술, 즉 모델 컨텍스트 프로토콜(Model Context Protocol, MCP)과 자산 관리 쉘(Asset Administration Shell, AAS, IEC 63278)의 통합에 대해 심층적으로 분석합니다. 이 보고서의 핵심 명제는 다음과 같습니다: **AAS가 산업 자산이 '무엇'인지에 대한 표준화된 데이터 모델을 제공한다면, MCP는 AI 에이전트가 그 모델을 이해하고 '어떻게' 행동할지에 대한 표준화된 상호작용 프로토콜을 제공합니다.** 이 두 기술의 융합은 단순한 기술적 연결을 넘어, 제조 현장의 자동화를 지능형 자율성으로 격상시키는 강력한 시너지를 창출합니다.

본 보고서는 먼저 MCP와 AAS의 핵심 개념과 아키텍처를 각각 상세히 분석하여 두 기술에 대한 깊이 있는 이해를 제공합니다. MCP는 AI 애플리케이션과 외부 도구 및 데이터 소스 간의 'N×M' 통합 문제를 해결하는 범용 어댑터로서의 역할을 하며 [3], AAS는 자산의 전체 생애주기에 걸쳐 모든 정보를 담는 표준화된 디지털 트윈으로서 기능합니다.[4]

이어서, 보고서는 MCP와 AAS를 통합하기 위한 구체적인 아키텍처 패턴을 제시하고, 사용자의 질의에 기반한 핵심 사용 사례—ERP 시스템과의 연동을 통해 신규 설비의 AAS를 자동으로 생성하는 AI 에이전트—를 심층 분석합니다. 이를 통해 두 기술의 통합이 어떻게 디지털 스레드(Digital Thread)의 완전한 자동화를 가능하게 하는지 구체적으로 보여줍니다.

또한, 본 보고서는 OPC UA와 같은 기존 산업 표준과의 관계를 명확히 하고, MCP와 AAS의 통합이 OPC UA를 대체하는 것이 아니라 상호 보완적인 시너지를 창출하는 방식을 설명합니다.[5] 레거시 시스템 통합, 데이터 품질, 조직적 준비 상태와 같은 현실적인 구현 과제와 더불어, 이

새로운 융합 아키텍처에서 발생하는 중대한 보안 문제들을 심도 있게 다룹니다.

마지막으로, 본 보고서는 기술 리더와 전략가들을 위해 단계별 도입 로드맵과 구체적인 실행 권고안을 제시하며 마무리됩니다. MCP와 AAS의 통합은 단순한 기술적 진보가 아니라, 기업이 미래의 자율 제조 환경에서 경쟁 우위를 확보하기 위한 전략적 필수로 자리매김할 것입니다.

Part I: 자율 제조의 근본적인 두 기둥

자율 제조라는 복잡한 목표를 달성하기 위해서는 견고한 기술적 기반이 필수적입니다. 이 장에서는 자율성의 새로운 패러다임을 구성하는 두 가지 핵심 기술인 모델 컨텍스트 프로토콜(MCP)과 자산 관리 쉘(AAS)에 대해 각각 심층적으로 분석합니다. 이 두 기술은 서로 다른 문제를 해결하기 위해 탄생했지만, 그들의 융합은 산업 자동화의 미래를 재정의할 잠재력을 지니고 있습니다.

Chapter 1: 모델 컨텍스트 프로토콜(MCP) - AI 에이전트를 위한 범용 버스

AI, 특히 대규모 언어 모델(LLM)의 능력은 모델 자체에 내장된 지식만으로는 제한적입니다. 실시간 정보에 접근하거나 외부 시스템에서 작업을 수행하는 능력 없이는 단순한 텍스트 예측기를 넘어서기 어렵습니다.[6] MCP는 이러한 한계를 극복하고 AI가 진정으로 유용한 '행동'을 할 수 있도록 설계된 개방형 표준 프로토콜입니다.

1.1. 핵심 개념: N×M 통합 문제의 해결

전통적인 AI 통합 방식은 심각한 확장성 문제를 안고 있었습니다. 개발자들은 모든 AI 애플리케이션(N)을 위해 모든 외부 도구 또는 데이터 소스(M)에 대한 맞춤형 커넥터를 각각 구축해야 했습니다. 이는 'N×M' 문제로 알려져 있으며, 새로운 시스템이 추가될 때마다 개발 비용과 복잡성이 기하급수적으로 증가하는 비효율적이고 취약한 접근 방식이었습니다.[3]

MCP는 이 문제를 근본적으로 해결하기 위해 '범용 어댑터'라는 개념을 도입합니다. 이는 마치 다양한 주변기기를 단일 표준 포트로 연결하는 USB-C와 유사합니다.[6] MCP는 AI 애플리케이션과 외부 서비스 사이에 표준화된 계층을 제공하여, MCP와 호환되는 모든

클라이언트(AI 애플리케이션)가 MCP와 호환되는 모든 서버(데이터 및 도구 제공자)에 연결될 수 있도록 합니다. 이로써 통합 패러다임은 비확장적인 'N×M'에서 선형적으로 확장 가능한 'N+M' 모델로 전환됩니다. 개발자들은 더 이상 반복적인 커넥터 개발에 시간을 낭비하는 대신, 훌륭한 AI 경험을 구축하는 데 집중할 수 있게 됩니다.[8]

1.2. 아키텍처 심층 분석: 클라이언트, 서버, 그리고 JSON-RPC 전송

MCP의 아키텍처는 명확한 역할 분담을 기반으로 설계되었습니다.

- **호스트(Hosts), 클라이언트(Clients), 서버(Servers):** MCP 생태계는 세 가지 주요 구성요소로 이루어집니다. **호스트**는 AI 기반 IDE나 Microsoft Copilot Studio와 같이 연결을 시작하는 AI 애플리케이션입니다. **클라이언트**는 호스트 애플리케이션 내에서 MCP 서버와 전용 일대일 연결을 유지하는 커넥터입니다. 마지막으로, **서버**는 MCP를 통해 특정 기능이나 데이터를 노출하는 경량 서버로, 로컬 또는 원격 데이터 소스에 연결됩니다.[9]
- **전송 계층(Transport Layer):** MCP는 기술적 기반으로 널리 검증된 표준을 의도적으로 재사용합니다. 메시지 흐름은 언어 서버 프로토콜(Language Server Protocol, LSP)에서 영감을 받았으며, 전송은 JSON-RPC 2.0을 통해 이루어집니다.[3] JSON-RPC 2.0은 경량의 상태 저장(stateful) 통신 표준으로, WebSockets과 유사하게 지속적이고 실시간 양방향 통신을 가능하게 합니다.[9] 이러한 선택은 개발자 생태계에 이미 친숙한 기술을 활용하여 프로토콜의 채택을 가속화하는 전략적 이점을 가집니다.

1.3. 기능적 기본 요소: 리소스, 도구, 프롬프트 노출

MCP 서버는 AI 에이전트가 사용할 수 있는 세 가지 핵심 기능을 노출하며, 이는 모든 에이전트 상호작용의 기본 구성 요소가 됩니다.

- **리소스(Resources):** 파일 읽기나 데이터베이스 조회와 같은 정보 검색을 위한 기능입니다. 리소스는 데이터를 반환하지만 시스템 상태를 변경하는 등의 부작용(side effect)을 일으키지 않습니다. 예를 들어, AI 에이전트는 리소스를 통해 회의록을 읽거나, 코드베이스에 대한 데이터를 조회할 수 있습니다.[6]
- **도구(Tools):** 계산 수행, 이메일 전송, 외부 API 호출과 같이 부작용을 동반하는 작업을 수행하기 위한 기능입니다. LLM은 사용자의 요청 컨텍스트를 기반으로 어떤 도구를 호출할지 스스로 결정합니다. 예를 들어, "지난주 팀 회의록을 요약하고 후속 조치가 필요한 사람들에게 미팅을 잡아줘"라는 요청에 대해, AI는 문서 검색 도구와 캘린더 도구를 순차적으로 호출하여 작업을 완료합니다.[6]

- **프롬프트(Prompts):** LLM과 서버 간의 통신을 안내하는 재사용 가능한 템플릿 및 워크플로우입니다. 이는 복잡한 작업을 위한 표준화된 상호작용 패턴을 정의하여 일관성과 효율성을 높입니다.[6]

1.4. 생태계와 채택: 성장하는 표준

2024년 11월 Anthropic에 의해 처음 소개된 MCP는 빠르게 업계 표준으로 부상하고 있습니다. OpenAI, Google DeepMind, Microsoft, IBM과 같은 주요 AI 기업들이 이 프로토콜을 채택했으며 [3], 이는 MCP가 AI 통합의 미래에 핵심적인 역할을 할 것임을 시사합니다.

이러한 빠른 성장의 동력은 프로토콜의 개방성에 있습니다. MCP는 오픈 소스 프로젝트로 운영되며, TypeScript, Python, Java, C#, Go 등 다양한 언어로 공식 SDK를 제공합니다.[3] GitHub에는 커뮤니티가 구축한 수백 개의 MCP 서버 저장소가 있으며, 이는 개발자들이 기존 작업을 활용하여 강력한 AI 애플리케이션을 더 쉽게 구축할 수 있는 풍부한 생태계를 형성하고 있습니다.[10]

Chapter 2: 자산 관리 쉘(AAS) - 표준화된 디지털 트윈

인더스트리 4.0의 비전을 실현하기 위한 가장 큰 과제 중 하나는 상호운용성(interoperability)입니다. 서로 다른 제조사의 장비, 다양한 IT 시스템, 그리고 공급망 파트너들이 원활하게 데이터를 교환하고 상호 활용할 수 있어야 진정한 스마트 제조가 가능합니다.[15] 자산 관리 쉘(AAS)은 바로 이 문제를 해결하기 위해 탄생한 국제 표준(IEC 63278)입니다.

2.1. IEC 63278의 비전: 인더스트리 4.0을 위한 진정한 상호운용성

AAS는 인더스트리 4.0을 위한 '디지털 트윈'의 공식적인 구현체로 정의됩니다.[4] 표준의 목적은 "두 개 이상의 소프트웨어 애플리케이션이 신뢰할 수 있고 안전한 방식으로 정보를 교환하고, 교환된 정보를 상호 활용할 수 있도록 하는 것"입니다.[20] AAS는 물리적 자산과 디지털 세계 사이의 표준화된 인터페이스 역할을 하여, 기존의 데이터 사일로를 허물고 기업 경계를 넘어선 원활한 데이터 교환을 가능하게 합니다.[4]

AAS는 개별 제조, 연속 공정, 배치 공정 등 모든 유형의 산업 공정에 적용될 수 있으며, 자산의 아이디어 구상부터 폐기에 이르는 전체 생애주기를 포괄합니다. 여기서 '자산'은 기계나 도구 같은 물리적 실체뿐만 아니라, 소프트웨어나 문서 같은 디지털 또는 무형의 실체까지 포함하는 광범위한 개념입니다.[21]

2.2. AAS 메타모델: 자산, 서브모델, 속성의 해부

AAS의 구조는 명확하고 체계적인 메타모델을 기반으로 합니다.

- **자산(Asset)과 AAS:** 하나의 AAS는 정확히 하나의 자산을 표현합니다. 이 자산은 AssetInformation 속성의 assetKind를 통해 유형(Type)인지 인스턴스(Instance)인지 구분됩니다.[26]
- **서브모델(Submodels):** AAS의 핵심은 '서브모델'의 집합입니다. 서브모델은 자산 정보의 특정 측면(예: 기술 데이터, 유지보수 이력, 에너지 소비)을 담는 표준화된 컨테이너입니다.[18] 이 모듈식 구조 덕분에 필요한 정보만 선택적으로 사용하거나 확장할 수 있어 유연성이 매우 높습니다.
- **서브모델 요소(SubmodelElements):** 서브모델은 속성(Property), 파일(File), 블롭(Blob), 관계 요소(RelationshipElement) 등 다양한 유형의 '서브모델 요소'들로 구성됩니다. 이 요소들은 실제 데이터를 담고 있으며, ECLASS나 IEC CDD(Common Data Dictionary)와 같은 표준화된 사전을 참조하는 '시맨틱 ID(Semantic ID)'를 통해 그 의미가 명확하게 정의됩니다.[28] 이는 기계가 데이터의 의미를 이해하고 해석할 수 있게 하는 시맨틱 상호운용성의 핵심입니다.

2.3. 서브모델의 힘: 디지털 명판에서 탄소 발자국까지

서브모델 개념의 진정한 힘은 표준화된 템플릿을 통해 발휘됩니다. 산업 디지털 트윈 협회(IDTA)와 같은 기관들은 다양한 사용 사례를 위한 서브모델 템플릿을 개발하고 공개하고 있습니다. 구체적인 예는 다음과 같습니다.

- **디지털 명판(Digital Nameplate):** 제조사, 모델 번호, 시리얼 번호와 같은 자산의 기본 식별 정보를 제공합니다. 이는 물리적 명판을 디지털화하여 QR 코드 등을 통해 쉽게 접근할 수 있게 합니다.[4]
- **기술 데이터(Technical Data):** 자산의 주요 운영 파라미터, 기술 사양, 성능 데이터 등을 표준화된 구조로 저장합니다.[29]
- **인수인계 문서(Handover Documentation):** VDI 2770과 같은 표준에 따라 사용

설명서, CE 인증서, 회로도 등의 문서를 자산과 연결합니다.[32]
- **환경 데이터(Environmental Data):** 제품의 생산, 사용, 폐기 과정에서 발생하는 탄소 발자국(Carbon Footprint) 정보를 기록합니다. 이는 유럽 연합의 디지털 제품 여권(Digital Product Passport, DPP)과 같은 규제 준수 및 지속 가능성 목표 달성에 필수적입니다.[18]

2.4. 통신 프로토콜 및 데이터 교환: HTTP/REST와 AASX

AAS와 상호작용하는 방법은 크게 두 가지로 나뉩니다. AAS 자체는 프로토콜에 구애받지 않지만, 온라인 접근을 위해서는 일반적으로 HTTP/REST 기반의 API를 제공합니다.[25] 이를 통해 다른 시스템들이 실시간으로 AAS 데이터를 조회하거나 수정할 수 있습니다.

오프라인 데이터 교환이나 자산의 전체 정보를 하나의 파일로 전달해야 할 경우, AASX 패키지 형식이 사용됩니다. AASX 파일은 본질적으로 ZIP 아카이브로, 그 안에는 AAS 구조를 기술하는 XML 또는 JSON 파일과 함께 PDF 문서, CAD 모델, 이미지 등 보충 자료들이 포함될 수 있습니다.[34] 이는 자산의 디지털 표현을 완전하고 이식성 있게 만들어 공급망 파트너 간의 정보 교환을 용이하게 합니다.

Part II: 융합 - 아키텍처 청사진과 고부가가치 사용 사례

MCP와 AAS라는 두 강력한 표준의 이론적 기반을 살펴보았으므로, 이제 이들을 어떻게 실질적으로 결합하여 자율 제조의 비전을 실현할 수 있는지 분석할 차례입니다. 이 장에서는 구체적인 통합 아키텍처 패턴을 제시하고, 사용자가 질의한 핵심적인 사용 사례를 심층적으로 분석하여 두 기술의 융합이 가져올 실질적인 가치를 탐구합니다.

Chapter 3: MCP-AAS 통합을 위한 아키텍처 청사진

MCP와 AAS의 통합은 단일한 접근법으로 이루어지지 않습니다. 조직의 목표, 기술 성숙도, 그리고 허용 가능한 리스크 수준에 따라 다양한 아키텍처 패턴을 적용할 수 있습니다. 이러한 패턴들은 서로 배타적이지 않으며, 오히려 자율 제조를 향한 진화적 경로를 제시합니다.

3.1. 패턴 1: MCP 리소스로서의 AAS (읽기 전용 컨텍스트)

- **설명:** 이는 가장 간단하고 직관적인 통합 패턴입니다. MCP 서버가 전체 AAS 또는 특정 서브모델을 읽기 전용 Resource로 노출합니다.[6] AI 에이전트는 이 리소스를 통해 디지털 트윈을 '읽어' 사용자의 질문에 대한 컨텍스트를 얻습니다. 예를 들어, "5번 스테이션 로봇의 유지보수 사양은 무엇인가?"라는 질문에 대해, AI 에이전트는 해당 로봇의 AAS를 리소스로서 조회하여 답변을 생성할 수 있습니다. MCP 서버는 내부적으로 AASX 파일을 파싱하거나 [35] AAS 레지스트리 및 리포지토리의 REST API를 호출하여 정보를 가져옵니다.[25]
- **사용 사례:** 컨텍스트 인식 챗봇, 장비 진단 보조 시스템, 현장 작업자를 위한 정보 검색 시스템.
- **장단점:** 구현이 간단하고 리스크가 낮아 초기 도입에 적합합니다. 그러나 읽기 전용 작업에 국한되므로, 시스템 상태를 변경하는 진정한 의미의 '에이전트적' 행동은 불가능합니다.

3.2. 패턴 2: MCP 도구로서의 AAS 서브모델 (에이전트적 상호작용)

- **설명:** 이 패턴은 AI 에이전트에게 더 강력한 능력을 부여합니다. MCP 서버가 AAS 서브모델의 특정 기능들을 실행 가능한 Tool로 노출합니다.[6] 예를 들어, 유지보수 관련 서브모델에 새로운 로그를 기록하는 update_maintenance_log 도구나, 자재 조달 관련 서브모델과 상호작용하여 예비 부품을 요청하는 request_spare_part 도구를 제공할 수 있습니다. 이제 AI 에이전트는 디지털 트윈의 상태에 영향을 미치는, 즉 부작용이 있는 작업을 수행할 수 있게 됩니다.
- **사용 사례:** 반자율적 유지보수 일정 계획, 자동화된 품질 보고서 작성, 자산 구성 변경.
- **장단점:** 진정한 에이전트 행동과 워크플로우 자동화를 가능하게 합니다. 반면, 에이전트가 자산의 상태를 직접 수정할 수 있으므로 구현 복잡성과 보안 리스크가 패턴 1에 비해 훨씬 높습니다.

3.3. 패턴 3: AAS 인식 MCP 파사드 (통합 자산 인터페이스)

- **설명:** 이는 가장 진보된 통합 패턴으로, 정교한 단일 MCP 서버가 전체 자산 생태계에 대한 '파사드(façade)' 또는 게이트웨이 역할을 합니다. 이 MCP 서버는 내부적으로 AAS 레지스트리(AAS 발견), AAS 리포지토리(구조 파악), 그리고 OPC UA 서버와 같은 실시간

데이터 소스(5장 참조)와의 연결을 모두 관리합니다.[23] AI 에이전트의 관점에서는, 분산된 AAS 아키텍처의 복잡성이 완전히 추상화되고, 자산이 풍부한 도구와 리소스를 갖춘 단일하고 일관된 개체로 보이게 됩니다.

- **사용 사례:** 완전 자율 오케스트레이션. 에이전트가 자산을 스스로 발견하고, 그 능력을 파악한 뒤, 복잡한 다단계 작업을 수행하기 위해 상호작용하는 시나리오.
- **장단점:** AI 에이전트에게 최고의 추상화 수준과 강력한 능력을 제공합니다. 그러나 MCP 서버 내부에 견고한 비즈니스 로직을 구현해야 하므로 구현 복잡성이 가장 높습니다.

이 세 가지 아키텍처 패턴은 조직이 자율 제조를 향해 나아가는 성숙도 모델을 형성합니다. 대부분의 조직은 신뢰를 구축하고 초기 가치를 입증하기 위해 가장 리스크가 낮은 읽기 전용 애플리케이션(패턴 1)으로 시작할 것입니다.[1] 이후 성공적인 파일럿을 통해 자신감을 얻으면, 잘 정의된 특정 작업을 자동화하는 도구(패턴 2)를 점진적으로 도입하여 반자율적 워크플로우를 구현할 것입니다. 궁극적으로 동적이고 복잡한 상황에 대응해야 하는 완전 자율 제조의 목표는, 에이전트가 자산을 전체적으로 파악하고 상호작용할 수 있는 파사드 패턴(패턴 3)의 강력한 추상화를 통해서만 달성될 수 있습니다. 따라서 기술 리더들은 이러한 진화적 경로를 이해하고, 간단한 '리소스' 기반 통합에서 시작하여 점차 복잡한 '도구' 및 '파사드' 아키텍처로 발전하는 장기적인 전략을 수립해야 합니다.

Chapter 4: 사용 사례 분석: 디지털 스레드의 자동화

이론적인 아키텍처 패턴을 넘어, MCP와 AAS의 융합이 실제로 어떻게 가치를 창출하는지 보여주기 위해 사용자가 제시한 구체적인 질문을 중심으로 심층 분석을 수행합니다. 이 사용 사례는 두 기술의 시너지가 어떻게 제조 현장의 핵심 프로세스를 근본적으로 변화시킬 수 있는지를 명확히 보여줍니다.

4.1. 심층 분석: ERP 시스템으로부터의 자동 AAS 생성

이 시나리오는 새로운 제조 설비가 도입될 때, 수동 개입 없이 해당 설비의 디지털 트윈(AAS)을 자동으로 생성하는 과정을 다룹니다.

- **트리거(The Trigger):** 새로운 제조 설비가 조달됩니다. 구매 담당자 또는 자동화된 프로세스가 회사의 ERP 시스템(예: Infor XA, Sage X3, Microsoft Dynamics 365)에 해당 설비에 대한 자산 마스터 레코드를 생성합니다.[37] 이 작업은 웹훅(webhook)이나 비즈니스 이벤트를 통해 후속 프로세스를 촉발합니다.
- **에이전트의 임무(The Agent's Task):** 이벤트를 수신한 AI 에이전트(예: Microsoft

Copilot 또는 LangChain 기반의 맞춤형 에이전트)가 활성화됩니다. 이 에이전트는 MCP 클라이언트로서 작동하며, 새로 도입된 설비를 위한 완전하고 표준화된 AAS를 생성하는 임무를 부여받습니다.

- **상호작용 흐름(The Interaction Flow):** 이 과정은 다음과 같은 단계로 이루어집니다.
  1. 에이전트는 먼저 전용 **ERP MCP 서버**에 연결합니다. 이 서버는 MCP SDK를 사용하여 구축되며 [40], ERP의 복잡한 API를 안전하게 래핑(wrapping)하여 get_asset_master_data, get_purchase_order_details, get_technical_specifications_from_attachment와 같은 기능들을 표준화된 MCP Tool 및 Resource로 노출합니다.[41] 이를 통해 취약하고 비용이 많이 드는 직접적인 API 통합을 피할 수 있습니다.
  2. 에이전트는 이 도구들을 호출하여 제조사, 모델 번호, 시리얼 번호, 기술 데이터 시트(PDF), 구매일 등 AAS 생성에 필요한 모든 정보를 수집합니다.
  3. 다음으로, 에이전트는 두 번째 **AAS 리포지토리 MCP 서버**에 연결합니다. 이 서버는 AAS 리포지토리의 기능들, 예를 들어 create_aas_instance, create_submodel_from_template, upload_file_to_submodel, register_aas_in_registry와 같은 작업들을 MCP 도구로 제공합니다.
  4. 에이전트는 이 두 번째 도구 세트를 사용하여 프로그래밍 방식으로 AAS를 구성합니다. ERP에서 가져온 데이터를 사용하여 "디지털 명판" 서브모델을 인스턴스화하고 [29], 기술 데이터 시트 PDF를 업로드하여 "인수인계 문서" 서브모델을 생성하며 [32], 사양서나 ERP의 구조화된 데이터를 파싱하여 "기술 데이터" 서브모델을 채웁니다.[31]
- **결과(The Result):** 이 모든 과정이 끝나면, 새로운 설비에 대한 완전한 IEC 63278 준수 AAS가 자동으로 생성되고 AAS 레지스트리에 등록됩니다.[44] 이로써 해당 자산은 MES, SCADA 등 다른 모든 인더스트리 4.0 애플리케이션에서 즉시 발견하고 활용할 수 있는 상태가 됩니다. 자산이 수동 개입 없이 '디지털로 태어나는(born-digital)' 순간입니다. 이 개념은 LLM 에이전트를 사용한 AAS 생성에 관한 학술 연구를 통해서도 그 타당성이 입증되었습니다.[45]

이 사용 사례는 중요한 함의를 가집니다. MCP가 AI가 도구를 *발견하고 사용하는* 방법을 표준화하고 [6], AAS가 산업 자산의

데이터와 기능을 표준화함으로써 [4], 우리는 새로운 패러다임에 도달하게 됩니다. 만약 ERP, MES, 그리고 개별 자산들이 각각의 기능을 MCP 서버를 통해 표준화된 '도구'로 노출한다면, AI 에이전트는 마치 앱 스토어처럼 MCP 서버 레지스트리를 탐색할 수 있습니다.[14] 에이전트는 복잡한 목표를 달성하기 위해 완전히 다른 도메인(ERP, MES, 자산)의 도구들을 동적으로 발견하고 연결(chaining)할 수 있게 됩니다. 예를 들어, 에이전트는 "기계의 진단 도구"가 결함을 보고했기 때문에 "ERP에서 새 부품을 주문"하는 결정을 자율적으로 내릴 수 있습니다. 이는 현재의 기술로는 구현하기 극도로 어려운 수준의 동적 오케스트레이션입니다. 결국, MCP는 '의도 기반(Intent-Based)' 제조 환경을 위한 범용 API가 되어, 산업 자동화를 사전에 프로그래밍된 경직된 워크플로우에서 동적이고 구성 가능한 생태계로 변화시킬 것입니다.

Part III: 현실 세계의 구현 환경 탐색

새로운 아키텍처의 청사진을 그리는 것과 이를 현실 세계에 성공적으로 배포하는 것은 별개의 문제입니다. 이 장에서는 새로운 융합 아키텍처를 도입할 때 직면하게 될 실질적인 문제들, 즉 기존 기술 환경과의 관계, 일반적인 장애물, 그리고 무엇보다 중요한 보안 고려사항을 심도 있게 다룹니다.

Chapter 5: 간과할 수 없는 존재: AAS 생태계 내 MCP와 OPC UA

자율 제조를 논할 때, 운영 기술(OT) 영역에서 이미 확고한 입지를 다진 표준인 OPC UA(Open Platform Communications Unified Architecture, IEC 62541)를 빼놓을 수 없습니다. MCP와 AAS의 통합을 고려하는 모든 기술 전략가는 OPC UA와의 관계를 명확히 이해해야 합니다.

5.1. OPC UA의 확고한 역할: 실시간 OT 데이터와 시맨틱 모델링

OPC UA는 인더스트리 4.0의 초석으로, 공장 현장의 기계, PLC, 센서 등 OT 계층에서 발생하는 데이터를 IT 계층으로 안전하고, 실시간으로, 그리고 의미론적으로 풍부하게 전송하는 데 필수적인 역할을 합니다.[46] OPC UA는 단순한 통신 프로토콜을 넘어, 정보 모델링 프레임워크를 제공하여 데이터에 컨텍스트를 부여합니다. 특히, I4AAS 동반 사양(Companion Specification)은 AAS 메타모델을 OPC UA 정보 모델로 매핑하는 방법을 명시적으로 정의하여, 두 표준 간의 긴밀한 통합을 공식화하고 있습니다.[49]

5.2. 상호 보완적 시너지: 데이터 파이프라인을 위한 OPC UA, AI 애플리케이션 계층을 위한 MCP

이 장의 핵심 주장은 **MCP가 OPC UA를 대체하지 않는다**는 것입니다. 두 기술은 현대 산업 데이터 아키텍처 내에서 서로 다른, 그러나 상호 보완적인 계층에서 작동합니다.[5]

- **OPC UA: '데이터 파이프(Data Pipe)'.** OPC UA는 물리적 장치로부터 고빈도의 저지연 데이터 수집에 최적화되어 있으며, 이 데이터를 구조화된 서버 기반 모델로 제공합니다. 이는 "펌프 A의 현재 압력은 얼마인가?"와 같은 실시간 상태 조회 질문에 답하는 데 특화되어 있습니다.
- **MCP: 'AI 컨텍스트 프로토콜(AI Context Protocol)'.** MCP는 AI 에이전트에게 복잡하고 종종 비동기적인 추론 기반 작업을 수행하는 데 필요한 컨텍스트와 도구를 제공하는 데 최적화되어 있습니다. 이는 "모든 펌프의 최근 압력 추세를 기반으로 유지보수를 계획해야 하는가?"와 같은 고차원적인 질문에 답하는 데 사용됩니다.

따라서 OPC UA가 OT 계층에서 신뢰할 수 있는 데이터 파이프라인을 확보하는 역할을 한다면, MCP는 이 데이터를 활용하여 AI 에이전트가 지능적인 의사결정과 행동을 할 수 있도록 하는 애플리케이션 계층의 인터페이스 역할을 합니다.

5.3. 통합 시나리오: MCP 서버가 OPC UA 데이터를 소비하는 방법

실질적인 통합 아키텍처는 다음과 같이 구성될 수 있습니다. 기계에 내장된 OPC UA 서버가 실시간 데이터를 노출합니다. 해당 기계의 AAS는 이 OPC UA 서버를 실시간 데이터의 소스로 참조합니다. 그리고 3장에서 설명한 'AAS 인식 MCP 파사드'(패턴 3)가 OPC UA 서버의 클라이언트 역할을 하여 데이터를 검색한 후, 이를 MCP Resource 또는 Tool 형태로 AI 에이전트에게 노출합니다.[5] 이 구조에서 AI 에이전트는 OPC UA 프로토콜을 직접 알 필요 없이, 오직 MCP를 통해서만 자산과 상호작용하면 됩니다. 이는 복잡성을 크게 줄이고 AI 개발을 가속화합니다.

Table 5.1: 기능 비교: AAS 통신을 위한 MCP 대 OPC UA

기술 전략가들이 각 표준을 언제, 어떻게 활용해야 할지에 대한 명확한 가이드를 제공하기 위해 다음 표를 제시합니다. 이 비교는 두 표준이 경쟁 관계가 아니라 협력 관계에 있음을 명확히 하여 전략적 오류를 방지하는 데 도움을 줄 것입니다.

기능	OPC UA	MCP	시너지 효과
주요 도메인	운영 기술(OT) - 실시간 기계 데이터	정보 기술(IT) / AI - 애플리케이션 컨텍스트	OT 데이터를 IT/AI 애플리케이션에서 원활하게 활용

통신 패러다임	실시간, 상태 기반, Pub/Sub 및 Client/Server	비동기, 요청/응답 기반, JSON-RPC	실시간 데이터(OPC UA)를 기반으로 한 고차원적, 비동기적 작업(MCP) 수행
데이터 초점	시계열 데이터, 상태 값, 알람 및 이벤트	작업 컨텍스트, 실행 가능한 도구, 구조화된 리소스	상태 데이터를 컨텍스트화하여 AI가 실행 가능한 통찰력으로 변환
주요 사용 사례	데이터 수집, 모니터링, 제어	AI 에이전트 오케스트레이션, 복잡한 워크플로우 자동화	OPC UA로 수집된 데이터를 MCP를 통해 AI 에이전트가 분석하고 조치
보안 모델	X.509 인증서 기반, 전송 계층 보안(TLS)	OAuth 2.0, API 키 등 토큰 기반 인증 및 권한 부여	계층화된 보안: OPC UA로 OT 네트워크를 보호하고, MCP로 애플리케이션 접근 제어

Chapter 6: MCP-AAS 도입을 위한 구현 장애물 극복

MCP와 AAS의 통합은 막대한 잠재력을 지니고 있지만, 그 구현 과정은 여러 현실적인 장애물에 직면하게 됩니다. 성공적인 도입을 위해서는 이러한 과제들을 사전에 인지하고 체계적으로 대응해야 합니다.

6.1. 브라운필드 과제: 레거시 시스템과 데이터 사일로

대부분의 공장은 처음부터 새로 짓는 그린필드 환경이 아닙니다. 수십 년에 걸쳐 구축된 다양한 레거시 시스템, 독점 프로토콜, 그리고 부서별로 고립된 데이터 사일로가 뒤섞인 브라운필드 환경이 일반적입니다.[1] MCP는 기존 시스템을 전면 교체하지 않고도 AI를 접목할 수 있도록 래핑(wrapping)하는 방식으로 이 문제를 해결하도록 설계되었습니다.[43] 마찬가지로, Eclipse BaSyx의 DataIntegrator와 같은 AAS 통합 도구는 ERP나 PLM과 같은 기존의 기록 시스템(Systems of Record, SOR)에서 데이터를 추출하여 AAS로 변환하는 기능을 제공합니다.[23] 그러나 이러한 초기 래퍼와 데이터 통합 파이프라인을 구축하는 데는 상당한

엔지니어링 노력이 필요하다는 점이 현실적인 과제입니다.[53]

6.2. 데이터 품질과 시맨틱 매핑

"쓰레기가 들어가면 쓰레기가 나온다(Garbage In, Garbage Out)"는 원칙은 AI 시스템에서 더욱 증폭됩니다. AI 에이전트의 의사결정 품질은 전적으로 입력받는 데이터의 품질에 달려있습니다.[53] 문제는 ERP, MES 등 다양한 소스에서 오는 데이터가 부정확하거나, 누락되었거나, 일관성이 없을 수 있다는 점입니다. 또한, 이 데이터를 AAS 서브모델 내의 표준화된 시맨틱 ID에 정확하게 매핑하는 작업도 중요합니다. 이를 위해서는 기술적 해결책뿐만 아니라, 전사적인 데이터 거버넌스 전략과 데이터 품질 관리 프로세스를 수립하는 것이 필수적입니다.

6.3. 조직적 준비 상태: 기술 격차, 변화 관리, 그리고 신뢰

기술 도입의 가장 큰 장벽은 종종 기술 자체가 아니라 사람과 조직에 있습니다.

- **기술 격차(Skill Gaps):** OT(AAS, OPC UA), IT(ERP, API), 그리고 AI(MCP, LLM) 분야의 전문 지식을 모두 갖춘 융합형 인재는 매우 드뭅니다.[2] 성공적인 프로젝트를 위해서는 이러한 기술 격차를 해소하기 위한 교육 및 인재 양성 계획이 필요합니다.
- **변화 관리와 신뢰(Change Management & Trust):** 현장 팀들은 자율 시스템의 신뢰성과 안전성에 대한 명확한 증거 없이는 자신들의 업무와 제어권을 넘겨주는 것을 주저할 수 있습니다.[1] 따라서 투명성을 확보하고, 작은 성공 사례부터 시작하여 점진적으로 신뢰를 구축하며, 자동화가 인간의 역할을 대체하는 것이 아니라 강화하는 방향으로 진행된다는 점을 명확히 소통하는 변화 관리 노력이 중요합니다.
- **리더십과 문화(Leadership & Culture):** 성공적인 AI 도입은 기술적 과제가 아니라 비즈니스 과제입니다.[55] 강력한 리더십을 바탕으로 변화를 주도하고, AI 도입이 기존 직무에 미치는 영향을 관리하며, 실험과 협업을 장려하는 문화를 조성해야 합니다.[56]

Chapter 7: 융합된 세계를 위한 통합 보안 태세

MCP와 AAS의 통합은 전례 없는 수준의 자동화와 지능화를 가능하게 하지만, 동시에 새로운 공격 표면과 복합적인 보안 리스크를 야기합니다. 특히 AI 에이전트에게 실제 시스템을 조작할

수 있는 권한을 부여하는 것은 매우 신중한 보안 설계가 요구되는 영역입니다.

7.1. MCP의 위협 표면 분석

MCP는 AI 에이전트와 백엔드 시스템을 연결하는 다리 역할을 하므로, 이 다리의 보안이 전체 시스템의 안전을 좌우합니다. 주요 위협은 다음과 같습니다.

- **공급망 리스크(Supply Chain Risks):** 신뢰할 수 없거나 악의적으로 변조된 오픈 소스 MCP 서버 또는 그 종속성을 사용하는 경우, 전체 시스템이 위험에 노출될 수 있습니다. 개발자는 사용하는 모든 구성 요소의 무결성을 검증하고 서명을 확인해야 합니다.[57]
- **인증 및 권한 부여(Authentication & Authorization):** '혼란된 대리인(Confused Deputy)' 문제는 MCP 보안의 핵심 과제입니다. 이는 권한이 낮은 사용자를 대신하여 서버가 자신의 높은 권한으로 작업을 수행하는 문제입니다. 이를 방지하기 위해 OAuth 2.0과 같은 표준 프로토콜을 올바르게 구현하고, 토큰의 유효성과 범위를 철저히 검증하는 것이 중요합니다.[57]
- **프롬프트 인젝션(Prompt Injection):** 공격자가 악의적으로 조작된 입력을 통해 LLM을 속여, 노출된 도구를 사용하여 의도하지 않은 위험한 작업을 수행하도록 유도하는 공격입니다. 예를 들어, 데이터베이스를 삭제하거나 민감한 정보를 유출하는 명령을 실행하게 할 수 있습니다.[58]
- **자격 증명/토큰 탈취(Credential/Token Theft):** MCP 서버가 손상되면, 해당 서버가 연결된 모든 백엔드 시스템(ERP, 데이터베이스 등)의 API 키와 인증 토큰이 유출될 수 있습니다. 이는 단일 장애점(single point of failure)이 되어 막대한 피해로 이어질 수 있습니다.[58]

7.2. AAS 보안

AAS 표준 자체도 보안을 중요한 요소로 고려합니다. AAS는 속성 기반 접근 제어(Attribute-Based Access Control, ABAC)와 같은 메커니즘을 통해 특정 사용자나 시스템만이 특정 서브모델을 보거나 수정할 수 있도록 접근을 제어할 수 있습니다.[19] 또한, HTTPS와 같은 보안 프로토콜을 통해 전송 중인 데이터를 보호하고, AASX 파일의 무결성을 보장하는 것이 중요합니다.

7.3. 결합된 과제: 자율 에이전트-자산 상호작용의 보안

MCP와 AAS의 보안 모델은 단순히 병렬적으로 구현되는 것을 넘어, 긴밀하게 통합되어야 합니다. 이 통합 지점에서 새로운 차원의 리스크가 발생하기 때문입니다. AI 에이전트가 MCP 서버에 인증하고, MCP 서버가 다시 AAS 리포지토리에 인증하는 과정에서 권한 매핑이 정확하게 이루어지지 않으면 치명적인 보안 허점이 발생할 수 있습니다.

예를 들어, 낮은 권한을 가진 AI 에이전트가 "사소한 관찰 결과 기록"을 요청했다고 가정해 보겠습니다. 만약 취약하게 구현된 MCP 서버가 이 요청을 처리하면서 AI 에이전트의 권한을 제대로 확인하지 않고 자신의 높은 권한을 사용한다면, 에이전트가 절대 접근해서는 안 되는 "안전 제어 파라미터" 서브모델에 데이터를 쓸 수도 있습니다. 이는 '혼란된 대리인' 문제가 산업 환경에서 얼마나 높은 파급력을 가질 수 있는지를 보여주는 극명한 예입니다.

따라서, MCP 서버의 구현은 전체 아키텍처에서 가장 중요한 보안 통제 지점입니다. MCP 서버는 AI 에이전트의 신원과 의도를 AAS의 접근 제어 규칙에 맞춰 제한되고 인가된 작업으로 변환하는 엄격한 '보안 게이트키퍼' 역할을 수행해야 합니다. 이를 위해서는 모든 구성 요소에 최소 권한 원칙(Principle of Least Privilege, PoLP)을 철저히 적용하는 것이 무엇보다 중요합니다.[62]

7.4. Table 7.1: 통합 보안 리스크 매트릭스 및 완화 전략

보안 아키텍트가 통합 MCP-AAS 솔루션을 배포할 때 활용할 수 있는 실행 가능한 체크리스트를 다음 표로 제시합니다.

리스크 범주	위협 벡터 설명	산업 운영에 미치는 영향	완화 전략
프롬프트 인젝션	악의적인 입력으로 LLM을 조작하여 의도하지 않은 도구 실행 유도	생산 중단, 장비 손상, 안전사고	입력/출력 데이터 살균(Sanitization), 도구 실행 전 사용자 확인, LLM 응답에 대한 엄격한 파싱
미승인 도구 실행	권한 없는 에이전트가 민감한 도구(예: 펌웨어 업데이트)를 호출	시스템 오작동, 데이터 무결성 훼손	최소 권한 원칙(PoLP) 적용, 역할 기반 접근 제어(RBAC), 위험한 도구에 대한 다단계 승인 워크플로우

AAS 데이터 오염	에이전트가 잘못되거나 악의적인 데이터를 AAS에 기록	잘못된 의사결정, 품질 저하, 규제 위반	AAS에 대한 엄격한 접근 제어, 데이터 유효성 검사 규칙 적용, 모든 변경 사항에 대한 감사 로그 기록
MCP 서버 자격 증명 탈취	MCP 서버 손상으로 연결된 모든 백엔드 시스템(ERP, DB)의 키 유출	전사적 데이터 유출, 시스템 제어권 상실	Vault와 같은 전용 비밀 관리 솔루션 사용, 환경 변수를 통한 자격 증명 주입, API 키 권한 최소화
공급망 공격	악성 코드가 포함된 MCP 서버 또는 종속성 사용	시스템 전체의 백도어 생성, 데이터 유출	신뢰할 수 있는 소스에서만 서버 다운로드, 소프트웨어 서명 및 무결성 검증(SCA, SAST)
서비스 거부(DoS)	에이전트 또는 자산에 과도한 요청을 보내 시스템 마비	생산 중단, 재정적 손실	MCP 서버에 대한 속도 제한(Rate Limiting) 및 회로 차단기(Circuit Breaker) 구현, 자원 사용량 모니터링
혼란된 대리인 공격	MCP 서버가 에이전트의 권한을 초과하여 자신의 높은 권한으로 작업 수행	치명적인 시스템 변경, 보안 정책 우회	MCP 서버에서 에이전트의 신원과 권한을 AAS의 접근 제어 정책에 정확히 매핑, 토큰 전달 금지

Part IV: 전략적 전망 및 권고

MCP와 AAS의 융합이 제시하는 기술적 가능성과 현실적 과제들을 분석한 것을 바탕으로, 이 장에서는 미래 지향적인 관점과 함께 기술 리더 및 전략가들을 위한 실행 가능한 지침을 제공합니다.

Chapter 8: 자율 제조의 미래: 도입을 위한 로드맵

자율 시스템의 전면적인 도입은 '빅뱅' 방식으로 이루어질 수 없으며, 그래서도 안 됩니다.[23] 리스크를 관리하고 조직의 역량을 점진적으로 구축하기 위해서는 단계적인 접근이 필수적입니다. 다음 표는 MCP-AAS 통합을 위한 단계별 도입 로드맵을 제시합니다.

Table 8.1: MCP-AAS 통합을 위한 단계별 도입 로드맵

단계	주요 목표	주요 통합 패턴 (3장 참조)	사용 사례 예시	주요 과제	성공 지표
1단계 (1-2년) 기반 통합 및 읽기 전용 애플리케이션	연결성 확보, 데이터 파이프라인 구축, 초기 가치 증명	패턴 1: MCP 리소스로서의 AAS	AI 기반 장비 진단 매뉴얼, 자산 상태 대시보드, 자연어 기반 정보 검색	데이터 품질 확보, 레거시 시스템 연동, MCP/AAS 초기 기술 학습	주요 자산의 AAS 생성률, 정보 검색 시간 단축, 운영자 만족도
2단계 (2-4년) 에이전트 보조 운영 및 반자율 워크플로우	반복적인 수동 작업 자동화, 인간 작업자 역량 강화	패턴 2: MCP 도구로서의 AAS 서브모델	자동화된 유지보수 티켓 생성, 품질 관리 데이터 자동 입력, 예비 부품 주문 요청	도구 기능의 안정성 확보, 에이전트-인간 협업 프로세스 설계, 보안 리스크 관리	수동 작업 시간 감소, 프로세스 오류율 감소, 생산성 향상
3단계 (5년 이상) 완전 자율 시스템 및 자율 관리 공장	동적인 의도 기반 오케스트레이션 구현, 자율 최적화	패턴 3: AAS 인식 MCP 파사드	자가 최적화 생산 라인, 자율적 공급망 조정, 예측 기반 자율 유지보수	복잡한 에이전트 로직 개발, 시스템 간 완전한 상호운용성, 조직적 신뢰 및 법적 책임 문제	전체 장비 효율(OEE) 극대화, 다운타임 '0'에 근접, 시장 변화에 대한 실시간 대응 능력

Chapter 9: 기술 리더와 전략가를 위한 실행 권고안

이 혁신적인 기술의 잠재력을 성공적으로 실현하기 위해, 기술 리더와 전략가들은 다음과 같은 조치를 고려해야 합니다.

- 권고 1: 전문가 조직(Center of Excellence, CoE) 설립
  OT(AAS, OPC UA), IT(ERP, API), 그리고 AI(MCP, LLM) 분야의 전문성을 갖춘 다기능 팀을 구성하여 통합된 전략을 추진해야 합니다. 이 조직은 전사적 표준을 수립하고, 기술 도입을 주도하며, 지식 공유의 허브 역할을 수행해야 합니다.
- 권고 2: 서브모델 표준화 우선순위 결정
  가장 중요하고 파급 효과가 큰 자산을 식별하고, 해당 자산에 대한 표준 AAS 서브모델 템플릿을 정의하고 채택하는 노력을 주도해야 합니다. 이는 상호운용 가능한 데이터의 기반을 마련하는 가장 근본적인 활동입니다.
- 권고 3: 고부가가치, 저위험 사용 사례로 시작
  초기 프로젝트로 'ERP-to-AAS 자동 생성' 사용 사례를 목표로 설정하는 것이 바람직합니다. 이 사용 사례는 수동 프로세스를 자동화하여 명확한 가치를 제공하고, ERP 측에서는 주로 읽기 전용 패턴을 사용하므로 리스크가 상대적으로 낮으며, 조직 내에 기본적인 MCP 및 AAS 역량을 구축하는 데 도움이 됩니다.
- 권고 4: 첫날부터 보안을 고려한 아키텍처 설계
  보안 아키텍트를 CoE에 포함시키고, 모든 신규 프로젝트에 대해 '통합 보안 리스크 매트릭스'(Table 7.1) 사용을 의무화해야 합니다. 특히, 모든 MCP 서버 구현에서 최소 권한 원칙(PoLP)을 철저히 강제하여 '혼란된 대리인' 공격과 같은 치명적인 리스크를 원천적으로 차단해야 합니다.
- 권고 5: OPC UA와 MCP에 대한 이중 트랙 전략 투자
  두 기술을 경쟁 관계로 보지 말아야 합니다. OT 데이터 수집을 위해 기존 OPC UA 인프라를 강화하는 동시에, 다가오는 AI 에이전트의 물결에 대비하여 애플리케이션 계층에서 MCP 역량을 구축하는 이중 트랙 전략에 투자해야 합니다. 이는 현재의 안정성과 미래의 확장성을 모두 확보하는 길입니다.

Works cited

1. Why should manufacturers embrace AI agents now? - The World Economic Forum, accessed August 2, 2025, https://www.weforum.org/stories/2025/01/why-manufacturers-should-embrace-next-frontier-ai-agents/
2. Industrial AI in action: How AI agents and digital threads will transform the manufacturing industries - Microsoft, accessed August 2, 2025, https://www.microsoft.com/en-us/industry/blog/manufacturing-and-mobility/manufacturing/2025/03/25/industrial-ai-in-action-how-ai-agents-and-digital-threads-will-transform-the-manufacturing-industries/
3. Model Context Protocol - Wikipedia, accessed August 2, 2025, https://en.wikipedia.org/wiki/Model_Context_Protocol

4. What is the Asset Administration Shell? - Arvato Systems, accessed August 2, 2025, https://www.arvato-systems.com/blog/what-is-the-asset-administration-shell
5. Bridging Context and Connectivity: How MCP Complements OPC UA in Industrial AI, accessed August 2, 2025, https://www.arcweb.com/blog/bridging-context-connectivity-how-mcp-complements-opc-ua-industrial-ai
6. What is Model Context Protocol (MCP)? - IBM, accessed August 2, 2025, https://www.ibm.com/think/topics/model-context-protocol
7. Model Context Protocol (MCP), clearly explained (why it matters) - YouTube, accessed August 2, 2025, https://www.youtube.com/watch?v=7j_NE6Pjv-E
8. FAQs - Model Context Protocol, accessed August 2, 2025, https://modelcontextprotocol.io/faqs
9. Model Context Protocol (MCP) Clearly Explained : r/LLMDevs - Reddit, accessed August 2, 2025, https://www.reddit.com/r/LLMDevs/comments/1jbqegg/model_context_protocol_mcp_clearly_explained/
10. Understanding the Model Context Protocol (MCP) | deepset Blog, accessed August 2, 2025, https://www.deepset.ai/blog/understanding-the-model-context-protocol-mcp
11. Specification - Model Context Protocol, accessed August 2, 2025, https://modelcontextprotocol.io/specification/2025-03-26
12. Extend your agent with Model Context Protocol - Microsoft Copilot Studio, accessed August 2, 2025, https://learn.microsoft.com/en-us/microsoft-copilot-studio/agent-extend-action-mcp
13. Introduction - Model Context Protocol, accessed August 2, 2025, https://modelcontextprotocol.io/introduction
14. Model Context Protocol - GitHub, accessed August 2, 2025, https://github.com/modelcontextprotocol
15. The Benefits of Manufacturing Interoperability Across Sites - GE Vernova, accessed August 2, 2025, https://www.gevernova.com/software/blog/benefits-manufacturing-interoperability
16. Interoperability holds the key to efficiency in modern-day logistics - Blog for mechanical engineering & industry, accessed August 2, 2025, https://blog.item24.com/en/automation/interoperability-holds-the-key-to-efficiency-in-modern-day-logistics/
17. What is the Asset Administration Shell? | Phoenix Contact, accessed August 2, 2025, https://www.phoenixcontact.com/en-pc/company/all-electric-society/asset-administration-shell
18. How the Asset Administration Shell Is Shaping the Future of Digital Twins - MHP, accessed August 2, 2025, https://www.mhp.com/en/insights/blog/post/asset-administration-shell

19. Details of the Asset Administration Shell - Plattform Industrie 4.0, accessed August 2, 2025, https://www.plattform-i40.de/IP/Redaktion/EN/Downloads/Publikation/vws-in-detail-presentation.pdf?__blob=publicationFile&v=12
20. BS EN IEC 63278-4 Ed 4 BS EN 63278-4 Ed 4 Asset administration shell for industrial applications -. Part 4: Use cases and modelling examples - British Standards Institution - Project, accessed August 2, 2025, https://standardsdevelopment.bsigroup.com/projects/2023-02139
21. IEC 63278-1:2023, accessed August 2, 2025, https://webstore.iec.ch/en/publication/65628
22. EN IEC 63278-1:2024 - Asset Administration Shell for industrial applications - Part 1 - iTeh Standards, accessed August 2, 2025, https://standards.iteh.ai/catalog/standards/clc/3bee3f87-b0d9-4a59-8f28-04bbd8b38e4e/en-iec-63278-1-2024
23. Integrating Systems of Record (SOR) into the Asset Administration Shell (AAS) Dataspace: Bridging the Gap by Leveraging Submodel-based Interface Descriptions (Part 1) - Blog des Fraunhofer IESE, accessed August 2, 2025, https://www.iese.fraunhofer.de/blog/sor-in-the-aas-dataspace/
24. The Asset Administration Shell – a universal tool for data exchange in industry, accessed August 2, 2025, https://device-insight.com/en/the-asset-administration-shell-a-universal-tool-for-data-exchange-in-industry/
25. BaSyx / Documentation / AssetAdministrationShell - Eclipsepedia, accessed August 2, 2025, https://wiki.eclipse.org/BaSyx_/_Documentation_/_AssetAdministrationShell
26. Details of the Asset Administration Shell - IDTA, accessed August 2, 2025, https://industrialdigitaltwin.org/wp-content/uploads/2022/06/DetailsOfTheAssetAdministrationShell_Part1_V3.0RC02_Final1.pdf
27. Asset Administration Shell (AAS) - CONTACT Software, accessed August 2, 2025, https://www.contact-software.com/en/products/iot-software-elements-for-iot/asset-administration-shell/
28. Submodel Templates of the Asset Administration Shell - Plattform Industrie 4.0, accessed August 2, 2025, https://www.plattform-i40.de/IP/Redaktion/EN/Downloads/Publikation/Specification_Submodel-Templates.pdf?__blob=publicationFile&v=1
29. AAS Submodel Templates - IDTA, accessed August 2, 2025, https://industrialdigitaltwin.org/en/content-hub/submodels
30. Submodel Templates of the Asset Administration Shell. Generic Frame for Technical Data for Industrial Equipment in Manufacturing (Version 1.1) | Request PDF - ResearchGate, accessed August 2, 2025, https://www.researchgate.net/publication/346607469_Submodel_Templates_of_the_Asset_Administration_Shell_Generic_Frame_for_Technical_Data_for_Industrial_Equipment_in_Manufacturing_Version_11
31. Submodel Templates of the Asset Administration Shell - ZVEI, accessed August 2, 2025,

https://www.zvei.org/fileadmin/user_upload/Presse_und_Medien/Publikationen/2020/Dezember/Submodel_Templates_of_the_Asset_Administration_Shell/201117_I40_ZVEI_SG2_Submodel_Spec_ZVEI_Technical_Data_Version_1_1.pdf
32. Submodel Templates of the Asset Administration Shell - Fluidtechnik 4.0, accessed August 2, 2025, https://fluidtechnik40.de/wp-content/uploads/2022/05/210322-I40-ZVEI-SG2-Submodels-Small-spec-Manufacturer-info-VDI2770v11-Final_2021-03-09-ak_MIHOv2.pdf
33. (PDF) Architecture for managing AAS-based business processes - ResearchGate, accessed August 2, 2025, https://www.researchgate.net/publication/367093558_Architecture_for_managing_AAS-based_business_processes
34. Details Of the Administration Shell - Part 1, accessed August 2, 2025, https://industrialdigitaltwin.org/wp-content/uploads/2021/09/07_details_of_the_asset_administration_shell_part1_v3_en_2020.pdf
35. The administration shell as a standardized "digital twin" < XITASO, accessed August 2, 2025, https://xitaso.com/en/the-administration-shell-as-a-standardized-digital-twin/
36. ZEISS Digital Innovation Blog - Example implementation of a digital twin exchange with the Asset Administration Shell concept, accessed August 2, 2025, https://blogs.zeiss.com/digital-innovation/en/digital-twin-aas/
37. Auto-creation Dimension 1 - Sage X3, accessed August 2, 2025, https://online-help.sagex3.com/erp/12/en-us/Content/OBJ/ADP_AAS_CRECCE1.htm
38. Infor XA | Enterprise Software for Discrete Manufacturers, accessed August 2, 2025, https://www.infor.com/products/xa
39. Introducing next-generation AI and Microsoft Dynamics 365 Copilot capabilities for ERP, accessed August 2, 2025, https://www.microsoft.com/en-us/dynamics-365/blog/business-leader/2023/06/15/introducing-next-generation-ai-and-microsoft-dynamics-365-copilot-capabilities-for-erp/
40. Building-a-model-context-protocol-mcp-server-for-ERP-integration - IWConnect, accessed August 2, 2025, https://iwconnect.com/building-a-model-context-protocol-mcp-server-for-erp-integration/
41. Revolutionizing ERP With The Model Context Protocol (MCP) - Kiktronik Limited, accessed August 2, 2025, https://kiktronik.com/revolutionizing-erp-with-the-model-context-protocol-mcp/
42. MCP for ERP Integration: AI-Powered Solutions - BytePlus, accessed August 2, 2025, https://www.byteplus.com/en/topic/541662
43. Model Context Protocol | AI MCP Server Consulting Experts - Advisor Labs, accessed August 2, 2025, https://www.advisorlabs.com/services/model-context-protocol
44. Asset Administration Shell (AAS) Quick Start Guide – Data Provider Step 6 - YouTube, accessed August 2, 2025,

https://www.youtube.com/watch?v=YYS3o3yU1EY
45. [2403.17209] Generation of Asset Administration Shell with Large Language Model Agents: Toward Semantic Interoperability in Digital Twins in the Context of Industry 4.0 - arXiv, accessed August 2, 2025, https://arxiv.org/abs/2403.17209
46. Does anyone have any use cases or examples on how they have used OPC-UA? - Reddit, accessed August 2, 2025, https://www.reddit.com/r/PLC/comments/15tqa82/does_anyone_have_any_use_cases_or_examples_on_how/
47. Asset Administration Shell meets OPC UA: Why Both Matter - Neoception, accessed August 2, 2025, https://www.neoception.com/asset-administration-shell-meets-opc-ua-why-both-matter/
48. 4 General information on the Asset Administration Shell and OPC UA, accessed August 2, 2025, https://reference.opcfoundation.org/I4AAS/v100/docs/4
49. Industry 4.0 Asset Administration Shell - 5.1 General rules for the mapping of the AAS metamodel to the OPC UA information model, accessed August 2, 2025, https://reference.opcfoundation.org/I4AAS/v100/docs/5.1
50. AAS Meets OPC UA: A Unified Approach to Digital Twins | Request PDF - ResearchGate, accessed August 2, 2025, https://www.researchgate.net/publication/391862081_AAS_Meets_OPC_UA_A_Unified_Approach_to_Digital_Twins
51. I4AAS - Industrie 4.0 Asset Administration Shell - OPC Foundation, accessed August 2, 2025, https://opcfoundation.org/markets-collaboration/i4aas/
52. Industrial Interoperability with OPC UA and the AAS, accessed August 2, 2025, https://opcconnect.opcfoundation.org/2023/03/industrial-interoperability-with-opc-ua-and-the-aas/
53. Overcoming the Hurdles: Common Challenges in AI Agent Integration (& Solutions) - Knit, accessed August 2, 2025, https://www.getknit.dev/blog/overcoming-the-hurdles-common-challenges-in-ai-agent-integration-solutions
54. AI Agent Development: 5 Key Challenges and Smart Solutions - Softude, accessed August 2, 2025, https://www.softude.com/blog/ai-agent-development-some-common-challenges-and-practical-solutions/
55. Superagency in the workplace: Empowering people to unlock AI's full potential - McKinsey, accessed August 2, 2025, https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/superagency-in-the-workplace-empowering-people-to-unlock-ais-full-potential-at-work
56. What Are the Biggest Challenges in AI Automation That No One Talks About? - Reddit, accessed August 2, 2025, https://www.reddit.com/r/automation/comments/1ja2hxi/what_are_the_biggest_challenges_in_ai_automation/
57. Model Context Protocol (MCP): Understanding security risks and controls - Red Hat, accessed August 2, 2025, https://www.redhat.com/en/blog/model-context-protocol-mcp-understanding-s

ecurity-risks-and-controls
58. Top 10 MCP (Model Context Protocol) Server Security Risks - SOCRadar, accessed August 2, 2025, https://socradar.io/top-10-mcp-model-context-protocol-server-risks/
59. Security Best Practices - Model Context Protocol, accessed August 2, 2025, https://modelcontextprotocol.io/specification/draft/basic/security_best_practices
60. Model Context Protocol (MCP): A Security Overview - Palo Alto Networks Blog, accessed August 2, 2025, https://www.paloaltonetworks.com/blog/cloud-security/model-context-protocol-mcp-a-security-overview/
61. The Security Risks of Model Context Protocol (MCP) - SECNORA, accessed August 2, 2025, https://secnora.com/blog/the-security-risks-of-model-context-protocol-mcp/
62. 4 Best Strategies to Secure Model Context Protocol - Knostic AI, accessed August 2, 2025, https://www.knostic.ai/blog/strategies-secure-model-context-protocol