5 COSMIC-X: Vertrauenswürdige Wertschöpfungsketten in kollaborativen industriellen Ökosystemen

N. Maisch, A. Lechler, O. Riedel (ISW), C. Reich, P. Ruf, F. Stodt (IDACUS), H. Jacobsen, N. Voigt, D. Haag (SW), J. Folmer (HAWE), P. Mueck (KROHNE), Y. Nezu, S. Zehentreiter (Datarella), M. Mohr, C. Gill, M. Mai (inovex), S. Igel, S. Bernauer (Stackable)

Titel	Kollaborative Smart Services für industrielle Wertschöpfungsnetze in GAIA-X
Förderlinie	ZdW - InGaia-X: Industrie 4.0 - Gaia-X-Anwendungen in Wertschöpfungsnetzwerken
Laufzeit	01.10.2022 bis 31.12.2024
Fördermittelgeber	Bundesministerium für Bildung und Forschung
Förderkennzeichen	02J21D140-02J21D147

5.1 Einführung: Problemstellungen in den Use Cases

Im Rahmen der Wartung und Instandhaltung von Maschinen und deren Einzelteilen sind in der Regel eine Vielzahl von Partnern und externen Dienstleistern beteiligt, die in unterschiedlichen Phasen der Lieferkette involviert sind oder IT-Services anbieten bzw. diese unterstützen. Um das verteilte Fachwissen effizient in Form digitaler Services einzusetzen, ist eine Zusammenarbeit auf der IT-Ebene notwendig. Folglich müssen Wege gefunden werden, wie kollaborativ an Daten gearbeitet werden kann und diese vertrauensvoll ausgetauscht werden können [1]. Fehlende Standards erschweren die firmenübergreifende Nutzung von Daten, um datengetriebene Geschäftsmodelle voranzutreiben und Wartungs- und Instandhaltungsmaßnahmen zu optimieren. Durch Gaia-X werden standardisierte Methoden geschaffen, Daten über Unternehmensgrenzen hinweg sicher nutzbar zu machen und legt dadurch die Grundlage für Optimierungsprozesse unter Beteiligung mehrerer Partner. Insbesondere die vorgestellten Frameworks (z. B. die Gaia-X Federation Services (GXFS)) können dabei helfen, das Vertrauensverhältnis der jeweiligen Geschäftspartner ineinander zu stärken. Besondere Relevanz bekommen standardisierte Policies für die wechselseitige Nutzung von Services und den Datenaustausch der Geschäftspartner untereinander. Die Nutzung eines so entstehenden Datenraums ermöglicht eine Optimierung der Wertschöpfung, da jeder Teilnehmer seine eigene Expertise in den Prozess einbringen kann und weniger ungewollte IT-Barrieren im Weg stehen, z. B. durch bürokratische Maßnahmen zum Zugriff auf fremde Netzwerke. Zentrales Element dafür ist die eindeutige und vertrauenswürdige Identifikation von Menschen und Maschinen als Basis jeglicher firmenübergreifenden Kollaboration. Erst

dies ermöglicht die Etablierung von vertrauenswürdigen Zugriffs-, Austausch- und Absicherungsmechanismen für Daten und Services. Essentielle Aspekte zur Herstellung von Vertrauen in Datenräumen sind unter anderem [2]:

- Datenintegrität: "Integrität bezeichnet die Sicherstellung der Korrektheit (Unversehrtheit) von Daten und der korrekten Funktionsweise von Systemen."
- Vertraulichkeit: "Vertraulichkeit ist der Schutz vor unbefugter Preisgabe von Informationen."
- Authentizität: "Mit dem Begriff Authentizität wird die Eigenschaft bezeichnet, die gewährleistet, dass ein Kommunikationspartner tatsächlich derjenige ist, der er vorgibt zu sein."

Die Nutzung der GXFS zur Herstellung von Vertrauen in industriellen Datenräumen kann durch den Einsatz der Blockchain-Technologie zusätzlich unterstützt werden. Eine Kombination der beiden Technologien ermöglicht sowohl die eindeutige Identifikation durch dezentrale Identitäten, die Absicherung von Schnittstellen zwischen verschiedenen Partnern, die Datensouveränität durch kryptografische Autorisierungsmechanismen und nicht zuletzt die Herstellung einer Ground Truth der Daten, die jeder Partner verifizieren und damit vertrauen kann [3, 4].

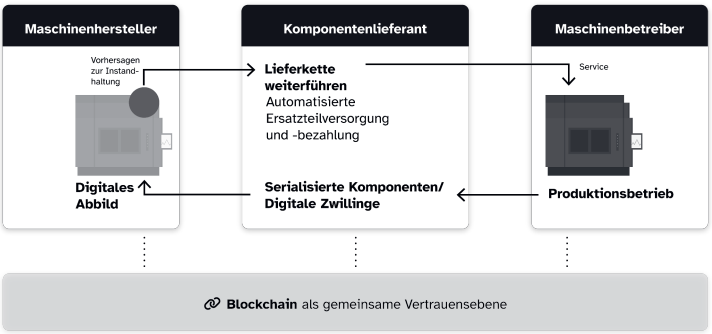

Abbildung 5.1: Rolle einer Blockchain bei der Zusammenarbeit verschiedener Firmen

Die in COSMIC-X bearbeiteten Use Cases basieren daher auf einer gemeinsamen Grundarchitektur mit dem Ziel der Herstellung von Vertrauen zwischen Partnern in einem kollaborativen Wertschöpfungsnetzwerk digitaler Services für die Unterstützung der Wartung und Instandhaltung. Dabei bildet die Blockchain-Technologie eine gemeinsame Vertrauensebene zwischen Maschinenhersteller, Komponentenlieferant und Maschinenbetreiber (Abbildung 5.1). Im Projekt wurden industrielle Use-Cases durch die technische Expertise der "Enabler" *Stackable GmbH*, *inovex GmbH* und *Datarella GmbH* im Bezug auf reale Maschinen der Konsortialpartner *Schwäbische Werkzeugmaschinen GmbH (SW)*, *HAWE Hydraulik SE* und *KROHNE Messtechnik GmbH* konzipiert und durch das *Institut für Steuerungstechnik der Werkzeugmaschinen und Fertigungseinrichtungen der Universität Stuttgart (ISW)* und das *Institut für Data Science, Cloud Computing und IT-Sicherheit der Hochschule Furtwangen (IDACUS)* im wissenschaftlichen Kontext begleitet.

Im Rahmen des Projekts wurden drei Problemstellungen adressiert:

- Vertrauenswürdige Lieferkette: In diesem Use Case werden Betriebsdaten technischer Anlagen durch die Nutzung einer Blockchain abgesichert. Dies ermöglicht die Implementierung von Third Party Machine Learning Services für vorausschauende Wartung, die sowohl dem Maschinenbauer selbst als auch seinen Kunden einen Mehrwert bietet. Durch eine algorithmische Bewertung der

Betriebsdaten einer Anlage können Verschleißanzeichen ermittelt und die Restlebensdauer ihrer Komponenten approximiert werden. Ein Zugriffsmanagement basierend auf den GXFS und die Absicherung der Betriebsdaten durch Blockchain-Technologien dienen dabei zur Herstellung von Vertrauen zwischen Betreiber, Maschinenbauer und dem Machine Learning Provider. Zusätzlich wird durch die Abbildung von Interaktionen entlang der Lieferkette in Datenräume und Blockchains die Grundlage der Automatisierung von Bestellprozessen von Ersatzteilen gelegt, die bisher durch eine hohe Zahl an beteiligten Partnern (Betreiber, Einkauf, Vertrieb, Service, ...) und durch einen hohen Grad an manueller Bearbeitung und Organisation geprägt ist.

- Digitale Zwillinge: Ziel dieses Use Cases ist die Erstellung eines digitalen Abbilds einer Maschine und ihrer Komponenten unter Verwendung einer Verwaltungsschale (engl. Asset Administration Shell - AAS). Sie soll Kunden als individuelle Schnittstelle für aktuelle Handbücher und Wartungsunterlagen dienen, indem die Informationen des Produkts durch den Hersteller aktualisiert werden. Die Zugänge zu dem AAS-Service werden durch ein Zugriffsmanagement basierend auf den GXFS gesteuert. Zusätzlich werden Betriebsdaten des Assets gespeichert und durch die Nutzung von Third-Party-Services auf maschinenspezifische Anomalien hin analysiert. Durch eine Absicherung der Betriebsdaten in einer Blockchain wird ihre Integrität gewährleistet. Im Kontext eines Weiterverkaufs der Maschine sind somit individuelle Fehlerquoten und Auswirkungen von bisherigen Einsätzen unveränderbar dokumentiert und transparent einsehbar.
- Plattformbasierte Wartung: Ziel dieses Use Cases ist die Entwicklung einer Industrial Internet of Things (IIoT)-Plattform zur Visualisierung von Betriebsdaten und zur Unterstützung des Servicepersonals bei der Wartung und Instandhaltung der Komponenten. Dabei teilt sich die Plattform in zwei Teile auf: In die analytische Auswertung von Betriebsdaten des Geräts und in einen KI-gestützten Chatbot, basierend auf historischen Wartungsberichten und offizieller Dokumentation in Form technischer Handbücher, zur Unterstützung der Wartung. Um die Preisgabe sensibler Daten zu vermeiden, ist neben der Anonymisierung von Rohdaten auch das Zugriffsmanagement für den Chatbot und die Visualisierungen notwendig. Zusätzlich entstehen in vielen Situationen, in denen derartigen KI-basierte Systeme eingesetzt werden, auch neuartige Bedrohungen, die sicherheitstechnisch betrachtet werden müssen.

5.2 Relevanz von Gaia-X für das Projekt: Authentifizierung und Autorisierung

Alle Use-Cases in COSMIC-X basieren auf der Kooperation verschiedener Firmen, indem den jeweiligen Partnern der Zugang zu Prozess-, Betriebs- oder Servicedaten zur Verfügung gestellt wird. Schon bei oberflächlicher Betrachtung der Use Cases ergibt sich auf Implementierungsebene die Anforderung einer stabilen und unternehmensübergreifenden Authentifizierung und Autorisierung. Etablierte Technologien zur Implementierung dieser Problemstellung setzen auf manuell eingerichtete Zugänge zu Datensilos oder zentralen Identitätsprovidern. Die Grundsätze von Gaia-X sehen eine Dezentralisierung von Authentifizierung und Autorisierung vor, um digitale Identitäten und digitale Interaktionen ohne die Abhängigkeit von zentralisierten Entitäten zu ermöglichen [5]. Gaia-X setzt dabei zur Umsetzung auf das Konzept der Self-Sovereign Identity (SSI), bei der jede Partei ihre eigenen digitalen Identitäten selbst kontrollieren kann [6]. Basis für Implementierungen von SSI ist der W3C-Standard der Verifiable Credentials (VC) [7]. VCs beschreiben Aussagen über eine digitale Identität und werden durch den Inhaber (Holder) selbst verwaltet. Ausgeber (Issuer) geben die VCs aus und ein Prüfer (Verifier) überprüft je nach Anwendung das durch den Holder präsentierte VC (Abbildung 5.2).

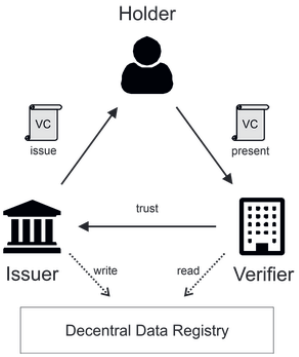

Abbildung 5.2: Funktionsweise von Verifiable Claims

Wesentlicher technischer Bestandteil einer VC ist der W3C-Standard der Decentralized Identifiers (DIDs), mit der VCs eindeutig identifiziert werden. Damit ist eine DID ähnlich einer URL im klassischen Internet, die zu einer Internetseite bzw. einer Ressource auflöst (z. B. Bild oder Dokument). DIDs sind aus drei Teilen aufgebaut (Abbildung 5.3) [8]:

1. DID Schema: Formale Syntax zum Signalisieren einer DID (z. B. 'did')
2. DID Methode: Definition der Implementierung der DID (z. B. 'example')
3. DID Identifikator: Eindeutige Identifikation des Objekts (z. B. '123456789abcdefghi')

did:example:123456789abcdefghi

Abbildung 5.3: Beispielhafte DID

Während viele DID-Methoden auf speziellen SSI-Blockchains basieren, wird in Gaia-X die Methode did:web vorausgesetzt, die beispielsweise folgenderweise formatiert wird: "did:web:example.com". Der methodenspezifische Identifikator ist in diesem Fall eine URL, die auf das DID Dokument verweist und Verifikationsmethoden (z. B. in Form eines öffentlichen Schlüssels) zur kryptografischen Authentifizierung des DID-Halters enthält. Die VCs verwaltet der Nutzer selbst in einem geeigneten SSI-Wallet, in dem die privaten Schlüssel verwaltet werden. Durch die GXFS werden Frameworks für die Umsetzung von SSI mithilfe von VCs, DIDs und Wallets zur Verfügung gestellt [9].

5.3 Methodik/Umsetzung: Vertrauenswürdiger Informationsaustausch in industriellen Geschäftsprozessen

5.3.1 Vertrauen für digitale Services mit Self-Sovereign Identities

Für die digitale Unterstützung der in den Use Cases bearbeiteten Wertschöpfungsprozesse steht im Mittelpunkt, den verschiedenen beteiligten Geschäftspartnern Zugriff auf digitale Informationen zu

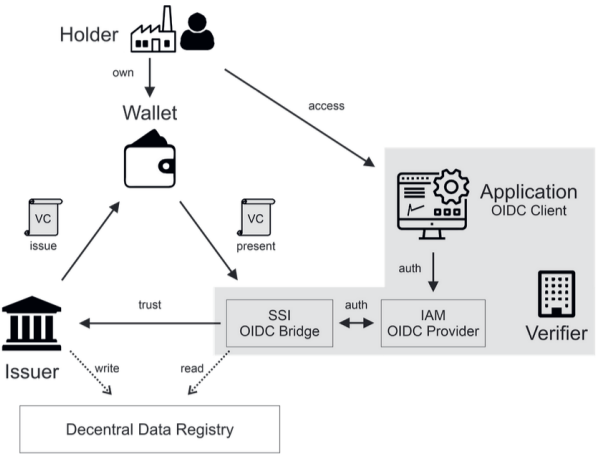

Abbildung 5.4: Vertrauen durch mit OICD und Verifiable Claims

gewähren: Hersteller (Anbieter, Data Owner) geben ihren Kunden (Daten-Konsumenten) Zugriff auf eigene Systeme (bspw. auf Monitoring Dashboards), damit diese Informationen über den Zustand ihrer Maschinen oder Messgeräte erhalten.

In den Unternehmen existieren klassische zentrale Sicherheitsinfrastrukturen zur Identifikation und zur Vergabe von Zugangsberechtigungen, wie ein Identity- und Access Management (IAM), in das neue Informationssysteme mittels Single-Sign-On eingebunden werden können (Abbildung 5.4). Dazu wurden die im Projekt entwickelten Anwendungssysteme, die eine grafische Benutzerschnittstelle haben, mit OpenID Connect (OIDC) ausgestattet. In den Demonstratoren wurde Keycloak als etablierte Open-Source IAM-Lösung verwendet. Die Autorisierung ermöglicht der Open Policy Agent (OPA), der die Durchsetzung beliebig flexibler Regelwerke ermöglicht, die mit der Policy-Sprache Rego als sog. "Rego Rules" deklarativ bereitgestellt werden. Durch die Verwendung von GXFS-Komponenten ist es möglich, diese zentralisierten IAM-Lösungen zu einer souveränen, dezentralen SSI-Architektur zu erweitern.

Jeder Nutzer speichert in seiner Wallet die geeigneten, Gaia-X konformen Verifiable Credentials, die von seinem Unternehmen ausgestellt werden. Die Geschäftspartner haben sich wechselseitig auf deren Akzeptanz und die Nutzungsrichtlinien (Policies) geeinigt. Eine SSI-OIDC Bridge dient als Verbindungskomponente: Wenn ein Anwender auf ein System zugreifen möchte, wird er über die Bridge aufgefordert, sich durch Präsentation seiner Verifiable Credentials zu identifizieren. Danach wird er zur Anwendung zurückgeleitet und kann diese in dem Umfang gemäß der hinterlegten Policies der anfragenden Entität nutzen.

5.3.2 Blockchain als dezentraler Sicherheitsanker

Während SSI einen robusten Ansatz zur Authentifizierung und Autorisierung von Datenzugriffen darstellt, kann die Authentizität und Integrität der angefragten Daten damit nicht sichergestellt werden. Hierfür eignet sich stattdessen die Verwendung einer Blockchain, mit der Informationen unveränderlich gespeichert und von allen beteiligten Parteien unabhängig verifiziert werden können.

Obwohl Stand heute viele unterschiedliche Blockchain-Protokolle existieren, ist deren Eig-

nung für industrielle Use Cases oftmals sehr spezifisch oder schlicht nicht gegeben. Um die größtmögliche Übereinstimmung zwischen den Anforderungen von COSMIC-X und den Möglichkeiten von Blockchain-Technologien zu erreichen, wurde ein ausführlicher Evaluationsprozess durchgeführt. Dieser stellte sowohl private als auch öffentliche Blockchain-Plattformen anhand der Bewertungskriterien Sicherheit, Privatsphäre, Skalierbarkeit und Interoperabilität gegenüber.

Während erprobte Blockchain-Plattformen der aktuellen Generation überwiegend gut in den Kategorien Sicherheit und Skalierbarkeit abschneiden, sind (vollständige) Privatsphäre und Interoperabilität in verfügbaren Lösungen oft limitiert. Um Privatsphäre in industriellen Szenarien wie COSMIC-X umzusetzen, wurden in der Vergangenheit fast ausschließlich private Blockchains oder Konsortium-Blockchains wie Hyperledger Fabric eingesetzt. Mit diesen gehen allerdings inhärent hohe Infrastrukturkosten für die betreibenden Parteien sowie eingeschränkte Dezentralisierung und Interoperabilität einher. Demgegenüber bieten öffentliche Blockchains einen hohen Grad an Resilienz, Kosteneffizienz und ein gewisses Maß an Interoperabilität. Ein Fokus auf Privatsphäre und Datenschutz entwickelte sich in diesem Umfeld jedoch erst in jüngerer Vergangenheit. Daraus hervorgegangene Blockchain-Plattformen mit entsprechenden Funktionalitäten sind deshalb noch vergleichsweise jung und unerprobt. Stellt man die Vor- und Nachteile der beiden Ansätze gegenüber, erweist sich ein Privatsphäre-fokussiertes öffentliches Netzwerk aber letztlich als präferierte Lösung im industriellen Kontext.

Damit dieses die Privatsphäre- und Datenschutzanforderungen von COSMIC-X erfüllt, muss es zwingend die Mandantenfähigkeit (*Multi-Tenancy*) unterstützen. Bei Multi-Tenancy bedient eine einzige Instanz einer Software-Anwendung mehrere Mandanten, indem eine logische Isolierung der Nutzer gewährleistet und gleichzeitig Anpassungen ermöglicht werden, die globale Gültigkeit besitzen. Es erlaubt verschiedenen Mandanten die gemeinsame Nutzung einer zugrunde liegenden Infrastruktur unter Einhaltung ihrer Privatsphäre. Der Einsatz von Multi-Tenancy-Lösungen in der Fertigungsindustrie bringt mehrere Vorteile mit sich. Zum einen optimiert sie die gemeinsame Nutzung von Ressourcen, da die Infrastrukturkosten unter den Mandanten aufgeteilt werden. Zum anderen verbessert sie die Effizienz des Zugriffs auf Kundendaten, rationalisiert die Datenverwaltung und fördert die Zusammenarbeit beim gemeinsamen Datenaustausch.

Am Ende des Evaluationsprozesses stellte sich das Cosmos-basierte *Secret Network* [10] als Blockchain-Plattform mit der größten Eignung für COSMIC-X heraus. Das Secret Network ist eine öffentliche Blockchain, die speziell für vertrauliche Datenverarbeitung entwickelt wurde. Mithilfe von etablierten Verschlüsselungstechniken in Kombination mit vertrauenswürdigen Ausführungsumgebungen (*Trusted Execution Environments*) ermöglicht sie die Bereitstellung von sogenannten *Secret Contracts*. Bei diesen handelt es sich um Ende-zu-Ende-verschlüsselte Smart Contracts, mit denen Konsens über Berechnungen hergestellt werden kann, ohne die eingehenden und ausgehenden Daten preiszugeben. Integrierte Zugangskontrollmechanismen (*Viewing Keys*) erlauben es, autorisierten Dritten Einsicht zu gewähren und die Verarbeitungskette auditierbar zu machen. Entsprechend erfüllt das Secret Network die Anforderung der Mandantenfähigkeit bei gleichzeitiger Erhaltung aller Vorteile eines öffentlichen Netzwerks.

5.3.3 Standardisierte Asset-Schnittstellen mit Asset Administration Shell

Im Rahmen des Forschungsprojektes wurde das Submodell *Asset Interfaces Description* (AID) der Industrial Digital Twin Association (IDTA) verwendet, um Zugriffe auf Live- oder historische Daten zu realisieren. Das AID beschreibt die Schnittstellen eines Assets (z. B. Maschinen oder einzelne Komponenten) im Kontext eines digitalen Zwillings. Es standardisiert die Definition physischer und digitaler Schnittstellen, um die Interoperabilität zwischen verschiedenen Assets und Systemen zu gewährleisten. Diese Standardisierung erleichtert die Integration in industrielle Umgebungen und optimiert die Kommunikation im Industrial Internet of Things (IIoT). Durch die klare Beschreibung der Schnittstellen

können Wartungs-, Diagnose-Tools oder auch Datenkonsumenten effizienter arbeiten, da relevante Zugriffs- und Dateninformationen transparenter sind und sie diese so besser nutzen können. Prozesse für die Datenbereitstellung können automatisiert werden, genauso wie Produktionsprozesse. So können bspw. OPC UA Endpoints, Zugriffspunkte von Datenbanken uvm. automatisiert bereitgestellt werden. Ebenso können Machine Learning Modelle oder auch KI diese Schnittstelle automatisiert nutzen, um Datenquellen zu erfragen und die Daten zu konsumieren. Zusammengefasst dient das Submodell *Asset Interfaces Description* dazu, die Kommunikation und Zusammenarbeit zwischen physischen und virtuellen Assets in vernetzten Umgebungen zu standardisieren und zu optimieren. Es fördert die Effizienz, Interoperabilität und Automatisierung in modernen industriellen Umgebungen und unterstützt die Einhaltung von Standards.

5.3.4 Maschinelles Lernen und Künstliche Intelligenz

Die Verwendung von großen Sprachmodellen (Large Language Models, kurz LLMs) ist in verschiedenen Bereichen in den letzten Jahren aufgekommen. LLMs eignen sich hervorragend, um große Menge an Text zu verstehen und sind in der Lage, Fragen zu den Texten präzise zu beantworten. Aus diesem Grund wurde bei der Entwicklung des Chatbots im Use Case Plattformbasierte Wartungäuf diese Technologie gesetzt. Damit ist es möglich, die technischen Handbücher der KROHNE Messgeräte mit natürlicher Sprache durchsuchbar zu machen. Das Servicepersonal kann dem Chatbot ausformulierte Fragen als Eingabe senden und erhält anschließend die dazu passenden relevanten Abschnitte aus dem jeweiligen Handbuch.

Für die beiden anderen Use Cases kommen Verfahren aus dem Bereich der Anomalieerkennung zum Einsatz. Damit ist es möglich, Anomalien in den technischen Betriebsdaten ausfindig zu machen und bei häufigen Auftritten eine Wartung einzuplanen bzw. eine Schätzung zur RUL abzugeben. Es wurden unterschiedliche Verfahren untersucht und miteinander verglichen und am besten eignen sich das Local-Outlier-Factor-Verfahren sowie der Isolation-Forest. Beide Techniken ermöglichen das zuverlässige Erkennen von anomalen Verhalten in den Betriebsdaten.

5.4 Ergebnisse: Einbindung in industrielle Use Cases

5.4.1 Vertrauenswürdige Lieferkette

Algorithmische Bewertung der Restlebenszeit von Maschinenkomponenten

Eine vertrauenswürdige, automatisierte Lieferkette setzt in diesem Anwendungsfall voraus, dass die Verschleißgrenze einer bestimmten Komponente algorithmisch ausgewertet werden kann. Frühere Forschungsergebnisse (Projekt PreCom [11]) zeigten in diesem Bereich gute Ansätze im Kontext von Kugelgewindetrieben, auf welchen nun aufgebaut wurde. Das Vorhaben profitierte dabei insbesondere von der gemeinschaftlichen Expertise hinsichtlich Hydraulik (HAWE), Bearbeitungszentrum (SW) und Machine Learning (inovex). In der Folge wurden drei Analyse-Szenarien definiert, die sich für eine derartige Auswertung eignen. Diese sollten aufgrund unterschiedlicher Komplexitätsgrade einen graduellen Entwicklungsprozess unterstützen:

1. Ein sich verstopfender Ölfilter,
2. Verlust der Vorspannung des Hydraulikspeichers,
3. Verschleiß im Ventilschaltkreis.

Faktoren für die Auswahl einer geeigneten Demonstrator-Maschine waren insbesondere die sensorische Ausstattung (Platzierung und Auflösung standardmäßig verbauter Sensoren vs. Nachrüstung), sowie Kontext bzw. Wiederholbarkeit der Messungen (d.h. möglichst isolierte Zeitpunkte, in denen

lediglich die betroffene Komponente hydraulisch aktiv ist). Für den Demonstrator wurden drei Maschinen eines Kunden ausgewählt und mit einer angepassten Konfiguration über einen Zeitraum von rund neun Monaten kontinuierlich ausgewertet. Dabei dienen protokollierte Serviceeinsätze als Referenz für Fehlerfälle, die post-mortem für das Training der Algorithmen genutzt werden sollten. Die gesammelten Maschinendaten wurden in einer zentralen Datenbank gespeichert und ausgewertet. Die im Untersuchungszeitraum dokumentierten Serviceeinsätze erwiesen sich letztlich als unzureichend, um eine RUL mit hinreichender Qualität zu berechnen - daher wurden die Maschinendaten im Demonstrator mit Verfahren zur Anomalieerkennung ausgewertet. Daraus kann näherungsweise eine RUL abgeleitet werden, unter der Annahme, dass mehr erkannte Anomalien in einer kürzeren RUL resultieren. Für die Berechnung kamen die in Kapitel 5.3.4 vorgestellten Verfahren zum Einsatz.

Abbildung einer automatisierten Lieferkette für Ersatzteile

Zur Modellierung einer automatisierten Lieferkette wurde der heute bereits bestehende Prozess analysiert und dessen manuelle Bearbeitungsschritte (Bestellung, Prüfungen, Bestätigungen, Dokumentation etc.) auf einen minimalen Umfang reduziert.

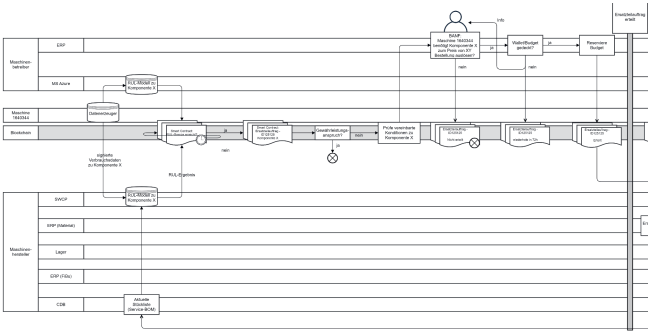

Abbildung 5.5: Der Algorithmus prüft laufend die Verschleißgrenze der betroffenen Komponente. Ist diese erreicht, erfasst ein Smart Contract den Ersatzteilbedarf und erzeugt den Bestellauftrag, sofern ausreichend Budget vorhanden ist. In diesem Beispiel ist zudem noch die Bestätigung im Einkauf des Kunden erforderlich.

Über den Beschaffungsprozess hinaus wurden zudem Möglichkeiten eines automatisierten Zahlungsverkehrs geprüft. Gemäß der deutschen Gesetzgebung sind bspw. von Maschinen geführte Zahlungskonten aktuell nicht rechtmäßig und erfordern demnach weiterhin Prozesse, bei denen z. B. die Vertragsparteien über angebundene ERP-Systeme manuell Zahlungsströme steuern. Ein im Rahmen des Forschungsprojekts "Recht-Testbed" gefälltes Gerichtsurteil konnte Mitte 2024 nachweisen, dass per öffentlicher Blockchain (bzw. Smart Contracts) geführte Vertragsbeziehungen rechtlich uneingeschränkt wirksam sind [12]. Dieser Umstand bekräftigt die Anwendung von industriellen Blockchain-Lösungen und könnte mittelfristig auch einer automatisierten Zahlungsabwicklung den Weg ebnen.

Die in COSMIC-X implementierte Blockchain-Lösung erlaubt im vorliegenden Use Case, die Datenintegrität von Maschinendaten über den gesamten Ersatzteilbeschaffungsprozess hinweg sicherzustellen. Dafür wird jedes Datenpaket auf der produzierenden Maschine signiert und unveränderbar in einem "Secret Contract" verankert (vgl. Kapitel 5.3.2). Jede Maschine ist dafür mit einem lokalen Wallet-Service ausgestattet, der die direkte Kommunikation mit der Blockchain ermöglicht. Bevor eine

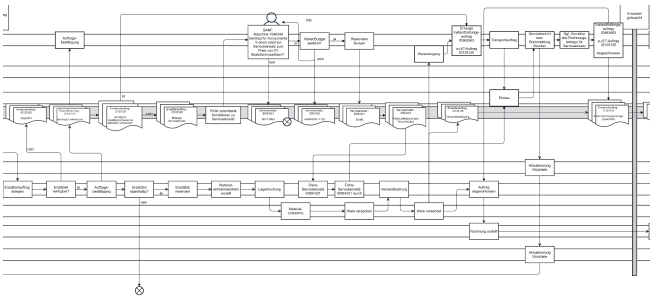

Abbildung 5.6: Die erfolgte Bestellung stößt den Prozess zur Materialbereitstellung an. Optionale Varianten können eine Unterbeauftragung an Sublieferanten, oder eine zusätzliche Buchung eines Serviceeinsatzes sein.

Berechnung zum Zustand einer spezifischen Komponente stattfindet, wird der Hashwert des zu verarbeitenden Datenpakets mit dem auf der Blockchain verankerten Wert abgeglichen. Dies garantiert die Korrektheit der Ergebnisse und schafft eine Vertrauensbasis für die nachgelagerten Geschäftsprozesse. In Smart Contracts kodifizierte Vertragsvereinbarungen ermöglichen darüber hinaus eine Disintermediation und Automatisierung der Lieferkette.

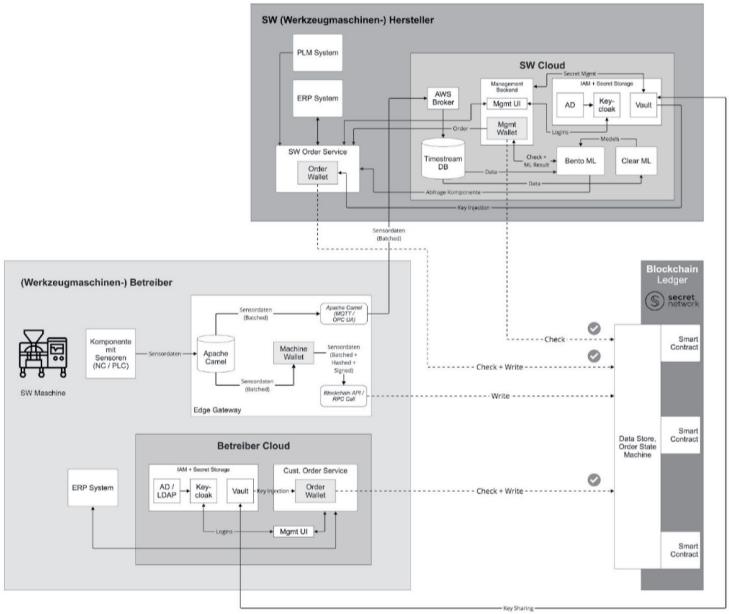

Abbildung 5.7: COSMIC-X Architektur im Use-Case *Vertrauenswürdige Lieferkette*

Weitere Zusammenhänge der bisher beschriebenen Module und Abläufe finden sich zudem in Abbildung 5.7, die einen Ausschnitt der in COSMIC-X umgesetzten Gesamtarchitektur repräsentiert.

5.4.2 Digitaler Zwilling zur Bereitstellung von Maschinendaten

Der in diesem Abschnitt vorgestellte Use-Case hat das Ziel, Maschinendaten bzw. Daten eines Hydraulikaggregates der HAWE Hydraulik SE für die Kunden und Service Provider verfügbar zu machen. Wichtig ist es dabei sowohl, historisch aufgezeichnete Daten als auch Live-Daten zur Verfügung zu stellen. Historische Daten werden verwendet, um bspw. Machine Learning Modelle trainieren und testen zu können. Live-Daten sollen angeboten werden, damit das Verhalten des trainierten Modells im Live-Betrieb evaluiert werden kann. Im Folgenden wird beschrieben, wie die Hydraulikdaten verfügbar gemacht wurden, über welche Schnittstellen kommuniziert wird und wie die Verwaltungsschale in dem Kontext eingesetzt wird.

Retrofit Industrie 4.0 - Hydraulikdaten verfügbar machen

Die Hydraulik der HAWE Hydraulik SE wird unter anderem in Werkzeugmaschinen eingesetzt, bspw. zum Verklemmen von Werkstücken auf dem Arbeitstisch, zum Arretieren desselben oder auch um ein Ausgleichsgewicht in der Spindel der Werkzeugmaschine zu schaffen, damit die Spindelantriebe weniger Last gegen die Erdgravitation zu bewegen haben. Da die HAWE Hydraulik SE eine hohe Fer-

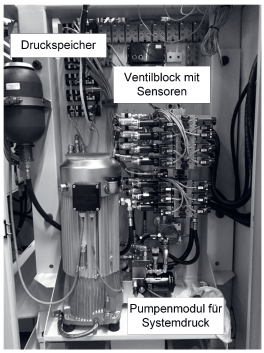

Abbildung 5.8: Hydraulikaggregat mit Zusatzsensorik für die Datenbereitsstellung, in einer Werkzeugmaschine [13]

tigungstiefe besitzt, ist sie im Besitz von Werkzeugmaschinen, die mit HAWE Hydraulik ausgestattet sind. Dieser Vorteil wurde im Rahmen eines internen Projektes ausgenutzt, wobei die Hydraulik mit weiterer Sensorik ausgestattet wurde, um Daten über die Hydraulik im Maschineneinsatz bereitzustellen / aufzuzeichnen. Die Daten der Hydraulik werden mit Betriebsdaten der Maschine aggregiert, um die Hydraulikdaten mit dem Betriebszustand (Produktion, Leerlauf etc.) der Maschine in Verbindung zu bringen. Abbildung 5.8 zeigt die Hydraulik, bestehend aus Pumpenmodul, die für den korrekten Systemdruck sorgt, den Ventilblock, der die hydraulischen Funktionen in der Maschine realisiert und den Druckspeicher, der den Systemdruck der Pumpe speichert und bereitstellt. Um für Forschungsprojekte, wie das vorliegende, Daten zur Verfügung zu haben, wurden über zwei Jahre Daten einer Maschine aufgezeichnet. Diese Daten wurden im Forschungsprojekt über zwei Dienste bereitgestellt. Zum einen sind sie in einer Datenbank gespeichert und können zum Training und Testen von Machine Learning Modellen verwendet werden (Abschnitt 5.3.4). Zum anderen werden die Daten als

Live-Daten über OPC UA angeboten. Die Bekanntmachung beider beiden Diensten geschieht über die Verwaltungsschale, die im Folgenden beschrieben wird.

Die AAS als Informationsbasis

Um die Betriebsdaten standardisiert bereitzustellen, werden die Verwaltungsschale (AAS) und standardisierte Teilmodelle der IDTA verwendet (Siehe Abschnitt 5.3.3). Die Besonderheit für den Einsatz dieser Technologie ist deren formale Beschreibung, also die syntaktische und semantische Eindeutig- und Interpretierbarkeit. Das ermöglicht jedem Nutzer entsprechende Informationen aus den jeweiligen Teilmodellen zu verwenden und zu verstehen, die von der IDTA standardisiert und freigegeben sind.

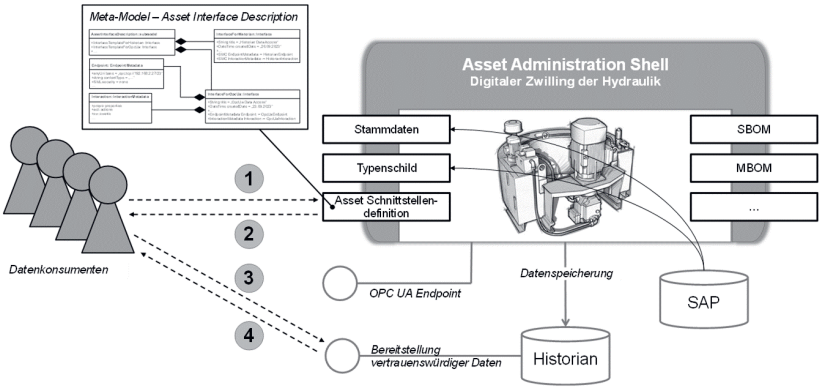

Abbildung 5.9: Verwendung der Asset Administration Shell im User-Case Digitaler Zwilling

Die AAS wird im Rahmen des Forschungsprojektes eingesetzt, um Informationen über die Hydraulik (das Asset) öffentlich einsehbar zu machen, so dass Kunden und Service Provider auf die AAS und deren Teilmodelle lesend zugreifen kann. Für den Digitalen Zwilling der Hydraulik wurden verschiedene Teilmodelle in der AAS eingesetzt, die in Abbildung 5.9 gezeigt werden. Zum einen werden Stammdaten und das digitale Typenschild als Teilmodelle angeboten (Abbildung 5.9, links), um die Hydraulik und deren Typ eindeutig zu identifizieren. Als Typ ist hierbei gemeint, ob es sich bspw. um eine Pumpe oder ein Proportionalschieberventil handelt. Die entsprechenden Informationen werden dafür aus dem unternehmensinternen SAP extrahiert und in den entsprechenden Parametern des AAS-Teilmodells eingefügt. Zum anderen wurde das Teilmodell Asset Interface Description (AID) angewendet [14]. Dieses Teilmodell spezifiziert ein Informationsmodell und eine gemeinsame Darstellung zur Beschreibung der Schnittstelle(n) eines Asset-Dienstes. Auf der Grundlage dieser Informationen ist es möglich, eine Verbindung zu einem solchen Dienst herzustellen und Datenpunkte anzufordern oder zu abonnieren und/oder Operationen durchzuführen. Im Rahmen des Forschungsprojektes wurde das AID-Teilmodell verwendet, um die angebotenen Dienste der Hydraulik abzubilden. Die Dienste sind hierbei Datenbereitstellungsdienste, um Datenpunkte - bspw. Spanndruck, Systemdruck oder auch Rücklauftemperatur des Öls in der Hydraulik - auf verschiedene Weise anbieten zu können. Zum anderen werden diese Datenpunkte durch zwei Dienste angeboten:

1. Historisch aufgezeichnete Langzeitdaten
2. Live-Daten über OPC UA

Bezogen auf Abbildung 5.9 können Datenkonsumenten das Teilmodell AID via REST API anfragen, welche Datenzugriffspunkte vorhanden sind (Abbildung 5.9, 1). Die AAS gibt die Zugriffsmöglichkeiten bekannt (Abbildung 5.9, 2). Der Datenkonsument fragt die gewünschte Schnittstelle an (Abbildung 5.9, 3) und empfängt die Daten bzw. den Endpoint für die OPC UA Subscription (Abbildung 5.9, 4). Die aktuell genutzte Version 1.0 spezifiziert laut IDTA lediglich Modbus, MQTT und HTTP, dennoch kann es auch genutzt werden, um zumindest rudimentär notwendige Zugriffpunkte zu spezifizieren. Es ist eine weitere Version der IDTA in Planung, die auch eine vollständige Beschreibung von OPC UA vorsieht und somit der hier vorgeschlagene Ansatz übertragen werden kann. Im Rahmen des Forschungsprojekts wurden Langzeitdaten der Hydraulik den Projektpartnern von inovex bereitgestellt, damit Machine Learning Modelle trainiert und getestet werden können. Aufgrund real bestehender IT-Security-Hürden war es im Zuge dieses Projekts nicht möglich, Daten einer realen Hydraulik via OPC UA aus dem Unternehmensnetzwerk heraus anbieten zu können, da hierfür ein Tor in die Produktion geöffnet werden muss, was einen möglichen Angriffsvektor darstellt. Stattdessen wurde eine Serverapplikation entwickelt, die die aufgezeichneten Hydraulikdaten via OPC UA abspielt, um das Machine Learning Modell im Live-Betrieb zu evaluieren. Durch die Anwendung von OPC UA sind die Standardzugriffe auf die abgespielten Daten jedoch identisch zu einer realen Hydraulik oder auch realen Maschine, so dass der hier vorgestellte Ansatz mit minimalem Aufwand auf reale Assets übertragbar ist. Die entsprechenden Daten wurden mithilfe der COSMIC-X Blockchain Lösung vertrauenswürdig gemacht (siehe Kapitel 5.3.2). Ähnlich wie im Use Case "Vertrauenswürdige Lieferkette" (siehe Kapitel 5.4.1) werden Datenpakete auf dem Secret Network verankert und in der Verwaltungsschale zum Abgleich referenziert. Datenkonsumenten können also sicherstellen, ob bspw. die Maschine Learning Modelle mit vertrauenswürdigen Daten trainiert und getestet wurden. Durch eine zukünftige Nutzung von SSI-Methoden durch Gaia-X können Use Cases wie dieser ermöglicht werden.

5.4.3 Plattformbasierte Wartung

In diesem Use Case werden Optimierungspotenziale für Betrieb und Wartung von Infrastruktur in unterschiedlichen Anwendungen der Prozessindustrie erforscht. Eine zentrale Rolle spielt dabei die IIoT-Plattform des Konsortialpartners KROHNE und die Evaluierung der Verwendung von Gaia-X-Föderationsdiensten, die die sichere Verwendung von Daten gewährleisten soll. Um den Betrieb und die Wartung von Maschinen zu verbessern, wurde im Rahmen des Forschungsprojekts eine neue Art der Verbindung von sich im Feld bzw. in einer Anlage befindlichen KROHNE Messgeräte mit der Cloud umgesetzt. Dabei wurden Durchflussmessgeräte über ein Gateway mit der IoT Plattform verbunden, in der die durch Messgeräte erhobenen Daten anschließend gespeichert, aggregiert und visualisiert werden. Der Kunde selbst und der KROHNE Service können diese Daten einsehen. Darüber hinaus wird der Serviceprozess durch Methoden des Natural Language Processings (NLP) optimiert. Dazu wurde im Rahmen des Forschungsprojekts ein Chatbot Service entwickelt, der es möglich macht, interaktiv in natürlicher Sprache Handbücher und Anleitungen zum Troubleshooting von KROHNE Geräten zu durchsuchen. Die Verbindung von Geräten und Plattform wurde mittels des HART-Kommunikationsprotokolls über ein Gateway hergestellt und die Daten auf der Datenplattform gespeichert. Zur Provisionierung der Edge- & Cloud-Komponenten wurden Ansätze für zertifikatsbasierte Authentifizierung für die Gateways untersucht. Außerdem wurde eine Security- und Auditierungstrategie für die Plattform entwickelt und Gaia-X Komponenten in diesem Zusammenhang betrachtet. Mögliche Komponenten wurden evaluiert und die Anwendung ist in Planung, bisher konnte allerdings noch kein abschließendes Mapping der Komponenten zu den KROHNE Anforderungen gefunden werden. Die aufgenommenen Daten wurden je Kunde zu Analysezwecken auf der Datenplattform aggregiert und visualisiert. Direkt einsehbar ist der Zustand des Geräts und Messwerte des Geräts über die

Zeit, sowie Ergebnisse von Gerätetests. Dadurch wurde die Voraussetzung für den Zeitreihenvergleich von Daten geschaffen. Probleme können dadurch frühzeitig aus der Ferne erkannt werden, da der Service mit einem Tablet remote Informationen auslesen und zusätzliche Überprüfungsmechanismen verwenden kann, um frühzeitig zu entscheiden, ob Wartungs- und Reparatureinsätze notwendig sind, und diese entsprechend zu planen. Die aufgenommenen Daten sollten außerdem weiterverwendet werden, um Predictive Maintenance und insbesondere Federated Learning Ansätze zu realisieren. Es hat sich früh herausgestellt, dass dazu keine Daten in ausreichender Menge und Qualität bereitgestellt werden können, weshalb der Ansatz von Machine Learning auf Daten aus dem Feld für vorausschauende Wartung nach diesem (Zwischen-) Ergebnis nicht weiterverfolgt wurde. Stattdessen wurde der Fokus im KI-Bereich auf die Entwicklung eines Chat Assistenten verschoben. Dieser wurde in Zusammenarbeit mit inovex nach den Anforderungen des KROHNE Service entwickelt. Der Chatbot ermöglicht die Durchsuchung mehrerer Datenquellen und ist an die Anforderungen aus dem KROHNE Umfeld angepasst. Die Interaktion mit dem Bot erfolgt in Slack über den Austausch von Nachrichten. Die Qualität der Antworten konnte dabei kontinuierlich verbessert werden. Besonderer Wert wurde bei der Entwicklung auf Datenschutz und Sicherheit gelegt. In Zusammenarbeit mit den Konsortialpartnern stackable und HFU wurden hierzu Sicherheitsanforderungen und mögliche Gefährdungen im Kontext von Ansätzen aus dem Gaia-X Umfeld untersucht. Dabei wurde insbesondere der Aspekt der Autorisierung und Authentifizierung betrachtet. Durch die Übersicht und die Möglichkeit des Remote Zugriffs auf Daten von den Messgeräten im Feld in der Kombination mit Zugriff auf Dokumentation und Hilfestellung zur Problemlösung in natürlicher Sprache konnten so im Forschungsprojekt prototypisch Prozesse und Infrastruktur optimiert betrieben und gewartet werden. Das Servicepersonal hat nun die Möglichkeit, Probleme schon aus der Ferne besser einschätzen und sich daher besser auf Einsätze vorbereiten zu können.

5.4.4 Kontinuierliche Betrachtung der COSMIC-X Bedrohungslandschaft

Eine kontinuierliche Betrachtung der COSMIC-X Architektur über den Projektverlauf hinweg und der Prüfung ausgewählter Sicherheitsanforderungen an die Implementierungen wirkte sich u. A. auf das Design verschiedener Komponenten, Datenflüsse und den angewandten Protokoll aus. Dabei ist ebenfalls ein durchgängiges Sicherheitskonzept bzgl. der verwendeten Technologien und Konzepten wie Virtualisierung, Containerisierung, und deren operativen Betrieb in Clustern notwendig. Mit der Erarbeitung von Sicherheitsmaßnahmen im Hinblick auf den Einsatz verschiedener Schlüsseltechnologien wie etwa OPC/UA wurden auch verschiedene Aspekte der Datensicherheit, Anforderungen an zu speichernde Metainformationen oder details der Laufzeitumgebungen von Systemkomponenten diskutiert. Die Bewertung der Sicherheit von Szenario-spezifischen Konfigurationen und Zusammensetzungen einzelner Komponenten basierte auf mehreren bewährten Strategien zur umfassenden Sicherheitsbewertung der COSMIC-X Architektur. Eine systematische Bedrohungsanalyse wurde hierbei mit der STRIDE Methodik realisiert, wodurch klassische Bedrohungen innerhalb der Systemarchitektur aufgedeckt wurden. Eine separate Betrachtung der Use-Cases in eigenständigen Bedrohungsmodellen ermöglichte dabei auch eine szenariospezifische Einordnung von Risiken einzelner Systemmodule. Die kontinuierliche Modellierung über den Projektverlauf hinweg ermöglicht eine dynamische Bewertung der Bedrohungslandschaft in der jeweiligen Iteration der Architektur. Unter Betrachtung der MITRE ATT&CK Datenbank [15] wurden potentielle Schwachstellen mit realen Angriffstechniken abgeglichen und im Kontext von COSMIC-X analysiert. Dabei lag der Fokus neben der systematischen Bewertung von relevanten Angriffstechniken vor allem auf der Realisierung von klassischen Sicherheitsanforderungen wie Datenverschlüsselung oder der Isolierung verschiedener Services mittels Virtualisierungs- bzw. Containerisierungsmechanismen. Da neuartige KI-basierte Technologien auch zusätzliche bzw. bisher unbedeutende Sicherheitsrisiken ermöglicht, wurden unter zusätzlicher Verwendung der MITRE

ATLAS (Adversarial Threat Landscape for Artificial-Intelligence Systems) Wissensdatenbank [16] bekannte Taktiken und Techniken von Angriffen auf KI-basierte Systeme berücksichtigt. Beisielsweise ist die Eingabevalidierung ein zentraler Punkt der Sicherheit von LLMs, wie im KROHNE Use-Case verwendet, die entscheidend für die Qualität der anschließenden Bearbeitung der Anfrage ist. Eine Überprüfung dieser Eingaben auf böswillige Inhalte, wie die Aufforderung zur Extraktion interner Wissensquellen oder interner Systemdetails, kann dabei Angriffsvektoren der an den Chatbot angebundenen Systeme abschwächen oder verhindern. Eine strenge Zugriffskontrolle sowie Authentifizierungsmechanismen für den Schutz sensibler Informationen, welche dem Chatbot zugänglich gemacht werden sollen, sind somit unerlässlich. Im speziellen Fall des KROHNE Demonstrators wird die Chatbot-Anwendung durch die 3rd-Party Platform "Slack" abgeschirmt und ist nur mittels expliziter Einladung zugänglich. Die Datenqualität wird durch den Betrieb und visuelle Dashboards geprüft. Während der Modellentwicklung ist der Schutz vor Manipulation wie Prompt Injection von großer Bedeutung. Durch regelmäßige Modell-Updates auf Grundlage neuer Daten, die durch Feedbackschleifen mit den Anwendern entstehen, kann sowohl die Leistungsfähigkeit der Modelle garantiert, als auch aufgedeckte Sicherheitslücken geschlossen werden. Neben dem Risiko von für das Training schädlichen Daten (Data Poisoning) muss ebenfalls der Kontext der operativen Infrastruktur und Auswirkungen auf Dienste des Ökosystems betrachtet werden. Im Kontext der Anwendung von auf künstlicher Intelligenz basierenden Systemen müssen auch neue Aspekte, wie bspw. Voreingenommenheit im Bezug auf bestimmte Themengebiete, (weiter)Verbreitung schädlicher Inhalte oder das Risiko der Halluzination, bei der das LLM eine möglichst passende, aber meist falsche Antwort erfindet, beachtet werden.

5.5 Diskussion & Fazit

Die durch Gaia-X definierten Mechanismen zum Austausch von Daten können ebenfalls in verschiedenen Aspekten der vorgestellten Use-Cases implementiert werden. Ein weiterführender Gedanke beinhaltet eine durchgängige Nutzung der sog. *Data Products*, welche in einem förderierbaren Katalog referenziert werden (Abbildung 5.10). So ergeben sich Szenarien, in denen bspw. eine von HAWE entwickelte Hydraulik spezifische Datensätze generiert, die anschließend von inovex zur Erstellung eines ML-Modells im Katalog gefunden und unter Verwendung eines sog. *Data Product Usage Contract* zur Verfügung gestellt werden. Obwohl Details des tatsächlichen Datenaustauschs wie die Bereitstellung von Realdaten und der Zugriff auf im Vertrag definierte Datenobjekt nicht von Gaia-X vorgeschrieben sind, kann die Wiederverwendung der Verifiable Credentials zur Authentifizierung am entsprechenden Service eine elegante Designentscheidung sein. In einem nächsten Schritt kann wiederum inovex ein auf den Hydraulikdaten basierendes Modell als Produkt im Katalog registrieren, welches nachfolgend in selber Manier von HAWE durch einen Usage Contract erworben und in beliebige Prozesse integriert werden kann.

Mit der Definition derartiger Datenstrukturen in einem AAS-spezifischen Submodell könnten zukünftig sowohl Produkte wie Daten oder Dienste, als auch ganze industrielle Prozesse näher an eine Konformität mit Gaia-X Umgebungen gebracht werden. Ein derartiges Vorgehen zum sicheren und auditierbaren organisationsübergreifenden Datenaustausch könnte zukünftig mit Gaia-X Bausteinen konfigurierbar gemacht werden.

Die Blockchain bildet in COSMIC-X eine unternehmensübergreifende Vertrauensebene, mit deren Hilfe sich komplexe Geschäftsprozesse vereinfachen und automatisieren lassen. Die Wahl des *Secret Network* als Blockchain-Plattform für COSMIC-X ist dabei von entscheidender Bedeutung, denn es erfüllt eine Reihe von kritischen Anforderungen, die für den industriellen Einsatz unerlässlich sind. So ist der Schutz sensibler Daten im industriellen Kontext eine absolute Notwendigkeit. Mithilfe von Ende-zu-Ende-Verschlüsselung und einem darauf aufbauenden Konsensmechanismus, ermöglicht das Secret Network eine vertrauliche Datenverarbeitungskette über eine beliebige Anzahl an Entitäten abzubilden, ohne Daten ungewollt preiszugeben. Im Fall von COSMIC-X werden Sensordaten von produzierenden

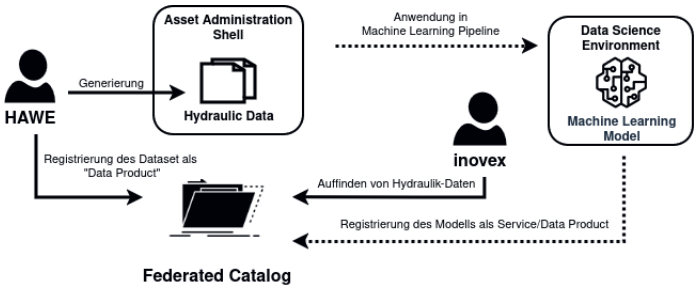

Abbildung 5.10: Sicherer Datenaustausch mit dem Gaia-X Federated Catalog

Maschinen signiert und auf dem Secret Network verankert, um deren Integrität für die spätere Verarbeitung durch Machine Learning Modelle sicherzustellen. Die integrierte Mandantenfähigkeit erlaubt die Nutzung einer gemeinsamen öffentlichen Blockchain für alle Use Cases und Nutzer, was einen hohen Grad an Resilienz, Skalierbarkeit und Kosteneffizienz mit sich bringt. Für COSMIC-X bedeutet dies, dass die Blockchain in der Lage ist, eine große Anzahl an Transaktionen und Prozessen zu unterstützen, ohne exponentiell steigende Infrastrukturkosten zu verursachen. Trotz Verschlüsselung bleibt die Blockchain dabei auditierbar. Mit *Viewing Keys* können Data Owner selektiven Zugriff auf vertrauliche Daten gewähren, um Ergebnisse entlang der Datenverarbeitungskette verifizierbar zu machen und Compliance Anforderungen zu erfüllen. Als Teil des Cosmos-Ökosystems [17] ist das *Secret Network* zudem so konzipiert, dass es mit anderen Cosmos-basierten Blockchain-Protokollen interagieren kann. So ist es möglich, die im Rahmen von COSMIC-X entstandene Lösung zukünftig an andere Plattformen innerhalb des Ökosystems anzubinden. Zusammenfassend bietet die Blockchain-Lösung auf Basis des *Secret Network* einen maßgeschneiderten Ansatz für die vertrauenswürdige Datenverarbeitung und Automatisierung von Geschäftsprozessen in der Industrie 4.0. Zukünftige Forschung könnte sich darüber hinaus mit der Integration eines Peer-to-Peer-Bezahlsystems befassen, sodass Maschinen für von ihnen bestellte Ersatzteile autonom bezahlen können.

In der Umsetzung der einzelnen Use Cases wurden aufgrund verschiedenen Datenformen unterschiedliche ML-Verfahren angewendet. Dabei hat sich im Bereich der Anomalieerkennung von Maschinendaten gezeigt, dass es nicht ein einzelnes optimales Verfahren gibt, sondern je nach Betrachtung der Komponentengruppen ein anderes Verfahren bessere Ergebnisse liefert. Als vielversprechendste Methoden wurden Local Outlier Factor, DBSCAN und Isolation Forest ausfindig gemacht. Diese liefern abhängig von der gewählten Komponente die besten Ergebnisse. Die unterschiedlichen Methoden sind innerhalb des Demonstrators für den Benutzer zugänglich gemacht, so dass mit Hilfe von Domänenwissen die beste Auswahl getroffen werden kann. Die Verwendung von Isolation Forests erlaubt zudem die Interpretation der Ergebnisse mit Hilfe von XAI (Explainable AI). Somit ist es möglich, die mathematischen Resultate besser und verständlicher aufbereitet zu präsentieren und zu interpretieren. Die Anwendung von XAI ergab sich aus der Limitation, dass sich der geplante Ansatz für Federated Learning nach genauerer Betrachtung für keinen der Use Cases eignet. Im Use Case *Plattformbasierte Wartung* wurden LLMs verwendet und untersucht. Dabei hat sich gezeigt, dass für das Auffinden von Text in Handbüchern kein Training oder Finetuning von LLMs notwendig ist. Stattdessen konnte auf den etablierten Ansatz des RAG (Retrieval Augmented Generation) gesetzt werden und die Suche der Daten mit bewährten Methoden wie Vektorsuche umgesetzt werden. Im Anschluss wurden die gefundenen Antworten an den Benutzer durch das LLM generiert. Als bestes LLM hat sich gpt-3.5-turbo von OpenAI gezeigt, da dieses besonders schnell und zuverlässig Antworten generiert hat. Mit Hilfe von Phoenix wurden auch andere Open Source Modelle verglichen, allerdings konnten

weder LLama noch Mistral bei der Qualität der Antwort und der Geschwindigkeit aufgrund fehlender GPU mithalten. In der Zukunft lässt sich mit größeren Open Source Modellen und einer GPU erneut ein Vergleich durchführen. Da die Modelle sich rasant weiterentwickeln und große Fortschritte machen, ist es denkbar OpenAI durch ein Open Source Modell abzulösen.

Literaturverzeichnis

[1] Bundesministerium für Wirtschaft & Klimaschutz. Das projekt gaia-x. eine vernetzte dateninfrastruktur als wiege eines vitalen, europäischen Ökosystems, 2019. URL https://www.bmwk.de/Redaktion/DE/Publikationen/Digitale-Welt/das-projekt-gaia-x.html.

[2] Bundesamt für Sicherheit in der Informationstechnik. It-grundschutz-kompendium, 2020. URL https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/it-grundschutz-kompendium_node.html.

[3] Bundesministerium für Wirtschaft und Klimaschutz. Gaia-x: Driver of digital innovation in europe. featuring the next generation of data infrastructure, 2020. URL https://www.bmwk.de/Redaktion/EN/Publikationen/gaia-x-driver-of-digital-innovation-in-europe.html.

[4] Sarah Lochter, Manfred; Maßberg. Sicherheit der blockchain-technologie, 2018. URL ... BSI-Forum, 2018#3, Jahrgang 26.

[5] Gaia-X European Association for Data and Cloud AISBL. Gaia-x – architecture document: 22.10 release, 2022. URL https://docs.gaia-x.eu/technical-committee/architecture-document/22.10/.

[6] Verband der Internetwirtschaft e.V. und Gaia-X European Association for Data and Cloud AISBL. Gaia-x-sichere und vertrauenswürdige Ökosysteme mit souveränen identitäten: Entwicklung eines dezentralen, benutzerzentrierten und sicheren cloud-Ökosystems, 2022. URL https://www.gxfs.eu/de/ssi-white-paper/.

[7] World Wide Web Consortium. Verifiable credentials data model v1.1.w3c recommendation, 2022. URL https://www.w3.org/TR/vc-data-model.

[8] World Wide Web Consortium. Decentralized identifiers (dids) v1.0: Core architecture, data model, and representations. w3c recommendation, 2022. URL https://www.w3.org/TR/did-core/.

[9] Gaia-X European Association for Data and Cloud AISBL. Idp bridge, 2024. URL https://gitlab.com/gaia-x/data-infrastructure-federation-services/deployment-scenario/idp-bridge.

[10] SecretNetwork. Secret network blockchain, 2024. URL https://scrt.network/.

[11] PreCom. Predictive cognitive maintenance decision support system, 2021. URL https://doi.org/10.3030/768575.

[12] VDI Nachrichten. Vdi-nachrichten vom 12.07.24, ausgabe 14, 2024. URL https://www.ikiosk.de/shop/epaper/vdi-nachrichten/1359148.html.

[13] Wolfgang Sochor, Christof Gilnhammer, Christian Hermer, and Jens Folmer. Retrofit industrie 4.0 – maschinenanbindung einer heterogenen maschinenflotte bis in die cloud. In Klaus-Jürgen Meier and Matthias Pfeffer, editors, *Produktion und Logistik in der digitalen Transformation: Analyse – Planung – Praxiserfahrungen*, pages 233–249. Springer Fachmedien Wiesbaden, Wiesbaden, 2022. ISBN 978-3-658-36560-8. doi: 10.1007/978-3-658-36560-8_14. URL https://doi.org/10.1007/978-3-658-36560-8_14.

[14] Industrial Digital Twin Association e.V. Asset interface description, January 2024. URL https://github.com/admin-shell-io/submodel-templates/tree/main/published/Asset%20Interfaces%20Description/1/0.

[15] The MITRE Corporation. Adversarial tactics, techniques, and common knowledge (att&ck), 2024. URL https://attack.mitre.org/.

[16] The MITRE Corporation. Adversarial threat landscape for artificial-intelligence systems (atlas), 2024. URL https://atlas.mitre.org/.

[17] Interchain Foundation (ICF). Cosmos blockchain network, 2024. URL https://cosmos.network/.