Dieses Buch gibt einen Überblick über die Desktop-Forschung und beleuchtet die Aspekte der Fernwartung in der Produktion, die in Qualifizierungskursen für die Wissenschaft und die Industrie berücksichtigt werden müssen.

RE-MAIN

Co-funded by the European Union

ISBN 978-3-20008-802-3

RE-MAIN

Co-funded by the European Union

REMOTE MAINTENANCE

Needs analysis for education and training

FERNWARTUNG

Bedarfsanalyse für allgemeine und berufliche Bildung

RE- MAIN Konsortium

Erste Ausgabe erschienen bei Selver Softic (CAMPUS 02 Hochschule für angewandte Wissenschaften) für das RE-MAIN Konsortium 2022

Erste Ausgabe

Autor: Roger Mouzo
Autor: Omar Busquests
Autor: Mirco Lovisetto
Autor: Liam Moore
Autor: Raymond Wolfe
Autor: Andrew de Juan
Autor: Michael Murray
Autor: Martin Hill
Autor: Pablo Paino de Pedro Autor: Gregor Kandare
Autor: Ioan Turcin Autor: Selver Softic
Bearbeitung: Selver Softic

Die Unterstützung der Europäischen Kommission für die Erstellung dieser Veröffentlichung stellt keine Billigung des Inhalts dar, welcher nur die Ansichten der Verfasser wiedergibt, und die Kommission kann nicht für eine etwaige Verwendung der darin enthaltenen Informationen haftbar gemacht werden

Vorwort

> ***"Die Technologie ermöglicht es den Menschen heute jederzeit und überall mit jedem auf der Welt von fast jedem Gerät aus in Verbindung zu treten. Diese verändert die Art und Weise, wie Menschen arbeiten, dramatisch und erleichtert die Zusammenarbeit mit Kollegen, die über Zeitzonen, Länder und Kontinente verstreut sind, rund um die Uhr." -***
> ***Michael Dell***

Danksagung

Wir danken der spanischen Erasmus+ Nationalagentur und der EU für die Finanzierung des ReMain-Projekts und die Unterstützung der Verbesserung der Qualifikationen im Bereich der Fernwartung.

Die spanische Nationale Agentur für die Entwicklung und Verwaltung des Programms Erasmus+ (SEPIE) hat das Projekt RE-MAIN (REmote MAINtenance of Smart Industry Installations) 2021-1-ES01-KA220-VET-000033027 im Rahmen der Leitaktion 2 (KA2) ZUSAMMENARBEIT ZWISCHEN ORGANISATIONEN UND EINRICHTUNGEN des Programms ERASMUS+ genehmigt.
Programm. Das ReMain-Projekt wird vom CRN Leganés geleitet und umfasst vier weitere europäische Partner aus Irland, Österreich, Italien und Spanien (Barcelona).

Co-funded by the European Union

Inhaltsübersicht

Eine

Einführung

Zu den Zustand von Fernwartung in Partnerländern

Selver Softic, Ioan Turcin, CAMPUS 02 University of Applied Science, Graz, Österreich, selver.softic@ campus02.at , ioan.turcin@ campus02.at

***

Dieses Kapitel bietet eine kurze Einführung in die Definition von Fernwartung und beschreibt die relevanten Technologien anhand einer kurzen Literaturübersicht. Als integraler Bestandteil dieses Kapitels werden die kumulierten Ergebnisse der in Österreich, Italien, Irland und Spanien durchgeführten Umfrage zum Bewusstsein für Fernwartung vorgestellt und als Ausblick auf mögliche Qualifikationslücken diskutiert.

Keywords: introduction, state of the art, remote maintenance, survey

1. Einführung

Das Wort "abgelegen" kann auf verschiedene Weise interpretiert werden. In der Regel bedeutet es "nicht am tatsächlichen Standort". Dies bedeutet, dass das Fachwissen von einem anderen Ort herangezogen wird. Dabei kann es sich um einen lokalen Experten handeln, der von einem Büro aus arbeitet, oder um einen Spezialisten, der von außerhalb der eigentlichen Einrichtungen arbeitet.

Die grundlegende Definition von "Fernwartung" besagt, dass Computersysteme von einem entfernten Standort aus überwacht und gesteuert werden können. Dies geschieht im Wesentlichen durch die Installation von Software auf lokalen Systemen, auf die von anderen Standorten aus zugegriffen werden kann.

Sehr oft arbeiten diese Systeme über eine Internetverbindung, obwohl die Software auch lokale Analysen durchführen, kritische und unkritische Situationen ermitteln und Rückmeldungen für Präventivmaßnahmen senden kann. Dies erfordert die Interoperabilität der Netze, sowohl der lokalen als auch der dezentralen Systeme und Diensteanbieter. Intern wird es ein Intranet geben

Lösung werden externe Dienste über eine Internetverbindung betrieben. Diese Dienste werden in der Regel als "Cloud-Dienste" bezeichnet, was für alle digitalen Dienste gilt, die über verschiedene Internetkanäle übertragen werden.

Es ist auch klar, dass die Sicherheit eine wichtige Rolle bei der Aufrechterhaltung einer sicheren und funktionalen Umgebung spielt. Jedes System, das mit einem anderen Gerät verbunden ist, ist angreifbar. Daher sind ausgereifte und tief durchdachte Szenarien für die Cybersicherheit fast ein Muss.

Insgesamt können wir sagen, dass die "Fernwartung" eine anspruchsvolle Aufgabe ist, die Kosten spart und die Nachhaltigkeit und Langlebigkeit der Systeme fördert. Es gibt jedoch eine Reihe von Fähigkeiten und Technologien, die diese Art von Unterstützung und Wartung möglich machen.

2. ERMÖGLICHENDE TECHNOLOGIEN

In diesem Kapitel werden die wichtigsten Technologien für die Fernwartung vorgestellt und ihr Beitrag zum Gesamtkonzept erörtert.

2.1 Internet of Things und Cloud Computing

Das Grundkonzept hinter dem Internet der Dinge (Io T) ist das Konzept der Verbindung jedes eindeutig identifizierbaren Geräts mit dem Internet und mit anderen angeschlossenen Geräten. Mittlerweile beeinflusst das Internet der Dinge (Io T) unser tägliches Leben und Cloud Computing spielt als infrastrukturelle Umsetzung eine bedeutende Rolle. Das Io T ermöglicht es, Menschen und Dinge (z.B. Sensoren, Aktoren und intelligente Geräte) ubiquitär und jederzeit zu vernetzen. Dies ist eine der Hauptvoraussetzungen für die "Fernwartung". Io T ist auch eine der Grundlagentechnologien für die "Fernwartung", und ihre Anwendung nimmt dramatisch zu, ebenso wie die Nachfrage nach zuverlässigen cloudbasierten Anwendungen, die auf gut geplanten und leistungsfähigen Algorithmen für Sensornetzwerke beruhen [1] Die Anwendungsbereiche von Io T sind vielfältig und reichen von der intelligenten Verwaltung städtischer Infrastrukturen wie Parkplätzen [2] über die Bewältigung von Sicherheitsproblemen in 5G-Netzwerken [3] bis zur Verwaltung intelligenter Energienetze [4] und der Unterstützung von Fernwartungsaufgaben.

2.2 Big Data

Neben IoT ist Big Data eine wichtige Basistechnologie für die Fernwartung. Im Zusammenhang mit der Smart Factory und Ansätzen, die Methoden der künstlichen Intelligenz zur Vorhersage, Berechnung oder Verfolgung von Wartungsindikatoren nutzen, werden Big-Data-basierte Dienste in Zukunft eine entscheidende Rolle spielen [5,6]. Mit der Explosion globaler Daten wird der Begriff Big Data hauptsächlich zur Beschreibung riesiger Datensätze verwendet [7]. Im Wesentlichen zeichnen sich Daten durch drei Eigenschaften aus, die in Anlehnung an ihre englischen Bezeichnungen als die "drei V's" von Big Data bezeichnet werden: Volume, Velocity und Variety. Während Volume das ständig wachsende Datenvolumen beschreibt, bezieht sich Velocity auf die Geschwindigkeit des Datenverkehrs und Variety auf die Art der Daten, die in mehreren und unterschiedlich strukturierten Datenquellen vorkommen. Sehr oft wird diesem Konzept der Begriff Value als viertes "V" hinzugefügt. Ein (erweiterter) Nutzen kann entstehen, wenn große Datenmengen analysiert werden, um ein wirtschaftliches Verwertungspotenzial zu identifizieren [8, 9]. Big Data eröffnet somit neue Möglichkeiten, neue Nutzwerte zu entdecken und bereits vorhandene, aber verborgene Werte besser zu verstehen [8]. Im Vergleich zu herkömmlichen Datensätzen enthalten Big Data in der Regel große Mengen unstrukturierter Daten, die neue Herausforderungen mit sich bringen, z. B. die

effektive Organisation und Verwaltung solcher Datensätze und die Ermöglichung von Echtzeitdaten.

Zeitanalytik [7]. Big Data stellt auch einen Paradigmenwechsel in der Art und Weise der Datenanalyse dar. Daten werden nun durch Korrelationsanalysen und Mustererkennung "zum Sprechen gebracht", was bedeutet, dass Datenwissenschaftler als Experten für computergestützte Datenanalyse neues Wissen aus Big Data ableiten können. Heutzutage können weitaus mehr Daten als je zuvor analysiert werden, was neue Wege der Erkenntnisgewinnung ermöglicht. Die riesige Datenmenge ermöglicht es, durch geschickte Fragen an die Daten komplexe Zusammenhänge aufzudecken [8] und bei Bedarf präventiv zu handeln (z.B. Wartungsarbeiten).

2.3 Cybersicherheit

Cybersicherheit [17] ist die Praxis des Schutzes von Computern, Servern, mobilen Geräten, elektronischen Systemen, Netzwerken und Daten vor bösartigen Angriffen. Sie wird auch als Sicherheit der Informationstechnologie oder elektronische Informationssicherheit bezeichnet. Der Begriff findet in einer Vielzahl von Kontexten Anwendung, von der Wirtschaft bis zur mobilen Datenverarbeitung, und kann in einige allgemeine Kategorien unterteilt werden.
Unter Netzsicherheit versteht man den Schutz eines Computernetzes vor Eindringlingen, sei es

gezielte Angreifer oder opportunistische Malware.

Die Anwendungssicherheit konzentriert sich darauf, Software und Geräte frei von Bedrohungen zu halten. Eine kompromittierte Anwendung könnte den Zugriff auf die Daten ermöglichen, die sie schützen soll. Erfolgreiche Sicherheit beginnt bereits in der Entwurfsphase, lange bevor ein Programm oder Gerät bereitgestellt wird.

Die Informationssicherheit schützt die Integrität und die Privatsphäre von Daten, sowohl bei der Speicherung als auch bei der Übertragung.

Die betriebliche Sicherheit umfasst die Prozesse und Entscheidungen zur Handhabung und zum Schutz von Datenbeständen. Die Zugriffsrechte der Benutzer auf ein Netzwerk und die Verfahren, die bestimmen, wie und wo Daten gespeichert oder gemeinsam genutzt werden können, fallen alle unter diesen Begriff.

Disaster Recovery und Business Continuity legen fest, wie ein Unternehmen auf einen Cyber-Sicherheitsvorfall oder ein anderes Ereignis reagiert, das einen Betriebs- oder Datenverlust verursacht. Die Richtlinien für die Wiederherstellung im Katastrophenfall legen fest, wie das Unternehmen seinen Betrieb und seine Daten wiederherstellt, um die gleiche

Betriebskapazität wie vor dem Ereignis zu erreichen. Geschäftskontinuität ist die Plan, auf den die Organisation zurückgreift, wenn sie versucht, ohne bestimmte Ressourcen auszukommen.

Die Schulung der Endbenutzer befasst sich mit dem unberechenbarsten Faktor der Cybersicherheit: den Menschen. Jeder kann versehentlich einen Virus in ein ansonsten sicheres System einschleusen, wenn er sich nicht an gute Sicherheitsverfahren hält. Es ist für die Sicherheit eines jeden Unternehmens von entscheidender Bedeutung, den Benutzern beizubringen, verdächtige E-Mail-Anhänge zu löschen, keine nicht identifizierten USB-Laufwerke anzuschließen und viele andere wichtige Lektionen zu lernen.

2.4 Industrie 4.0 und Cyber Physical Systems

Industrie 4.0 beschreibt die vierte industrielle Revolution, getrieben durch Informations- und Kommunikationstechnologien (IKT) und das Internet der Dinge (IoT) [10]. International wird unter Industrie 4.0 die Digitalisierung der Industrie verstanden, mit dem Ziel der horizontalen und vertikalen Integration der Wertschöpfungsketten, wobei sowohl die Prozesse entlang der Wertschöpfungskette mit Lieferanten und Kunden als auch die Kommunikation zwischen Mensch, Maschine und Ressourcen

vollständig automatisiert werden sollen.

Die Idee der autonomen Steuerung und Optimierung von Produktionssystemen sowie intelligente Werkstücke sind ein integraler Bestandteil von Industrie 4.0 oder Smart Factory. Die technologische Voraussetzung dafür sind die sogenannten cyber-physischen Systeme (CPS). Unter CPS versteht man die Verbindung von eindeutig identifizierbaren physischen "Dingen" oder Objekten mit dem Internet oder anderen vergleichbaren virtuellen Strukturen, was dem IoT-Paradigma entspricht. Die Produktionsprozesse werden durch vernetzte CPS nicht nur aktiv gesteuert, sondern bieten mitunter auch Plattformen für innovative Geschäftsmodelle und Dienstleistungen. Damit muss nicht nur die Unternehmensstrategie angepasst werden, sondern auch die bestehenden "monoorganisatorischen" Geschäftsmodelle müssen völlig neu überdacht und definiert werden [11, 12, 13]. Einer der Hauptvorteile des IoT ist auch die Möglichkeit, digital vernetzte Produkte, Dienstleistungen und Lösungen zu nutzen, da die Hersteller versuchen, die Rolle des Kunden im Wertschöpfungsprozess zu vertiefen [14]. Die Vernetzung intelligenter Produkte erhöht die Qualität der Automatisierung und steigert damit die Wettbewerbsfähigkeit von Hochlohnstandorten [15]. Durch die Vernetzung von Produktionssystemen und die damit einhergehende Zunahme der Machine-to-Machine-Kommunikation (M2M) steigt nicht nur die Anzahl der benötigten und im System installierten Sensoren, sondern auch die

Gesamtkomplexität des Systems im Allgemeinen betroffen. Die Anhäufung von Sensoren und damit steigende Gesamtkomplexität als Folge der fortschreitenden Digitalisierung führt in letzter Zeit zur Erzeugung von Daten in großen Mengen, in diesem Zusammenhang auch als Big Data bezeichnet.

2.5 Augemented und Mixed Reality

Augmented Reality (AR) in der Fernwartung ist eine audiovisuelle Methode zur Systemanalyse und Unterstützung der Mitarbeiter bei Wartungsaufgaben. Die grundlegende Erklärung von Augmented Reality ist eine Überlagerung von digitalen Informationen über die tatsächliche Umgebung [18].

Ein in diesem Zusammenhang häufig verwendeter Begriff ist auch Mixed Reality (MR), ein Ansatz, bei dem die reale und die virtuelle Welt zusammengeführt werden, um neue Umgebungen und Visualisierungen zu schaffen. Mixed Reality findet weder ausschließlich in der physischen noch in der virtuellen Welt statt, sondern ist ein Hybrid aus Augmented Reality und Virtual Reality [16]. Um den Unterschied zu verdeutlichen: Augmented Reality findet in der physischen Welt statt.

Die virtuelle Realität (Virtual RealityVR) lässt Sie in eine vollständig virtuelle Welt eintauchen, ohne dass Sie in die physische Welt eingreifen müssen.

Mögliche Nutzungsszenarien wären zum Beispiel, dass AR-Brillen wie virtuelle Assistenten funktionieren, die sowohl akustische als auch visuelle Hinweise für den Nutzer geben. Einige dieser Funktionen sind offline verfügbar, während andere eine aktive Internetverbindung erfordern.

Bei der Fernwartung werden Augmented-Reality-Geräte zur Analyse und Kontrolle der Infrastruktur eingesetzt. In diesem Fall spielen sowohl der menschliche Aspekt als auch die Online-Konnektivität eine wichtige Rolle in der Gleichung.

Die AR/VR- oder MR-Fernwartung bietet eine neue Perspektive für das dezentrale Management von Hardware, Software und Personal, mit erheblichen Vorteilen für den Industriesektor.

3. UMFRAGE UND RESULTATE

Um das Bewusstsein lokaler Unternehmen für Fernwartung und entsprechende Technologien einzuschätzen, hat das RE-MAIN Konsortium

beschlossen, eine Umfrage durchzuführen und deren Ergebnisse bei der Vorbereitung der Qualifizierungskurse zu nutzen. Die Umfrage sollte einen tendenziellen Überblick über die Vertrautheit der Unternehmen aus den Partnerregionen mit dem Thema "Fernwartung" und den damit verbundenen Technologien geben. Außerdem sollte sie einige Orientierungshilfen für die Planung von Qualifizierungskursen im Bereich "Fernwartung" liefern.

Die Umfrage wurde von Anfang Juni bis Anfang August in Österreich, Italien, Irland und Spanien durchgeführt. In diesem Zeitraum erhielten die Partner 47 Antworten von lokalen Unternehmen: 18 aus Österreich, 13 aus Italien, 8 aus Irland und 8 aus Spanien. Das Ergebnis wird kumuliert dargestellt, da eine länderspezifische Unterscheidung der Antwortstichproben aus statistischer Sicht keinen Sinn machen würde.

3.1 Wirtschaftszweige

Die erste Frage bezog sich auf den Wirtschaftszweig der Unternehmen. Es waren mehrere Auswahlmöglichkeiten möglich. Wie in Abbildung 1 zu sehen ist, kamen die meisten Antworten aus der Maschinenbau- und Elektroindustrie, gefolgt vom Bildungswesen.

und der Rest der Antworten ist auf verschiedene Sektoren verteilt, was eine schöne Verteilung der Erhebungsproben ergibt.

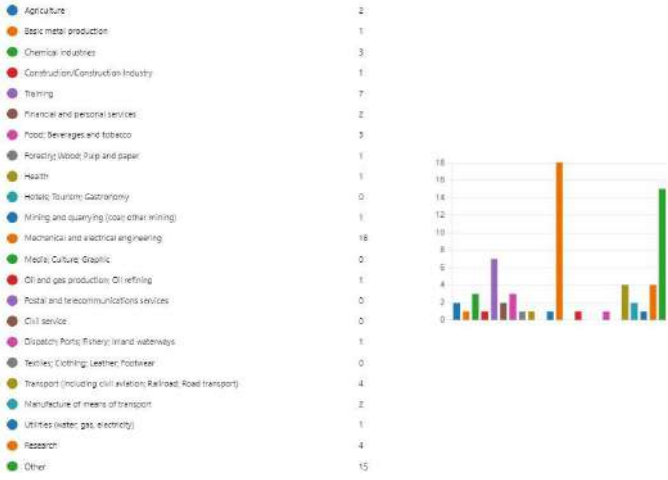


Abbildung 1: Überblick über die Antworten der einzelnen Sektoren

3.2 Größe des Unternehmens

Abbildung 2: Befragte nach Anzahl der Beschäftigten

Die überwiegende Mehrheit der Befragten stammte aus mittleren und großen Unternehmen, die in irgendeiner Weise mit dem Thema Fernwartung vertraut sein sollten.

3.3 Zielmärkte

Abbildung 3: Befragte nach Zielmärkten

Auf die Frage, wo sie ihr Geschäft betreiben, antworteten 55 % der Teilnehmer, dass sie sowohl auf dem nationalen als auch auf dem internationalen Markt tätig sind. 28% nannten nur den internationalen Markt und die restlichen 17% nur den inländischen. Auch diese Streuung der Antworten lässt erwarten, dass die meisten der Befragten eine Vorstellung von "Fernwartung" und den entsprechenden Technologien haben dürften.

3.4 Vertrautheit mit IoT

Abbildung 4 zeigt, dass alle Teilnehmer an der Umfrage in gewisser Weise mit dem Konzept des

Internets der Dinge (IoT) vertraut sind. 62% der Befragten gaben außerdem an, dass ihre Vertrautheit auf einem mittleren bis hohen Niveau liegt. Dies lässt darauf schließen, dass potenziell wertvolle Antworten zu den relevanten Qualifikationsthemen gegeben werden können, sofern sich dieser Trend bei anderen Basistechnologien fortsetzt.

Abbildung 4: Vertrautheit mit IoT als Grundlagentechnologie

3.5 Vertrautheit mir Cyber Sicherheit

Abbildung 5: Vertrautheit mit Cyber Sicherheit als Grundlagentechnologie

Nach nach Abbildung 5. um 53% der Befragten antworteten, dass sie ein mittleres

Vertrautheit mit dem Konzept der Cybersicherheit. Weitere 17 % stuften den Bekanntheitsgrad ebenfalls als hoch ein, was bereits 70 % aller Antworten ausmacht. Nur 1 Befragter hatte keinerlei Bezug zu diesem Thema, während rund 28% ihre Vertrautheit als gering einstuften.

3.6 Vertrautheit mit Cloud Computing

Abbildung 6. zeigt die Antworten bezüglich der Vertrautheit mit Cloud Computing. 51 % der Befragten gaben an, dass sie mit Cloud Computing auf mittlerem Niveau vertraut sind. Weitere 13% auf hohem Niveau. 32% der Teilnehmer sehen ihr Wissen über Cloud Computing auf niedrigem Niveau, während 2 Befragte oder 4% keinerlei Verbindung zu diesem Konzept haben.

Abbildung 6: Cloud Computing als Basistechnologie

3.7 Vertrautheit mit Industrie 4.0

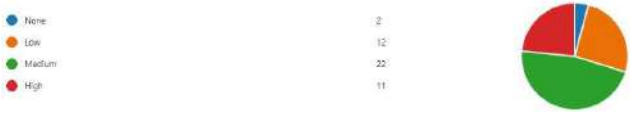


Abbildung 7: Vertrautheit mit Industrie 4.0 als ermöglichender Trend

Sehr ähnliche Antworten können auch in Bezug auf Indusutrie 4.0. beobachtet werden, wie in Abbildung zu sehen ist. 7. 47 % der Befragten gaben an, dass sie auf mittlerem Niveau vertraut sind. Etwa 23 % auf hohem Niveau und 26 % ungefähr auf niedrigem Niveau. Nur 2 oder 4 % der Befragten haben keine Vorstellung von Industrie 4.0.

3.8 Vertrautheit mit Fernwartung

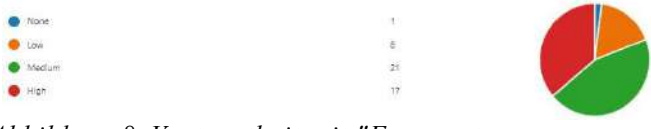


Abbildung 8: Vertrautheit mit "Fernwartung

Ermutigende Ergebnisse zeigen sich jedoch hinsichtlich der Vertrautheit mit der Fernwartung. Rund 81 % gaben an, mit dem Begriff "Fernwartung" sehr oder mittelmäßig vertraut zu sein. Nur 8 Personen oder rund 17 % antworteten, dass sie mit diesem Konzept wenig vertraut sind, und nur ein Teilnehmer oder 2 % gaben an, dass dieser Begriff nicht bekannt ist.

3.9. Vertrautheit mit AR/Mixed Reality

Abbildung 9: Vertrautheit mit AR/Mixed Reality als Basistechnologie

Hinsichtlich der Vertrautheit mit AR/ Mixed Reality (Abbildung 9) können wir feststellen, dass diese Technologie am unbekanntesten ist. Über 51% der Befragten wissen nichts oder nur sehr wenig über das AR/ Mixed Reality Konzept. Der andere Teil von 49%, der mit diesem Thema vertraut ist, hat nur 2% der Befragten, die sehr gut informiert sind.

3.10 Bekanntheit von Fernwartung

Abbildung 10: Bekanntheit von "Fernwartung

Die Antworten auf die Frage, ob die Befragten schon einmal von "Fernwartung" gehört haben, sind recht eindeutig, denn 98 % beantworteten diese Frage mit
"Ja", wie in Abbildung 10 dargestellt.

3.11 Bereits integrierte Fernwartungsszenarios

Abbildung 11: Aspekte der "Fernwartung" im eigenen Szenario

Auf die Frage nach bereits involvierten Szenarien aus dem Bereich 'Fernwartung' wurden die Antworten gleichmäßig auf vier verschiedene Aspekte verteilt. Mehrfachnennungen waren möglich. Als am meisten beteiligtes Szenario kann gelten

punktgenaue Fernaktualisierung von Programmen und Funktionalitäten und sichere Fernverbindung mit anschließender korrektiver Wartung und Fernüberwachung von Anlagenvariablen und Ferndatenerfassung (siehe Abbildung 11).

3.12 Interessanteste Aspekte der Fernwartung

Abbildung 12: Die interessantesten Aspekte der "Fernwartung

Die Bedeutung bereits implementierter Szenarien spiegelt sich auch in den Antworten auf die Frage nach möglichen Szenarien der Fernwartung wider. Die Antworten wurden ebenfalls gleichmäßig auf vier verschiedene Aspekte verteilt. Mehrfachnennungen waren möglich. Als am stärksten betroffenes Szenario kann die Fernaktualisierung von Programmen und Funktionalitäten und die sichere Fernverbindung in der gleichen Relevanzstufe verortet werden wie die korrigierende Fernwartung und die Fernüberwachung von Anlagenvariablen und Ferndaten

Erwerb, die in den Antworten nur unwesentlich niedriger waren als die beiden vorangegangenen Aspekte (siehe Abbildung 12).

3.13 Interessanteste Aspekte der Fernwartung für Trainings und Asubildung

Auf die Frage, welcher Aspekt in einer Schulung zum Thema "Fernwartung" am interessantesten ist, haben die Teilnehmer die folgenden fünf wichtigsten Themen in der Reihenfolge ihrer Relevanz gewählt (Skala: 1 am wenigsten und 5 am relevantesten): *Industrie 4.0, korrektive Fernwartung, Fernaktualisierung von Programmen und Funktionalitäten, Variablen und Ferndatenerfassung sowie Überwachung und Fernsupport*. (siehe Abbildung 13).

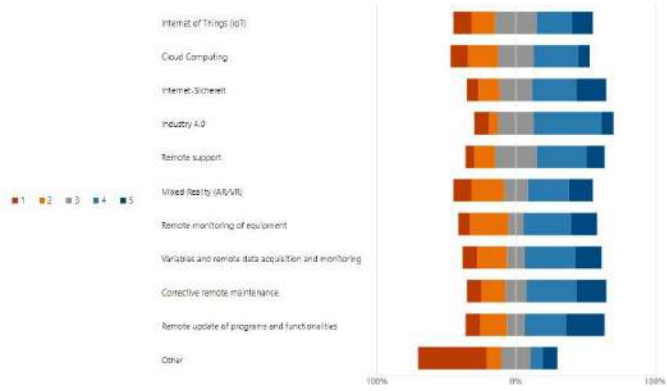


Abbildung 13: Interessanteste Aspekte der "Fernwartung" für die Ausbildung

4. SCHLUSSFOLGERUNGEN

Abschließend können wir sagen, dass "Fernwartung" nicht nur ein Schlagwort ist. Sie umfasst eine Reihe hochentwickelter Technologien wie Cloud Computing, AR/ Mixed Reality, Big Data und auch künstliche Intelligenz. Sie umfasst auch die Ferneinstellung von Menschen und Prozessen. Die durchgeführte Umfrage hat uns gezeigt, dass das Bewusstsein für "Fernwartung" bei den Befragten hoch ist und alle Aspekte eines typischen "Fernwartungsszenarios" für die Zielgruppe der Unternehmen gleichermaßen interessant sind. Die Ergebnisse sind jedoch teilweise eingeschränkt durch ungleiche

Die Verteilung der Befragten auf die Länder und die Verteilung auf mittlere und große Unternehmen ist jedoch recht akzeptabel. Um die gezogenen Schlussfolgerungen zu präzisieren, können wir sagen, dass die meisten Antworten auf die mittleren und großen Unternehmen zutreffen. Die fünf wichtigsten Wunschthemen für Schulungen, die in der Umfrage genannt wurden, sind Industrie 4.0, korrigierende Fernwartung, Fernaktualisierung von Programmen und Funktionalitäten, Variablen und Ferndatenerfassung sowie Überwachung und Fernunterstützung.

5. REFERENZEN

[1] Al-Turjman, F., Hasan, M.Z. & Al-Rizzo, H. (2019). Task Scheduling in cloud-basierten Survivability-Anwendungen unter Verwendung von Schwarmoptimierung im IoT. Transactions on Emerging Telecommunications Technologies 30(8): e3539, doi: 10.1002/ ett.353

[2] Al-Turjman, F. & Malekloo, A. (2019). Smart Parking in iot-enabled cities: A survey. Sustainable Cities and Society 49: 101, 608, doi: 10.1016/ j.scs.2019.101608

[3] Al-Turjman, F. (2020). Intelligenz und Sicherheit in Big 5g-orientiertem IoT: An overview.

Future Generation Computer System 102: 357 - 368, doi: 10.1016/ j.future.2019.08.009

[4] Al-Turjman, F. & Abujubbeh, M. (2019). Iot-enabled smart grid via sm: An overview. Future Generation Computer Systems 96: 579 - 590, doi: 10.1016/ j.future.2019.02.012

[5] Al-Turjman, F., Zahmatkesh, H. & Mostarda, L. (2019). Quantifizierung der Unsicherheit in Internet der medizinischen Dinge und Big-Data-Diensten mit Hilfe von Intelligenz und Deep Learning. IEEE Access, 7:115, 115, 759, doi: 10.1109/ ACCESS.2019.2931637

[6] Lüftenegger, E. & Softic, S, (2019). Finanzielle Validierung von dienstleistungsdominanten Geschäftsmodellen: Kosten-Nutzen-Analyse bei Geschäftsprozessen und service-dominanten Geschäftsmodellen. In: Strahonja V., Kirinic V. (eds) Proceedings of 30th Central European Conference on Information

[7] Chen, M., Mao, S. & Liu, Y. (2014). Big Data: A survey. Mobile Networks and Applications, 19(2): 171- 209, doi: 10.1007/ s11036-013-0489-0

[8] Softic, S., Zoier, M. & Stocker, A. (2014). Big Data. Mit sprechenden Daten zu optimierten Geschäftsprozessen. Virtual Vehicle Magazine 1(20): 16- 17

[9] Ngai, E.W.T., Gunasekaran, A.,Wamba, S.F., Akter, S, &Dubey, R. (2017). Big-Data-Analytik in elektronischen Märkten. Electronic Markets 27(3): 243- 245, doi: 10.1007/ s12525-017-0261-6

[10] Bauer, W., Schlund, S., Marrenbach, D. & Ganschar, O. (2014). Industrie 4.0 - Volkswirtschaftliches Potenzial . für Deutschland. Studie, Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (Bitkom) mit dem Fraunhofer-Institut f¨ur Arbeitswirtschaft und Organisation (IAO, Stuttgart), Berlin, https:// www.bitkom.org/Bitkom/Publikationen/Industrie- 40- Volkswirtschaftliches-Potenzial-fuer- Deutschland.html

[11] Becker, W., Ulrich, P. & Botzkowski, T. (2017). Industrie 4.0 im Mittelstand - Best Practices und Implikationen f¨ur KMU, 1st edn. Springer-Verlag, Berlin Heidelberg New York

[12] Borgmeier, A., Grohmann, A. & Gross, S.F. (2017). Smart Services und Internet der Dinge: Geschäftsmodelle, Umsetzung und Best Practices - Industrie 4.0, Internet of Things (Io T), Machine-to-Machine, Big Data, Augmented Reality Technologie. Carl Hanser Verlag GmbH Co. KG

[13] Kaufmann, T. (2015). Gesch¨aft smodelle in Industrie 4.0 und dem Internet der Dinge - Der Weg vom Anspruch in die Wirklichkeit, 1st edn. Springer-Verlag, Berlin, Heidelberg, New York

[14] Lüftenegger, E. (2014). Service-dominant business design. Eindhoven University of Technology, doi: 10.6100/ IR 774591

[15] Brenner, W., Hess, T., Brenner, W. & Hess, T. (2014). Wirtschaftsinformatik in Wissenschaft und Praxis - Festschrift für Hubert Österle, 1st edn. Springer-Verlag,
Berlin, Heidelberg, New York

[16] Milgram, P. & Kishino, F. (1994). Eine Taxonomie von visuellen Mixed-Reality-Displays. IEICE Trans. Information Systems. vol. E77-D, no. 12. 1321-1329.

[17] Was ist Cybersicherheit? (2022). kaspersky. https:// www.kaspersky.com/resource- center/ definitions/ what-is-cyber-security

[18] Was ist Fernwartung und wie kann Ihre Branche sie nutzen? - AR Remote Support Software (2022). argus-remote.com. https:// argus-remote.com/ was-ist-Fernwartung-und-wie-kann-ihre-Industrie-es-verwenden/

Zwei

Sichere Fernverbindung

Industrielle Cybersicherheit

Pablo Paino de Pedro, Centro de formación en Electricidad, electrónica y aeronáutica (CFELYA), Leganés, Madrid, Spanien,
cf.elecyaeronautica@madrid.org

***

Wenn im Rahmen von Industrie 4.0 eine Fernüberwachung einer Industrieanlage erforderlich ist, um Informationen zu erhalten und eine Fernwartung durchzuführen, ist es unerlässlich, Verbindungen über das Internetnetz herzustellen. Sobald ein Gerät oder eine Anlage an ein öffentliches Netz angeschlossen ist, ist sie unzähligen Bedrohungen ausgesetzt, die der Anlage großen Schaden zufügen können. Wir müssen uns der Schwachstellen bewusst sein, die Industrieanlagen und

Kommunikation, um sie zu minimieren und so das Risiko eines Anschlags zu verringern.

Es ist absolut notwendig, die Schwachstellen unserer Industrieanlagen und der Kommunikation zu berücksichtigen, um sie zu minimieren und so das Risiko eines externen Angriffs zu verringern, der Informationen auslesen und verändern oder, was noch schlimmer ist, die Industrieanlage unbrauchbar machen könnte.

Die Ausbildung in industrieller Cybersicherheit und die Anwendung ihrer Grundsätze ist derzeit obligatorisch, um die Risiken in den Fabriken des 21. Jahrhunderts, die ständig vernetzt sein müssen, zu verringern.

Key words: remote monitoring, IT information technologies, OT operational technologies, confidentiality, integrity, availability, OT cybersecurity, safety, ICS industrial cybersecurity, ISA99/IEC-62443, ISO/IEC-27001, vulnerability, external threat, risk, communication network, protocol, ethernet, profinet, modbus TCP, LAN, WAN, WLAN, VLAN, VPN, router, switch, gateway, network, redundant system, OPC UA, MQTT, local service, Cloud service.

1. EINFÜHRUNG

In diesem Kapitel werden wir die Merkmale industrieller Kommunikationsnetze untersuchen und die möglichen Bedrohungen aufzählen, denen eine Industrieanlage ausgesetzt ist, wenn ein Fernzugriff erforderlich ist, und Schwachstellen ermitteln, um sie zu beheben und das Risiko eines Cybersicherheitsproblems zu verringern.

Im Rahmen von Industrie 4.0 ermöglichen neue Technologien fortschrittlichere Fähigkeiten zur Unterstützung der Geschäftsanforderungen. Unternehmen tauschen zunehmend Informationen zwischen industriellen Steuerungssystemen, der Betriebsumgebung und Geschäftssystemen aus. Dieses höhere Maß an Integration bietet wichtige geschäftliche Vorteile, darunter eine bessere Sichtbarkeit von Aktivitäten, integrierte Fertigungs- und Produktionssysteme, gemeinsame Schnittstellen zur Kostensenkung oder die Fernüberwachung von Systemen.

Diese Beziehungen können zwar gut für das Geschäft sein, aber sie erhöhen auch das potenzielle Risiko, die Sicherheit von Industrieumgebungen zu gefährden. Da die Bedrohungen für Unternehmen zunehmen, steigt auch der Bedarf an Sicherheit.

1.1 Industrielle Cybersicherheit

Die industrielle Cybersicherheit muss im industriellen Umfeld eingeführt werden, und die Fachleute, die für die Wartung und Kontrolle von Industrieanlagen zuständig sind, müssen über die Gefahren von Fernverbindungen in Industrieanlagen geschult werden.

Die perfekte Sicherheit gibt es nicht. Wenn es sie gäbe, könnte das bedeuten, dass unser Geschäft nicht richtig funktioniert. Sicherheit ist Risikomanagement, und die Risikominderung muss gegen die Kosten der Risikominderungsmaßnahmen abgewogen werden.

Industrielle Steuerungssysteme arbeiten in komplexen Umgebungen. Ein detailliertes Verständnis dieser Umgebungen ist eine wesentliche Voraussetzung, um ihre Sicherheit zu gewährleisten.

Abbildung 1: Bedürfnisse und Prioritäten

Traditionell hat sich die IT-Sicherheit auf die Erreichung diese drei Ziele: Vertraulichkeit, Integrität und Verfügbarkeit.

Die IT-Sicherheitsstrategie für Unternehmensnetze räumt der Vertraulichkeit und den dafür notwendigen Zugangskontrollen oberste Priorität ein. An zweiter Stelle der Prioritätenliste steht die Integrität, und am Ende der Liste steht die Verfügbarkeit.

In Betriebsumgebungen (OT) liegt die Hauptpriorität auf der Aufrechterhaltung der Verfügbarkeit von Systemkomponenten. Die Integrität ist zweitrangig

Bedeutung, wobei die Vertraulichkeit am wenigsten wichtig ist. Die Tatsache, dass in diesem Umfeld die Vertraulichkeit kein relevantes Gewicht hat, bedeutet nicht, dass die Daten unwichtig sind, da dies direkte Auswirkungen auf die Datensicherheit hat (Patente, geheime Formeln usw.).

Das Wichtigste im OT-Umfeld ist jedoch die Sicherheit, sowohl im Hinblick auf die menschliche Gesundheit als auch auf die Umwelt.

Da die Sicherheitsanforderungen in der einen

oder anderen Umgebung unterschiedlich sind, sollte die industrielle Cybersicherheit von der Informationssicherheit (IT) "getrennt" werden, wobei eine Möglichkeit darin besteht, sie unterschiedlich zu bezeichnen und den industriellen Teil OT-Cybersicherheit oder ICS-Cybersicherheit zu nennen.

1.2 Was ist Industrielle Cybersicherheit

Die industrielle Cybersicherheit ist ein Bereich, der international immer mehr an Bedeutung gewinnt, und es gibt zahlreiche Vorschriften/Normen. Bei diesen Normen handelt es sich um freiwillige, konsensgesteuerte Dokumente. Die ISA99/IEC-62443-Norm gewinnt in der industriellen Welt zunehmend an Bedeutung, da sie von Experten aus der Industrie entwickelt wird.

Welt ISA99 und IEC-52443 in Absprache mit ISO/IEC-27001. ISA99/IEC-62443 gilt für
alle Beteiligten im industriellen Umfeld, vom Anlageneigentümer, der angibt, wie ein Cybersicherheitsprogramm aussehen sollte, bis hin zum Lieferanten der zu liefernden Komponenten, der die technischen Merkmale aufzeigt, die die gelieferten Komponenten auf der Grundlage von Konstruktionskriterien aufweisen sollten.

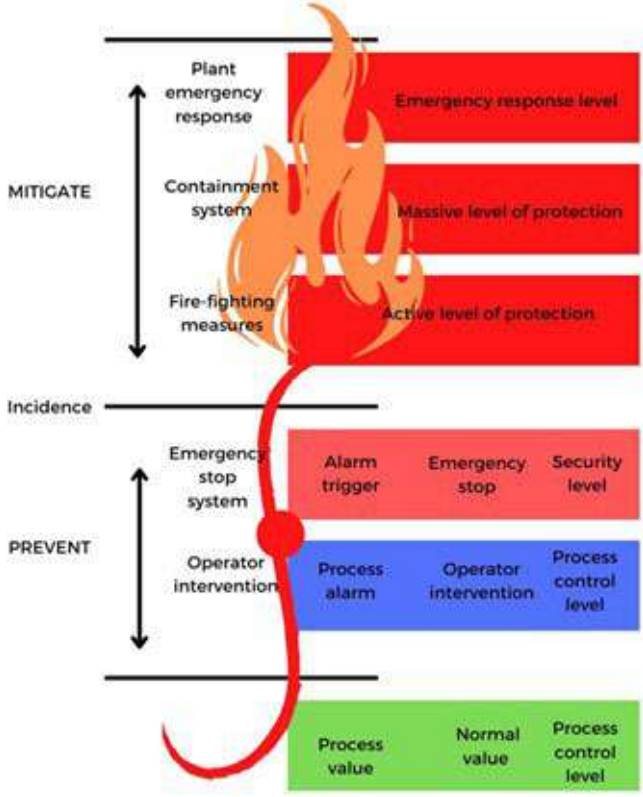


Abbildung 2: Sicherheit: Kontrolle statt Vorbeugung, um keine Abhilfe schaffen zu müssen

Bei der industriellen Cybersicherheit geht es um mehr als nur um die in Kontrollsystemen verwendete Technologie. Sie umfasst auch die Menschen und Prozesse, die für ihre Umsetzung erforderlich sind. Wenn das Personal nicht ausreichend

geschult, technologische Gegenmaßnahmen und die erforderlichen Verfahren werden während

des gesamten Lebenszyklus einer Anlage nicht ausreichend entwickelt sein. In diesem Sinne wird es Schwachstellen geben, die in Verbindung mit (immer häufigeren) Bedrohungen das Risiko eines böswilligen Cyberangriffs erhöhen.

Externe Bedrohungen sollten nicht die einzige Sorge sein. Auch Insider mit böswilligen Absichten oder sogar eine unbeabsichtigte unschuldige Handlung können ein ernsthaftes Sicherheitsrisiko darstellen.

Ausgehend von diesen Prämissen sollte die industrielle Cybersicherheit entwickelt werden, um die wichtigsten Bedrohungen, denen Unternehmen ausgesetzt sind, zu entschärfen:

- Ransomware . Der Cyberkriminelle übernimmt die Kontrolle über einen der Computer des Unternehmens, verschlüsselt wichtige Daten und fordert ein Lösegeld.

- Corporate phishing. Der Cyberkriminelle sendet E-Mails an wichtige Mitarbeiter des Unternehmens, gibt sich als leitender Angestellter aus und bittet z. B. um die Angabe von Bankkontodaten.

  Customised Malware. Dabei handelt es sich um kleine Blöcke mit bösartigem Code, die unbemerkt im Hintergrund laufen. Der Zweck dieser Codeblöcke ist sehr

unterschiedlich: vom Sammeln sensibler Informationen bis hin zu deren Veränderung.

Das Risiko für die Unternehmen ist in erster Linie wirtschaftlicher Natur, aber das zusätzliche Risiko, dass ihre Glaubwürdigkeit und ihr Ruf Schaden nehmen, sollte nicht unterschätzt werden.

In einem 2021 veröffentlichten Bericht prognostiziert das Beratungsunternehmen GARTNER [1], dass die beschleunigte Digitalisierung vieler Wirtschaftsbereiche, wie z. B. der Industrie, dazu führen wird, dass Cyberkriminelle bis 2025 in der Lage sein werden, mit ihren Angriffen Menschenleben zu gefährden und sogar Morde zu begehen.

Der Bericht stellt fest, dass Cyberangriffe auf Betriebstechnologien, d. h. Hard- und Software zur Überwachung oder Steuerung von Anlagen, Vermögenswerten oder Prozessen, immer häufiger vorkommen und dass die Eskalation und zunehmende Effektivität dieser Angriffe in industriellen Umgebungen zu kritischen Ausfällen im Betrieb von Maschinen und Sicherheitssystemen führen und die physische Unversehrtheit gefährden könnte.

der Menschen, die in ihnen arbeiten. Das beste Beispiel für die Auswirkungen eines Cyberangriffs auf die Betriebstechnik eines Unternehmens war dem Bericht zufolge kürzlich

der Angriff auf die US-amerikanische Ölgesellschaft Colonial Pipeline, eines der wichtigsten Pipelinenetze in den Vereinigten Staaten, der das Unternehmen dazu zwang, den Betrieb als Vorsichtsmaßnahme vorübergehend einzustellen, um weitere Schäden zu vermeiden.

1.3 Schwierigkeiten der heutigen Zeit

Viele Unternehmensleiter sehen die industrielle Cybersicherheit immer noch als ein Problem an, das auf einer "Wenn es funktioniert, warum sollte man es ändern"-Mentalität beruht, und es ist bekannt, dass ohne die Unterstützung des Managements keine Ressourcen zugewiesen werden. Spezifisches Wissen über Sicherheit in OT-Umgebungen ist absolut notwendig.

Es gibt keine Verständigung zwischen den Mitarbeitern in der Werkstatt und den IT-Mitarbeitern im IT-Bereich, da jeder seine eigene "Sprache" spricht. So verwenden sowohl die IT- als auch die OE-Techniker eine Sprache voller Fachbegriffe, die für die Techniker des jeweils anderen Bereichs undurchschaubar sind. Ein OE-Techniker wird zum Beispiel kaum die Bedeutung folgender Begriffe kennen

"Jitter", während für einen IT-Techniker die Begriffe Profibus oder Profinet vage klingen mögen.

Das IT-Personal ist für das Unternehmensnetz zuständig und muss oft bestimmte Standards

einhalten, die in der industriellen Welt oft nicht gelten.

Aber es wird immer häufiger gewünscht, auf Daten aus dem OT-Bereich zugreifen zu können. Das Management möchte alle Informationen, die für eine sofortige Entscheidungsfindung in Echtzeit erforderlich sind. Das bedeutet, dass die industriellen Elemente ständig miteinander verbunden sein müssen und dass Fehler sofort diagnostiziert und behoben werden können.

Der oben erwähnte GARTNER-Bericht enthält als Dekalog eine Reihe von Aspekten, die berücksichtigt werden sollten:

Auf Unternehmensebene sollte für jede Einrichtung ein OT-Sicherheitsbeauftragter ernannt werden, der für die Zuweisung und Dokumentation der sicherheitsrelevanten Aufgaben und Zuständigkeiten für alle Mitarbeiter, Führungskräfte und Dritte verantwortlich ist.

Das gesamte OT-Personal sollte über die für seine Aufgaben erforderlichen Fähigkeiten verfügen. Mitarbeiter auf jeder

Die Mitarbeiter der Einrichtung sollten darin geschult werden, Sicherheitsrisiken und gängige Angriffsmethoden zu erkennen und zu wissen, was im Falle eines Sicherheitsvorfalls zu tun ist.

Sicherstellen, dass jede Einrichtung einen OT-spezifischen Prozess für das Management von Sicherheitsvorfällen einführt und aufrechterhält.

Es sollte auch sichergestellt werden, dass angemessene Sicherungs-, Wiederherstellungs- und Notfallwiederherstellungsverfahren vorhanden sind. Um die Auswirkungen physischer Ereignisse wie z. B. eines Brandes zu begrenzen, sollten die Sicherungsmedien nicht am selben Ort wie das gesicherte System gelagert werden. Die Sicherungsmedien sollten auch gegen unbefugte Offenlegung oder Missbrauch geschützt werden. Bei schwerwiegenden Vorfällen muss es möglich sein, das Backup auf einem neuen System oder einer virtuellen Maschine wiederherzustellen.

Es muss eine Richtlinie erstellt werden, die sicherstellt, dass alle tragbaren Datenspeichermedien wie USB-Sticks und Laptops gescannt werden, unabhängig davon, ob ein Gerät einem internen Mitarbeiter oder Dritten wie Subunternehmern oder Vertretern gehört von des Geräteherstellers gehört. Nur Medien, die frei von bösartigem Code oder Software sind, sollten an den OT-Bereich angeschlossen werden.

Die für die Sicherheit zuständige Stelle muss ein laufend aktualisiertes Inventar aller OT-Geräte und -Software führen.

OT-Netze müssen physisch oder logisch von allen anderen Netzen getrennt sein, sowohl intern als auch extern. Der gesamte Netzwerkverkehr zwischen einem OT-Gerät und einem anderen Teil des Netzes muss über eine sichere Gateway-Lösung wie eine demilitarisierte Zone (DMZ) laufen. Interaktive Sitzungen für OT müssen sich am Gateway authentifizieren.

Es sollten geeignete Richtlinien oder Verfahren für die automatische Protokollierung und Überprüfung tatsächlicher und potenzieller Sicherheitsereignisse vorhanden sein. Diese sollten klare Aufbewahrungsfristen für die Sicherheitsprotokolle und den Schutz vor Manipulationen oder unerwünschten Änderungen beinhalten.

Sichere Konfigurationen müssen für alle anwendbaren Systeme wie Terminals, Server, Netzwerkgeräte und Feldgeräte entwickelt, standardisiert und implementiert werden. Endpunktsicherheitssoftware, wie z. B. Anti-Malware, muss auf allen Komponenten der OT-Umgebung, die sie unterstützen, installiert und aktiviert werden.

Schließlich muss ein Verfahren festgelegt werden, nach dem die Gerätehersteller die Patches vor ihrer Bereitstellung qualifizieren. Sobald sie qualifiziert sind, können Patches nur auf geeigneten Systemen in einer vorher festgelegten Häufigkeit eingesetzt werden.

1.4 Zukunft des technischen Personals in OT Bereich

Technisches Personal, das im OT-Bereich arbeitet, muss geschult werden, um die Kenntnisse und Fähigkeiten des IT-Personals zu erwerben (und umgekehrt) [4]. Da ihre Aufgaben darin bestehen werden, die Geräte zu installieren, sie untereinander und mit anderen, bereits installierten Geräten zu verbinden, sie zu konfigurieren, in Betrieb zu nehmen und den korrekten Betrieb des Geräts zu überprüfen, muss der zukünftige OT-Techniker Folgendes können:

- Diagnose von Schwachstellen in Industrieanlagen, wenn diese an ein Netz angeschlossen sind, und Verständnis für interne und externe Bedrohungen.

- Seien Sie sich über die Risiken im Klaren, denen Kontrollgeräte ausgesetzt sind, wenn sie an ein von außen zugängliches Netz angeschlossen sind.

- Sie müssen die IT-Terminologie fließend beherrschen.
- Wissen, wie ein Kommunikationsnetz aufgebaut ist und welche Protokolle die gängigsten Konfigurationen für den Datenaustausch im OT-Bereich verwenden (Ethernet, Profinet, Modbus TCP, u.a.).

- Installation, Konfiguration und Überprüfung von Ethernet-, Profinet- und Modbus TCP-Netzwerken.

- Unterscheidung zwischen verschiedenen Arten von Kommunikationsnetzen (LAN, WAN, WLAN, VLAN, VPN, u.a.)

- Wissen, wozu der Router (Router), der Switch (Switch) oder das Gateway (Gateway) dient und wie man es konfiguriert.

- Kenntnis der Netzkonfigurationen und der spezifischen Protokolle zur Gewährleistung der Verfügbarkeit der beteiligten Geräte (redundante Systeme).

- Kenntnis der gängigsten Protokolle für den sicheren Datenaustausch (OPC UA und MQTT).

Kennen Sie und verwalten lokale und Cloud-Dienste.

- Kennen Sie und betreiben spezifische Hardware (EWON Flexy, SINEMA S615).

- Kenntnisse und Bedienung von spezifischer Software (OpenVPN, SINEMA RC Server, NODE-red).

Abbildung 3: Geschultes Personal im Bereich der industriellen Cybersicherheit.

2. METHODOLOGIE

Die folgenden Leitlinien orientieren sich an dem Konzept der beruflichen Bildung als Verbesserung Ihrer beruflichen Fähigkeiten und persönlichen

Entwicklung. Die Ausbildung sollte das Wissen und die Praxis vermitteln, die den im Berufsbild aufgeführten beruflichen Kompetenzen entsprechen Zu diesem Zweck wird der Rahmen, der die Entwicklung der Ausbildung leiten sollte, in den folgenden Punkten dargelegt:

2.1 Trainingskonzept und Design

Das Konzept einer offenen, flexiblen und zugänglichen Ausbildung, die modular aufgebaut ist, um das Lernen zu erleichtern. Die Schulungsmodule werden in Lerneinheiten unterteilt. Die Berücksichtigung verschiedener Formen der Schulungsdurchführung: Face-to-Face, E-Learning oder Blended Learning.

2.2 Mehodologische Strategien

Die Schulungsmaßnahmen orientieren sich an der realen Arbeit, mit der die Studierenden in der Industrie konfrontiert werden können. Sie umfasst den Umgang mit den manuellen Werkzeugen des Wartungstechnikers und den technischen Werkzeugen, die für die Installation und Konfiguration der für die Umsetzung der Cybersicherheit in industriellen Umgebungen erforderlichen Geräte erforderlich sind.

Anwendung von methodischen Strategien, die die aktive Beteiligung der Schüler erleichtern

bei der Gestaltung ihres Lernens, der Entwicklung von Motivation, Autonomie, Initiative und Verantwortung, die für die berufliche und persönliche Entwicklung notwendig sind.

Die Anwendung von Praktiken während der Ausbildung, die den Transfer des Gelernten bei der Bewältigung von Situationen, der Durchführung von Tätigkeiten und der Lösung von arbeitsplatzspezifischen Problemen erleichtern.

Anhand von Modellen kleiner Industrieanlagen, die sich sowohl vor Ort als auch aus der Ferne befinden, werden die notwendigen Praktiken der Cybersicherheit erprobt.

Einsatz von didaktischen Mitteln und Ressourcen, die den zu erwerbenden Kenntnissen und Fähigkeiten angemessen sind und mit dem beruflichen Kontext in Verbindung stehen.

Die aktive Beteiligung der Studierenden an der Entwicklung der Sitzungen wird jederzeit gefördert.

Neben den Bedürfnissen der Gruppe wird auch auf die individuellen Bedürfnisse der einzelnen Schüler eingegangen.

3. SCHLUSSFOLGERUNG

Die mit der Wartung von Industrieanlagen betrauten Fachleute müssen über eine aktuelle Ausbildung im Bereich der Cybersicherheit in industriellen Umgebungen verfügen und sich jederzeit des tatsächlichen Risikos bewusst sein, dem die Industrieanlage, für die sie verantwortlich sind, ausgesetzt ist.

4. REFERENZEN

[1] Gartner prognostiziert, dass Cyber-Angreifer bis 2025 operative Technologieumgebungen waffenfähig gemacht haben werden, um Menschen erfolgreich zu schädigen oder zu töten (2021). Gartner. https://www.gartner.com/en/newsroom/press-releases/ 2021-07-21-gartner-predicts-by-2025-cyber-attackers-will-have-we

[2] IT-OT Konvergenz (2018). INCIBE-Cert. Zuletzt . abgerufen 15.12.2022 aus: https://www.incibe-cert.es/en/blog/itot- konvergenz

[3] INCIBE-Cert. (2017) . Risiken und Herausforderungen der Cybersicherheit und des Datenschutzes in IoT.

[4] INCIBE-Cert. (2018). IT und TO, sind wir schon Freunde?

Drei

Fernüberwachung

Martin Hill, Michael Murray, Andrew de Juan, Raymond Wolfe, Liam Moore,
Technologische Universität Munster
Universität, Cork, Munster", Irland, Martin.Hill@ mtu.ie, Michael.Murray@mtu.ie, andrew.dejuan@mtu.ie, raymond.wolfe@mtu.ie, liam.moore@ mtu.ie

***

In diesem Kapitel wird das Konzept von Industrie 4.0 vorgestellt und erläutert, wie es sich mit den derzeit in der Industrie am meisten genutzten Automatisierungsrahmen überschneidet. Es wird eine Untersuchung der aktuellen Ansätze zur Datenerfassung in der Fabrikumgebung durchgeführt und untersucht, wie sich diese mit den Anwendungsbereichen von Industrie 4.0 und IIOT überschneiden. Es wird ein Überblick über die Ansätze zur Übertragung von Daten aus der Fabrikumgebung in die Cloud gegeben, wobei ein Ansatz, der MQTT als Datenkommunikationsschnittstelle verwendet, als der beste herausgestellt wird.

eine vielversprechende Option, um eine echte Fernüberwachung auf Cloud-Ebene zu ermöglichen. Abschließend wird eine Fallstudie vorgestellt, in der MQTT und ein Layered-Broker-Ansatz verwendet werden, um die Machbarkeit der Verwendung von MQTT als Haupttechnologie für die Fernüberwachung und -erfassung von Daten zu demonstrieren.

Keywords: remote monitoring, remote maintenance, automation stack, industrial Internet of Things, OPC UA, MQTT, MODBUS

1. EINFÜHRUNG

Moderne Fertigungsprozesse erfordern eine genaue Überwachung der Fertigungsdaten in der Werkstatt, um einen integrierten, effizienten Betrieb mit Anwendungen wie Qualitätssicherung, Bestandsmanagement, Finanzplanung und Wartung zu gewährleisten. Die Entwicklung dieser datengesteuerten Fertigungsanwendungen, die oft als Industrie 4.0 bezeichnet werden, beinhaltet die Kommunikation, Verwaltung und Analyse großer Datenmengen. Dieses Kapitel befasst sich mit der Systemarchitektur, dem Aufbau und den Rahmenbedingungen für die Fernüberwachung und Ferndatenerfassung in diesem industriellen Kontext.

Die Fernüberwachung spielt eine zentrale Rolle bei der vorausschauenden Wartung, bei der es in erster Linie darum geht, den Ausfall des zu wartenden Systems vorherzusehen, indem frühzeitige Anzeichen von Störungen erkannt werden, was einen proaktiven Ansatz für Wartungsarbeiten ermöglicht, der die Betriebszeit maximiert und die Betriebskosten senkt [1]. Für größere Hersteller mit mehreren Anlagenstandorten bietet die Fernüberwachung ein konsolidiertes Modell der Leistungstrends an allen Standorten. Von einer zentralen Stelle aus können die Daten verglichen werden, um die Erfolge der leistungsstärksten Anlagen zu ermitteln und zu wiederholen [2]. In der Vergangenheit war die Datenübertragung einer der größten Engpässe bei der Fernüberwachung. In der Industrie 4.0 erfordert die Echtzeit-Fernüberwachung, dass Live-Daten an den Standorten gesammelt und dann an einen Datenserver übertragen werden, auf den Endnutzer an jedem beliebigen Standort zugreifen können. Um die Betriebstechnik (OT) dieser Feldnetzwerke in das Informationstechnologie (IT)-System des Unternehmens zu integrieren, werden industrielle IoT-Gateways (oder IIoT-Gateways) eingesetzt, die die von den OT-Geräten extrahierten Daten an Server in lokalen Datenzentren oder in der Cloud übertragen können [3]. Der Fernzugriff auf diese Daten wird dann mit einer unternehmenseigenen (privaten) Cloud über ein geschlossenes virtuelles privates Netzwerk (VPN) oder mit der

öffentlichen Cloud (über das Internet) unterstützt.

Die Schlüsselelemente eines Fernüberwachungssystems sind daher: ein digitalisierter Sensorwert, ein Gerät zur Übermittlung dieses Wertes innerhalb des OT-Systems, ein Protokoll und Tools zur Weiterleitung dieses Wertes vom OT an ein entferntes IT-System, ein System zur Verwaltung dieser Daten und Anwendungen zur Anzeige und Analyse der Daten. Internet-basierte Protokolle und Standards sind der Schlüssel, um die Fernverbindung und Koordination dieser Systeme zu ermöglichen.

In diesem Kapitel werden die gängigsten industriellen Optionen für jedes dieser Elemente vorgestellt und Anleitungen für die Auswahl und Konfiguration der gängigsten Elemente zur Entwicklung einer Fernüberwachungsanwendung gegeben [1]. In diesem Kapitel wird ein Überblick über die folgenden Themen gegeben:

- Industrie 4.0 Automatisierungsmodell
- Interne Datenkommunikation
- Externe Datenkommunikation
- Fallstudie: Ein funktionierendes Beispiel für eine IIo T-Architektur

2. INDUSTRIE 4.0-AUTOMATISIERUNGSMODELL

Industrie 4.0 bezieht sich auf den aktuellen Trend der Automatisierung und des Datenaustauschs in der Fertigungstechnik und eine digitale Konvergenz zwischen Industrie, Unternehmen und anderen Prozessen. Die Industrie 4.0-Infrastruktur bietet robuste Unterstrukturen, die von OT unterstützt werden, einschließlich Sensoren, Maschinen und Steuerungen, die sicher mit lokalen und entfernten IT-Systemen integriert sind. IT bezieht sich auf die Computer- und Netzwerktechnologie, die das Rückgrat eines jeden Unternehmens bildet. und ermöglicht Managementanwendungen wie Finanzen, Ressourcenplanung und Wartung werden auf dem lokalen Unternehmensserver oder in der Cloud betrieben. OT verbindet die industriellen Prozesse eines Unternehmens und umfasst Robotersysteme, SCADA-Systeme (Supervisory Control And Data Acquisition), speicherprogrammierbare Steuerungen (PLCs) und CNC-Maschinen (Computer Numerical Control). Der Hauptunterschied zwischen IT und OT besteht darin, dass sich die IT auf die Front-End-Informationsaktivitäten eines Unternehmens konzentriert, während die OT auf die Back-End-Produktion (Maschinen) ausgerichtet ist. der Interoperabilitätsstandard Open Platform Communications (OPC), der die OT-Ebenen mit den OT-Ebenen verbindet.

benutzerdefinierte Anwendungsprogrammierschnittstellen (APIs), die IT-Ebenen miteinander verbinden. Abbildung 1 zeigt nicht nur den traditionellen Kommunikationsansatz, sondern auch, wie ein IIoT-Ansatz unter Verwendung eines Protokolls wie MQTT alle Stack-Schichten, die OT- und IT-Prozesse umfassen, verbinden kann.

Ein gängiges Modell des Automatisierungsstapels ist in Abbildung 1 dargestellt. Diese Abbildung zeigt die Hierarchie der Verbindungen von den Sensoren in der Fabrikhalle bis zu den Planungsanwendungen der Geschäftsleitung. Dieses von der Industrie angenommene Referenzmodell, das so genannte Purdue-Modell, zeigt die Verbindungen und Abhängigkeiten aller Hauptkomponenten eines typischen industriellen Kontrollsystems (ICS) [5]. In modernen Netzwerken ist die Trennung zwischen IT- und OT-Systemen nicht absolut, da viele Autoren ein sich überschneidendes Kontinuum von OT- und IT-Systemen aufzeigen. Für dieses Kapitel wird in Abbildung 1 eine indikative Unterteilung zwischen diesen Systemen angegeben. Die gewählte Unterteilung basiert auf den traditionellen Kommunikationssystemen, die am häufigsten mit

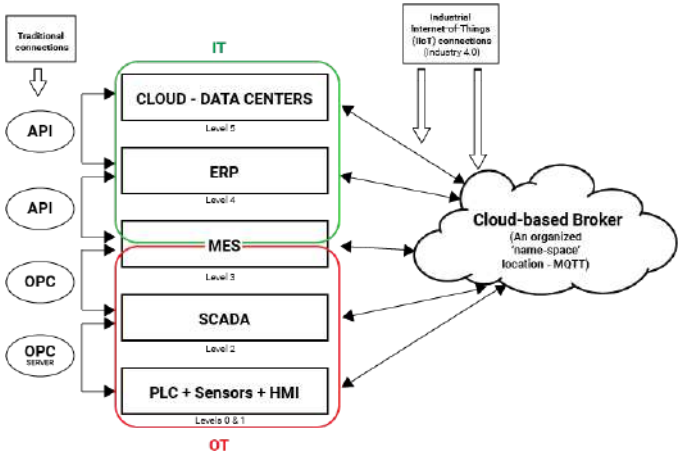


Abbildung 1: 5-Schichten-Modell der Automatisierung - Der Automatisierungsstapel [6]

In der Automatisierungskette befindet sich die Prozessausrüstung auf der untersten Ebene - Ebene 0, wo Geräte reale Informationen (physikalische Bedingungen) von Sensoren wie Temperatur- oder Drucksensoren messen, die zusammen mit Motoren, Pumpen, Ventilen und Instrumenten zu finden sind. Geräte wie PLCs und Remote Terminal Units (RTUs) wandeln die Messdaten in numerische Digitalwerte um, die von einem Computer verändert werden können [7]. Diese Geräte können die digitalen Werte mit Hilfe von proprietären, herstellerübergreifenden oder standardisierten Systemen an höhere Ebenen im Automatisierungssystem weitergeben.

Kommunikationsprotokolle wie Profinet, Modbus® oder MQTT.

In einer herkömmlichen Verbindungskonfiguration können die Benutzer den Echtzeitstatus und die Trends eines Prozesses überwachen und die Steuerung lokal über eine Mensch-Maschine-Schnittstelle (HMI) oder ein lokales Überwachungs- und Datenerfassungssystem (SCADA) auf der Grundlage einzelner Client-Server Verbindungen. Verbindungen zu IT-Funktionen auf Unternehmensebene werden durch eine Kombination aus OPC-Datentransfer zu einer Unternehmensdatenbank und proprietären API-Verbindungen zu dieser Datenbank von Managementanwendungen aus ermöglicht. Bei dieser Betriebsart werden alle Sicherheits- und Schnittstellenprobleme in jeder einzelnen Client-Server-Verbindung verwaltet, was erhebliche Ressourcen für die Verwaltung der verschiedenen unterstützten Protokolle und APIs erfordert.

In einer Industrie 4.0-Anwendung, wie sie in der Abbildung 1 des industriellen Internet der Dinge (IIo T) dargestellt ist, kann die Datenübertragung zwischen allen Automatisierungsschichten mit einem einzigen Protokoll wie MQTT unterstützt werden, wobei die Verbindung zu den Anwendungen von einem Systembroker verwaltet wird, der lokal oder an einem entfernten Standort sein kann. Dieser Ansatz

kann die Verwaltung von Sicherheits- und Schnittstellenfragen, da es ein gemeinsames Protokoll und einen zentralen Makler für die Zugangskontrolle gibt.

Bei der Fernüberwachung werden die Echtzeitdaten und die Leistung von Maschinen, Geräten und kompletten Prozesssystemen verfolgt, ohne dass der Benutzer physisch am Standort der Anlage anwesend sein muss. Da sich Industrie- und Produktionssysteme in der Regel an mehreren Standorten befinden und nicht auf einen einzigen Standort beschränkt sind, kann das technische Personal von der Möglichkeit der Fernwartung und -überwachung profitieren [5]. Die Fernüberwachung verschiedener Schlüsselparameter innerhalb einer Fertigungsanlage oder eines Produktionsprozesses erfordert die Echtzeit-Erfassung der verfügbaren Daten aus allen verschiedenen Ebenen bis hinunter zur Maschinenebene. Große Mengen von Produktionsprozessdaten, die in Echtzeit (Big Data) aus verschiedenen Quellen und in unterschiedlichen Formaten erzeugt werden, müssen
1) von der Fabrik aus aufgezeichnet und übermittelt Boden zu 2) einem Datenverwaltungssystem, das die Daten 3) für IT-Anwendungen zur langfristigen Speicherung und Analyse mit fortschrittlichen Algorithmen zur Verfügung stellt [9]. Diese Schlüsselphasen und eine Fallstudie zur Fernüberwachung sind in Abbildung 2 dargestellt. Zur Verdeutlichung zeigt

Abbildung 2 die einfachsten Architekturoptionen für Fernüberwachung Überwachung. Eine industrielle Implementierung der Fernüberwachung wird wahrscheinlich eine Mischung aus OPC- und MQTT-Protokollen beinhalten und kann mehrere lokale und entfernte Broker umfassen.

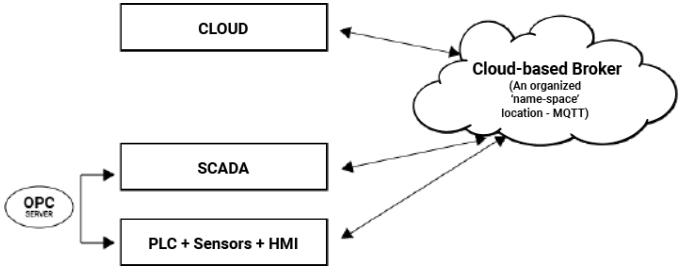


Abbildung 2: Fernüberwachung des Sensordatenstroms mit IIoT-Protokollen.

3. INTERNE DATENKOMMUNIKATION

Alle Komponenten der industriellen Automatisierung müssen effektiv miteinander kommunizieren, damit Produktionssysteme funktionsfähig und produktiv sind, daher ist die Kommunikation die Grundlage jeder industriellen Komponente [10]. Der Datenaustausch zwischen Geräten und Anwendungen auf verschiedenen Ebenen der Unternehmenshierarchie, d. h. zwischen der

Fertigungs- und der Unternehmensebene, einschließlich des Austauschs zwischen verschiedenen Anwendungen auf derselben Ebene

Ebene erfordert Kommunikationsprotokolle. Die heterogene Zusammensetzung der installierten Fertigungs-/Prozessausrüstung, der unterstützenden IT-Infrastruktur und der Anwendungen in typischen Anlagen spiegelt die verschiedenen Arten von Kommunikationsprotokollen wider, die in Bezug auf Funktionalität und Leistung erforderlich sind [11]. Industrielle Automatisierungssysteme werden häufig als offene verteilte Architektur mit Kommunikation über digitale Kommunikationsnetze implementiert. Industrielle Netze decken ein breites Spektrum von Fertigungsanwendungen ab. Zahlreiche Fertigungsanwendungen werden durch gemeinsame industrielle Netze unterstützt, die digitale Kommunikationstechnologie verwenden. Bei vielen Anwendungen bestimmen die Art der Geräte und die Leistung die Art des Netzes [12]. Die Auswahl des richtigen Netzes für die spezifischen Anwendungsanforderungen ist der Schlüssel zur nahtlosen Integration zwischen Systemen und Ebenen.

Industrielle Automatisierungssysteme können sehr komplex sein und haben typischerweise mehrere hierarchische Ebenen. Für diese

Ebenen gibt es ein geeignetes Kommunikationsprotokoll, wobei jede Ebene unterschiedliche Anforderungen an das Kommunikationsnetz stellt

3.1 Serielle und Ethernet-basierte Protokolle

Serielle Schnittstellen, die zunächst von verschiedenen Anbietern entwickelt und schließlich als De-facto-Standard akzeptiert wurden, bildeten die Grundlage für die erste Generation industrieller Kommunikation Netzwerke. Viele davon, insbesondere mit Master-Slave-Konfigurationen, sind jedoch aufgrund des langen Lebenszyklus von Industriesystemen auch heute noch sehr beliebt. Logiksteuerungen und ältere Feldgeräte kommunizieren größtenteils über serielle Leitungen der Ebenen 0 und 1, die die wichtigsten Teile des Steuerungssystems darstellen, in denen physikalische Vorgänge stattfinden. Aufgrund ihrer weiten Verbreitung, ihrer Zuverlässigkeit und der beträchtlichen Kapitalinvestitionen und Betriebsressourcen, die mobilisiert werden müssten, um diese Systeme in großem Umfang zu ersetzen, sind seriell angeschlossene Geräte seit mehr als 40 Jahren ein wichtiger Bestandteil der Kommunikation in Steuerungssystemen und werden dies auch in absehbarer Zukunft bleiben. Zu diesen seriell basierten Protokollen gehören PROFIBUS®, CANbus, Modbus® und CC-Link®.

Die Entwicklung von Echtzeit-Ethernet zum Anschluss von Geräten ist von erheblichem wirtschaftlichem Interesse, um traditionelle Feldbussysteme zu ersetzen [13]. Feldbussysteme waren die primären

Bestandteil der Netze auf der Feldebene zu Beginn. Mit der Entwicklung des Internets begannen jedoch Ethernet-basierte Netzwerktechnologien aus dem Bereich der Informationstechnologie (IT) die Netzwerke der Betriebstechnik (OT) zu durchdringen. Dies führte zur Entwicklung von Echtzeit-Ethernet (RTE)-Standards und -Technologien wie PROFINET, EtherCAT, EtherNet/ IP usw., die in Automatisierungsnetzwerken der Feldebene in der Fertigungs- und Prozessindustrie weit verbreitet sind [14], [15]. Die Feldbusse werden derzeit in Bezug auf die Vernetzung von der weit verbreiteten Ethernet-Technologie übertroffen [16]. Das Grundprinzip von IIo Ts hingegen [14], [15], [16],[18] zeichnet sich dadurch aus, dass es die strengen Strukturen der Automatisierungspyramide und die bestehenden Hierarchien aufhebt und z.B. den Zugriff auf Sensordaten auf allen Netzebenen ermöglicht. Damit sich die verschiedenen Knoten untereinander verstehen, setzen IIo T-Protokolle auf eine offene, herstellerneutrale Kommunikation. Ein weiterer entscheidender Faktor ist die Tatsache, dass die Sicherheit zu einem großen Problem wird, sobald viele Netzknoten miteinander verbunden sind. Daher werden auch Sicherheitsüberlegungen in diese IoT-Protokolle einbezogen.

Obwohl es ideal wäre, nur ein Protokoll zu haben, haben die verschiedenen Anwendungsfälle und Anwendungen jeweils ihre eigenen Anforderungen. Daher haben MQTT- und OPC-UA-Protokolle einzigartige Stärken und Schwächen (siehe Tabelle 1). Gewünscht wird eine solide Architektur, die Sicherheit, Leistung, Betriebszeitanforderungen und Ausfallsicherheit berücksichtigt, ein leichtgewichtiges Protokoll mit minimalem Protokoll-Overhead und geringer Bandbreitennutzung.

3.2 OPC UA (Vereinheitlichte Architektur)

Die OPC Foundation dokumentierte eine Reihe von Anforderungen, die eine OPC UA-Anwendung erfüllen muss, und veröffentlichte 2006 ihre erste Spezifikation für die neue Generation von OPC, die OPC Unified Architecture, auch bekannt als OPC UA. Der Interoperabilitätsstandard OPC UA für den sicheren und zuverlässigen Datenaustausch in der industriellen Automatisierung wurde 2008 als Überarbeitung des ursprünglichen OPC-Standards eingeführt. Die Client/Server-Architektur ist die Kernstruktur von OPC UA. Der OPC-Server setzt das Hardware-Kommunikationsprotokoll um, und jedes Programm, das sich mit der Hardware verbinden muss, wird dann zur OPC-Client-Software [21].

Der aktuelle OPC-Standard verwendet OPC UA, ein völlig anderes Modell als sein Vorgänger OPC DA. Es basiert auf den normalen Regeln der Vernetzung. Die Verbindungen bestehen zwischen IP-Adressen und basieren nicht auf proprietären Microsoft-Technologien. Es ist sehr sicher und kann zwischen zwei beliebigen PCs mit IP-Adressen über jede Art von LAN, WAN oder sogar das Internet verwendet werden und ist auch sehr Firewall-freundlich. Es ist vollständig interoperabel mit unterschiedlichen Geräten und Betriebssystemen, wodurch es den heutigen Anforderungen gerecht wird.

OPC-UA-Clients können mit OPC-UA-Servern problemlos kommunizieren, wobei die einzige Voraussetzung darin besteht, dass sie die IP-Adressen der anderen Teilnehmer sehen können (d. h. HTTPS/SSL/TCP), und zwar über jedes beliebige Netzwerk. Die Netzwerkroute kann Firewalls und Router über verschiedene Domänen hinweg sicher passieren, was es zu einem idealen Protokoll für die Zusammenführung von OT und IT macht. In OPC UA sind viele Verschlüsselungs- und Sicherheitsfunktionen integriert. Die Verwendung der Verschlüsselung mit privaten und öffentlichen Schlüsseln in beiden Richtungen authentifiziert und sichert die Interaktionen, wodurch es für den Einsatz in jeder Art von Topologie geeignet ist. Zusätzlich zum OPC UA-Standard umfasst die Plattform Kepserver erweiterte OPC-Client-

Zugriffskontrollen, die eine

kostenloses Plugin, das eine granulare Sicherheit für den Client ermöglicht, so dass er auf bestimmte Kanäle, Geräte, Gruppen und Tags zugreifen und ihnen Lese- und Schreibrechte erteilen kann [Abbildung 3].

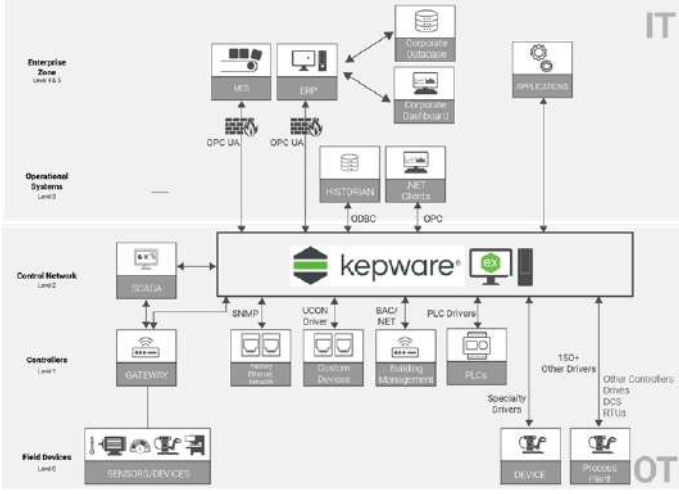


Abbildung 3: Kepserver (OPC Server Plattform) Industrielle Kommunikation - Topologie & Anwendungen

OPC UA ist mehr als nur ein Standardprotokoll, es ist ein umfassendes Rahmenwerk, das standardisierte Daten mit End-to-End-Sicherheit über mehrere Protokolle definiert und austauscht. Die größte Stärke von OPC UA ist, dass es eine

Rahmen und Normen für die Informationsmodellierung, die in allen Automatisierungssystemen verwendet werden können, um eine nahtlose Interoperabilität zu erreichen [22].

3. 3 Message Queue Telemetry Transport Protocol (MQTT)

Das IoT-Protokoll MQTT gewinnt zunehmend an Bedeutung und ist ein solider Konkurrent für das weit verbreitete OPC UA. Es wurde entwickelt, um entfernte Geräte mit einem minimalen Code-Fußabdruck und der kleinstmöglichen Netzwerkbandbreite zu verbinden. Es wurde als ein leichtgewichtiges Publish/Subscribe-Messaging-Transportprotokoll entwickelt. MQTT wird in vielen verschiedenen Branchen eingesetzt, z. B. in der Automobilindustrie, der Telekommunikation, der Öl- und Gasindustrie und der Fertigung.[23] Es ist leichtgewichtig, offen, einfach und leicht zu implementieren. Diese Eigenschaften machen es ideal für den Einsatz in vielen Situationen, einschließlich eingeschränkter Umgebungen, wie z. B. für die Kommunikation in Machine-to-Machine- (M2M) und Internet-of-Things- (IoT) Kontexten, in denen ein kleiner Code-Fußabdruck erforderlich ist und/oder die Netzwerkbandbreite sehr knapp bemessen ist. MQTT bietet kein Anfrage/Antwort-Muster und ist daher nicht zustandslos. Es handelt sich um eine sofortige, push-basierte Veröffentlichungs- und Abonnement-

Anwendungsschicht.

Messaging-Protokoll, das eine laufende TCP-Verbindung benötigt[24]. Das Protokoll läuft über TCP/ IP oder über andere Netzwerkprotokolle, die geordnete, verlustfreie, bidirektionale Verbindungen bereitstellen. Die neueste Version der Spezifikation, Sparkplug-B, bietet folgende Funktionen:

- Nutzt Pub / Sub
- Unterstützt Bericht nach Ausnahmen
- Bietet kontinuierliche Session Awareness
- Bietet Sterbe- und Geburtsurkunden
- Kümmert sich um dauerhafte Verbindungen
- Keine Daten verloren
- Aktiviert die automatische Erkennung
- Bietet a standardisierte Nutzlast-Definition
- Bietet a standardisiertes Themen-Namensraum

In dieser Architektur gibt es drei Rollen: MQTT-Publisher, MQTT-Broker und MQTT-Teilnehmer.[25] Die MQTT-Architektur ist einfach zu implementieren, verfügt über Datensicherheitsmechanismen und nutzt die Netzwerkbandbreite nur mäßig.

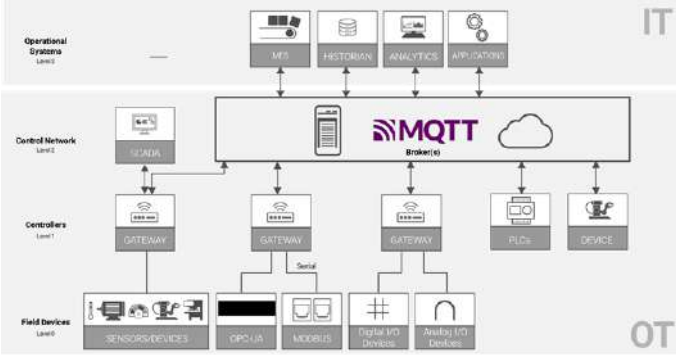


Abbildung 4: Verwendung eines Cloud-basierten MQTT-Brokers zur Verwaltung von OT-Daten für IT-Anwendungen, um Echtzeitaktualisierungen über das Pub/Sub-Modell zu erreichen.

Sparkplug-B

MQTT wurde entwickelt, um so offen und flexibel wie möglich zu sein, und das führte zu einem Protokoll, dem bestimmte Eigenschaften fehlten, die den industriellen Einsatz unterstützen würden. Der MQTT-Standard Sparkplug B befasst sich mit diesem Problem und beschreibt

die Übertragung und den Empfang von Daten. Anwendungen wie SCADA-Systeme, Historiker und Analyseprogramme können mit Sparkplug B eine Schnittstelle zu Geräten und Sensoren am Rande eines Netzwerks bilden. Der gesamte Austausch wird von einem MQTT-Broker abgewickelt [27].

Die Sparkplug-Spezifikation ergänzt MQTT um die folgenden Punkte:

- Ein einheitlicher Themen-Namensraum, der die Kommunikation zwischen verschiedenen Geräten und Anwendungen ermöglicht.

- Ein einheitliches Nutzdatenformat zur Definition des Datenformats, das von den Geräten und den Anwendungen gemeinsam genutzt wird.

- Ein Lebenszyklus, der festlegt, wie Geräte ein System koppeln und entkoppeln können.

	OPC UA	MQTT/Sparkplug B
Simplicity	Complicated to implement. Most companies do not implement the full OPC server. Requires routers, firewalls, VPN, etc. New devices will need to be re-configured. 1250 spec pages.	Developers can follow the specification. Easier to implements with devices added and auto discovered. Plenty of reference code.
Lightweight	Poll/response protocol traditionally – not reported by exception. Many devices that support OPC cannot handle a lot of subscriptions. Comes with basic tags and values but no meta data or objects.	Event-driven, reports by exception, minimal data footprint. Protocol overhead is significantly smaller. Includes essential meta data without adding bloat.
Flexibility	OPC has a hard time handling data from various legacy devices, operating systems and network architectures. Fall short for big data analytics applications as focus is predominantly OT and not IT.	Subscribers do not need to know who delivers the information they are subscribing to because MQTT is based on a pub/sub paradigm that decouples data providers from consumers. The protocol has a lot of versatility because the message's payload can be in any type of data format, including Base64, encrypted binary, JSON, and XML.
Cost Effectiveness	As a result of the architecture's requirement to include an OPC UA server into goods, prices and time-to-market are increased, along with CPU usage, footprint size, development costs, and continuing support expenses.	Brownfield device data access is made affordable with the IIoT driven by MQTT. From a sensor, to a device (such a PLC), to an Edge gateway, and finally up to the SCADA/MES system on the factory floor, MQTT can convey data.
Support	Although OPC has existed for a while, many IIoT solutions do not have native support for OPC communication. Only Microsoft employs both the older OPC UA client-server connections and the more recent OPC UA publish-subscribe connections. There aren't many OPC UA software clients available, and hardware vendor support has been meagre.	Vendors that natively support MQTT-Sparkplug on both the hardware and software sides are multiplying quickly. MQTT is supported by all of the top cloud providers, IoT platforms, edge computing platforms, big data apps, and other third-party software. To deliver auto discovery data modelling, forward-thinking cloud providers are utilizing Sparkplug.
Use Case	Multiple data consumers are difficult for OPC architectures to supply with all the necessary data. The real decoupling required for one-to-many is not done by an OPC UA server, but it does offer some one-to-some functionality. Additionally, most implementations don't include meta tag data, which again implies it fails to provide data to IT services in a way that they can use.	In today's IIoT environment, polling widely scattered assets for their data makes little sense. Any data consumer may easily subscribe to the data using MQTT, and pub/sub reduces bandwidth usage and streamlines the solution. However, when it comes to transferring data to the cloud and interacting with big data applications, discrete and process manufacturers who may be dedicated to OPC or OPC UA can also experience the benefits of MQTT.

Tabelle 1: OPC UA und MQTT(Sparkplug) im Vergleich

4 EXTERNE DATENKOMMUNIKATION

Für eine echte Fernüberwachung und Datenerfassung müssen interne Betriebsmittel in der Lage sein, relevante Daten nicht nur aus der Automatisierungsumgebung, sondern auch aus der Fabrikinfrastruktur heraus zu übermitteln, damit sie für externe Beteiligte zugänglich sind. Es gibt zahlreiche Technologien, die diese Funktion ermöglichen könnten. Jede verwendete Technologie muss nicht nur die Anforderungen an den Fernzugriff auf Daten erfüllen, sondern auch von den Automatisierungs- und IT-Teams innerhalb der Fabrikumgebung akzeptiert werden.

Zu den Überlegungen, die bei der Auswahl einer Technologie aus betrieblicher Sicht angestellt werden müssen, gehören die verfügbaren Sicherheitsvorkehrungen, die einfache Implementierung, die einfache Integration in bestehende Anlagen, die Skalierbarkeit der Lösung sowie die Fähigkeit, die Technologie in den bestehenden Rahmen des Fabrikmanagements zu integrieren. In diesem Abschnitt werden die vorhandenen Datenkommunikationstechnologien untersucht, die potenziell eingesetzt werden können, und es wird aufgezeigt, wo sich der aktuelle Trend zur Datenfernüberwachung in Bezug auf die Kommunikation außerhalb der Fabrik

abzeichnet.

4.1 Ziele der Cloud-Integration

In den letzten Jahren wurde Cloud-basiertes Computing als der nächste logische Schritt für die industrielle Automatisierung angesehen, der eine Reihe von potenziellen Vorteilen für die Automatisierungsbranche mit sich bringt. Einer der wichtigsten Vorteile der Cloud ist die Möglichkeit, fortschrittliche Analysen zur Verbesserung des Gesamtbetriebs zu nutzen. Daten von Betriebsanlagen, die an einem zentralen Ort gesammelt und analysiert werden, können Einblicke in die Fabrikhalle bieten, die bisher nicht möglich waren. Die potenziellen Anwendungen für diesen Einsatz der Cloud-Technologie sind in der Literatur gut dokumentiert [28] - [32], eine zusammenfassende Liste umfasst u. a. vorausschauende Wartung [28], Digital Twining von Anlagen [29], bessere Produktionsplanung [30], Energiemanagement von Anlagen [31], Integration mit Lieferkettensystemen [32]

Cloud-Integrationen könnten auch die Grundvoraussetzung für künftige Fortschritte in der Fertigung sein, wie z. B. den Übergang zu Einzel- und Serienfertigung sowie zur modularen und rekonfigurierbaren Fabrik [33].

Eines der traditionellen Hindernisse für eine vollständige Datenintegration auf Cloud-Ebene (oder sogar auf lokaler Ebene) ist die Schwierigkeit, anbieterspezifische Protokolle und Geräte zu integrieren und alte Abläufe einzubeziehen. Selbst die Verbindung mit ERP- oder MES-Systemen ist ein komplizierter Prozess, und selbst wenn eine Fabrik die Konnektivität gut hinbekommt, kann die Verwaltung oder Überwachung der großen Datenmengen, die generiert werden, ein Schritt zu weit sein. Eine Cloud-basierte Integration, bei der alle Daten an einem zentralen Ort zur weiteren Verarbeitung und Analyse gespeichert werden, bietet Vorteile für eine Reihe von Betriebsindikatoren. Damit eine Fabrik den Übergang zu einer intelligenten Fabrik vollziehen kann, muss die Integration verschiedener Datenströme in Angriff genommen werden, und es müssen Methoden für den Datentransport ermittelt werden.

Diese Cloud-Konnektivität erfordert die Zusammenarbeit zwischen den Automatisierungsteams, den IT-Teams und den Analyseteams einer Fabrik, um erfolgreich und effektiv zu sein. Die Gewinnung und Verwaltung der Daten und die Rückführung der Erkenntnisse in Ihr Werk erfordern eine sorgfältige Planung aus Sicht des Betriebs, der Infrastruktur, der Sicherheit und der Schulung (für Automatisierungs- und IT-Mitarbeiter).

Cloud-basierte Plattformen sind bereits vorhanden und bieten Unterstützung für Datenspeicherung, Datenmanagement und Datenanalyse. Microsofts Azure-Plattform, Amazons AWS oder die Google-Cloud sind gut etabliert und werden bereits in großem Umfang auch von anderen Bereichen der Unternehmensaktivitäten genutzt. Alle diese Plattformen bieten Unterstützung für privates und öffentliches Cloud-Hosting und ermöglichen die Nutzung einer beliebigen Anzahl von Datenspeicher-, Analyse- und Berichtsoptionen.

Um die Vorteile der Cloud nutzen zu können, müssen etablierte Methoden für das Streaming der erforderlichen Daten aus der Fabrik in die Cloud-basierte Infrastruktur ermittelt werden, und es muss ein Verständnis dafür geschaffen werden, wohin sich die Industrie derzeit bewegt.

4.2 Optionen für die Kommunikation

Es gibt viele etablierte Optionen, die die Anforderung erfüllen können, Daten aus der Automatisierungsumgebung in die verfügbaren Cloud-basierten Plattformen zu bringen. Die meist in Betracht gezogenen Protokolle sind [34], [35]

- AMQP

MQTT

- Co AP
- DDS
- OPC-UA
- HTTP

Ein kurzer Vergleich der Protokolle ist in Tabelle 2 dargestellt.

Features	AMQP	CoAP	MQTT	DDS	OPC-UA	HTTP
Message Interface	Broker,	Response, Request	Broker,	Response, Request	Response Request, Subscribe/publish*	Response Request
Quality of service	At most once , At least once, Exactly once	At most once, At least once	At most once , At least once, Exactly once	Guaranteed, Best effort	Best Effort	Best Effort
Persistence	Yes	No	Yes	Yes	No	No
Security Support	TLS / SSL	DTLS, IPSEC	TLS / SSL	TLS / DTLS /DDS	OPC-UA Specific	OSCORE, DTLS, etc.
Latency / Speed	QOS Dependent , but quicker than HTTP and other RR protocols	Relatively slow	QOS Dependent , but quicker that AMQP, HTTP and others	Configuration dependent	Slow	Slow
Complexity	High	Medium	Low	High	High	Medium
Primary Use case today	Business applications	Machine to Machine	Machine to Machine	Industrial IOT	IIOT	Web services
Strengths	Configurable QOS, different message patterns, extendable, good support,	Inbuilt support for content negotiation and discovery , relatively light weight	Lightweight, Configurable QOS, Performs well in intermittent connections, Good Support, Low Bandwidth, Low footprint	Highly configurable, good performance characteristics	Content negotiation inbuilt, fully defined specification wide acceptability within the factory floor.	Well established, high security options.
Weaknesses	High Bandwidth, Complex, Large message size, Slower than other options	Uses UDP as primary package type, adds overhead to make reliable, Slower than other options.	Lacks some advanced protocol features, security tied to TLS primarily, No ability to label messages	Service interruption is catastrophic UDP Messages only.	For external access security concerns, complex, large overhead to implement, slow.	Slow, Complex , Response only to clients

Tabelle 2: Vergleich externer Protokolle

Aufgrund der möglichen Optionen für die Verbindung von Daten aus der Fabrikhalle in die Cloud findet MQTT in einer Reihe von Branchen breite Akzeptanz [36]. Das Brokermodell ist aufgrund seiner Fähigkeit, schnell zu skalieren und die Kontrolle darüber, wie die Daten übertragen werden und wer was abhört, zu erweitern, sehr attraktiv. Es verfügt über eine integrierte Sicherheitsunterstützung, ist leichtgewichtig und relativ schnell und ermöglicht eine schnelle Datenerfassung zur Unterstützung von Anwendungen wie dem digitalen Zwilling. Der größte Nachteil ist die unstrukturierte Natur der Datenpakete und die fehlende Möglichkeit, Inhalte auszuhandeln und zu finden. Es gibt jedoch Standards wie Spark PlugB von Eclipse, die diese Lücke schließen sollen.

MQTT arbeitet mit einem Broker im Zentrum des Netzes, und die Clients veröffentlichen und abonnieren die Themen des Brokers, an denen sie interessiert sind. Abbildung 5 zeigt ein Beispiel für diese Struktur [37].

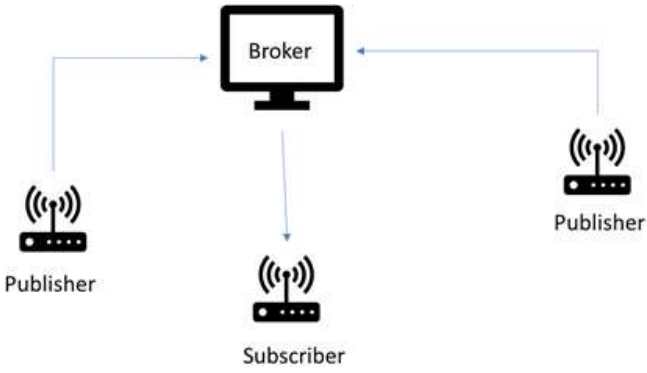


Abbildung 5: MQTT-Netzwerk

4.3 Maklerbasierte Kommunikation

Der Broker ist das Herzstück eines jeden Publish/Subscribe-Protokolls. Der Broker ist verantwortlich für den Empfang aller Nachrichten, das Filtern der Nachrichten, die Feststellung, wer jede Nachricht abonniert hat, und das Senden der Nachricht an diese abonnierten Clients. Der MQTT-Broker fungiert auch als Gatekeeper, da er die Sicherheitsanmeldeinformationen eines Clients anhand der festgelegten Regeln überprüft.

Der Broker kann auch den letzten Willen eines Kunden speichern und auf Wunsch Nachrichten von einem Herausgeber aufbewahren, bis ein interessierter Teilnehmer eine Verbindung herstellt. Diese entkoppelte Kommunikationsmethode ermöglicht eine skalierbare und leichtgewichtige Infrastruktur, und diese Skalierung ist für die Kunden transparent. Broker können für den Endnutzer durch Dienste wie Azure Io T Hub oder AWS Io T Core verwaltet oder selbst gehostet werden.

Ein weiteres Merkmal des MQTT-Brokers ist die Möglichkeit, Broker miteinander zu verbinden und Nachrichten von Broker zu Broker weiterzuleiten. Diese Funktion ermöglicht eine einfache horizontale Skalierung der MQTT-Infrastruktur und die Bildung von Broker-Clustern (aus Sicht der Endnutzer wird dies als ein einziger Broker betrachtet). Darüber hinaus kann die Infrastruktur auf diese Weise widerstandsfähig gemacht werden, und wenn dies richtig gemacht wird, können die Broker als eine Art Bollwerk fungieren, um eine weitere Sicherheitsebene zu jeder externen Verbindung hinzuzufügen [38]. Die nachstehenden Abbildungen zeigen, wie ein Broker-Cluster aussehen würde [Abbildung 5] und wie man Broker schichten könnte, um eine Verbindung zwischen dem Automatisierungsnetz und einer Cloud-Infrastruktur herzustellen [Abbildung 6]. Diese Abbildung zeigt einen mehrschichtigen Ansatz für die Implementierung eines

externe Cloud-Verbindung über MQTT. Eine Reihe von mehreren Brokern wird intern auf verschiedenen Ebenen innerhalb der Fabrik verwendet. Auf jeder Ebene können verschiedene Fabrikdienste auf den MQTT-Broker zugreifen (OT-Anwendungen auf den Ebenen 0-2, IT-Dienste 3 und 4 mit der endgültigen externen Verbindung nur von Ebene 4). OT-Dienste der Ebene 0-2 könnten die SPS, das SCADA-System, intelligente Sensoren oder sogar Daten sein, die direkt vom Historiker vor Ort abgerufen werden, falls gewünscht.

Der wichtigste Punkt ist, dass es nur auf Ebene 4 eine direkte Verbindung über MQTT zur Cloud gibt. Es gibt keine direkte Verbindung zu einer anderen Ebene der Fabrikdienste, und durch die Verwendung von überbrückten Brokern zu jeder Ebene sind die anderen Ebenen immer noch hinter ihren eigenen Brokern sicher, wenn eine Ebene kompromittiert wird.

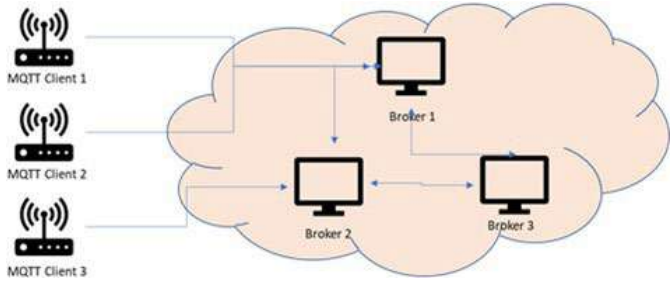


Abbildung 6: MQTT-Broker-Cluster

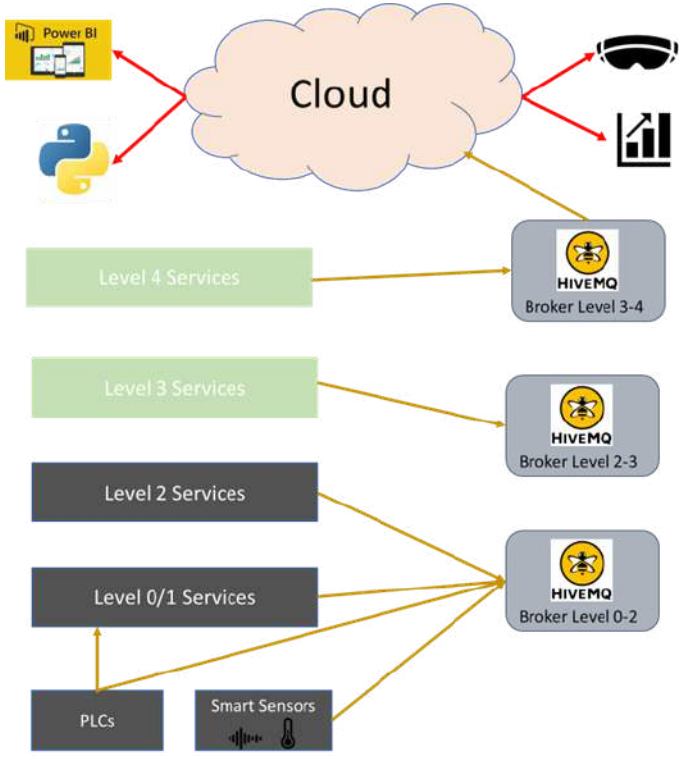


Abbildung 7: Mehrschichtiger Broker-Ansatz

5 Fallstudie: Arbeitsbeispiel

Hier wird eine Fallstudie zur Fernüberwachung vorgestellt. Die Systemkonfiguration umfasst den Einsatz einer Siemens SPS auf Werksebene, eines Eclipse Mosquitto Open Source (EPL/ EDL lizenziert) MQTT Message Brokers sowie NodeRed und andere Anwendungen zur Datenvisualisierung. In diesem Abschnitt werden die Hardwarezusammensetzung und die vorgeschlagene Systemarchitektur für die IoT-basierte Überwachung in einer Automatisierungsprozesslinie vorgestellt.

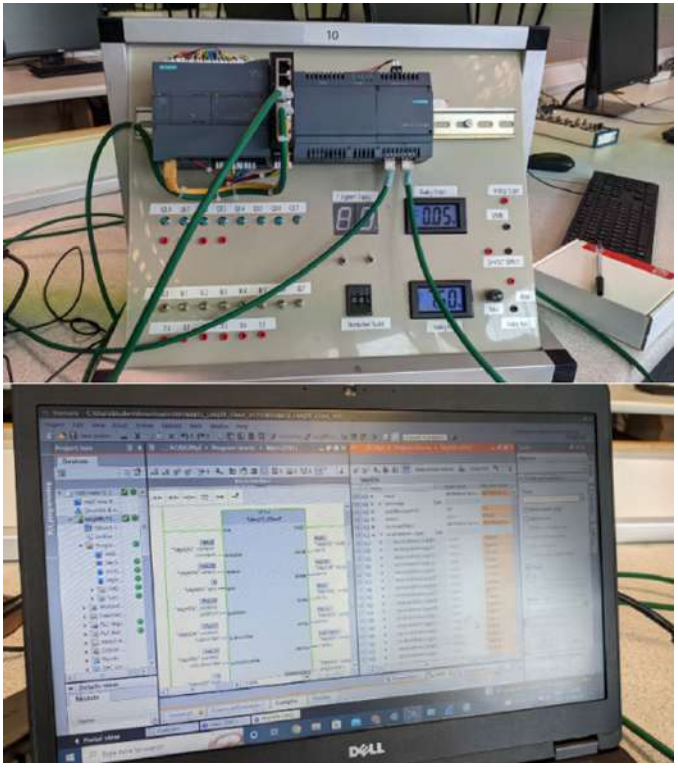


Abbildung 8: SPS (Siemens Simatic S7-1200) mit einem analogen Sensor. Totally Integrated Automation Portal (TIA Portal) als Schnittstelle zur Blockkonfiguration, um MQTT zu aktivieren.

Das leichtgewichtige IIo T-Kommunikationsprotokoll MQTT wurde in Verbindung mit einer SPS (Siemens Simatic S7-1200 [39], [40, S. 7-1200]) verwendet.

und dem dazugehörigen Gateway (Simatic IOT2000 [41]). Der Siemens LMQTT-Client-Block wurde verwendet, um Nachrichten an den Mosquitto MQTT-Broker auf der Simatic IOT2000 zu abonnieren und zu veröffentlichen, der wiederum mit einem externen MQTT-Broker (HiveMQ [42]) verbunden war. Um die Kommunikation zwischen dem LMQTT-Block und dem Simatic IOT2000 MQTT-Broker zu ermöglichen, müssen mindestens die IP-Adresse des Brokers, der MQTT-Port (1883 unsicher und 8883 sicher TLS), die Verbindungs-ID, der Payload und das Topic angegeben werden. Der LMQTT-Client verfügt auch über eine Qo S (Quality of Service) zur Qualitätssicherung der Nachrichtenübertragung. Es gibt drei Stufen von Qo S

0 - Auf der untersten Ebene gibt es keine Garantie, dass die Nachricht ankommt, und es gibt keine Bestätigung durch den Broker.

1 - die Nachricht wird garantiert an den Broker gesendet, aber die Nachricht kann mehr als einmal an den Broker gesendet werden.

2 - die höchste Dienstebene, bei der es einen Handshake gibt, um zu gewährleisten, dass die Nachricht nur einmal gesendet wird.

Um ein Topic zu veröffentlichen oder zu abonnieren, muss der publish/ subscribe-Parameter gepulst werden; wenn er gepulst wird, sendet der Block die Nutzlast der Nachricht an den Broker. Der LMQTT-Block unterstützt auch die Funktion "Letzter Wille und Testament", mit der andere MQTT-Client-Teilnehmer benachrichtigt werden können, wenn die Verbindung zum MQTT-Publisher unterbrochen wurde.

Abbildung 9: Netzwerkübersicht der S7-1200, Siemens IOT 2040, 5G-Modem und dem internetbasierten Hive MQ Test MQTT Broker.

Ein Siemens JSON (JavaScript Object Notation) Serializer-Block wurde ebenfalls verwendet, um die Nachricht in das JSON-Format zu konvertieren, bevor sie an

den LMQTT-Client-Block. Das JSON-Format ermöglicht die Übermittlung mehrerer Datenpunkte in einer einzigen Nachricht und die Möglichkeit, bei Bedarf Metadaten hinzuzufügen. . Es werden Echtzeit-Fernmesswerte von einem analogen Sensor (Potentiometer) demonstriert, der über eine Schnittstelle mit der SPS verbunden ist und über MQTT übertragen wird. (Abbildung 9). Die sichere MQTT-fähige SPS (durch die Verwendung der Protokollbibliothek (LMQTT) über TLS (MQTTs)) wurde so konfiguriert, dass sie das Publish/Subscribe-Modell mit dem externen Broker implementiert. Die erstellten Topics ermöglichen es verschiedenen Clients, Daten zu veröffentlichen und zu abonnieren, wodurch eine direkte Schnittstelle zu Telemetriedaten geschaffen wird. Die übertragenen Sensorwerte liegen im String-Format vor, das dann auf der Client-Seite zur Datenmanipulation in den Integer-Typ geparst wird. Die Nutzlast ist in diesem speziellen Fall ein einzelner Stream zu einem Thema. Es ist jedoch zu beachten, dass der Datenstrom vom Sensor zur Visualisierung strenge Sicherheitsmaßnahmen an jedem Knoten erfordert, um die sichere Zusammenführung von OT- und IT-Daten zu gewährleisten. Dies wird durch die Verwendung einer Zertifikatsauthentifizierung mit SSL-Protokoll sowie einer identitäts- und passwortgeschützten Verbindung erreicht [43]. Ein Vorteil der Verwendung von MQTT gegenüber anderen Protokollen wie OPC-UA ist die Flexibilität und die vereinheitlichende Natur der

Publish/Subscribe-Architektur gegenüber dem komplizierteren Client-Server-Modell

von OPC-UA. Diese "einzige Quelle der Wahrheit" und diese einheitliche Namespace-Struktur mit dem MQTT-Broker als Kernstück sowie das leichtgewichtige Protokoll und die einfache Integration sprechen für MQTT als Protokoll der Wahl [44]. Auf der Seite der Client-Anwendung parst ein MQTT-Client, M2MQTT, der eine Verbindung zu jedem MQTT-Broker ermöglicht [45], die Echtzeit-Stringwerte in Ganzzahlen, die in einem dynamischen Zeitseriendiagramm dargestellt werden. Die Möglichkeit, Nachrichten von der MR-Anwendung zurück in ein separates Thema im MQTT-Broker zu veröffentlichen, kann die SPS-Steuerung als abonnierter Client ermöglichen und qualifiziert die bidirektionale Kommunikation zwischen der physischen und der virtuellen Welt [Abbildung 10].

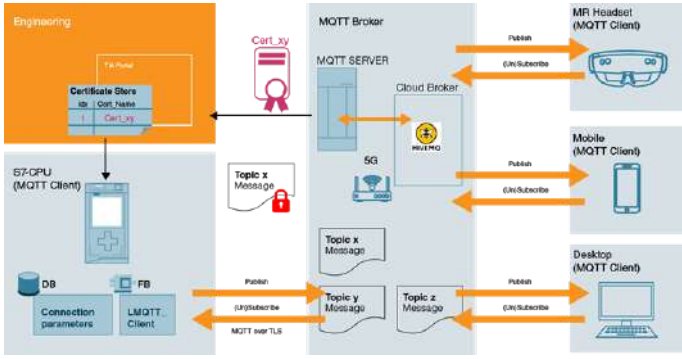


Abbildung 10: Sensordaten von einer MQTT-fähigen SPS veröffentlichen Daten an den

Broker, an den die Client (MR app) abonniert ist.

6 REFERENZEN

[1] Selcuk, S. (2017). Vorausschauende Wartung, ihre Umsetzung und neueste Trends. *Proceedings of the Institution of Mechanical Engineers, Part B: Journal of Engineering Manufacture*, *231*(), 1670-1679. doi: 10.1177/ 0954405415601640

[2] 5 Gründe für industrielle Fernüberwachung wird aufsteigen in 2021. (2021). abgerufen 12. Dezember 2022, von BehrTech Website: https:// behrtech.com/ blog/ 5-Gründe-fuer-iT-Driven-Remote-Monitoring-wird-im-Jahr-2021-aufsteigen/

[3] Lopes, G., & Junior, R. F. F. (2021). A MQTT-basiertes Datenüberwachungssystem für Energieeffizienz in industriellen Umgebungen, " VETOR-Rev. *VETOR-Rev. Ciênc. Exatas E Eng*, *31*(2), 25- 35.

[4] Rojko, A. (2017). Industrie 4.0 Konzept: Background and overview. *International Journal of Interactive Mobile Technologies (IJIM)*, *11*(5), 77. doi: 10.3991/ ijim.v 11i5.7072

[5] Ackerman, P. (2021). *Industrielle Cybersicherheit: Effiziente Überwachung der Cybersicherheitslage Ihrer ICS-Umgebung*. Packt Publishing Ltd.

[6] 4. 0 Solutions [@4.0Solutions]. (2018). Das 5-Schichten-Modell der Automatisierung... The 'automation stack'. Abgerufen von .12 Dezember 2022, von https:// www.youtube.com/watch? v=3u2cRRMlG7Q

[7] Emilio, M. D. P. (2013). *Datenerfassungssysteme: From Fundamentals to Applied Design*. Springer Science & Business Media.

[8] "Arten von industriellen Fernüberwachungslösungen und -prozessen - Technische Artikel. (2022). Abgerufen am 12. Dezember 2022, von https:// control.com/ technical-articles/ types-of- industrial-remote-monitoring-Solutions-and- processes/

[9] Almada-Lobo, F. (2016). Die Revolution der Industrie 4.0 und die Zukunft der Manufacturing Execution Systems (MES). *Journal of Innovation Management, 3*(4), 16- 21. doi: 10.24840/ 2183-0606_003.004_0003

[10] Lin, Z., & Pearson, S. (2013). An inside look at industrial Ethernet communication protocols, " Tex. *Tex. Instrum. White Pap*.

[11] Zurawski, R. (2019). *Integration technologies for industrial automated systems*. London, England: CRC Press.

[12] Elektrizität Forum. (2022). Industrielle Automatisierung undKommunikationNetzwerke. Abrufbar unter 12 Dezember 2022, von https:// www.electricityforum.com/iep/building-automation/industrielle-automatisierung-kommunikation

[13] Danielis, P., Skodzik, J., Altmann, V., Schweissguth, E. B., Golatowski, F., Timmermann, D., & Schacht, J. (2014). Umfrage zur Echtzeitkommunikation über Ethernet in der industriellen Automatisierung environments. *Proceedings of the 2014 IEEE Emerging Technology and Factory Automation (ETFA)*. Präsentiert auf der 2014 IEEE Emerging Technology and Factory Automation (ETFA), Barcelona, Spanien. doi: 10.1109/ etfa.2014.7005074

[14] Sauter, T. (2010). Die drei Generationen der Netzwerke auf Feldebene - Evolution und

Kompatibilitätsfragen. *IEEE Transactions on Industrial Electronics (1982)*, *57*(11), 3585- 3595. doi: 10.1109/ tie.2010.2062473

[15] Wollschlaeger, M., Sauter, T., & Jasperneite, J. (2017). Die Zukunft der industriellen Kommunikation: Automatisierungsnetzwerke im Zeitalter von Internet der Dinge und Industrie 4.0. *IEEE Industrial Electronics Magazine*, *11*(1), 17- 27. doi: 10.1109/ mie.2017.2649104.

[16] Gebäude, P. (2013). *Verdoppelung der Ethernet-Nutzung in der Prozessautomatisierung bis 2016*.

[17] Modbus Organisation. (2022). Abgerufen am 12. Dezember 2022, von https:// modbus.org/

[18] EETimes. (2022). Verstehen von Ethernet-gestützten industrielle Kommunikation Protokolle. Abgerufen von 12 Dezember 2022, von https:// www.eetimes.com/understanding- ethernet-based-industrial-communication- protocols/

[19] SA instrumentation & control. (2017). EtherCAT: Den Entwicklungen von Industrie 4.0 und IIo T voraus sein - technews industry guide: Industrial Internet of Things 2017. Abgerufen am 12.

Dezember 2022, von https:// www.instrumentation.co.za/57705n

[20] Processonline. (2010). Determinismus im Industrie-Ethernet: das EtherCAT-Protokoll. Abrufbar unter . 12 Dezember 2022, von http://processonline.com.au/content/industrial-networks-buses/ article/ determinism-in-industrial-ethernet-the-ethercat-protocol-1147271644

[21] Media, O. (2020). Ein modernes Protokoll: OPC UA vs MQTT. Abgerufen am 12. Dezember 2022, von der Embedded Computing Design Website: http://embeddedcomputing.com/technology/security/iec-iso-andere-standards/ a-modern-protocol-opc-ua-vs-mqtt

[22] isa.org (2019.). OPC UA: Die Vereinten Nationen der Automation. Abgerufen am 12. Dezember 2022, vonisa.org. Website: https://www.isa.org/intech- home/ 2019/ november-dezember/ features/ opc- ua-the-united-nations-of-automation

[23] mqtt.org. (2022). MQTT - der Standard für IoT-Nachrichten. Abgerufen am 12. Dezember 2022, von https:// mqtt.org/

[24] HiveMQ, (2022). MQTT Wesentliches. Abrufbar unter 12 Dezember 2022, von https:// www.hivemq.com/mqtt-essentials/

[25] mqtt.org. (2022). MQTT Spezifikation.Zurückgeholt 12 Dezember 2022, von https:// mqtt.org/ mqtt-specification/

[26] Obermaier, D. (2020). MQTT sparkplug essentials Teil 2 - Architektur. Abgerufen am 12. Dezember 2022, von https:// www.hivemq.com/blog/sparkplug-essentials-part-2-architecture/

[27] DataHub. (2021). MQTT SPARKPLUG B . Abgerufen am 12. Dezember 2022, von der Cogent DataHub Website: https:// cogentdatahub.com/ connect/ mqtt/ sparkplug- b/

[28] Kanawaday, A., & Sane, A. (2017, November). Maschinelles Lernen für die vorausschauende Wartung von Industriemaschinen mit IoT-Sensordaten. *2017 8th IEEE International Conference on Software Engineering and Service Science (ICSESS)*. Präsentiert auf der 2017 8th IEEE International Conference on Software

Engineering and Service Science (ICSESS), Peking, China. doi: 10.1109/icsess.2017.8342870

[2] Qi, Q., & Tao, F. (2018). Digitaler Zwilling und Big Data in Richtung Smart Manufacturing und Industrie 4.0: 360-Grad-Vergleich. *IEEE Access: Practical Innovations, Open Solutions*, *6*, 3585- 3593. doi: 10.1109/ access.2018.2793265

[30] Liu, J.-L., Wang, L.-C., & Chu, P.-C. (2019). Entwicklung eines cloudbasierten Planungs- und Terminierungssystems für die Automobilzuliefererindustrie. *Procedia Manufacturing*, *38*, 1532- 1539. doi: 10.1016/ j.promfg.2020.01.133

[31] Katrakazas, P., Costantino, M., Magnea, F., Moore, L., Ismail, A., Bourithis, E., ... Ferrario, F. (2021). Ein Rahmen für ein gleichberechtigtes Energiemanagement im Hinblick auf Benchmarking-Praktiken und Erwartungen: Der Ausblick des EnerMan-Projekts. *Systems*, *10*(1), 2. doi: 10.3390/ systems10010002

[32] Lu, Y .-K., Liu, C .-Y., & Ju, B .-C. (2012, November). Cloud Manufacturing Collaboration: An Initial Exploration. *2012 Third World Congress on Software Engineering*.

Vorgestellt auf dem 2012 4th World Congress on Software Engineering (WCSE), Wuhan, China. doi: 10.1109/ wcse.2012.39

[33] Chen, B., Wan, J., Shu, L., Li, P., Mukherjee, M., & Yin, B. (2018). Smart Factory of Industry 4.0: Schlüsseltechnologien, Anwendungsfälle und Herausforderungen. *IEEE Access: Practical Innovations, Open Solutions*, *6*, 6505- 6519. doi: 10.1109/ access.2017.2783682

[34] Chen, F., Huang, Y., Zhu, J., Gao, S., Sui, Z., & Duan, M. (2020, October 28). Messung und Analyse von Netzwerkdaten basierend auf dem MQTT-Protokoll. *2020 IEEE 20th International Conference on Communication Technology (ICCT)*. Vorgestellt auf der 2020 IEEE 20th International Conference on Communication Technology (ICCT), Nanning, China.
doi: 10.1109/ icct 50939.2020.9295944

[35] Silva, D., Carvalho, L. I., Soares, J., & Sofia, R. C. (2021). Eine Leistungsanalyse von Internet der Dinge Netzwerkprotokollen: Evaluating MQTT, Co AP, OPC UA. *Applied Sciences (Basel, Schweiz)*, *11*(11), 4879. doi: 10.3390/ app11114879

[36] Shahri, E., Pedreiras, P., & Almeida, L. (2022). Erweiterung von MQTT mit Echtzeit-Kommunikationsdiensten auf Basis von SDN. *Sensoren (Basel, Schweiz)*, *22*(9), 3162. do i: 10.3390/ s22093162

[37] Mishra, B., & Kert esz, A. (2020). Die Verwendung von MQTT in M2M- und IoT-Systemen: A surv ey. *IEEE Access: Practical Innovations, Open Solutions*, *8*, 201071- 201086. do i: 10.1109/ access.2020.3035849

[38] Protskaya, Y., & Velt ri, L. (2019, Oct ober). Makler Überbrückung Mechanismus für die Bereitstellung von Ano nymit y in MQTT. *2019 10th International Conference on. Netzwerke von der Zukunft (NoF)*. Aktuelle Ausgabeder 2019 10t Internat io nal Conference on Net works of the Fut ure(No F), Rom, Italien. do i: 10.1109/ nof47743.2019.9015087

[39] siemens.com. (2022, November 28). SIMATIC S7-1200 -Takeco nt rolof co mmunicat ion. Abgerufen am 12. Dezember 2022, von siemens.com Glo bal Websit e: ht t ps: / / new.siemens.co m/ glo bal/ de/ pro duct s/ aut o mat io n/ s 1200.ht ml

[40] Sable, A., Dongre, T., Modase, M., Surushe, A., & Diware, V. (2018). *Brooding Systems in Poultry Farm a Review*.

[41] *siemens.com.* (2021, 2. Dezember). Simat ik iot 2000. Abgerufen am 12. Dezember 2022 von der Website siemens.com Glo bal Websit e: ht t ps: / / new.siemens.co m/ glo bal/ de/ pro duct s/ aut o mat io n/ p based/ io t -gat eways/ io t 2000.ht ml

[42] hiv emq.com. (2022). Der kostenlose öffentliche MQTT-Broker von Hiv eMQ - Sehen Sie sich unsere MQTT-Demo an. Abgerufen am 12. Dezember 2022, von ht tps:// www.hiv emq.com/public-mqt t-broker/

[43] IBM. (2022, November 30). IBM do cument at ion. Zurückgezogen am 12. Dezember 2022, von ht tps://prod.ibmdocs-pro duct io n-dal-6099123ce774e592a519d7c33db8265e-0000.us-so ut h.co nt ainers.appdomain.cloud/ docs/ de/ ibm- mq/ 7.5? to pic=m2m-mqt t-securit y

[44] Mandit ereza, K. (2022, Juli 12). Die Hauptunterschiede zwischen OPC UA und MQTT Sparkplug. Abgerufen am 12. Dezember 2022, von ht tps:// www.hiv emq.com/blog/iiot-protocols-o pcua-v s-mqt t-spark plug-digit al- transfo rmat ion/

[45] M2Mqtt & Gnat MQ. (2022). M2Mqtt. Abgerufen am 12. Dezember 2022, von M2Mqtt & Gnat MQ Website: https:// m2mqtt.wordpress.com/

Vier

Korrigierende Fernwartung

Mirco Lovisetto, ENAIP VENETO, Padua, Italien, padova@enaip.veneto.it

***

Ziel dieses Beitrags ist es, den Begriff "Wartung 4.0" oder Fernwartung im Rahmen der breiteren Debatte über Industrie 4.0 (oder die vierte industrielle Revolution) zu definieren. Dieser Begriff steht für den radikalen Paradigmenwechsel, den das verarbeitende Gewerbe in den letzten Jahren dank der Verbreitung digitaler Technologien und ihrer Integration in die Produktionskette erlebt hat. Diese Revolution hat sich zum einen auf die Unternehmen ausgewirkt, indem sie sie "intelligent" gemacht hat, und zum anderen auf die betrieblichen Abläufe.

Angesichts der immer intelligenteren Fabriken und Produktionsanlagen, die mit modernsten Werkzeugen ausgestattet sind

und Technologien ist klar, dass die Ausbreitung von Industrie 4.0 ein Phänomen ist, das in den kommenden Jahren nicht nur die Abbildung und den Betrieb von Prozessen, sondern das gesamte Fertigungsparadigma grundlegend verändern wird.

Keywords: Remote Maintenance, Remote Corrective Maintenance, Industry 4.0, IoT, Cloud, AR, VR

1. EINFÜHRUNG

Der Startschuss für Industrie 4.0 fiel 2011 mit der Vorstellung des deutschen Industrie 4.0-Programms.
4.0-Politik zur Erneuerung der verarbeitenden Industrie [4]. Nur wenige Länder, wie die USA und Japan, verfolgten bereits eine ähnliche Politik ohne großes Interesse an der wissenschaftlichen Forschung, aber mit der Zeit begannen immer mehr Länder, Pläne zur Innovation ihres Industriesektors zu verabschieden.

Heutzutage verfolgen alle Staaten der ersten Welt eine entsprechende Wirtschaftspolitik.

Dieser Wandel wurde von der Wissenschaft als eine echte industrielle Revolution bezeichnet, genauer gesagt als die vierte, und zwar aufgrund folgender Faktoren

der tiefgreifende Wandel in der Konzeption der Industrieanlage im Vergleich zu früher.

Die Grundsätze der Umgestaltung sind im Wesentlichen auf die Digitalisierung und Vernetzung von Geräten zurückzuführen, um zahlreiche Vorteile zu erzielen: Überwachung, Autonomie, erweiterte Realität, Analyse, Vorhersagen, Simulationen, Verwaltung von Ereignissen in Echtzeit, Zusammenarbeit zwischen Maschinen und Mensch-Maschine, Optimierung des Endprodukts im Allgemeinen.

Dies führt zu einer besseren Leistung in Bezug auf Geschwindigkeit, Qualität, Sicherheit und Kosteneffizienz. Auch der Arbeiter profitiert von den verschiedenen Werkzeugen zur Verwaltung und Überwachung der Anlage, die seine Arbeit vereinfachen und gleichzeitig das Endergebnis optimieren.

Insbesondere wollen wir die Umsetzung der Analyseseite in der Industrie 4.0 durch die Anwendung von Prognostik und Predictive Maintenance zeigen.

Das auf Maschinen angewandte maschinelle Lernen kann eine Reihe von Vorhersagen ableiten, die den Arbeitern helfen, Entscheidungen für die Anlage zu treffen

Management und machen die Maschinen selbst intelligent, um ihre Arbeit zu optimieren und so autonom wie möglich zu werden. Das ideale Szenario für die Industrie
4.0 ist die totale Maschinenautonomie; Maschinen können ihre eigene Leistung verstehen und auf dieser Grundlage Entscheidungen treffen, um die Produktion zu verbessern, ohne dass der Mensch eingreifen muss [4].

2. METHODOLOGIE

Die Forschungsmethode des vorliegenden Kapitels sah eine Sammlung von Informationen durch die Analyse von Handbüchern, wissenschaftlichen Artikeln und anderen vor, um den Begriff "korrigierende Fernwartung" im weiteren Sinne als "Wartung 4.0" im Rahmen des Szenarios "Industrie 4.0" zu definieren.

Um das Szenario der "korrigierenden Fernwartung" im Rahmen des RE-MAIN-Projekts zu verstehen, haben wir beschlossen, einen Fragebogen einzureichen, um eine Momentaufnahme des Stands der Technik in Italien, einem der Projektpartner, zu erhalten.

Die eher kleine, aber für die allgemeine Situation illustrative Stichprobe führt uns zu einer Erzählung zurück, die unterstreicht, wie die

Die Übergangsphase zu Industrie 4.0 ist aktueller denn je [4].

Dies zeigen die erhobenen Daten, die bestätigen, dass die befragten Unternehmen auf verschiedenen Ebenen zu einem grundlegenden Wandel der Instandhaltungssysteme tendieren, indem sie sich mehr und mehr auf eine vorausschauende und vernetzte Instandhaltung zubewegen, was mit Sicherheit zu einer Senkung der Betriebskosten führt, einem immer wichtigeren Budgetposten für die Wettbewerbsfähigkeit der Unternehmen im internationalen Umfeld.

2.1 Defintion

Die grundlegende Definition von Fernwartung bedeutet, dass Computersysteme von einem entfernten Standort aus überwacht und gesteuert werden können.

Dies geschieht durch die Platzierung von Software auf lokalen Systemen, auf die von anderen Standorten aus zugegriffen werden kann.

Häufig arbeiten diese Systeme über eine Internetverbindung, doch kann die Software auch lokale Analysen durchführen, kritische und unkritische Situationen ermitteln und Rückmeldungen für

Präventivmaßnahmen. Darüber hinaus unterstützt uns die Technologie auch bei der sogenannten AR-Fernwartung.

Die Funktionsweise von Augmented Reality für die Fernwartung besteht in der Kombination von kopfgetragenen Helmen, die an die Sicherheitsbedürfnisse vor Ort angepasst sind, und der Nutzung der neuesten AR-Technologie. Auf diese Weise kann die Wartung aus der Ferne schneller und effizienter durchgeführt werden.

Die AR-Fernwartung bietet eine audiovisuelle Methode zur Analyse des Systems und zur Unterstützung der Mitarbeiter bei Wartungsarbeiten.

Wir werden erläutern, wie Augmented Reality dezentrale Dienste für eine Vielzahl von Organisationen verbessern kann.

2 2.1 Organisation

Im Mittelpunkt der Fernwartung steht die Organisation, die die Wartung benötigt, und nicht der Dienstleister, der aus der Ferne arbeitet. Dies gilt in der Regel für Prozesse, die unter Verwendung von Computerhardware und -software mit irgendeiner Art von Konnektivität durchgeführt werden.

Dabei kann es sich um ein Computerterminal handeln, das die Beleuchtung eines ganzen Gebäudes steuert, um einen PC, der für Verwaltungszwecke verwendet wird, oder um eine Maschine in einer Fabrik mit einer zentralen Verarbeitungseinheit [2]. Praktisch jede Maschine verfügt über irgendeine Art von Software, und oft sind diese Geräte miteinander verbunden.

Um sicherzustellen, dass Maschinen und Geräte weiterhin funktionieren, müssen verschiedene Sicherheitsmaßnahmen getroffen werden. Zum Beispiel Spyware- und Virenscanner, Möglichkeiten zur Wiederherstellung der Werkseinstellungen oder aktualisierte Backup-Images, damit Daten nicht verloren gehen. Viele dieser Aufgaben werden automatisch mit der lokal installierten Software erledigt, einige Aufgaben werden manuell von geschulten Mitarbeitern durchgeführt. Für den Support und den fortgeschrittenen Betrieb kann die Fernwartung auf verschiedene Weise genutzt werden.

2.2.2 Netzwerk

Einige Wartungsarbeiten können lokal durchgeführt werden, aber fortgeschrittenere Tätigkeiten erfordern mehr Fachwissen oder maßgeschneiderte Lösungen. Dies erfordert die Interoperabilität sowohl lokaler als auch dezentraler Netze, Systeme und Diensteanbieter.

Intern wird eine Intranetlösung zur Verfügung stehen, externe Dienste werden über eine Internetverbindung funktionieren.

Diese Dienste werden im Allgemeinen als "Cloud-Dienste" bezeichnet, die für alle digitalen Dienste gelten, die über verschiedene Internetkanäle übertragen werden.

Es liegt auf der Hand, dass die Sicherheit ein wichtiger Faktor bei der Aufrechterhaltung einer sicheren und funktionalen Umgebung ist, denn jedes System, das mit einem anderen Gerät verbunden ist, ist anfällig.

Dies gilt auch für lokale Netze, z. B. für USB-Laufwerke, die an Firmencomputern verwendet werden.

Bei der Fernwartung ist das Netzmanagement von entscheidender Bedeutung, um eine sichere und zuverlässige Methode zur Steuerung von Computersystemen zu bieten, bei der das richtige Gleichgewicht zwischen intelligenter Software und kompetenten Fachleuten vorhanden sein sollte.

2.2.3 Augumented Reality

Die grundlegende Erklärung von Augmented Reality ist eine Überlagerung von digitalen Informationen mit der realen Umgebung [3]. Nehmen wir einen Lagerarbeiter als Beispiel.

Ein Kommissionierer trägt eine AR-Brille, die die richtige Linie im Lager anzeigt. Während er ein EPT fährt, zeigt das tragbare Gerät deutlich Pfeile an, die den Mitarbeiter durch das Lager zum richtigen Ort führen.

Sobald das Ziel erreicht ist, wird die integrierte Kamera zum Scannen des Produkt-Barcodes verwendet. Der Bediener kann beide Hände zum Entnehmen der Bestellung verwenden, da alle AR-Aktionen über Sprach- oder Bilderkennung ausgeführt werden.

Die AR-Brillen fungieren als virtuelle Assistenten, die akustische und visuelle Signale für den Nutzer nutzen. Einige dieser Funktionalitäten sind offline verfügbar, andere erfordern eine aktive Internetverbindung.

Ein Beispiel dafür ist die AR-Fernwartung, bei der Augmented-Reality-Geräte zur Analyse und Kontrolle der Infrastruktur eingesetzt werden. In diesem Fall spielen sowohl der menschliche Aspekt als auch die Online-Konnektivität eine wichtige Rolle in der Gleichung.

2.2.4 Remote AR

Das Wort "remote" kann auf unterschiedliche Weise interpretiert werden. In der Regel bedeutet es "nicht am aktuellen Standort", was bedeutet, dass das Fachwissen

von einem anderen Ort herbeigeholt werden. Dabei kann es sich um einen lokalen Experten handeln, der von einem Büro aus arbeitet, oder um einen Spezialisten, der außerhalb der bestehenden Anlagen tätig ist. Es gibt mehrere Möglichkeiten, wie die AR-Fernwartung für industrielle Zwecke eingesetzt werden kann, hier einige Beispiele:

1. Ein Wartungsarbeiter wird mit der Reparatur eines Aufzugs beauftragt. Während der Fahrt zum Einsatzort sucht er in einem AR-Viewer nach Informationen über dieses spezielle Modell und die Revisionshistorie. Vor Ort angekommen, untersucht der Techniker den Aufzug und stößt auf einige Probleme. Der Arbeiter kontaktiert die Zentrale und bittet um Informationen über das weitere Vorgehen. Der Kollege kann Informationen einholen und den Techniker vor Ort durch den Prozess führen.

2. Eine Anlage in einem Hochrisikobereich der Fabrik funktioniert nicht mehr. Ein Bediener ist in der Lage, den Ort zu erreichen, aber aus Sicherheitsgründen ist es einem Experten nicht möglich, diesen Ort zu erreichen. Der Bediener stellt eine audiovisuelle Verbindung mit dem Experten her und

zeigt die aktuelle Situation an. Dies ist möglich, weil das AR-Gerät mit einem Mikrofon und einer Kamera ausgestattet ist. Dieses Mikrofon funktioniert auf zwei Arten, so dass der Bediener und der Experte eins zu eins kommunizieren können. Der Experte führt den Bediener durch den Prozess, damit die Störung behoben werden kann. Es ist nicht wichtig, wo sich der Experte befindet. Er kann sich im selben Gebäude oder in einem anderen Land befinden. Solange eine audiovisuelle Verbindung hergestellt werden kann, kann das Ad-hoc-Team die betreffende Aufgabe durchführen.

AR Telemaintenance bietet eine neue Perspektive für die dezentralisierte Verwaltung von Hardware, Software und Personal, mit erheblichen Vorteilen für den Industriesektor.

2.2.5 Vorteile

Natürlich ist die Einführung der Fernwartung für das Unternehmen mit Investitionen verbunden, z. B. in Sensoren und Software für die Verwaltung und Analyse von Daten in Echtzeit, doch mittelfristig sind die Vorteile in Form von Produktivitäts- und Effizienzsteigerungen weitaus größer, da zahlreiche negative Auswirkungen

auf Geschäft Kontinuität und Geschäft vermieden werden. Lassen Sie uns kurz sehen, welche das sind:

1. Null Ausfallzeit und konsequente Verbesserung der Produktivität

2. Verlängerung der Lebensdauer von Anlagen und Aufschub von Neuanschaffungen

3. Verringerung der Kosten und der Komplexität von Reparaturen

4. Milderung von zusätzlichen oder verbundenen Schäden

5. Verbesserte Einhaltung der Vorschriften mit Regulierungsstandards

6. Optimale Verwaltung von Ersatzteilen und Beständen

The numbers of predictive maintenance

All dies wirkt sich letztlich positiv auf den Unternehmensumsatz aus, insbesondere für all jene Unternehmen, die ihre Produktion intensiv und flexibel nutzen

Vermögenswerten, um dem immer stärker werdenden globalen Wettbewerb standhalten zu können.

Man hat auch versucht, die tatsächlichen Einsparungen durch vorausschauende Instandhaltung abzuschätzen: Laut einer Studie von Deloitte [5] steigert eine solche Strategie die Produktivität im Durchschnitt um 15 %, reduziert die Ausfälle um 15-30 % und die Wartungskosten um 25 %.

Der Studie zufolge liegt der Hauptnutzen in der Verringerung ungeplanter Ausfallzeiten, deren Kosten für Industrieunternehmen weltweit auf 50 Milliarden Dollar pro Jahr geschätzt werden können.

Eine weitere Untersuchung, diesmal von dem Branchenforschungsunternehmen Enterprise Strategy Group (ESG) durchgeführt, schätzt die durchschnittliche Ausfallzeit nach einem Unfall auf etwa 1,5 Stunden, während andere Studien von einem höheren Durchschnitt von drei bis vier Stunden ausgehen.

Wenn es also zu einer Betriebsunterbrechung kommt, die zu einer Untätigkeit der Arbeitnehmer führt, hat das Auswirkungen auf die Arbeitskosten, die sich auf mehrere tausend Euro belaufen können.

				
	Industry 1.0	**Industry 2.0**	**Industry 3.0**	**Industry 4.0**
Timeline	18th Century (1784)	19th Century (1870)	20th Century (1969)	21st Century (Today)
Production System	First Mechanical Loom	First Production Line Cincinnati Slaughter House Car assembly	First Programmable Logic Controller (PLC) Modicon 084	Cyber Physical System (CPS)
Technology	Introduction of water and steam powered mechanical manufacturing system	Introduction of electrically powered mass production based on the division of labour	Uses electronics, IT and OT to achieve further automation of manufacturing	Convergence IT and OT, autonomous machine based on Cyber-Physical Systems (CPS)
Competitive Priorities Evolution	Quality, Cost	Quality, Cost, Time	Quality, Cost, Time, Flexibility	Quality, Cost, Time, Flexibility, Innovation, Adaptability
Manufacturing Concept	Mass Manufacturing	Moving Assembly Line	Mass Customisation	Mass Personalisation

Abbildung 1: Der Übergang von der Industrie 1.0 zur Industrie 4.0 Digital Abbildung von https://electgo.com/resources/what-is-industry-4-0-Teil3 (2022)

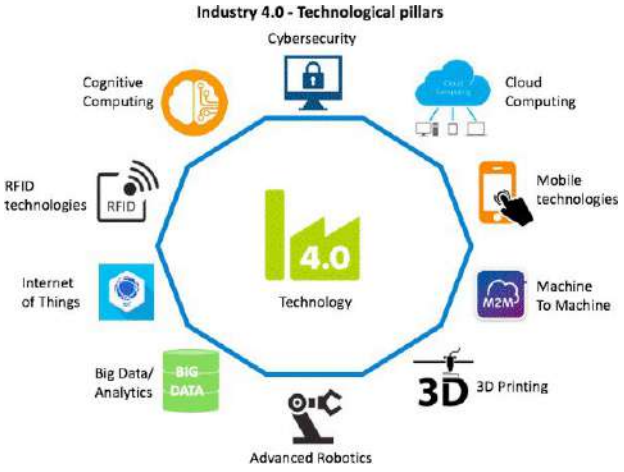


Abbildung 2: Allgemeiner Blick auf Industrie 4.0 Digitales Bild von https://universoabierto.org/2020/03/26/mapeo-del-panorama-actual-del-compromiso-de-la-biblioteca-de-investigacion-con-las-tecnologias-emergentes-en-investigacion-y-aprendizaje/ (2022)

Abbildung 3: Fernwartung (AR) Digitales Bild aus

https://www.industriaitaliana.it/dove-vuole-arrivare-lenze/ (2022)

3. RESULTATE

Im Rahmen dieses Kapitels haben wir beschlossen, die Ergebnisse einer kurzen Umfrage in den Partnerländern des Projekts einzubeziehen. Der Fragebogen, der aus 11 Multiple-Choice-Fragen besteht, wurde an Unternehmen verschickt, die sowohl auf dem nationalen als auch auf dem internationalen Markt tätig sind und - gemessen an der Zahl der Beschäftigten - aus kleinen, mittleren und großen Branchen stammen.

Es zeigte sich, dass IOT, Cybersicherheit [7,8], Cloud Computing, Industrie 4.0 und Fernwartung Themen sind, die intern durchaus diskutiert werden und mit denen auf verschiedenen Ebenen eine gewisse Vertrautheit besteht.

Insbesondere auf die Frage *"Haben Sie schon einmal von Fernwartung gehört?"* antworteten 92 % der Befragten mit "Ja", was sehr deutlich zeigt, dass zumindest die Debatte über dieses Thema im Gange ist.

Analysiert man stattdessen das Interesse an einer bestimmten Ausbildung, so zeigt sich, wie heterogen die Daten sind, aber sie bestätigen das Interesse von mindestens 50 % der Befragten an den folgenden Bereichen:

- Internet der Dinge (IoT)
- Cyber-Sicherheit
- Industrie 4.0
- Fernüberwachung Überwachung von Installationsvariablen und Ferndatenerfassung

Fernaktualisierung von Programmen und Funktionalitäten

4. SCHLUSSFOLGERUNGEN

Angesichts der durchgeführten Analyse, die durch die Suche nach Informationen im Internet und die Verabreichung des Fragebogens an Unternehmen erstellt wurde, können wir sagen, dass der Übergang zu Industrie 4.0 zweifellos auf dem Weg in eine neue Ära ist.

Dies wird auch durch die Tatsache bestätigt, dass die ENAIP, einer der größten Berufsbildungsanbieter in Italien, zahlreiche Anfragen für geschulte Techniker im Bereich der Fernverbindungen hat; eine davon ist ein Unternehmen namens Arneg, ein multinationales Unternehmen, das sich mit Kühlsystemen für Lebensmittel beschäftigt.

Die technische Figur, die sie brauchen, ist der Kältetechniker, der im Bau und in der Wartung von Anlagentechnik für die Großverteilung tätig ist.

Die typische Ausbildung in den Schulen für diese Zahl umfasst die Grundlagen der Thermotechnik, Elektrotechnik, Elektronik, Hydraulik und

Mechanik; Themen wie Fernverbindungen und Cybersicherheit werden nur am Rande behandelt.

Der typische Einsatz eines Kältetechnikers ist eine Serviceanfrage eines Kunden, nachdem die Kühlanlage ausgefallen ist. In diesem Szenario muss der Techniker sofort persönlich zum Kunden gehen, ohne zu wissen, was das Problem sein könnte.

Mit der vorausschauenden Wartung können Fehler vorhergesagt und mit einem Überwachungssystem und einer Fernverbindung die auszutauschenden Komponenten identifiziert werden [1].

Das Ergebnis wäre, den Kunden mit allem zu erreichen, was zur Wiederherstellung der Funktionsfähigkeit erforderlich ist, ohne unnötige Fahrten.

Man kann also erahnen, welche Vorteile sich für alle Beteiligten ergeben würden: Der Techniker spart Zeit, die er anderen Arbeiten widmen kann, und der Kunde spart aus wirtschaftlicher Sicht Zeit.

Nicht zuletzt geht es um die Einsparung von Energieressourcen.

In Anbetracht dieser Überlegungen ist klar, in welche Richtung die Ausbildung von Technikern in allen Aspekten der Industrie 4.0, die in allen europäischen Industriesektoren zunehmend gefragt ist, in naher Zukunft gehen muss.

5. REFERENZEN

[1] Stefano Monti. (2018-2019). Masterarbeit, POLITECNICO DI TORINO, Studiengang Technische Informatik mit Spezialisierung auf Software. Industrie 4.0: Io T-Architektur und vorausschauende Wartung. Abgerufen von https:// webthesis.biblio.polito.it/ 9519/ 1/ tesi.pdf

[2] Jorge Calvo. (2018). Die Fabrik der Zukunft. Zurückgeholt . von . https:// www.thefuturefactory.com/blog

[3] VR OWL. Augmented Reality, (2022). Abgerufen von von https:// argus-remote.com/ was-ist-Fernwartung-und-wie-kann-ihre-Branche-es-verwenden/

[4] Colin Koh. (2021). Senior . Business Development Manager, Industrie 4.0, abgerufen

von https:// www.electgo.com/what-is-industrie-4/

[5] Deloitte. (2017). Touche Tohmatsu Limited, Iot Lösungen, abgerufen . von https:// www2.deloitte.com/ it/ it/ pages/ technology- media-and-telecommunications/ articles/ iot- solution-world-congress---deloitte-italy---tmt.html

[6] Techtarget inc. (2022). Cibersecurity, abgerufen von https:// www.esg-global.com/

[7] Arneg s.p.a. (2022). 24h Überwachung, zurückgezogen von https:// www.arneg.it/it/monitoraggio-h24

Fünf

Fernaktualisierung von Programmen und Funktionen

Gregor Kandare, CAMPUS 02 Hochschule für angewandte Wissenschaften, Graz, Österreich,
gregor.kandare@campus02.at

Die Aktualisierung von Funktionalitäten ist ein wichtiges Element im Lebenszyklus von industrieller Steuerungssoftware. Die Fernaktualisierung von Programmen und Funktionalitäten in industriellen Steuerungssystemen ermöglicht es, die Leistung industrieller Anlagen mit sehr geringem Kosten- und Ressourcenaufwand aufzurüsten und zu verbessern. Allerdings muss dem Thema Cybersicherheit große Aufmerksamkeit gewidmet werden, da industrielle

Kontrollsysteme stellen häufig kritische und damit anfällige Infrastrukturen dar.

Keywords: industrial control systems, software update, remote, cybersecurity

1. EINFÜHRUNG

Moderne Industrieanlagen stehen heute vor großen Herausforderungen, die sie bewältigen müssen, um auf dem Markt zu bestehen und zu überleben. Die wichtigsten Herausforderungen sind der wachsende Wettbewerb, unvorhersehbare Energiequellen und deren Preise aufgrund der Marktvolatilität und der turbulenten geopolitischen Lage. Die Unternehmen müssen die immer strenger werdenden Umweltvorschriften einhalten. Darüber hinaus ändern sich in der heutigen, sich schnell verändernden Welt auch die Marktanforderungen aus vielen Gründen rasch, und die industriellen Produktionsanlagen müssen darauf vorbereitet sein, auf diese Veränderungen umgehend zu reagieren.

Eine Antwort auf die beschriebenen Herausforderungen ist die Übernahme und Umsetzung der Prinzipien von Industrie 4.0 mit digitaler Transformation der Wertschöpfungsketten. Ein wichtiger Aspekt der Digitalisierung im Kontext von Industrieanlagen ist auch die Fähigkeit zur Remote

Zugang/Kontrolle von industriellen Kontrollsystemen. Fernzugriff Zugang ist wichtig in zwei Erscheinungsformen:

1. Fernüberwachung und -wartung von Geräten

2. Entfernte aktualisieren von Software und Funktionalitäten

In diesem Kapitel geht es um die Fernaktualisierung von Software und Funktionalitäten industrieller Steuerungssysteme.

2. METHODIK

2.1 Industrielle Kontrollsysteme (ICS)

Industrielle Kontrollsysteme (ICS) sind automatisierte Systeme, die zur Steuerung und Überwachung von Prozessen in Industrie- und Produktionsanlagen eingesetzt werden. Industrielle Steuersysteme integrieren Hardware und Software mit Netzanbindung. Zu den ICS-Technologien gehören die folgenden wichtigsten Technologien, Systeme und Geräte:

· Speicherprogrammierbare Steuerungen (PLC)

- Programmierbare Automatisierungssteuerungen (PAC)
- Verteilte Steuerungssysteme (DCS)
- Industrielle Automatisierungs- und Steuerungssysteme (IACS)
- Überwachungssteuerung und Datenerfassung (SCADA)
- Fernbedienungseinheiten (RTU)
- Mensch-Maschine-Schnittstellen (HMI)
- Intelligente elektronische Geräte (IED)
- Sensoren

Speicherprogrammierbare Steuerungen sind eines der wichtigsten Geräte, die in industriellen Steuerungssystemen eingesetzt werden. Eine SPS ist ein Industriecomputer, der für den Einsatz in einer rauen Umgebung konzipiert ist. Die Hauptbestandteile einer SPS sind Eingabemodule, eine zentrale Verarbeitungseinheit und Ausgabemodule. Die Struktur einer SPS ist in Abbildung 1 dargestellt.

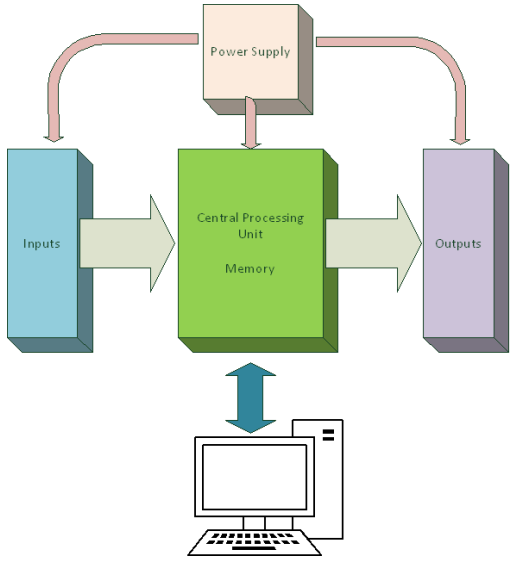


Abbildung 1: PLC-Struktur.

Das Programm in einer SPS wird zyklisch in einer Endlosschleife ausgeführt und besteht aus den 3 wichtigsten Schritten:

- Eingangsabfrage - Lesen der Eingänge.
- Programm scannen - Ausführung von des Programms

- Output Scan - Schreiben der berechneten Werte an die entsprechenden Ausgänge.

SPS werden auf einem externen Gerät (PC) in einer der fünf SPS-Programmiersprachen programmiert, die in der Norm IEC 1131-3 definiert sind. In der Vergangenheit war eine der beliebtesten SPS-Programmiersprachen der Kontaktplan. Dabei handelt es sich um eine grafische Programmiersprache, deren Code den Sprossen einer Leiter ähnelt - daher der Name. Abbildung 2 zeigt ein Beispiel für einen Teil eines Kontaktplanprogramms.

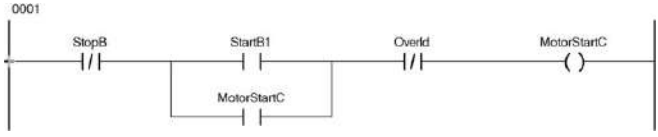


Abbildung 2: Beispiel für ein Kontaktplanprogramm.

Um ein SPS-Programm zu aktualisieren, muss ein externes Programmiergerät (in der Regel ein Personal Computer) angeschlossen werden, um das Programm in die Steuerung zu laden. Traditionell wurde dies mit einem

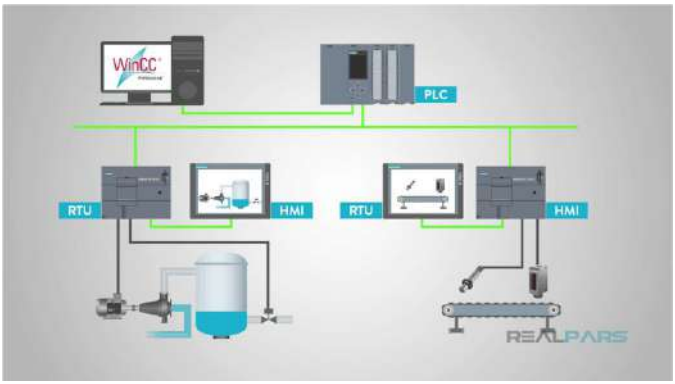
proprietäre Verbindung. Dieser Teil könnte aus der Ferne erfolgen, was alle Vorteile des Fernzugriffs mit sich bringt.

Ein weiteres sehr wichtiges System im ICS ist die Supervisory Control and Data Acquisition (SCADA). SCADA ist ein Aggregat von Hardware- und Softwaresystemen, das die folgenden Funktionen in einem industriellen Kontrollsystem ausführt:

- Steuerung eines industriellen Prozesses.
- Überwachung, Erfassung und Verarbeitung von Echtzeitdaten.
- Direkte Interaktion mit Sensoren und Aktoren wie Motoren, Pumpen, Ventilen usw. über die HMI-Software.
- Ändern Sie Sollwerte und andere geräte- und prozessrelevante Parameter.
- Ereignisse und Messungen aufzeichnen.

PLCs sind ein wichtiger Bestandteil der SCADA-Systeme. Die Software von Scada-Systemen hat auch die

potenziell Gegenstand einer Fernaktualisierung sein



können.

Abbildung 3: Die Rolle von SPS in SCADA-Systemen (aus https://realpars.com/scada/).

Abbildung 4 zeigt eine einfache Darstellung eines ICS, das aus zwei Controllern und einer Reihe von Ein- und Ausgängen besteht, die mit verschiedenen Sensoren und Aktoren verbunden sind.

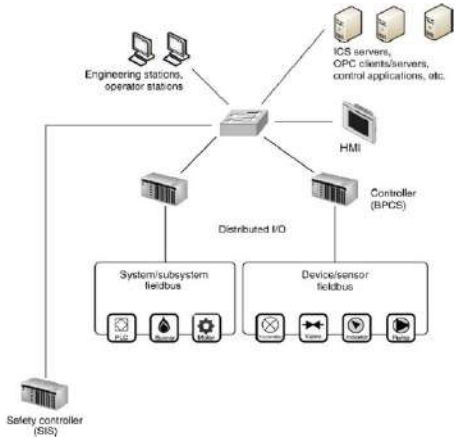


Abbildung 4: Einfaches industrielles Kontrollsystemnetz.

In der Praxis sind industrielle Steuerungssysteme Teil eines viel größeren Systems in einem Unternehmen, das in Abbildung 5 dargestellt ist.

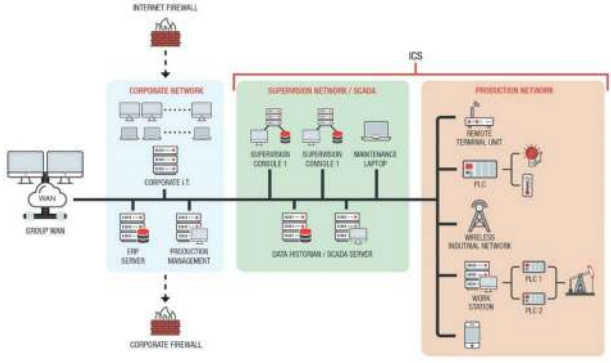


Abbildung 5: Integration eines industriellen Steuerungssystems in das Unternehmensnetz.

Aus Abbildung 5 geht auch die Trennlinie zwischen den Bereichen Informationstechnologie (IT) und Betriebstechnologie (OT) hervor. Vereinfacht gesagt, befasst sich die IT mit Informationen und die OT mit Maschinen. OT bezieht sich auf die Technologie, die Geräte und Prozesse überwacht und steuert. In der Abbildung 5 gehört die rechte Seite zur OT und die linke Seite zur IT.

2.2 Was ist Fernzugriff?

Zunächst einmal muss der Begriff Fernzugriff definiert werden. Nach [1] kann der Fernzugriff definiert werden als "die Möglichkeit für die Benutzer und Betreiber einer Organisation, von externen Standorten, die als außerhalb des Netzes dieser Organisation liegend betrachtet werden können, auf ihre nicht-öffentlichen Computerressourcen, Daten und Systeme zuzugreifen, die sich innerhalb eines physisch und/oder logisch geschützten Netzes befinden". Eine vereinfachte Definition würde lauten: Fernzugriff ist die Möglichkeit, über eine Netzverbindung von jedem Ort der Welt aus auf ein Datenverarbeitungsgerät (Computer, SPS, ...) zuzugreifen.

Der Fernzugriff auf ein industrielles Steuerungssystem wird für die folgenden Aufgaben verwendet:

- Überwachung von Prozesses Variablen, Meldungen und Alarme
- Durchführung von Wiedergutmachungsmaßnahmen
- Optimierung und Aktualisierung von Sollwerten und anderen prozessrelevanten Parametern
- Aktualisierung von Software und Funktionalitäten

2.3 Haupteile

Der Hauptvorteil eines Fernzugriffs auf das industrielle Steuerungssystem der Anlage besteht darin, dass eine Verbindung zu einer Anlage unabhängig von ihrem geografischen Standort möglich ist. Durch die Verbindung können die folgenden Aktivitäten am Steuerungssystem der Anlage durchgeführt werden:

1. Überwachung der Anlagenleistung
2. Wartung der Ausrüstung

Unterstützung für die Betreiber

4. Fehlerbehebungen in der Software und Sicherheitspatches

5. Aktualisierung der Softwarefunktionen und damit Verbesserung der Anlagenleistung

Als Beispiel können wir uns ein Entwicklungsteam für die Prozesssteuerung in Europa vorstellen, das die Funktionalität einer in Argentinien betriebenen Industrieanlage aktualisieren möchte. Ohne den Fernzugriff müssten die Entwickler nach Südamerika reisen, die Software und die Ausrüstung aktualisieren und alle erforderlichen Tests durchführen. Sollten nach ihrer Rückkehr nach Europa Probleme auftreten, könnten sie diese nicht mehr beheben. Dies würde erhebliche Kosten in Form von Geld, Zeit und Ressourcen verursachen. Dies gilt insbesondere für die Kosten der Ausfallzeiten im Falle von Problemen. In der Zeit von Covid 19 ist es ein enormer Vorteil, dass man dank der Fernzugriffsmöglichkeit nicht mehr anreisen und eine Anlage betreten muss.

2.4. Industrielles Internet der Dinge (IIoT)

Das industrielle Internet der Dinge ist die Erweiterung des Internets der Dinge (IoT) auf den Bereich der

industrielle Systeme und Geräte wie industrielle Steuerungssysteme. Der Schwerpunkt von IIo T liegt auf Big Data, maschinellem Lernen und der Kommunikation von Maschine zu Maschine. Bei IIo T geht es um die Konvergenz und Integration von OT- und IT-Systemen. Eine bessere Integration von IT- und OT-Systemen ermöglicht eine bessere Sichtbarkeit von OT-Geräten. Dies ermöglicht es, große Datenmengen aus industriellen Systemen zu sammeln, die Daten analytisch zu verarbeiten und bessere Entscheidungen in Bezug auf die Prozesse zu treffen. Diese Daten ermöglichen es den Unternehmen, Fehler besser zu analysieren und Optimierungen nicht nur in den Fertigungsprozessen, sondern auch in den Lieferketten vorzunehmen. Außerdem lassen sich Ausfälle von Systemen und Anlagen besser vorhersagen, und die Wartung kann rechtzeitig erfolgen.

Viele ICS-Geräte wie z. B. SPS sind Altgeräte und haben als solche eine schlechte oder nicht vorhandene Netzwerkkonnektivität. Wenn wir einen vollständigen Fernzugriff auf solche Geräte zum Zweck der Fernüberwachung oder der Aktualisierung von Funktionen haben wollen, müssen wir sie sichtbar machen (sie in IIoT-Cloud-Dienste umwandeln). Dies geschieht durch Edge-Geräte. Wir können uns ein Edge-Gerät als industrielles IIo T-Gateway vorstellen (Abbildung 6). Die Funktion eines Edge-Devices ist es, Daten zwischen lokalen Netzwerken zu

übertragen

(Profinet, Ethernet...) und der Cloud. Außerdem stellt ein Edge-Gerät eine sichere Verbindung zur Cloud her.

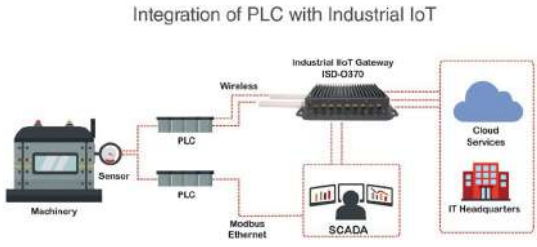


Abbildung 6: Integration von SPS mit industriellem IoT (aus https://www.lanner-america.com/blog/iot-gateway-integration-von-plc-mit-iot/).

2.5. Fernaktualisierung von Funktionalitäten

Die Fernaktualisierung von Software ist eine gängige Praxis für Verbrauchergeräte wie Personalcomputer und mobile Geräte. In jüngster Zeit sind auch in der Automobilindustrie Over-the-Air (OTA)-Updates recht üblich geworden. Im Bereich der industriellen Steuerungssoftware ist dies jedoch noch nicht der Fall. Der Bereich der industriellen Steuerungssoftware ist traditionell recht konservativ, was die Übernahme neuer Technologien angeht. Es genügt ein Blick auf die SPS-Programmiersprachen. Kontaktplan,

die immer noch eine der populärsten SPS-Programmiersprachen ist, basiert auf elektrischen Schaltplänen und hat wenig Ähnlichkeit mit modernen Programmiersprachen, die in der allgemeinen Datenverarbeitung verwendet werden. Ein konservativer Ansatz ist verständlich, wenn man bedenkt, dass industrielle Kontrollsysteme mit entsprechender Software oft in sehr kritischen Infrastrukturen eingesetzt werden. Ein Ausfall einer solchen Infrastruktur kann erhebliche finanzielle Schäden oder sogar Umweltkatastrophen und den Verlust von Menschenleben verursachen.

Die wichtigsten Vorteile der Softwareaktualisierung aus der Ferne:

- Schnelle Reaktionszeit. Im Falle eines Sicherheitsverstoßes können wir dank der Fernaktualisierung der Software sehr schnell reagieren, unabhängig davon, wie weit die betroffene Anlage entfernt ist. Die Fähigkeit, rasche Funktionsänderungen vorzunehmen, ermöglicht es der verarbeitenden Industrie, schnell auf veränderte Marktanforderungen oder Schwankungen in der Lieferkette zu reagieren.

- Massiv reduzierte Kosten in Bezug auf Ressourcen und Zeit. Durch die Möglichkeit, die Software aus der Ferne

zu aktualisieren, müssen die Techniker nicht mehr zu entfernten Standorten reisen.

Und wenn viele Systeme gleichzeitig aktualisiert werden müssen, kann dieser Prozess durch automatisierte Remote-Updates viel schneller und effizienter durchgeführt werden.

In der Automobilindustrie wird für die Fernaktualisierung von Firmware, Software und Funktionalitäten der Begriff Software-Over-The-Air-Updates (SOTA) verwendet. Bei industriellen Steuerungssystemen werden die Aktualisierungen, auch wenn sie aus der Ferne erfolgen, in vielen Fällen über das Kabel (OTC) durchgeführt. Das Konzept ist jedoch dasselbe, nur das Medium ist ein anderes.

An dieser Stelle kommt IIo T ins Spiel. Im Rahmen von IIo T gibt es die folgenden verschiedenen Methoden von OTA-OTC-Updates:

- Edge-To-Cloud: Das Industriegerät (z. B. SPS), das über ein Edge-Gerät mit dem Internet verbunden ist, erhält das Software-Image von einem entfernten Server. Die Cloud übernimmt die Rolle eines Dispatchers, der die Software über das Edge-Gerät an das Industriegerät überträgt.

- Gateway-zu-Cloud: Eine Reihe von lokalen Edge-Geräten sind mit einem Gateway verbunden, das

  verwaltet sie. Das Gateway empfängt Updates von einem entfernten Server. Mit dieser Aktualisierung kann die Firmware des Gateways aktualisiert werden.

Edge-To-Gateway-To-Cloud. Das mit dem Internet verbundene Gateway empfängt Updates vom entfernten Server und verteilt diese Updates an die lokalen Edge-Dienste. Hier ist das Edge-Gateway ein Dispatcher, der die Software vom Server herunterlädt und sie dann an ein anderes Edge/Gateway oder IoT-Gerät weiterleitet.

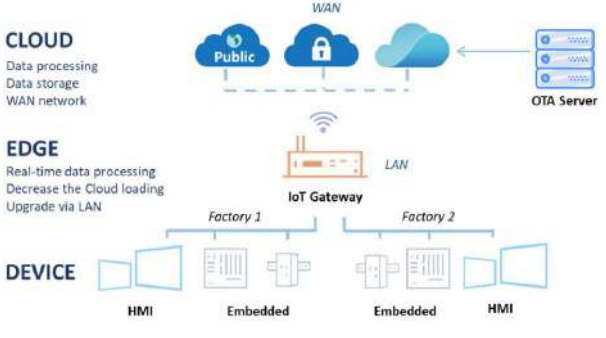


Abbildung 7: Infrastruktur für OTA/OTC-Updates (aus https://embeddedcomputing.com/application/industrial/industria iot/cloud-gateway-zur-verwaltung-ota-process-in-iiot

1.

Ein typisches Remote-Software-Update sollte in den folgenden Schritten durchgeführt werden:

2. Vorbereitung. Die Dienstleistungen sind gestoppt, Abhängigkeiten installiert.

3. Aktualisieren Sie Prozess. Die Dateien werden ersetzt, Aktualisierungsroutinen ausgeführt.

4. Aufräumen. Entfernen der vom Aktualisierungsprozess übrig gebliebenen Dateien.

Rollbackroutine. Wenn die Aktualisierung aus irgendeinem Grund fehlschlägt (z. B. unterbrochene Internetverbindung), sollte eine Fallback-Routine den ursprünglichen Zustand der Software vor Beginn der Aktualisierung wiederherstellen.

2.6. Cybersecurity

Als Einführung in die Cybersicherheit und warum sie auch im Bereich der industriellen Kontrollsysteme wichtig ist, wollen wir uns eine Fallstudie über den bösartigen Computerwurm Stuxnet ansehen, der ein ganz bestimmtes industrielles Kontrollsystem angriff.

Stuxnet ist eine im Jahr 2010 entdeckte Computer-Malware. Sie ist eine der ersten Malwares, die nicht nur in der virtuellen, sondern auch in der physischen Computerwelt Schaden anrichtete. Sie wurde entwickelt, um das iranische Atomprogramm zu schädigen, indem sie das industrielle Kontrollsystem der Nuklearanlage Natanz angriff bzw. manipulierte.

Stuxnet griff in drei Schritten an:

1. Windows-Infektion. Microsoft Windows-Rechner wurden über ein infiziertes USB-Flash-Laufwerk angesteuert, das den Luftspalt überquerte, und der Wurm replizierte sich auf dem Rechner.

2. Step7-Infektion. Der Wurm fing die Kommunikation zwischen dem SCADA WinCC und den SPSen ab. So konnte er den Code auf den SPSen verändern, ohne dass WinCC dies bemerkte.

3. PLC-Infektion. Der Wurm befällt Systeme, die Zentrifugen steuern (nur solche mit bestimmten Frequenzumrichtern). Der SPS-Code wird so manipuliert, dass er die Drehfrequenz der Zentrifugen verändert und sie dadurch beschädigt.

Wir sehen, dass die Cybersicherheit bei industriellen Kontrollsystemen von größter Bedeutung ist, da ihr (absichtlich) unerwünschtes Verhalten in der physischen Welt zu Katastrophen führen kann, von einfachen Produktionsanlagen bis hin zu Atomkraftwerken.

Bei industriellen Kontrollsystemen stoßen wir auf die gleichen Arten von Herausforderungen wie in klassischen IT-Umgebungen und auch auf die folgenden, die spezifisch für ICS sind:

- Hohe Anforderungen an die Verfügbarkeit. ICS werden häufig in kritischen Infrastrukturen und in der Produktion eingesetzt Industrien eingesetzt, wo Ausfallzeiten auf ein Minimum reduziert werden müssen, was die Installation von Sicherheitsupdates erschwert.

- Unsichere, proprietäre und veraltete Protokolle. In industriellen Steuerungssystemen gibt es oft alte Protokolle, die nicht ausreichend sicher sind, weil sie entwickelt und implementiert wurden, als es noch keine Cyber-Bedrohungen gab. Ältere Geräte wurden für Zuverlässigkeit und nicht für Sicherheit entwickelt.

Darüber hinaus stellt die Konvergenz von Informationstechnologie (IT) und Betriebstechnologie (OT) eine Sicherheitsbedrohung dar, da ein Air-Gapping (Trennung von ICS-Geräten und -Netzen von Geschäftsanwendungen und nicht privaten Netzen) nicht mehr möglich ist. Obwohl Air-Gapping nicht die ultimative Lösung ist, wie wir im Fall von Stuxnet gesehen haben. Luftlücken können auch durch so genannte HVACKers-Angriffe überbrückt werden ([8]). Bei dieser Art von Angriffen nutzen die Angreifer eine kompromittierte Klimaanlage (die mit dem Internet verbunden ist), um durch Manipulation der Temperatur Befehle an Malware zu senden, die sich innerhalb des (vermeintlich) luftdichten Netzwerks befindet. Die Malware interagiert mit den Wärmesensoren, misst Temperaturschwankungen und "liest" so die Befehle aus, die von der manipulierten Klimaanlage des externen Netzwerks gesendet werden.

Um Systeme vor Bedrohungen und Angreifern schützen zu können, müssen Schutzziele definiert werden. Schutzziele kategorisieren die Arten von Angriffen. Die wichtigsten Schutzziele sind:

- Authentizität. Authentische Daten sind solche, die aus einer eindeutig identifizierbaren Quelle stammen.

- Verfügbarkeit. Eine Steuerungssoftware muss trotz eines Angriffs normal funktionieren. Wenn z. B. eine speicherprogrammierbare Steuerung eine nicht authentische Software empfängt, muss sie damit fertig werden und ihren normalen Dienst anbieten.

- Vertraulichkeit. Dieses Schutzziel betrifft Daten. Daten sind vertraulich, wenn nur befugte Personen auf sie zugreifen können.

- Integrität. Integrität bedeutet, dass Daten, die übertragen oder gespeichert werden, nicht manipuliert werden können, ohne entdeckt zu werden. Um beispielsweise Daten über eine Netzverbindung zu übertragen, müssen wir einen Mechanismus vorsehen, der überprüft, ob die Daten manipuliert wurden (z. B. zyklische Redundanzprüfung - CRC).

3. SCHLUSSFOLGERUNG

Die Fernaktualisierung von Software und Funktionen ist schon seit geraumer Zeit ein Standardmerkmal gängiger Computerbetriebssysteme (wie MS Windows oder Linux) und mobiler Geräte. In jüngster Zeit ist auch die Fernaktualisierung (OTA) von Fahrzeugsoftware in Autos auf dem Vormarsch. Die Fernaktualisierung hat viele Vorteile

Software-Updates, die deutlich geringere Kosten verursachen und die Möglichkeit bieten, auf Änderungen zu reagieren, wenn diese aus irgendeinem Grund erforderlich sind (Sicherheitspatches, rasche Änderung der Funktionalität). Allerdings müssen gerade in einem so sicherheitskritischen Bereich wie den industriellen Steuerungssystemen Fragen der Cybersicherheit noch gründlicher als in anderen Bereichen berücksichtigt werden. In diesem Kapitel zeigen wir, wie die Fernaktualisierung von Software und Funktionalitäten im Bereich der industriellen Steuerungssysteme eingeführt werden kann.

4. REFRENZEN

[1] Innere Sicherheit. Zentrum für den Schutz der nationalen Infrastruktur. (2010). Konfiguration und Verwaltung des Fernzugriffs für industrielle Steuerungssysteme.

[2] Macaulay, T., Singer, B. (2012). Cybersecurity for industrial control systems. CRC Press. Taylor & Francis Group.

[3] Trendmicro. (2022). ICS-System. Bild abgerufen von: https://documents.trendmicro.com/images/tex/articles/ics_system.jpg.

[4] Inderwies, T., Mottok, J. (2020). Sicheres Software-Update eines sicheren Moduls im Stromnetz. Proceedings of the Regensburg Applied Research Conference 2020. DOI: 10.35096/ othr/ pub-641.

[5] Sicherheit von Industrienetzwerken, Absicherung kritischer Infrastrukturen für Smart Grid, SCADA und andere industrielle Kontrollsysteme. Knapp,
E. D., Langill, J. T. (2015). Elsevier.

[6] Ackermann, P. (2017). Industrial Cybersecurity. Packt publishing.

[7] John, K.-H., Tiegelkamp M. (2010). IEC 61131-3: Programmierung von industriellen Automatisierungssystemen. Springer.

[8] Mirsky, Y., Mordechai, G., und Elovici, Y. (2017). HVACKer: Bridging the Air -Gap by Attacking the Air Conditioning System. Depth Security.

Sechs

Zeugnis 1

Maximum Security in the Production Network

Omar Busquests & Roger Mouzo, Festo Ag, Esslingen, festo.es@ festo.co

ABSTRACT:

Zellsegmentierung der Produktionsanlagen sowie gesicherter Internet- und Intranetzugang dank der Managementplattform für das Remote-Netzwerk.

Keywords: Festo, segmentation, secured internet

1. EINLEITUNG

Die Festo AG hat in ihrer Technologiefabrik in Scharnhausen, Deutschland, eine neue Sicherheitsplattform für die Produktionsautomatisierung eingerichtet.

Funktionen wie Firewall und VPN-Verschlüsselung sorgen für einen erhöhten Schutz bei der Datenübertragung und schotten die Produktionsnetze gegen unberechtigte interne und externe Zugriffe ab. Dies verbessert die Prozesssicherheit und steigert die Produktivität der gesamten Produktionsumgebung

Die Festo AG ist ein Global Player auf dem Gebiet der pneumatischen und elektrischen Automatisierungstechnik. Mit Industrial Remote Access hat die Festo AG ihre Idee einer sicheren, vernetzten Produktionsumgebung realisiert. Die Mitarbeiter aus den Bereichen Global IT und Maintenance haben eine Lösung implementiert, die nicht nur die Kommunikation von Maschinen und Produktionsanlagen sowie deren Anwendungen untereinander ermöglicht, sondern auch einen sicheren Internet- und Intranetzugriff z.B. auf die speicherprogrammierbare Steuerung (SPS) der Maschinen gewährleistet.

Eine große Herausforderung für die Werksinstandhaltung sind die vielfältigen Netzwerkkomponenten und Router in den Anlagen, die nicht patchbar sind und für Festo eine unsichere "Black Box" darstellen.

Abbildung 1: Festo Sharnhaussen

2.METHODOLOGIE

2.1 Einführung in die Anforderungen an die Sicherheit einer Produktionsumgebung auf der Kommunikationsebene Netzwerke.

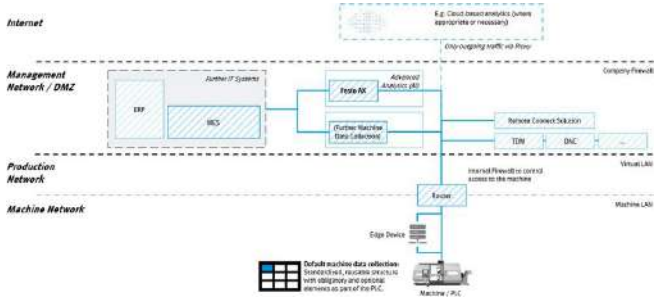


Abbildung 2: Architektur Maschinendatenerfassung & Netzwerk

Innerhalb einer Produktionsanlage gibt es verschiedene Ebenen, die miteinander verbunden sind, und um die Unverletzlichkeit der Daten zu gewährleisten, müssen wir eine strenge Cybersicherheitspolitik betreiben, bei der wir sicherstellen müssen, dass wir intern und extern eine Zugangskontrolle haben. Dazu müssen wir uns mit Hilfssystemen behelfen, um diese Sicherheitsniveaus erreichen zu können.

Alle Maschinen, die Teil unserer sicheren Linie sind, müssen mindestens einen Router enthalten, der die Segmentierung und Firewalling der Ports ermöglicht (z. B. Scalance XC208). Dieser Router ermöglicht es uns, das interne Netzwerk der Maschine mit

die unserer Produktionsanlagen, um dann alle Informationen an Produktionsmanagementsysteme, vorausschauende Wartung, Datenspeicherung in der Cloud... weiterleiten zu können.

2.2. Prozess des Fernzugriffs einer dritten Partei auf unser Produktionssystem

Die Gewährung des Zugangs für Dritte ist immer ein kritischer Punkt in jeder Produktionsumgebung, es ist komplex, den Zugang sicher und aus der Ferne zu gewährleisten. Um diese Fernwartungsmaßnahmen durchzuführen, müssen wir über eine spezifische Struktur und einen spezifischen Prozess verfügen. Ein Beispiel hierfür ist das folgende, in dem ein Dritter auf eine Anlage einer Produktionsstätte zugreifen möchte, die über ein fortschrittliches Cybersicherheitssystem verfügt.

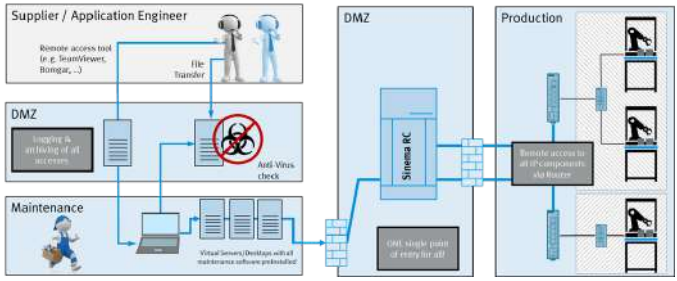


Abbildung 3: Schema des Verfahrens für den Zugriff auf die Daten und ihre Speicherung.

Eine der Voraussetzungen für den Zugang dieses externen Benutzers ist, dass er immer autorisiert sein und seine Zugangsdaten verifizieren muss. Sobald der externe Benutzer autorisiert ist, verbindet er sich über einen Fernzugriffsdienst (z. B. Teamviewer, Bomgar ...) mit einem physischen Server/PC im Werk, der wiederum vom System registriert wird. An diesem Punkt der Verbindung befindet sich ein weiterer kritischer Punkt, an dem wir den gesamten bidirektionalen Datenverkehr zwischen der Anlage und der Remote-Verbindung analysieren müssen, um zu verhindern, dass nicht autorisierte Daten gestohlen oder Malware eingeschleust werden kann.

Über einen einzigen SINEMA RC-Server wird der gesamte Datenverkehr auf Anlagenebene abgewickelt, so dass eine Segmentierung des Netzes möglich ist.

2.3. Dateisteuerung

Um eine umfassende Kontrolle der Firmware-/Softwareversionen aller in unserer Anlage eingebauten Systeme zu gewährleisten. Ein Dienst wird auf dem Verbindungsserver zwischen dem externen Benutzer und dem PC/Server in der Anlage hinzugefügt.

Dieses System ermöglicht es uns, von jeder Datei, die der Anbieter in unser System eingibt, eine Sicherungskopie zu erstellen und eine Versionskontrolle durchzuführen, um sicherzustellen, dass die Aktualisierungen kontrolliert werden und auf dem Rechner installiert sind, was das Risiko von Systemausfällen verringert, da eine der Sicherheitslücken die Inkompatibilität zwischen Online- und Offline-Version ist.

3. RESULTATE

3.1 Zuverlässige Prozesse im gesamten Produktionsnetzwerk

Im Bereich der Betriebstechnik (OT) kam man an einen Punkt, an dem es notwendig wurde, die Produktionsnetze sicherer und zentral verwaltbar zu machen. Bis zu diesem Zeitpunkt gab es keinen einheitlichen Standard für den Fernzugriff. Erklärtes Ziel war es, den Zugriff auf die Werkzeugmaschinen durch externes und internes Servicepersonal erheblich einzuschränken. Produktionsnetzwerke bilden das Rückgrat unserer Automatisierungsumgebungen. Ein externer Techniker, der mit einem Service-Notebook versehentlich einen Virus in das Netzwerk einschleust, könnte unter Umständen zu einem "Flächenbrand" führen, der das Anlagennetz der gesamten Fabrik lahmlegt.

Das Projektteam plante daher gleichzeitig eine weitere Feinsegmentierung, um auch einzelne Produktionsanlagen oder einzelne Altkomponenten vollständig zu isolieren.

Abbildung 4: Produktionsstätte von Festo scharnhauser

Für die Fertigung von Präzisionsbauteilen setzt Festo Produktionsinseln ein. Die Maschinen sind in das Produktionsnetzwerk integriert und über die SCALANCE S615 vor unberechtigtem Zugriff geschützt.

Die Hersteller haben individuelle Fernwartungslösungen für ihre Werkzeugmaschinen und bauen Anlagenteile als Netzwerkkomponenten auf, was die Wartungsarbeiten immer komplexer macht. Bis zur Einführung der neuen Sicherheitsplattform waren die Maschinen

in der Lage, sich selbständig mit dem Internet zu verbinden. Die Hersteller rüsteten ihre Anlagen mit Mobilfunkmodems aus, über die sie z.B. Alarmmeldungen per SMS oder E-Mail auf Basis von Grenzwerten verschickten. Aber auch für jede Einstellung wählten sich die Maschinenhersteller direkt in das Festo Netz ein. Das Wartungspersonal konnte nicht aus der Ferne auf interne Anlagenteile zugreifen und musste sich teilweise erst beim Hersteller einloggen, um SPS-Programmänderungen und Statusabfragen durchzuführen. Von dort aus ging die Verbindung zurück zu der jeweiligen Maschine im Werk.

Dieses Verfahren war sehr unsicher und veranlasste das Projektteam, die Hersteller zu bitten, die IP-Adressen ihrer Maschinen nach den Vorgaben von Festo neu zu ordnen. Diese Lösung war jedoch in den meisten Fällen nicht praktikabel. Außerdem könnte durch die Änderung der IP-Adressen die Garantie der Systeme erlöschen.

3.2. Beseitigung von IP-Adresskonflikten und Segmentierung von Profinet-Geräten

Die Nutzung der SINEMA Remote Connect Management Plattform bietet neben der

Maschinenlieferanten den Vorteil, dass die IP-Adressen nicht mehr geändert werden müssen. Alle Anlagenzugriffe laufen nur noch über SINEMA Remote Connect mit einer zentralen IP-Adresse für den Zugriff von außen. Die Serverapplikation empfängt alle Tunnelverbindungen (VPN) und vermittelt so zwischen den Client-PCs der externen Servicetechniker und den Maschinen. Die Kommunikation ist protokollunabhängig, nicht-proprietär und IP-basiert. Ein direkter und unkoordinierter Zugriff auf die Produktionsnetze wird vermieden.

Mit dem SINEMA RC Client steht auch eine Adressbuchfunktion zur Verfügung, über die Maschinen und Anlagen in der Technologiefabrik eindeutig identifiziert und für den gesicherten Fernzugriff ausgewählt werden können. Die Maschinen werden vom Gerätehersteller mit unveränderten IP-Adressen installiert und über die Security Appliance SCALANCE S615 mit dem Netzwerk verbunden. SCALANCE S615 übernimmt auch die Übersetzung der IP-Adressen (Network Address Translation, NAT), so dass zwei verschiedene Netzwerke (intern und extern) über eine Firewall verbunden werden können.

Die Maschinen im Produktionsbereich sind von außen nicht direkt zugänglich, weil

sie werden durch NAT und eine Firewall verdeckt. Eingehende Datenpakete, die aus einem externen Netz kommen und an eine externe IP-Adresse der Maschine gerichtet sind (Ziel-IP-Adresse), werden im SCALANCE S615 durch die interne IP-Adresse ersetzt. Nur wenige Profinet-Geräte dürfen über IP mit dem Festo-Büro-Netzwerk oder Applikationen kommunizieren. Auch der frühzeitige und manchmal notwendige Fernzugriff auf neue Anlagen, die sich noch in der Produktionsphase beim OEM befinden, kann mit den Security Appliances realisiert werden.

Zunächst rüstete das Wartungspersonal von Festo eine Ventilfertigungslinie mit SINEMA Remote Connect aus. Die Fertigungslinie umfasst eine CNC-Rundtaktmaschine zum Bohren und Drehen der Werkstücke, eine Maschine zum Hochdruckentgraten, einen Handling-Roboter und ein System zur Zuführung und Entnahme der Werkstücke. Die einzelnen Stationen sind an die Ports der Sicherheitsappliance SCALANCE S angeschlossen. Die Security Appliance kommuniziert über einen verschlüsselten VPN-Tunnel mit der Management-Plattform. Zur Wartung kann der VPN-Tunnel über einen Schlüsselschalter am SCALANCE S aktiviert werden, oder der Remote User wird temporär auf der SINEMA

Verwaltungsplattform Remote Connect. Ähnlich wie ein USB-Stick, aber ohne das Risiko, von Viren infiltriert zu werden, speichert ein Key-Plug alle Konfigurationsdaten der Security Appliances, was einen schnellen und unkomplizierten Gerätetausch im Produktionsbetrieb ermöglicht.

Bild 5: Die Security Appliance SCALANCE S615, der Controller SIMATIC S7-1500 und das Netzteil SITOP PSU8200 sind Komponenten, die im Schaltschrank bei Festo installiert sind.

Durch die Kombination der Maschinensteuerungen SIMATIC S7-1500 und der HMI-Panels aus dem SIMATIC-Portfolio mit dem TIA Portal

Bei der Entwicklung des Engineering Frameworks stand die hohe Effizienz und Flexibilität der Lösung im Mittelpunkt der Entscheidungsfindung. Nach außen werden nur die Bildschirm- und Tastaturdaten eines Festo-Wartungsingenieurs übertragen, da der Zugriff auf die Anlagenzelle durch externe Nutzer nur über einen virtuellen Jump-Host-Rechner erfolgt, auf dem auch das TIA Portal als Floating-Lizenz für die Parametrierung der Anlagen zur Verfügung steht. Die Remote-Sitzung wird zur Revisionssicherheit auch auf Video aufgezeichnet, und die Projekte werden zentral auf einem Festo Backup-Server gesichert. Ein externes Feld-PG oder Notebook wird durch dieses zweistufige Fernwartungskonzept vom Festo Netzwerk entkoppelt.

3.3. Festo Didactic Training mit SINEMA Remote Connect und SCALANCE-Switches

Parallel zur Einführung dieser Fernwartungslösung in der Produktion bietet die Festo Didactic SE ein Trainingsprogramm für Festo Mitarbeiter an, das auf den eingesetzten Produkten wie SINEMA Remote Connect und SCALANCE S615 sowie weiteren Komponenten wie Managed Switches der SCALANCE X-Familie basiert. Mitarbeiter aus der Instandhaltung und verwandten Berufsfeldern werden in der Netzwerktechnik geschult.

und IT-Sicherheitsinhalte, die zum Verständnis und Betrieb der eingesetzten Lösung erforderlich sind.

3.4. Kompetente Beratung in allen Projektphasen

Sie haben eine zuverlässige Basis für den weiteren Ausbau der Produktionsnetzwerke geschaffen. Die Hard- und Software ist sehr gut durchdacht, die Komponenten sind optimal aufeinander abgestimmt. Bei anderen Alternativen hätten sie die Anwendungen selbst entwickeln müssen. Die Bediensoftware ist so einfach gestaltet, dass sie auch von weniger erfahrenen Anwendern mühelos parametriert werden kann. Die SCALANCE-Geräte sind DIN-Schienen-kompatibel, verfügen über 24-V-DC-Anschlüsse und sind sehr kompakt gebaut, was bei der Installation sehr vorteilhaft ist. Der Key-Plug ermöglicht eine einfache und effiziente Vorkonfektionierung der SCALANCE-Router. Die Kollegen aus dem Prüfmittelbau sind so in der Lage, ihre Prüfsysteme betriebsbereit an andere Werksstandorte zu liefern.

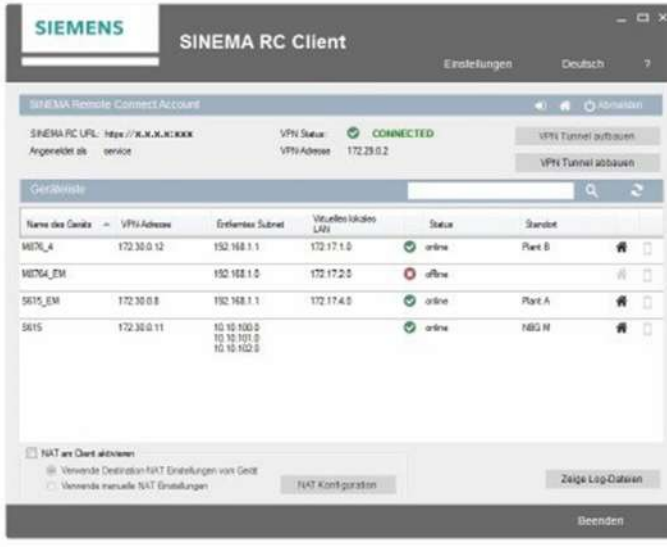


Abbildung 6: Screenshot der benutzerfreundlichen Oberfläche des SINEMA RC Client.

Ursprünglich war die Managementplattform nur für das Werk Scharnhausen geplant. Das IT-Management prüft, ob das Konzept auch für andere Standorte übernommen werden kann. Was die neue Lösung für die Werksinstandhaltung interessant macht, ist der geringe Zeitaufwand für den Anschluss einer neuen Anlage, der von zwei Wochen auf einen halben Tag gesunken ist. Mit dem SINEMA RC Client lassen sich die einzelnen Ports einfach anpassen. So konnten alle Anwendungsfälle im Werk Scharnhausen realisiert werden.

Technologiefabrik mit SINEMA Remote Connect.

Die Projektbeteiligten sind sich einig, dass ohne die neue Management-Plattform das Portfolio an IP-fähigen Komponenten und Maschinen von Festo nicht effizient verwaltet werden könnte. Auch die Gefahr, durch die Eingabe einer falschen IP-Adresse einen Netzwerkausfall zu verursachen, besteht nicht mehr. Darüber hinaus bietet der Profinet-Zugang die Basis für weitere Innovationsprojekte wie das Energiedatenmanagement oder den Aufbau eines Predictive Maintenance Cockpits zur Überwachung von Sensorwerten in einer intelligenten Fabrik.

Abbildung 7: Die Stationen der Produktionslinie sind mit den Ports des SCALANCE S615 verbunden.

4. SCHLUSSFOLGERUNG

o Zugriff auch von außerhalb des Produktionsnetzes → Zeitersparnis/ Flexibilität.

o Verbindung besteht nur bei Bedarf → Sicherheitsvorteil

o Standardisierter Maschinenzugang für Wartungspersonal → Klare Zugangsstruktur und Netzwerkarchitektur; keine IP-Adressenkonflikte

- Es sind keine Vereinbarungen über IP-Adressbereiche erforderlich.

o Entsprechend keine Anpassungen im SPS-Projekt. → Hoher Kommunikations- und Anpassungsaufwand mit/an den Lieferanten.

o Beim Umsetzen von Maschinen: Einfache Umstellung möglich. Keine Anpassungen des SPS-Programms bei Neuvergabe der festen IP-Adresse notwendig.
→ Keine Anpassungen im SPS-Programm notwendig.

- Geringere Installationskosten für Systeme mit mehreren internen Netzwerken (z. B. nur ein LAN-Kabel anstelle mehrerer)

Einfache Vervielfältigung von sicheren Konfigurationen (→ "Vorlagen")

- Zentrale Verwaltung über CLI (z.B. zentrales Einspielen neuer Firmware mit Sicherheitsupdates, Öffnen von Ports, ...)

- Leistungsstarke virtuell Wartung Server (LVI):

o Kosteneinsparungen durch weniger (leistungsfähige) Hardware in der Filiale / bei der Wartung.

o Globaler, von der IT verwalteter virtueller Windows-Server mit allen erforderlichen Wartungstools und Entwicklungsumgebungen

§ Keine "Probleme" mit der Verwaltung und Einrichtung der Siemens PGs

§ Automatische Backups

§ Einfache und kostengünstige Leistungssteigerung möglich

§ Perspektive: Keine (oder zumindest weniger) Programmiergeräte (PD) notwendig

- Perspektive: Lieferanten müssen ihre PDs nicht mehr physisch an unsere Systeme anschließen, sondern verbinden sich über SINEMA RC → Sicherheitsvorteil.

- Der Zugang zu SINEMA RC kann über AD verwaltet werden

Sieben

Zeugnis 2

Customer success story with Smartenance

A packing solution

Omar Busquests & Roger Mouzo, Festo Ag, Esslingen, festo.es@ festo.co

ABSTRACT:

Sammlung und Dokumentation von Wissen über Mängel und Fehler.

Keywords: Festo, knowledge, documentation, Smartenance

1. EINFÜHRUNG

Die herkömmliche korrektive Instandhaltung wird dann angewandt, wenn ein Element oder eine Anlage ausgefallen ist, was zu unkontrollierten Produktionsstopps führt, ohne dass ein Kostenvoranschlag für den Eingriff vorliegt. In den meisten Fällen verlängert sich die Eingriffszeit durch den Kommunikationsprozess und das Management von Zwischenfällen. Eines der Probleme bei der nicht ferngesteuerten korrektiven Instandhaltung ist, dass die Informationen und das Management nicht an einer Stelle kanalisiert oder zentralisiert sind. Dies führt auch zu Problemen mit veralteten Informationen. Dank der Konnektivität in der Industrie besteht die Möglichkeit, digitale Tools zu nutzen, die helfen, Informationen zu zentralisieren, Reaktionszeiten zu optimieren, Ausfallzeiten zu reduzieren und die Historie von Vorfällen an einem Punkt zu haben. Darüber hinaus ermöglicht der Einsatz dieser Tools die Gruppierung der technischen Dokumentation nach den einzelnen Anlagen des Prozesses, so dass die Bediener oder das Wartungspersonal ihre Aufgaben effizienter erledigen können. Diese Tools helfen nicht nur dem Personal vor Ort, sondern auch bei der Verwaltung der Ressourcen, indem sie Aufgaben je nach Bedarf und Fähigkeiten planen und zuweisen können. Schließlich können diese Systeme mit Managementsystemen verbunden werden, um den Einkauf von Ersatzteilen zu automatisieren. Ein anschauliches Beispiel für

den Einsatz von Software

Abhilfe Fernwartung
Fernwartung ist Smartenance.

2. METHODIK

Die Unternehmen sind bestrebt, ihre Produktivität weiter zu steigern. Eine Voraussetzung dafür ist eine effiziente Wartung und Instandhaltung von Maschinen und Anlagen. Ein bedeutendes deutsches Verpackungsunternehmen entschied sich, das Instandhaltungsmanagement in seinem Werk von klassischen Tabellenkalkulationsausdrucken auf die Instandhaltungssoftware Smartenance von Festo umzustellen. 16 Mitarbeiter kümmern sich um bis zu 100 einzelne Wartungspunkte pro Anlage, die von Maschinenherstellern und Produktionsleitung vorgegeben werden - bisher per Hand. Mit Smartenance kann die Wartungsplanung und -dokumentation deutlich vereinfacht und präzisiert werden. Die Mitarbeiter werden über Pop-up-Fenster auf ihren mehr als 20 Tablets informiert, was, wann, wo und wie zu tun ist.

2.1. Mehr Transparenz und Planungssicherheit mit Smartenance

Bevor Smartenance bei uns eingeführt wurde, haben wir die einzelnen Wartungspunkte immer zu Beginn in Tabellen eingetragen

des Jahres in mühevoller Kleinarbeit erfasst, mit einem Foto versehen, ausgedruckt, archiviert und gleichzeitig für das Wartungspersonal an den Linien ausgelegt. Smartenance bietet viel mehr Transparenz und ist sehr benutzerfreundlich. Durch den Überblick über den Wartungsprozess kann das Unternehmen bei ungeplanten Maschinenstillständen auf anstehende Wartungsarbeiten hinweisen und die durchgeführten Arbeiten einfach per Kommentar und Foto dokumentieren.

3. ERGEBNISSE

Smartenance sorgt für mehr Transparenz. Nicht jeder Mitarbeiter möchte wegen eines kleinen Schadens sofort seinen Vorgesetzten anrufen. In der Vergangenheit gingen so wichtige Informationen verloren. Mit Smartenance kann der Wartungstechniker einfach einen kurzen Kommentar in das Maschinenlogbuch eintragen und bei Bedarf ein Foto anhängen. So werden alle Arbeiten detailliert dokumentiert und sind über die Smartenance-Desktop-Version auch für die Produktionsleitung einsehbar. Eine weitere Vereinfachung der Wartungsarbeiten ist die farbliche Kennzeichnung in Smartenance für Arbeiten, die nur von speziellen Fachkräften, wie z.B. einem Elektriker oder einem Schlosser, durchgeführt werden können.

Abbildung 1: Bild der smartenance-Anwendung