Technische Universität Graz

Institut für Fertigungstechnik

Univ.-Prof. Dipl.-Ing. Dr. techn. Franz Haas

Fernzugriffe auf MRK-Systeme
Sicherheitstechnische Prävention im Hinblick auf Safety und Security

Masterarbeit

von

Michael Pichler, BSc

Vorgelegt zur Erlangung des
akademischen Grades eines Diplom-Ingenieurs
der Studienrichtung Maschinenbau

Betreuer
Dipl.-Ing. Dr. techn. Rudolf Pichler

Graz, Juni 2021

Eid (Ehrenwörtliche Erklärung)

Ich erkläre an Eides Statt, dass ich die vorliegende Arbeit selbstständig und ohne fremde Hilfe verfasst, andere als die angegebenen Quellen nicht benutzt und die den benutzten Quellen wörtlich und inhaltlich entnommenen Stellen als solche kenntlich gemacht habe.

Ich versichere, dass ich dieses Masterarbeitsthema bisher weder im In- noch im Ausland (einer Beurteilerin oder einem Beurteiler) in irgendeiner Form als Prüfungsarbeit vorgelegt habe.

Graz, Juni 2021 .....

Danksagung

Einen besonderen Dank möchte ich an meinen Betreuer, Herrn Rudolf Pichler, aussprechen, der mir stets mit Rat und Tat zur Seite stand. Meinen Kollegen in der smartfactory, Johannes Schmid und Stefan Trabesinger, möchte ich für die Unterstützung im Laufe der Arbeit danken.

Darüber hinaus möchte ich mich herzlich bei Herrn Viktorijo Malisa (AUVA) bedanken, der mit mir in zahlreichen Online-Meetings seine herausragende Expertise geteilt hat.

Des Weiteren bedanke ich mich herzlich bei sämtlichen Unternehmen, die mir wertvolle Informationen und Hardware zur Verfügung stellten. Im Speziellen sind dies Maximilian-Alexander Burret (ABB), Jochen Ratzesberger (Fanuc), Martin Mayr (Fronius), Paul Guerin (Robotiq), Martin Lorenz (Tosibox), Gerald Steinkellner (Secomea) und Peda Mijailović (FJ Mayer).

Abschließend möchte ich mich noch bei meinen Eltern für die jahrelange Unterstützung während meines gesamten Werdegangs bedanken.

Kurzfassung

Die vorliegende Masterarbeit zum Thema „Fernzugriffe auf MRK-Systeme – Sicherheitstechnische Prävention im Hinblick auf Safety und Security“ setzt sich mit dem Thema Fernwartung im Bereich der Mensch-Roboter-Kollaboration auseinander, welche zu den am stärksten wachsenden Arbeitsformen im Rahmen der Digitalisierung von Produktionen gehört, aber immer noch viele Sicherheitsfragen aufwirft.

War die Fernwartung auf Grund des Fachkräftemangels schon immer ein wichtiger Systemerhalter, wird es in Zeiten einer Pandemie, in denen Personenkontakt vermieden werden soll, nochmals wichtiger denn je. Gerade im neuen Bereich der MRK-Systeme müssen die Betreiber solcher Anlagen garantieren, dass ein sicheres Arbeiten gewährleistet ist. Im Betriebszustand „Fernwartung“ gibt es jedoch noch immer potenziell unsichere Situationen, die entweder nicht bekannt sind oder für die sich keine unmittelbaren, einfachen Lösungen anbieten.

Ziel dieser Arbeit ist es, aus vorhandenen Normen und Richtlinien mit Hilfe von Roboterherstellern, Experten für Arbeitssicherheit und Anlagenbetreibern Lösungen für eine sichere Fernwartung der MRK-Systeme zu entwickeln. Diese Ergebnisse werden in der smartfactory@tugraz des Instituts für Fertigungstechnik verifiziert. Aus der Arbeit ergeben sich ein Katalog aus Handlungsempfehlungen, der sowohl dem Betreiber als auch dem Fernwartenden Informationen bereitstellt, wie bis dato offene Risiken in Bezug auf die Arbeitssicherheit minimiert werden können.

Abstract

The present master's thesis on the topic of "Remote access to HRC-Systems – safety related prevention with regard to safety and security" deals with the topic of remote maintenance in the field of human-robot-collaboration, which is one of the fastest growing forms of work in the context of digitization of productions, but still raises many security and safety issues.

While remote maintenance has always been an important system maintainer due to the shortage of skilled workers, it will be even more important than ever in times of a pandemic in which personal contact should be avoided. Especially in the new area of HRC-systems, the operators of such systems must guarantee safe work conditions. In the "remote maintenance" operating state, however, there are still potentially unsafe situations that are either not known or for which no direct, simple solutions are available.

The aim of this work is to develop solutions for safe remote maintenance of HRC-systems from existing standards and guidelines with the help of robot manufacturers, occupational safety experts and system operators. These results are verified in the smartfactory@tugraz of the Institute for Manufacturing Technology. The work results in a catalog of recommendations, which provides both the operator and the remote maintenance operator with information on how risks that have been open to date can be minimized with regard to occupational safety.

Inhaltsverzeichnis

Abkürzungsverzeichnis

BSI ..... Bundesamt für Sicherheit in der Informationstechnik

DCS ..... Dual Check Safety

DCS/PLS ..... Prozessleitsystem

DMZ ..... Demilitarisierte Zone

ERP ..... Enterprise-Resource-Planning

EULA ..... End User License Agreement (Endbenutzer-Lizenzvertrag)

GSM ..... Global System for Mobile Communications

HMI ..... Human-Machine-Interface

HRC ..... human robot collaboration

IACS ..... Industrial Automation and Control System

IED ..... Intelligent Electronic Device

IIoT ..... Industrial Internet of Things

IoT ..... Internet of Things

IP ..... Internet Protocol

IPC ..... Industrial Personal Computer

ISDN ..... Integriertes Sprach- und Datennetz

ISMS ..... Informationssicherheits-Managementsystem

IT ..... Informationstechnik

KMU ..... Kleine und mittlere Unternehmen

LAN ..... Local area network

MES ..... Manufacturing Execution System

MRK ..... Mensch-Roboter-Kollaboration

OPC ..... Open Platform Communications

PLC/SPS ..... Speicherprogrammierbare Steuerung

RAC ..... Remote Access Concentrator

RAS ..... Remote Access Service

RTU ..... Remote Terminal Unit

SCADA ..... Supervisory and Data Acquisition

SIL ..... Sicherheits-Integritätslevel

SIS ..... Safety Instrumented Systems

SL ..... Security-Level

VCL ..... Virtual Center Lock

VDMA ..... Verband Deutscher Maschinen- und Anlagenbau

VFD ..... Variable Frequency Drive

VPN ..... Virtual Private Network

WAN ..... Wide area network

WLAN ..... Wireless local area network

WSUS ..... Windows Server Update Service

1. Einleitung

Hersteller und Integratoren von Anlagen verlangen seit geraumer Zeit einen Zugang für die Fernwartung, ungeachtet dessen, in welchem Bereich das Unternehmen tätig ist.[1] Gründe dafür sind die Internationalisierung der Firmen, die weltweit verteilten und oft schwer zugänglichen Anlagen und der Mangel an fachlich kompetenten Mitarbeitern am jeweiligen Standort. Die Implementierung von Tools für die Fernwartung sowie Fernüberwachung stellt sicher, dass die Fehlerbehebung oder beispielsweise das Ausführen von Updates zeitnah durch den entsprechenden Experten umgesetzt werden kann.[2] Auch der Entfall von Reisekosten stellt einen wesentlichen Aspekt der Kostenersparnis dar, die im Rahmen der Fernwartung erzielt werden kann. Die anhaltende Weiterentwicklung von Telekommunikationstechniken, wie beispielsweise der 5G-Ausbau, fördern eine erleichterte Umsetzung eines Fernzugriffs über das Internet.

Die genannten Vorteile führen in Verbindung mit Industrie 4.0 und dem IoT zu einem erhöhten Interesse an Fernwartungen. Die aktuelle Corona-Krise hat durch die Bestrebungen, Reisen und zwischenmenschliche Kontakte einzuschränken, nochmals zu einer Steigerung der Nachfrage von Systemen für Fernzugriffe und Fernwartungen geführt.

Sicherheitsprobleme werden dabei oft übersehen, da im KMU-Umfeld oftmals das Bewusstsein für Informationssicherheit und Risikomanagement nicht ausreichend vorhanden ist. So ergaben Untersuchungen von Experten, dass Systeme für Automatisierungs- und Steuerungstechnik über verschiedene Protokolle frei im Internet erreichbar sind. Geschützt werden diese durch Passwörter, deren Konfigurationen oftmals mangelhaft und somit leicht zu entschlüsseln sind. Nicht selten bleiben die Passwörter sogar auf der Default-Kombination, die der jeweiligen Betriebsanweisung zu entnehmen ist.[3]

[1] Vgl. Schrade, 2015, S. 3.

[2] Vgl. Conti, Sal, 2017, S. 43.

[3] Vgl. Schrade, 2015, S. 3–4.

Die smartfactory@tugraz repräsentiert das Modell einer modernen Fabrik, in der MRK-Systeme eine immer größere Rolle spielen und eignet sich daher sehr gut für Untersuchungen im Bereich der MRK-Robotik. Bei diesen Anlagen entstehen durch die MRK-Betriebsmodi neue Anforderungen bezüglich Maschinen- und Anlagensicherheit. Der Fernzugriff auf ein solches MRK-System stellt eine besondere Herausforderung für den Fernwartenden und den Anlagenbetreiber dar, da der Betreiber die Steuerung einer Anlage, die in seiner Verantwortung liegt, an eine nicht vor Ort befindliche Person übergibt.

Die folgende Arbeit soll aufzeigen, wie in diesem Zusammenhang Sicherheitslücken entstehen können und letztlich eine sichere Fernwartung von MRK-Systemen durchgeführt werden soll. Der Anlagenbetreiber sollte nach der Umsetzung dieser Empfehlungen in der Lage sein, eine sichere Fernwartung durchzuführen.

2. Theoretische Grundlagen der Arbeit

In der Einleitung erscheinen bereits die wichtigsten Begriffe dieser Arbeit. MRK-System, Fernwartung und Arbeitssicherheit sind drei Schlüsselbegriffe, die daher im folgenden Kapitel genauer erläutert werden.

2.1 Arbeitssicherheit

Eine Statistik der AUVA aus dem Jahr 2018 zeigt auf, dass mit 39 % die meisten Arbeitsunfälle österreichweit aus dem „Verlust der Kontrolle über eine Maschine, ein Handwerkszeug, ein Fahrzeug, u.ä.“ resultieren.[4] Die Arbeitssicherheit spielt in der Industrie daher eine große Rolle. In den folgenden Kapiteln wird eine kurze Einführung in die Thematik „Arbeitssicherheit“ gegeben. Ergänzend wird der Wandel der Arbeitssicherheit in der Industrie 4.0 kurz erläutert.

2.1.1 Definition von Safety und Security

Die Begriffe Safety und Security spielen gerade im Zusammenhang mit dem Thema dieser Arbeit, der Fernwartung, eine große Rolle. Im Deutschen sind diese Begriffe sinngemäß als „funktionale Sicherheit“ und „Sicherheit gegen ungewollte Zugriffe“ zu übersetzen.

Unter dem Begriff Safety versteht man den Schutz des Menschen vor der Maschine, aber auch den Schutz der Maschine selbst sowie der Umwelt. Oftmals wird auch der Begriff Betriebssicherheit verwendet. Der Begriff Security soll die Maschine vor der Umgebung schützen.[5] Als Beispiel kann der Schutz gegen Systemausfälle, Sabotage sowie Spionage genannt werden. Das Ziel ist es, die Verfügbarkeit der Anlage, die Integrität und Vertraulichkeit der Daten abzusichern. Security wird auch oft als IT- /bzw. Informationssicherheit bezeichnet. Die Gesamtsicherheit einer Anlage wird aus der Kombination von funktionaler und Informationssicherheit bestimmt.[6]

[4] AUVA, 2019, S. 21.

[5] Vgl. Malisa, 2018, S. 5

[6] Vgl. Malisa, 2018, S. 5.

2.1.2 Verschmelzen von Safety und Security in Industrie 4.0

Die Bereiche Safety und Security sind untrennbar miteinander verknüpft und können vielfach auch zu Gegenspielern werden. So können Maßnahmen, die zur Gewährleistung der Safety dienen sollen, gleichzeitig auch ein Risiko für die Security darstellen. Ein einfaches Beispiel verdeutlicht die teilweise unterschiedlichen Werte und Ziele von Safety und Security. Eine Notausgangstür ist vorhanden, damit ein Gebäude jederzeit verlassen werden kann. Im Idealfall steht diese Tür, aus der Safety-Betrachtung heraus, permanent offen. Aus Sicht der Security sollte diese Türe überhaupt nicht existieren, da sie unerlaubten Zutritt ermöglicht.[7] Übertragen auf die Thematik dieser Arbeit stellt der Fernwartungszugang eine solche Türe dar. Er soll den kontrollierten Zugriff auf eine Anlage erlauben, eröffnet aber auch einen potenziellen, ungewollten Zugang.

Das Konzept Industrie 4.0 setzt vernetzte Anlagen und Maschinen voraus. Die dazu benötigten IT-Schnittstellen ermöglichen theoretisch den Zugriff auf wichtige Sicherheitssysteme, die zur Gewährleistung der funktionalen Sicherheit notwendig sind. Im IEC TR 63069:2019 wurde dazu die Idee einer sogenannten Security Umgebung entwickelt, die sämtliche Gegenmaßnahmen beinhaltet, welche eine geschützte Umhüllung der Betriebsumgebung sowie der Safety Systeme gewährleisten. Das Ziel ist es, Bedrohungen durch Angriffe oder menschlichem Versagen daran zu hindern, Schwachstellen auszunutzen, die die Safety beeinträchtigen. [8]

Abbildung 1 stellt die Struktur bildlich dar und zeigt zudem auf, dass Bedrohungen nicht nur für den äußersten Bereich existieren, sondern beispielsweise durch Social Engineering direkt in die Betriebsumgebung gelangen. Dieser Aspekt führt dazu, dass auch im Safety System Security-Gegenmaßnahmen implementiert sein müssen.

[7] Vgl. Springer, 2016.

[8] Vgl. Technical Report IEC TR 63069, 2019, S. 20–21.

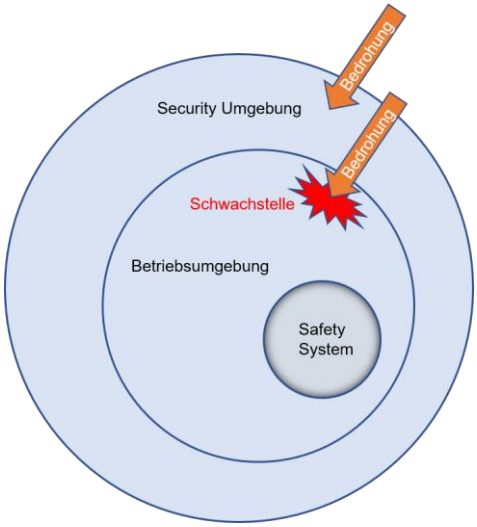

Abbildung 1: Konzept der Security Umgebung, Quelle: IEC TR 63069 (2019)

Es wird deutlich, dass die Security einen wesentlichen Einfluss auf die Safety hat. Im IEC TR 63069:2019 wurde dies auch erstmals festgehalten. Wie in Abbildung 2 ersichtlich, ist eine Zusammenarbeit der beiden Bereiche notwendig, um die gewünschte Anlagensicherheit zu erreichen. Es müssen sowohl im Security als auch im Safety Bereich Risikoanalysen durchgeführt werden, die zu Safety-Maßnahmen bzw. Security-Gegenmaßnahmen führen. Bei diesen Maßnahmen und Gegenmaßnahmen entstehen oft Konflikte, die gelöst werden müssen.

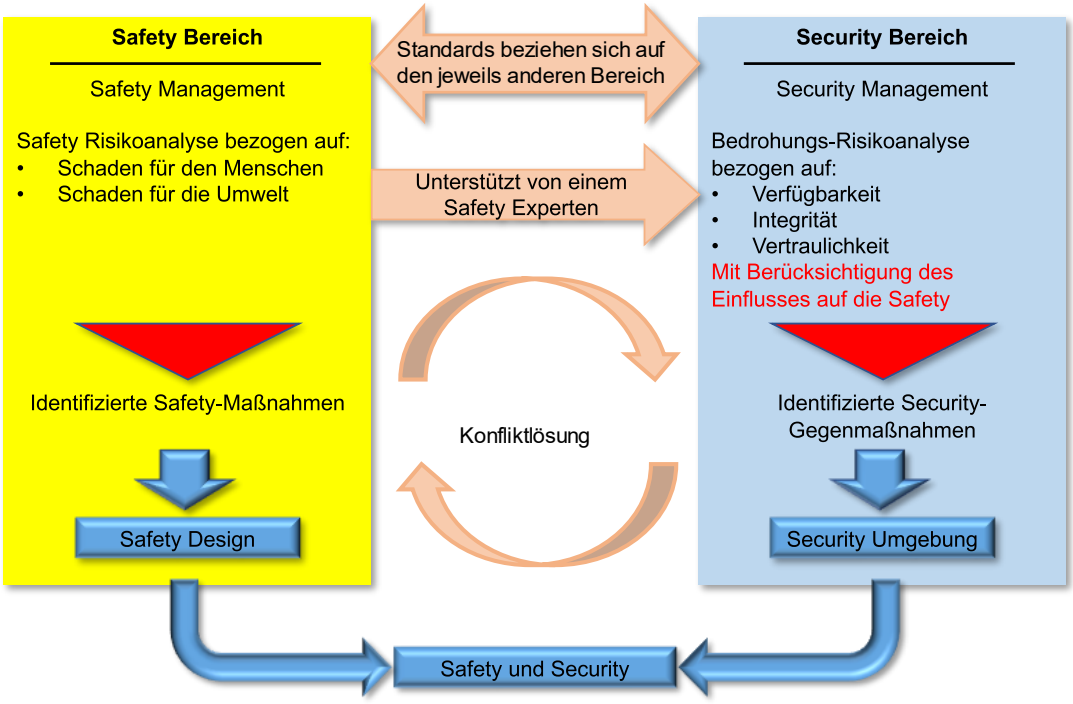

Abbildung 2: Zusammenhang Safety und Security, Quelle: IEC TR 63069 (2019)

2.1.3 Fallbeispiel „TRITON“

Dass Zwischenfälle im Security-Bereich massive Auswirkungen auf die Safety von Anlagen haben können, zeigt der Fall „TRITON“ (auch bekannt als „TRISIS“ oder „HatMan“), bei dem im Dezember 2017 der erste gezielte Angriff auf die Sicherheitssteuerung einer Maschine stattfand. Ziel des Angriffs war der Produktionsprozess eines saudi-arabischen Chemiewerks. Dabei wurde versucht, die Triconex SIS des Herstellers Schneider Electric, die für Notabschaltungen zuständig ist, wenn es in der Chemieanlage zu Störungen kommt, mit einer Schadsoftware zu infizieren. Der nächste Schritt wäre vermutlich das Hervorrufen ebendieser Störung gewesen, um so eine Katastrophe in dem Werk auszulösen. Dank eines Fehlers in der Schadsoftware kam es zu einer Notabschaltung, deren Untersuchung dann den Hackerangriff aufdeckte.[9]

Forscher vermuten, dass dieser Angriff nicht aus finanzieller Motivation entstand, sondern dass er das Ziel hatte, schwere physische Schäden an Mensch und Umwelt hervorzurufen. Dies stellt ein neues Level von Cyberattacken dar und kann wesentlich ernstere Folgen haben, als bisher bekannt war. Ermöglicht wurde diese Attacke durch die Kombination von mangelhafter Einrichtung des IT-Netzwerks und fehlerhafter Bedienung. So wurde unter anderem bekannt, dass die Safety Systeme nicht sauber vom restlichen Automatisierungsnetzwerk abgeschottet waren. Zusätzlich befand sich der physische Schlüsselschalter, der in dem Typus der Triconex Systeme integriert ist, auf der Stellung „Programmiermodus“, was ein Einspielen von Software über das Netzwerk überhaupt erst ermöglichte.[10]

Vieles spricht dafür, dass der Engineering PC, der für die Sicherheitssteuerung zuständig war, über sogenanntes Social Engineering vom Virus verseucht wurde. Dabei wurden Files eingespielt, wie „trilog.exe“, deren Benennung den Bediener im Glauben lässt, dass dieses File in Zusammenhang mit der Triconex Steuerung steht und er es deshalb am Rechner ausführt.[11]

---

[9] Vgl. Di Pinto/Dragoni/Carcano, 2018, S. 2–3.

[10] Vgl. Geiger, 2019.

[11] Vgl. Di Pinto/Dragoni/Carcano, 2018, S. 3.

Das aufgezeigte Beispiel verdeutlicht, welch schwerwiegende Folgen unzureichend abgesicherte IT-Infrastrukturen haben können. In modernen Anlagen stellen die Safety Systeme auch verwundbare IT-Systeme dar und müssen durch eine ausreichende Security geschützt werden. Die Verknüpfung von Security und Safety ist daher in Zeiten von IoT unumgänglich. Das Beispiel TRITON stützt diese These nachdrücklich.

2.1.4 Häufige Zwischenfälle bei Fernwartungen

Der vorherige Fall „Triton“ zeigt auf, dass Hacker durchaus Interesse haben, Industrieanlagen zu sabotieren. Dies zeigt auch der Angriff auf eine Wasseraufbereitungsanlage in Florida im Februar 2021, die über den TeamViewer, welcher als Fernwartungstool fungierte, manipuliert wurde. Es wurde den Angreifern damit möglich, die Natriumhydroxidkonzentration, eine Chemikalie, die zur Wasseraufbereitung verwendet wird, um das 100-fache zu erhöhen und somit das Leben von etwa 15000 Menschen zu gefährden. Glückliche Umstände führten dazu, dass der Fehler entdeckt und rechtzeitig behoben wurde.[12]

Vorfälle, bei denen eine an einer Fernwartung beteiligte Person durch einen ferngesteuerten Roboter verletzt wurde oder allgemein beim Prozess der Fernwartung zu Schaden gekommen ist, sind der AUVA nicht bekannt, da die Forensik bei Unfällen mit Robotern nicht in die Thematik Fernwartung oder Wartung vor Ort unterteilt.[13] Die neutrale Betrachtung der Möglichkeiten, die die Fernwartung bietet, zeigt das Gefahrenpotenzial, das sich darin verbirgt und verdeutlicht die Notwendigkeit ausreichender Schutzvorkehrungen, um alle beteiligten Personen und Anlagen ausreichend zu schützen.

[12] Vgl. Berghoff, 2021.

[13] lt. Interview V.Malisa, AUVA am 09.04.2021

2.2 MRK–Systeme

Durch Industrie 4.0 steigen die Anforderungen an Qualität, Produktivität und Flexibilität von industrieller Fertigung.[14] Ein Mittel zur Erreichung dieser Ziele stellt die MRK-Robotik dar, die in folgenden Kapiteln definiert wird. Anschließend werden Aufbau und Betriebsarten eines kollaborativen Roboters beschrieben.

2.2.1 Definition MRK-Robotik

In der Norm ISO 10218 spricht man vom „kollaborierenden Betrieb“, wenn ein Roboter mit dem Menschen in einem festgelegten Arbeitsraum direkt, d.h. zeitgleich, zusammenarbeitet. Innerhalb dieses gemeinsamen Arbeitsraums können Mensch und Roboter zur gleichen Zeit am gleichen Objekt Arbeiten verrichten. Dies wird als Kollaboration bezeichnet. Eines der Hauptziele der MRK-Robotik ist die Erhaltung der kognitiven Fähigkeiten des Menschen in der Produktionskette.[15] Die Vorteile ergeben sich aus der Möglichkeit, die Stärke, Reproduzierbarkeit und Kontinuität von Maschinen mit der Flexibilität, Anpassungsfähigkeit und Intelligenz von Menschen zu verknüpfen. Daraus resultierend kann die MRK-Robotik zur Steigerung von Produktivität und Verbesserung der Qualität führen, während sie gleichzeitig die körperliche und mentale Belastung der Produktionsmitarbeiter reduziert.[16] Die Möglichkeit des Entfalls von physischen Barrieren, wie Absperrgittern, stellt das größte sichtbare Unterscheidungsmerkmal zu den herkömmlichen Industrierobotern dar.

[14] Vgl. Buxbaum, Hans; Kleutges, Markus; Sen, Sumona, 2018, S. 3299.

[15] Vgl. Buxbaum, Hans; Kleutges, Markus; Sen, Sumona, 2018, S. 3299.

[16] Vgl. Rusch/Ender/Kerber, 2020, S. 1228–1229.

2.2.2 Betriebsarten eines kollaborativen Roboters

Der Betrieb des Roboters im Kollaborationsraum wird in der Norm ISO 10218-2 in vier verschiedene Betriebsmodi unterteilt:[17]

a) Sicherheitsbewerteter überwachter Halt

b) Handführung

c) Geschwindigkeits- und Abstandsüberwachung

d) Leistungs- und Kraftbegrenzung durch inhärente Konstruktion oder durch die Steuerung

Ad a)

Sobald eine Person den Kollaborationsraum betritt, stoppt der Roboter seine Bewegung und nimmt den sicherheitsüberwachten Halt nach ISO 10218-1 ein, damit der Werker mit dem Roboter zusammenwirken kann. Die Zugangskontrolle kann beispielsweise mittels einer Lichtschranke realisiert werden. Verlässt die Person den Kollaborationsraum, nimmt der Roboter seine Arbeit wieder auf.

Ad b)

Verfügt die Bedienperson über eine Führungseinrichtung und hat klare Sicht auf den gesamten Kollaborationsraum, ist es möglich, den Roboter mittels Handführung in die gewünschte Position zu bringen.

Ad c)

Mittels einer Risikobeurteilung werden Grenzwerte festgelegt, die garantieren, dass der Roboter zum Bediener den Abstand in einer dynamischen Art und Weise aufrechterhält. Die Erkennung des Umfeldes kann beispielsweise mittels Lidar Sensoren erfolgen. Diese

[17] Vgl. Norm DIN EN ISO 10218-2, 2011, S. 46–47.

Methode stellt nach aktuellem Stand der Technik die am schwersten realisierbare Variante dar.

Ad d)

In diesem Betriebsmodus stoppt der Roboter bei Überschreitung von Kraft- und Leistungsgrenzwerten, die auf eine Kollision rückschließen lassen. Wie auch schon unter c) erwähnt, müssen sämtliche Parameter mittels Risikobeurteilung ermittelt werden. Der Aufbau der Roboter muss der Norm ISO 10218-1 genügen. Wie in Abbildung 3 ersichtlich, achten die Hersteller darauf, sämtliche Kanten der MRK-Roboter abzurunden, um im Kollisionsfall die Verletzungsgefahr zu minimieren.

Abbildung 3: kollaborationsfähiger Roboter „YuMi" Quelle: ABB (2020), Onlinequelle [07.09.2020]

2.2.3 Prinzipieller und sicherheitstechnischer Aufbau eines MRK-Systems

Um im späteren Verlauf dieser Arbeit die Gefahren nachzuvollziehen, welche von einem kollaborativen Roboter ausgehen können, ist es notwendig, den genauen Aufbau und die Abläufe, die sich hinter einem MRK-System befinden, zu beschreiben. Das folgende Kapitel gibt sowohl einen Überblick über die hardwaretechnische Systemgestaltung als auch über die softwarebasierte Steuerungstechnik.

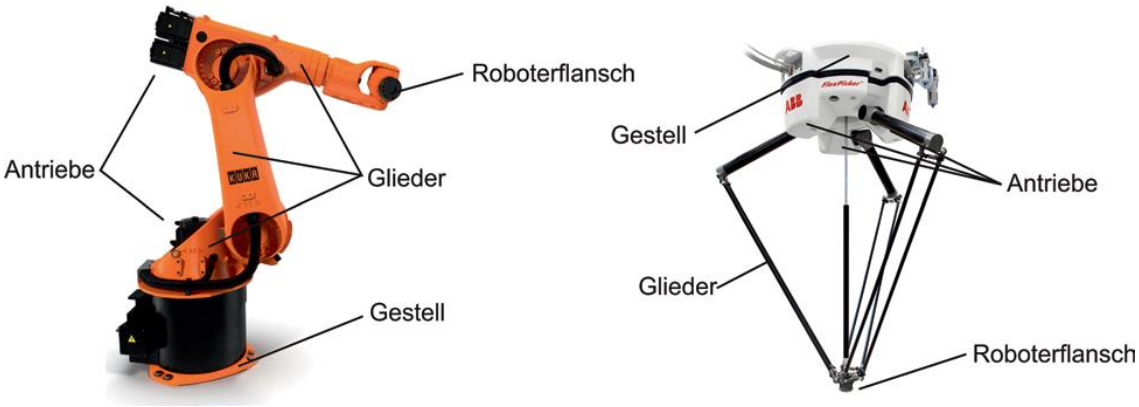

Abbildung 4: Struktur serielle (links) und parallele (rechts) Kinematik, Quelle: Müller u.a. (2019)

In der Robotik wird prinzipiell zwischen serieller und paralleler Kinematik unterschieden. Letztere zeichnet sich dadurch aus, dass mehrere Glieder und deren Antrieb direkt mit dem Roboterflansch verbunden sind. Der Antrieb paralleler Systeme ist im Gegensatz zu den seriellen Systemen ortsfest. Die parallele Technologie kommt in der MRK-Robotik jedoch kaum zum Einsatz und wird daher in vorliegender Arbeit nicht weiter erläutert. In der seriellen Roboterkinematik sind die einzelnen Glieder in einer Serie hintereinandergeschaltet, wobei jedes Glied das Gewicht der nachfolgenden Glieder trägt. In Abbildung 4 (links) sind die einzelnen Komponenten eines Vertikalknickarmroboters ersichtlich. Das Gestell beschreibt den unbeweglichen Teil des Roboters, an dem dieser befestigt wird. Es überträgt sämtliche an der Roboterstruktur auftretenden Kräfte. Angetrieben wird diese Roboterart von sechs mit elektrischen Antrieben ausgestatteten Gelenken. Zur genauen Positionierung ist eine Auswertung der Gelenkwinkel erforderlich, welche mittels eines Drehgebers durchgeführt wird. Über Drehmomentsensoren oder Messung des Motorstroms kann detektiert werden, ob der Roboter mit einem Hindernis kollidiert. Am Roboterflansch, der das letzte Glied der Kette

darstellt, wird der Endeffektor befestigt. Dieser ist stark anwenderspezifisch und kann beispielsweise ein Backen- oder Vakuumgreifer sein.[18]

Im Gegensatz zu dem in Abbildung 4 (links) dargestellten klassischen Industrieroboter können MRK-Systeme oft mehr als sechs Achsen besitzen. Der in Abbildung 5 dargestellte MRK-Roboter iiwa des Herstellers Kuka verfügt über sieben Achsen. In den Achsen A6 und A7 befinden sich die Motoren, im Inneren der Gelenkmodule (2) die Antriebseinheiten, welche über die Gelenkmodule miteinander verbunden sind. Das in der Abbildung dargestellte Modell verfügt über eine zweiachsige Zentralhand (1). Die Basis des Roboters bildet das Grundgestell (3). Die Achsen A1 bis A7 sind auf der rechten Seite der Abbildung 5 ersichtlich. Diese Roboter, mit mehr als sechs Achsen, sind kinematisch überbestimmt. Man bezeichnet sie als redundant. Es ist nicht immer möglich, diese Roboter durch Programmierverfahren, welche auf mathematischen Berechnungen basieren, zu programmieren. In der MRK-Robotik kommen daher neue Anlernverfahren, wie die „Teach-In-Programmierung“ zum Einsatz. Dabei bewegt der Bediener im Rahmen der Programmierung den Roboter per Hand zu den einzelnen Positionen. Die zuvor angesprochene Redundanz eröffnet aber neue, für die MRK-Robotik nützliche Funktionen, wie beispielsweise das Bewegen von Achsen ohne Positionsänderung des Endeffektors im Raum.[19]

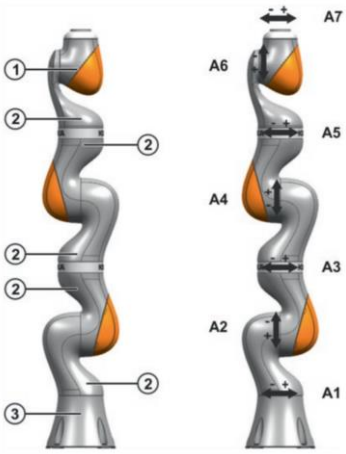

Abbildung 5: MRK-Roboter Kuka iiwa 14 R820, Quelle: Bendel (2018)

[18] Vgl. Franke, Jörg, et al., 2019, S. 39–40.

[19] Vgl. Bendel, 2018, S. 4–5.

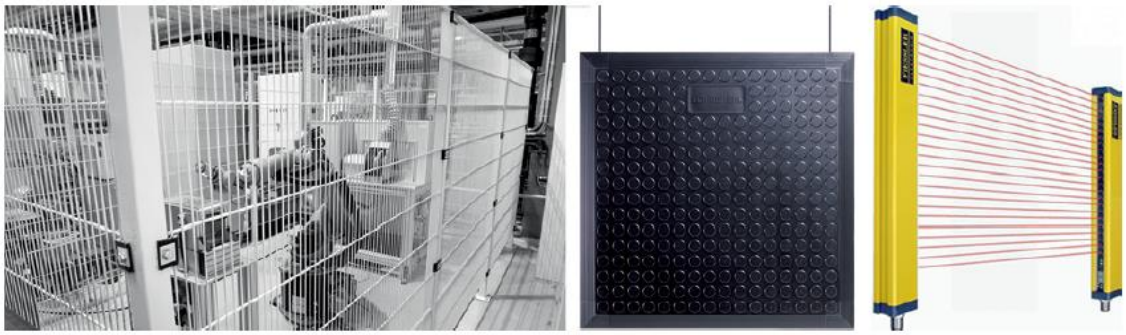

Abbildung 6: Sicherheitseinrichtungen für Robotersysteme v.l.n.r. Schutzzaun, Trittmatte, Lichtschranke, Quelle: Müller u.a. (2019)

Jeder kollaborative Roboter muss über geeignete Sicherheitsfunktionen und eine unabhängige Not-Halt Funktion verfügen. Es müssen Vorkehrungen vorhanden sein, die den Anschluss von externen Schutzeinrichtungen erlauben.[20] Beispiele hierfür sind Schutzzäune, Trittmatten oder Lichtschranken (siehe Abbildung 6), wobei vor allem Schutzzäune in der kollaborativen Robotik nicht zwingend notwendig sind und daher kaum Anwendung finden.

Softwaretechnisch unterscheidet sich der prinzipielle Aufbau einer Steuerung eines kollaborativen Roboters nicht wesentlich von einer gängigen industriellen Steuerung, wie in Abbildung 7 dargestellt. Ein Anwendungsprogramm, das auf einem Engineering-PC entwickelt wird, definiert das Verhalten der Steuerung. Diese ist über Sensoren (Eingänge) und Aktoren (Ausgänge) mit dem Prozess verbunden. In modernen Anlagen besteht die Steuerung aus speicherprogrammierbaren Steuerungen und Bewegungssteuerungen, die oft nur als Softwaremodule in der industriellen Steuerung vorhanden sind.[21]

[20] Vgl. Norm DIN EN ISO 10218-1, 2011, S. 15.

[21] Vgl. Franke, Jörg, et al., 2019, S. 117.

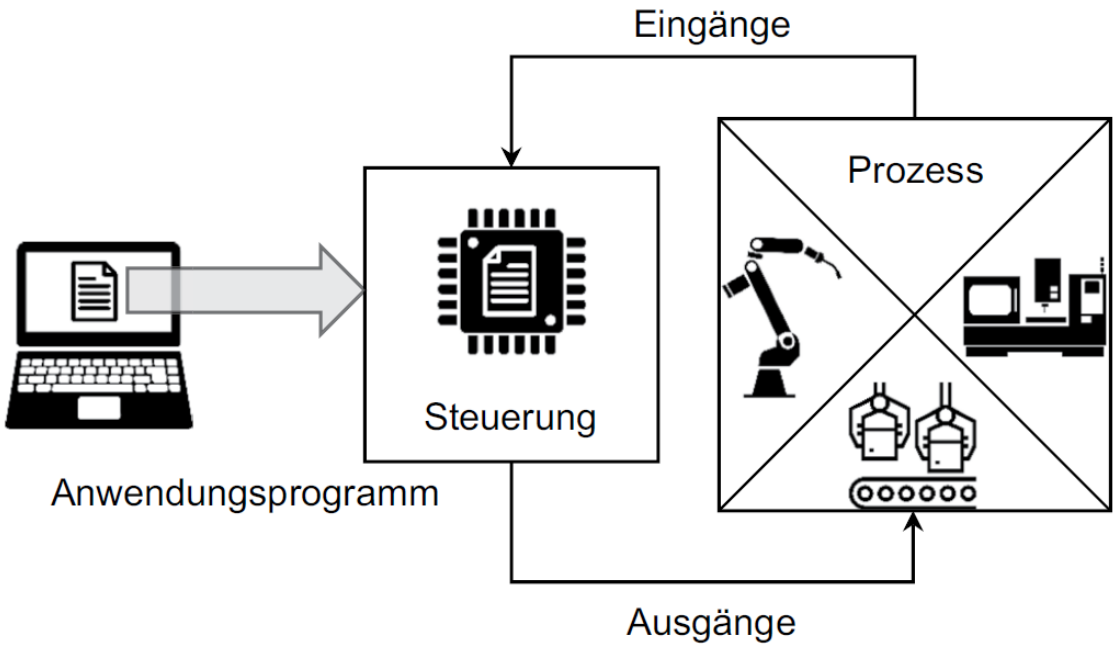

Abbildung 7: Übersicht einer industriellen Steuerung, Quelle: Müller u.a. (2019)

Für kollaborative Roboter schreibt die Norm ISO 10218-1 zusätzlich eine Sicherheitssteuerung vor, die gemäß ISO 13849-1:2006 mindestens die Struktur der Kategorie 3 erfüllt, diese ist in Abbildung 8 dargestellt. Sie beinhaltet eine logische Redundanz in der Verarbeitung der Ein- und Ausgänge. Damit wird die Anforderung erfüllt, dass einzelne Fehler nicht zum Ausfall der Sicherheitsfunktion führen.[22]

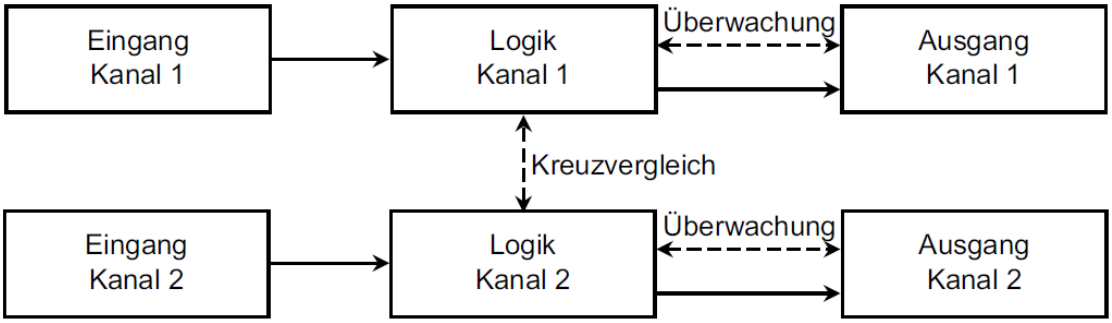

Abbildung 8: Struktur Kategorie 3 gemäß EN ISO 13849, Quelle: Müller u.a. (2019)

[22] Vgl. Franke, Jörg, et al., 2019, S. 122–123.

2.3 Fernwartung

Die in Kapitel 2.1 beschriebenen Systeme können zu Wartungs-, Update- oder Reparaturzwecken ferngewartet werden. Im folgenden Kapitel wird zunächst eine Definition des Begriffs „Fernwartung“ gegeben, bevor ein Überblick über aktuelle Entwicklungen dieser Thematik geschaffen wird.

2.3.1 Definition des Begriffs „Fernwartung“

Der Begriff Fernwartung kann definiert werden als Zugriff einer nicht vor Ort befindlichen Person auf eine Maschine oder Industrieanlage über ein Kommunikationssystem. „Der Zugriff kann z.B. dazu dienen, Konfigurations-, Wartungs- oder Reparaturarbeiten durchzuführen“[23]. Es wird zwischen passiver und aktiver Fernwartung unterschieden, wobei aktiv bedeutet, dass durch direkte Eingriffe in laufende Anwendungen Änderungen vorgenommen werden. Passiv bedeutet in diesem Zusammenhang, dass ausschließlich ein betrachtender Zugang auf das System erfolgt.[24]

Ziel der Hersteller ist es, spezielle Tools für die industrielle Fernwartung bereitzustellen, die auch einem entfernten Experten einen guten Einblick in die Produktionsumgebung des Kunden vermitteln. Die interaktive Unterstützung kann durch Technologien, wie Videostreaming, Chat, Dateiaustausch und Augmented Reality an das jeweilige Ausbildungsniveau der vor Ort befindlichen Servicekraft angepasst werden.[25]

Für die aktive Fernwartung besagt der VDMA, dass eine festgelegte Nutzergruppe zu einem bestimmten Zeitraum für eine beschränkte Dauer mit genau definierten Rechten ausgestattet wird. Zum Zeitpunkt des Zugriffs muss sichergestellt sein, dass der Betrieb der Maschine einen Fernzugriff erlaubt. Werden nach einer bestimmten Dauer keine Aktivitäten ausgeführt, muss die Fernzugriffssitzung automatisch gesperrt werden. Der Anmeldezeitpunkt, die

[23] Bundesamt für Sicherheit in der Informationstechnik, 2020a, S. 249.

[24] Vgl. Bundesamt für Sicherheit in der Informationstechnik, 2021, S. 1.

[25] Vgl. Sittner u. a., 2014, S. 1.

Sitzungsdauer sowie die vorgenommenen Änderungen sind zu protokollieren.[26] Rechtsverbindlich wird die Durchführung in der in Kapitel 3.1 beschriebenen ISO 10218-2 für kollaborative Roboteranwendungen erläutert.

2.3.2 Stand der Technik

In vielen Unternehmen ist eine Mischung aus alten und neuen Anlagen vorhanden. Aus diesem Grund unterscheiden sich auch die Zugriffsmöglichkeiten auf diese Anlagen. Prinzipiell geht der Trend vom Verbindungstyp „bei Bedarf“ zu „dauerhaft an ein Kommunikationsnetz angebundene Anlagen“. Die klassische physische Methode via ISDN-Kabel stellt eine leicht trennbare Verbindung dar und findet vor allem bei älteren Anlagen Anwendung. Es handelt sich dabei um eine Punkt-zu-Punkt-Verbindung. Technologien, die eine Cloud oder VPN verwenden, greifen auf eine Ende-zu-Ende-Verbindung zurück.

Wie in Abbildung 9 dargestellt, findet beim klassischen Remote Access Service (RAS) die Einwahl über das Telefon- oder Mobilfunknetz statt. Dies kann entweder via ISDN-Verbindung, analogem Modem oder GSM-Modem geschehen. Der Einwählvorgang erreicht den Primärmultiplexer, der mit dem Remote Access Concentrator (RAC) verbunden ist. Im einfachsten Fall ist der RAC durch einen RAS-Server realisiert, der via Modem oder ISDN-Karte mit der Telefonanlage verbunden ist. Nach Eingabe der Einwahlnummern wird die Authentifizierung mittels Benutzername und Passwort durchgeführt.[27] Abbildung 10 zeigt ein Modem von Siemens zur Herstellung einer duplexen Punkt-zu-Punkt-Verbindung für die Datenübertragung über ISDN-Standleitungen. Siemens weist darauf hin, dass diese Modems nicht mehr als Neuprodukte erhältlich sind, sondern nur im Austausch gegen ein defektes Modem als Ersatzteil. Es wird empfohlen, auf die IP-basierende Technologie SIMATIC NET umzusteigen.[28]

[26] Vgl. VDMA 66418, 2017, S. 10–11.

[27] Vgl. Schnabel, 2020.

[28] Vgl. Siemens AG, 2010.

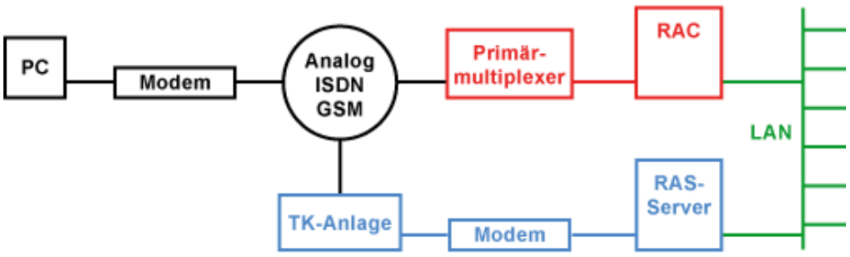

Abbildung 9: RAS-Architektur Quelle: Schnabel (2020), Onlinequelle [09.09.2020]

Der Nachteil dieser RAS-Methode ist die sehr geringe Bandbreite von wenigen Kilobytes/Sekunde, eine teils sehr instabile Verbindung und die Abrechnung nach Verbindungszeit, die zu hohen Kosten führen kann. Dennoch wird es bei heutigen Systemen oft als Backup-Lösung verwendet, da es eine hohe Verbindungsstabilität bietet. Ein weiterer Vorteil ist, dass diese Verbindung sehr abhörsicher ist und fest definierte Antwortzeiten besitzt.[29]

Abbildung 10: SINAUT-Modem MD4 Quelle: Siemens (2002), Onlinequelle [10.09.2020]

Die aktuellen Entwicklungen rund um die Thematik Industrie 4.0 erfordern die dauerhafte Anbindung von Anlagen und deren Steuerungen an ein IT-Netzwerk. Mittels verschiedener Hard- und Software werden Betriebsdaten erfasst und ausgewertet, um beispielsweise Predictive Maintenance zu realisieren. Solche Architekturen ermöglichen unter gewissen Voraussetzungen auch einen Fernzugriff

[29] Vgl. Schnabel, 2020.

über das Internet, der ohne ISDN Verbindungen auskommt. In Kapitel 3.4 werden die Systeme ausgewählter Hersteller genauer erläutert.

2.3.3 Fallbeispiele aktueller Fernwartungen

Das folgende Beispiel eines KMUs zeigt die ursprünglichen Vorgehensweisen von Fernwartungen auf. Im Falle einer Störung kontaktiert der Anlagenbetreiber den Servicetechniker telefonisch. Daraufhin wird die zu untersuchende Anlage per LAN-Kabel, bei älteren Modellen auch per ISDN-Kabel, mit einem Kommunikationsnetz verbunden. Am Bedienpanel der Anlage werden die telefonisch übermittelten Zugangsdaten eingegeben, welche einen direkten Zugang des Servicetechnikers auf die speicherprogrammierbare Steuerung (SPS) erlauben. Dieser kann daraufhin den Schaltplan der SPS analysieren, Fehlermeldungen auslesen und interpretieren sowie eine Simulation der SPS starten, die zeigt, welche Schalter das elektrische Signal nicht überwinden kann. Softwarefehler können über den Fernwartungszugang korrigiert werden, kleine Hardwarefehler, wie beispielsweise festsitzende Endschalter, werden in der Regel per telefonischer Anweisung an den vor Ort befindlichen Arbeiter des Anlagenbetreibers gelöst. Ergibt die Untersuchung einen irreparablen Defekt einer Hardwarekomponente, so wird diese bei Bedarf mit einem Servicetechniker des Herstellers zur Montage vor Ort gebracht. Dem Techniker liegt dann bereits ein vollständiges Protokoll der Fernwartung vor. Im Regelbetrieb ist die Anlage nicht mit einer Kommunikationseinrichtung via ISDN oder Ethernet verbunden.[30]

Anhand eines Beispiels des Systemintegrators Fronius kann der Wandel dieser Technologie aufgezeigt werden. Bei Fernwartungen setzt man dort schon seit 10 Jahren auf Router des Herstellers „INSYS“, welche in die Steuerungen der Anlagen integriert und mit dem Internet via LAN oder Mobilfunk verbunden werden. Diese Router verfügen über einen Schlüsselschalter, der im Falle einer Fernwartung einen VPN Tunnel zu einem Server herstellt, der direkt bei Fronius stationiert ist. Gleichzeitig erhält ein Servicemitarbeiter eine E-Mail-Benachrichtigung der Verbindungsanfrage. Er nimmt telefonisch Kontakt zum Bediener vor Ort auf und

[30] lt. Interview U.Sigl, Geschäftsführer Sigl Elektromotoren GmbH am 17.10.2020

führt dann über diesen die gewünschten Aktionen aus der Ferne durch. Neben den zuvor genannten Diagnosemöglichkeiten im Fehlerfall wird die Fernwartung von Fronius auch oftmals für die Erweiterung um vom Kunden gewünschte Zusatzfunktionen der Anlage genutzt. Es können Softwareupdates, welche zuvor von Fronius selbst in Simulationen getestet wurden, auf bestehende Kundensysteme aufgespielt werden. Servicetechniker berichten von drei oder mehreren Fernwartungssitzungen pro Woche im internationalen Umfeld mit steigender Tendenz. Dies verdeutlicht die größer werdende Bedeutung von Fernwartungsdienstleistungen. Das Unternehmen entwickelt gerade ein Cloud-Portal, an dem auf Wunsch sämtliche Kundensysteme angebunden werden können, über welches Updates automatisiert durchgeführt werden können.[31]

[31] lt. Interview M.Mayr, Team Leader Automation Software Engineering Fronius International GmbH am 18.02.2021

3. Aktueller Stand und Handhabung von Fernzugriffen auf ein MRK-System

In diesem Kapitel werden zunächst die normativen Randbedingungen beschrieben. Infolge Risikoanalysen werden etwaige Verbesserungsvorschläge für eine gesteigerte Arbeitssicherheit aufgezeigt. Anschließend verdeutlichen Fallbeispiele und die Hardware ausgewählter Unternehmen den aktuellen Entwicklungsstand dieser Thematik.

3.1 ISO 10218-2 Durchführung einer Fernwartung

Diese Norm befasst sich mit Robotersystemen und deren Integration. Sie dient vor allem den Anlagenbetreibern und Systemintegratoren. Auch die Thematik des Fernzugriffs wird in dieser Norm behandelt, wie das folgende Kapitel aufzeigt.

3.1.1 Durchführungsvorschrift der Norm

Nachstehend folgt ein Ausschnitt aus der Norm ISO 10218-2, welche in Absatz 5.6.5 den Fernzugriff für manuelles Eingreifen wie folgt reguliert:

„Wird ein Robotersystem von einer Bedienperson ferngesteuert, die sich an einem anderen Ort als dem Roboterstandort aufhält, z. B. in einem entfernten Büro, ist Folgendes erforderlich:

a) manuelle Fernsteuerung darf nur möglich sein, wenn sich der Roboter oder das Robotersystem in der manuellen Betriebsart [T1] befindet;

b) zum gleichen Zeitpunkt darf nur eine Bedienstation aktiv sein - lokal oder fern - (ausschließliche Bedienung von einer Bedienstation)

c) die in b) aufgeführte Steuerungsart darf die lokale Auswahl nicht überlagern und eine lokale Gefährdungssituation verursachen;

d) die Aktvierung der Funktion der manuellen Fernsteuerung darf nur von der lokalen Steuerung aus möglich sein;

e) alle Stellteilfunktionen, die eine Gefährdung verursachen können (z. B. Roboterbewegung, Beeinflussen von Ausgängen, die gefährdende Ausrüstung steuern, Veränderung von Werten, die gefahrbringenden Einfluss auf den Roboter haben, Quittierung von Sicherheitsfunktionen, Tippschaltung, usw.) dürfen nur von einer einzigen ausgewählten Bedienstation aus erfolgen können;

f) ohne eine lokale Bestätigung, dass die Änderung akzeptiert wurde und keine Gefährdung verursacht, darf es nicht möglich sein, die Parameter in Bezug auf die Begrenzung der Roboterbewegung mittels sicherheitsbewerteter Software zur Achs- und Raumbegrenzung ferngesteuert zu verändern […];

g) eine Anzeige an der lokalen Steuerung (Steuerpult, Programmierhandgerät, usw.) muss signalisieren, dass das Robotersystem ferngesteuert wird;

h) begleiteter manueller Eingriff darf nur möglich sein, wenn das Robotersystem sich in der Betriebsart „Manuell mit reduzierte Geschwindigkeit“ befindet;

i) wenn sich niemand im geschützten Bereich aufhält und die Schutzeinrichtungen aktiv sind, können die ferngesteuerten Funktionen ohne lokale Handlungen ausgeführt werden;

j) muss sich eine Person im geschützten Bereich aufhalten, dürfen Steuerungsfunktionen von einem Fernbediener, die Gefährdungen verursachen können, nur ausgeführt werden können, wenn der lokale Bediener die Funktion durch Drücken einer Zustimmungseinrichtung freigibt.

k) jegliche Ausrüstung, die für die ferngesteuerte Handlung nicht benötigt wird und eine Gefährdung verursachen könnte, muss in einem sicheren Zustand gehalten werden.

Die Benutzerinformation muss geeignete Anforderungen an die Schulung der Fernbediener und der lokalen Bediener für ferngesteuerte Aufgaben enthalten.“[32]

[32] Vgl. Norm DIN EN ISO 10218-2, 2011, S. 29–30.

3.1.2 Interpretation der Normaussagen

Die in Kapitel 3.1.1 zitierte Norm stellt eine Mindestanforderung für den Fernwartenden und den Anlagenbetreiber dar. Diese Anforderungen sollen im folgenden Kapitel, bezogen auf ein kollaboratives Robotersystem, ausgearbeitet werden.

Punkt a) sieht vor, dass sich der Roboter in der „manuellen Betriebsart“ (T1) befindet. Diese wurde für die manuelle Betätigung der Maschine einer vor Ort befindlichen Person implementiert. Eine noch in keiner Norm enthaltene Betriebsart „Fernwartung“ (wird in Kapitel 5.4 genauer erläutert), die zusätzlich definiert, welche Eingriffsmöglichkeiten bei dieser Operation erlaubt sind und welche Sicherheitsmechanismen aktiv sein müssen, würde sowohl die bestehenden Normen erfüllen als auch Safety und Security verbessern. In dieser Betriebsart könnten auch die Punkte b), c) und e) implementiert werden.

Im Punkt f) wird gefordert, dass für die Änderung der Begrenzung der Roboterbewegung eine lokale Bestätigung notwendig ist. Es setzt voraus, dass die Person vor Ort genaue Kenntnis über die Änderung hat und somit ausschließen kann, dass durch diese eine Gefährdung entsteht. Die Umsetzung gestaltet sich schwierig, denn die Person muss jeden Wert überprüfen, der geändert werden kann. Eine übersichtliche Tabelle, in der adaptierte Werte, samt Ursprungswert und Bedeutung aufgelistet sind, ist hier zu empfehlen. Des Weiteren würde eine grafische Simulation den Überblick erleichtern. In Abbildung 11 ist exemplarisch dargestellt, wie diese bildliche Aufbereitung aussehen könnte.

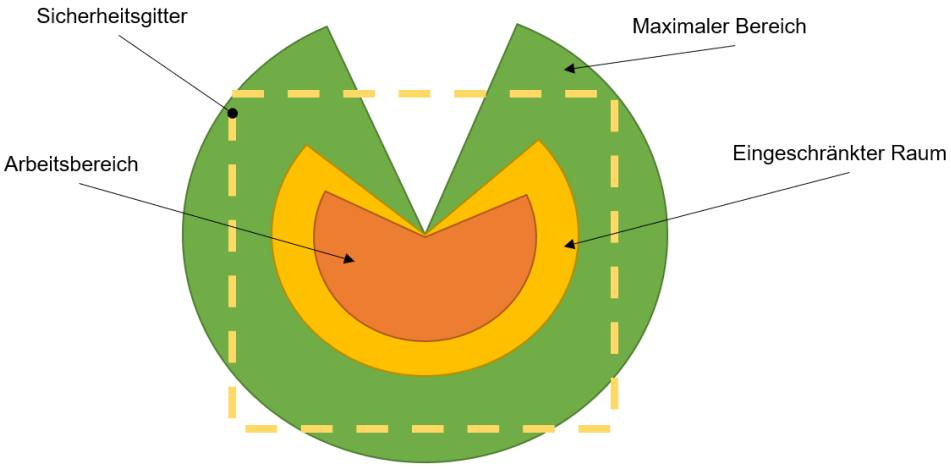

Abbildung 11: Bewegungsbereiche eines Roboters, Quelle: Malisa (2019)

In Punkt g) ist eine Anzeige gefordert, die der Person vor Ort signalisiert, dass die Maschine ferngewartet wird. Diesbezüglich ist es sinnvoll, ein einheitliches Signal auszuarbeiten, damit auch betriebsfremde Personen sofort erkennen, dass die Maschine ferngesteuert wird. Da ein rotes Signal eher auf eine Störung hinweist und dazu verleitet, sich der Maschine zu nähern, ist ein solches Leuchtsignal nicht geeignet. Alternativ könnte ein gelbes Drehlicht verwendet werden, es ist mit den vorhandenen Hardwarekomponenten am einfachsten realisierbar. Eine Beschreibung der Leuchtsignale, die direkt sichtbar an der Anlage angebracht ist, kann zum besseren Verständnis der verschiedenen Signale dienlich sein.

Punkt i) stellt ebenfalls eine Schwierigkeit in der Umsetzung dar. Die Möglichkeiten des Fernwartenden, zu überprüfen, ob sich jemand im geschützten Bereich aufhält, sind sehr begrenzt. Dieser ist hier auf Kamerasysteme oder Personen vor Ort angewiesen.

Punkt k) stellt, ähnlich wie vorher für i) beschrieben, ein Problem bei der Umsetzung dar. Es ist schwierig, für die nicht vor Ort befindliche Person sicherzustellen, dass alle Anlagen in der näheren Umgebung im sicheren Zustand sind. Auch hier ist die Bestätigung einer vor Ort anwesenden und geschulten Person notwendig.

Es wird hier bereits deutlich, dass die Umsetzung der Norm in der Praxis teilweise Schwierigkeiten bereitet. Die vorliegende Arbeit versucht als Ergebnis von Risikoanalysen und Untersuchung bereits bestehender Systeme möglichst einfache und normkonforme Lösungen zu entwickeln.

3.2 Varianten zum Verbindungsaufbau für Fernwartungszugänge

Um eine Fernwartung zu ermöglichen, wird eine Internetanbindung benötigt, über die ein Fernwartungsspezialist dann auf die Steuerung zugreifen kann. In Kapitel 2.3.2 wurde die ISDN-Verbindung bereits genannt, neuere Systeme, wie in Kapitel 3.4 noch erwähnt werden, verwenden jedoch andere Verbindungstypen, die im folgenden Kapitel genauer beschrieben werden.

Möglichkeit 1: „Engineering PC und Remote App“

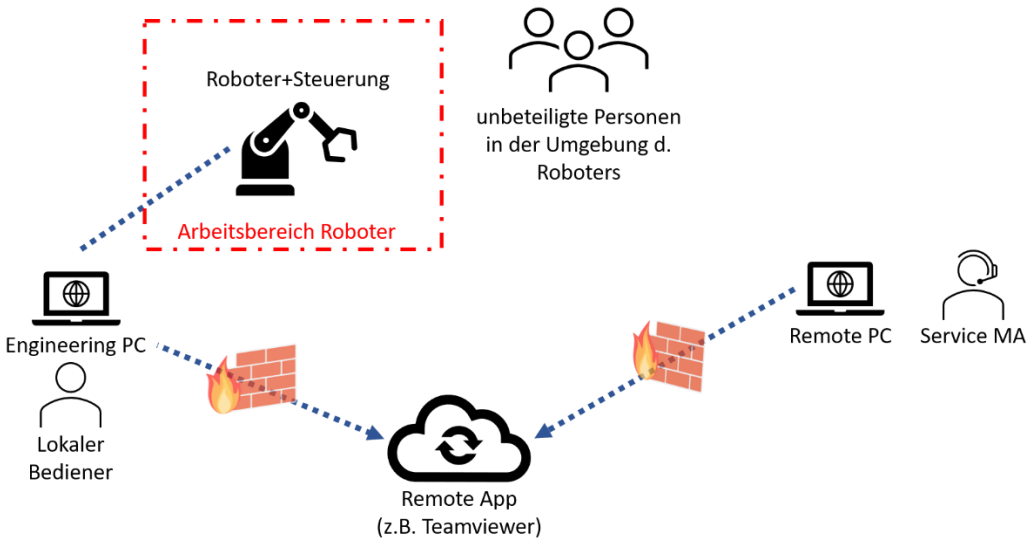

Abbildung 12: Verbindungsaufbau über Engineering PC und Remote App, Quelle: eigene Darstellung

In der in Abbildung 12 dargestellten Möglichkeit des Verbindungsaufbaus schließt ein lokaler Bediener den Engineering PC an die Robotersteuerung an. Dies kann entweder direkt via Ethernet-Kabel oder indirekt über das Firmennetzwerk geschehen. Im nächsten Schritt stellt er eine durch Firewall geschützte Verbindung zu einer Remote Anwendung, wie beispielsweise das Software-Paket „TeamViewer“ her und übergibt mittels telefonischer oder schriftlicher Bekanntgabe die Zugangsdaten einem Servicemitarbeiter, der daraufhin die Steuerung des Engineering PCs erhält.

Vorteile:

+ Einfacher Verbindungsaufbau ohne spezielle Hardware
+ Bediener vor Ort kann Handlungen am PC beobachten
+ Kostengünstig und spontan realisierbar

Nachteile:

- Daten gehen über den Server eines Drittanbieters, mit dem u.U. keine speziellen Verträge im Hinblick auf Fernwartung bestehen
- Änderungen werden im Namen der Person durchgeführt, die am Engineering PC eingeloggt ist
- Keine speziellen Autorisierungsmechanismen
- Anlage erkennt nicht, ob sie von einer Person direkt am Engineering PC oder von einem Fernwartenden gesteuert wird
- U.U. keine Reglementierung des Zugriffs möglich

Möglichkeit 2: „Service-Box und Service-Cloud“

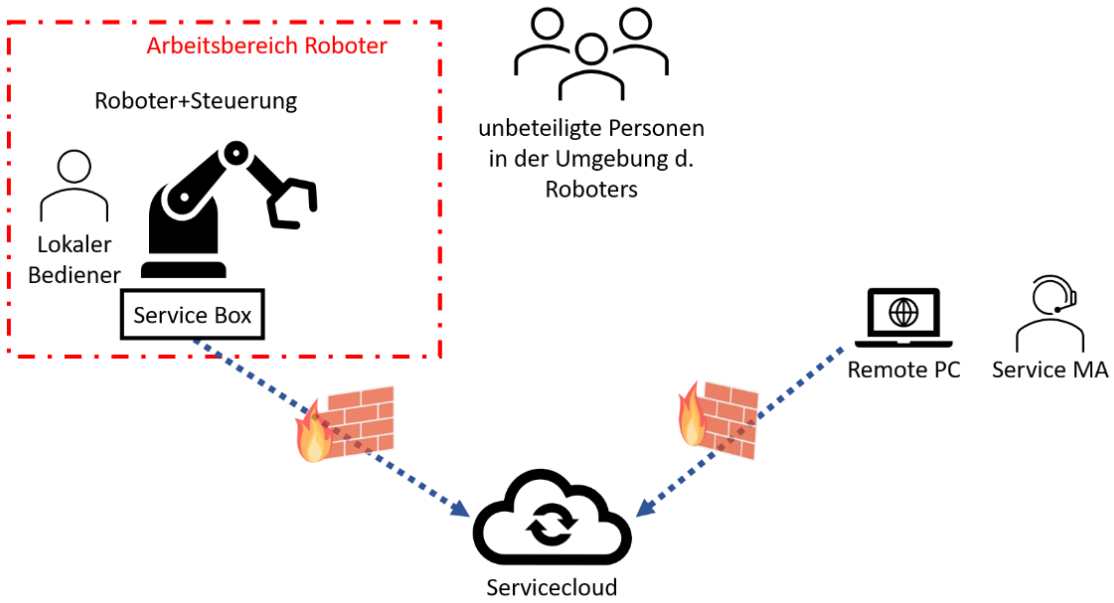

Abbildung 13: Verbindungsaufbau über Service-Box und Service-Cloud, Quelle: eigene Darstellung

Eine weitere Möglichkeit des Verbindungsaufbaus stellt die in Abbildung 13 illustrierte Architektur dar. Hierzu muss eine netzwerkfähige Service-Box in die Steuerung integriert werden, die mit einem Cloudservice verbunden wird. Im Bedarfsfall kann der Servicetechniker mit gewissen Zugangsdaten über die Service-Cloud auf die Servicebox zugreifen und erhält dann Rechte in der Robotersteuerung, welche zuvor definiert wurden.

Vorteile:

+ Verbindung erfolgt über spezielle Hard- und Software für die Fernwartung, die Safety Maßnahmen und Security Gegenmaßnahmen enthalten kann
+ Spezielle Verträge mit den Anbietern garantieren die Security
+ Service-Cloud kann im eigenen Unternehmen gehostet werden

Nachteile:

- Bei externer Service-Cloud verlassen die Daten den Betrieb
- Spezielle Hard- und Software wird benötigt
- Kein Einblick vor Ort in die Handlungen des Fernwartenden
- Ggf. laufende Kosten (Cloud als Dienstleistung)

Möglichkeit 3: „VPN-Tunnel“

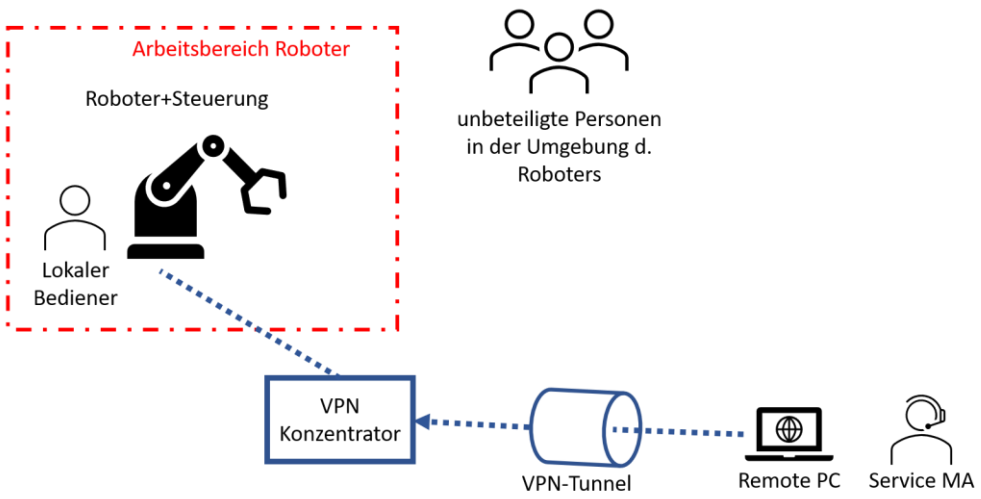

Abbildung 14: Verbindungsaufbau über einen VPN Tunnel, Quelle: eigene Darstellung

Die in Abbildung 14 dargestellte Variante zeigt den Verbindungsaufbau über einen VPN-Tunnel auf. Hierzu wird ein VPN Konzentrator benötigt, der sämtliches Regelwerk für die Einwahl und Zugriffsberechtigung enthalten kann. Der Service Mitarbeiter wählt sich mit seinen Zugangsdaten am Konzentrator ein und erhält dann Zugriff auf zuvor festgelegte Anlagen sowie deren zugehörige Steuerungen. An einem VPN Konzentrator können mehrere Maschinen angebunden sein.

Vorteile:

+ Direkte Ende-zu-Ende-Verbindung ohne Zwischenstelle
+ VPN Konzentrator kann den Zugriff reglementieren
+ Mehrere Anlagen über einen VPN Konzentrator erreichbar

Nachteile:

- Spezielle Hard- und Software wird benötigt
- Kein Einblick vor Ort in die Handlungen des Fernwartenden
- Safety und Security stark abhängig von der Konfiguration des VPN Konzentrators

3.3 Risikobeurteilung Fernwartung

In der Technik versteht man unter Risikobeurteilung die Identifikation, Analyse, Bewertung und Bewältigung technischer Risiken. Sie ist wesentlicher Bestandteil zur Erreichung der Ziele in den Bereichen Produktsicherheit und Produkthaftung, Produktimage, Arbeitnehmer-/ Umweltschutz, Anlagensicherheit und Schutz von kritischer Infrastruktur. Ziele der Risikobeurteilung sind zum einen das Erarbeiten von Maßnahmen zur Steigerung der Arbeitssicherheit, um Personenschäden zu vermeiden, zum anderen die Vermeidung von Umweltschäden und Schäden an Sachgütern, Vermeidung von Fehlern und Störfällen an Anlagen, die negative Auswirkungen auf Image und Reputation hervorrufen können, Erhöhung der Verfügbarkeit und Wirtschaftlichkeit einer Produktion sowie das Erkennen von Schwachstellen und Entwicklung von Verbesserungsmaßnahmen. Durch die Untersuchung und Dokumentation wird zudem eine Rechtssicherheit erreicht, die für alle involvierten Parteien von Vorteil ist.[33]

Eine Risikoanalyse, wie sie im IEC TR 63069 beschrieben ist, verfolgt das Ziel, durch Verringerung der Safety- und Security-Risiken die gesamte Sicherheit der Anlage zu verbessern, um die Arbeitssicherheit zu gewährleisten. Wie bereits in Kapitel 2.1.2 erwähnt, verschmelzen mit zunehmender Digitalisierung die Bereiche Safety und Security. Daher wird im Folgenden für das Beispiel Fernwartung eine Risikobeurteilung beschrieben, wie sie im IEC TR 63069 empfohlen ist.

3.3.1 Problematiken der Risikobeurteilung

Die Recherchen zur vorliegenden Arbeit haben gezeigt, dass die Risikobeurteilung gerne in eine Safety- sowie eine Security-Betrachtung unterteilt wird. Wie sich die beiden Bereiche gegenseitig beeinflussen, wird auf Grund getrennter Betrachtungsweise oftmals vernachlässigt.

Bei genauerer Untersuchung fällt auf, dass eine Security- und eine Safety-Risikoanalyse zwar Gemeinsamkeiten, wie beispielsweise die Identifikation der Risiken und der daraus resultierenden Bedrohungen und etwaigen Ausfällen hat,

[33] Vgl. Preiss, 2017, S. 12–13.

sich aber die Definition des „Risikos“ in beiden Fällen unterscheidet. Während man aus Safety-Sichtweise bei einem Risiko von der „Kombination aus der Wahrscheinlichkeit, mit der ein Schaden auftritt, und dem Ausmaß dieses Schadens“[34] spricht, bedeutet Risiko aus der Security-Betrachtung heraus die Erwartung eines Verlusts, definiert durch die Wahrscheinlichkeit, dass eine Bedrohung eine bestimmte Sicherheitslücke mit einer bestimmten Konsequenz ausnutzt.[35]

Im IEC TR 63069 wird nun erstmals eine Herangehensweise definiert, die beide Bereiche vereinen soll, indem eine sog. „Risikobeurteilung auf höherer Ebene“ durchgeführt wird. Diese kann als eine Aktivität beschrieben werden, die bei der Identifizierung und Klassifizierung der Risiken beide Bereiche berücksichtigt.[36]

3.3.2 Risikobeurteilung auf höherer Ebene

Die Idee hinter der Risikobeurteilung auf höherer Ebene ist die bereichsübergreifende Bereitstellung von Informationen, auf deren Basis die jeweiligen Risikoanalysen zunächst getrennt durchgeführt und letztendlich aufeinander abgestimmtwerden . Experten aus dem Safety- und Security-Bereich kooperieren, um potenzielle Konflikte sowie Kompatibilitätsprobleme zu identifizieren und lösen. In Abbildung 15 ist dieser Prozess aufgezeigt, der auch bereits in anderer Darstellung in Abbildung 2 ersichtlich ist. Es geht daraus hervor, dass aufgrund der unterschiedlichen Herangehensweisen beide Risikoanalysen getrennt voneinander durchgeführt werden und am Ende ein Übereinkommen der beiden Bereiche, abgestimmt auf die jeweiligen Richtlinien, getroffen wird.[37]

[34] Norm ÖVE/ÖNORM EN 61508-4, 2011, S. 10.

[35] Vgl. Norm IEC/TS 62443-1-1, 2009.

[36] Vgl. Technical Report IEC TR 63069, 2019, S. 25.

[37] Vgl. Technical Report IEC TR 63069, 2019, S. 25–26.

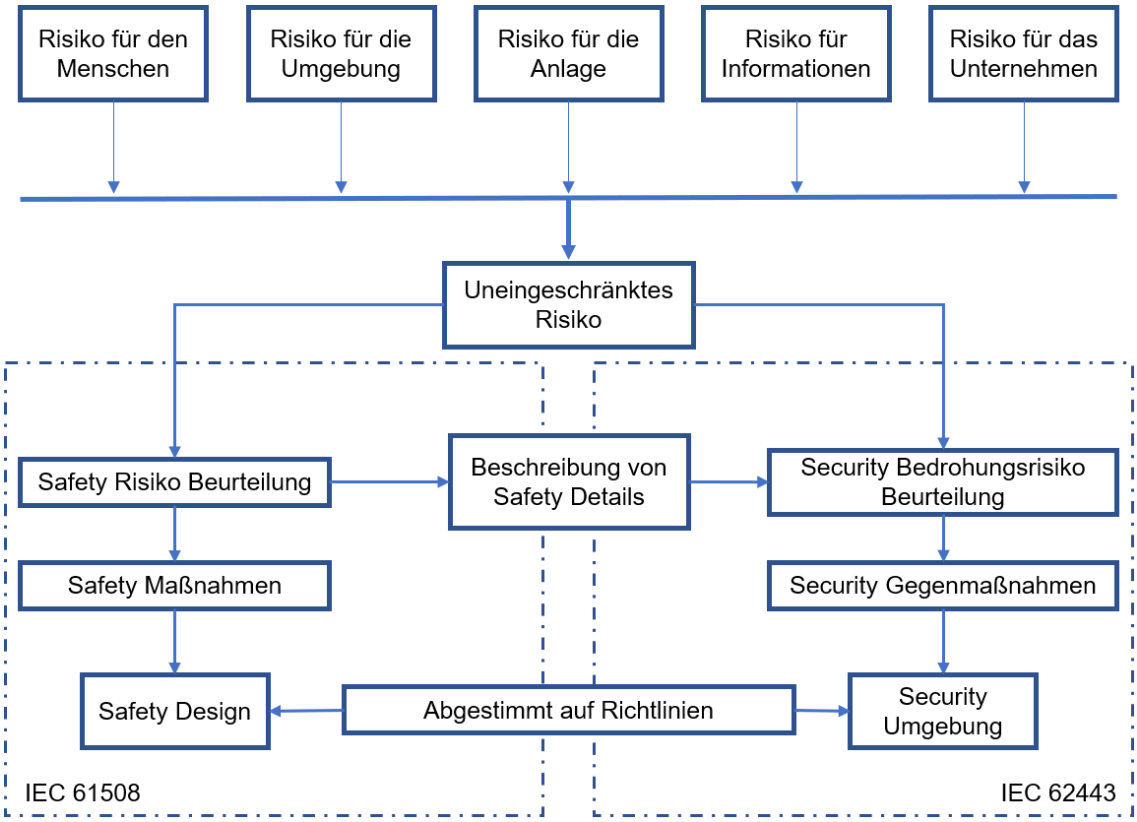

Abbildung 15: Safety- und Security-Risikoanalyse als Teil einer Risikoanalyse auf höherem Level, Quelle: IEC TR 63069 (2019), S.26

Es stellt sich die Frage, wer diese Risikoanalyse auf höherer Ebene durchzuführen hat bzw. welche Parteien bei diesem Prozess involviert sein sollten. Darüber hinaus müssen alle nötigen Informationen gesammelt und ausgewertet werden. Empfehlenswert ist hierzu z.B. die Einbeziehung externer Sicherheitsfirmen in Form eines Sicherheitsbeauftragten, der aus einer neutralen Betrachtungsweise heraus eine Expertise einbringt, die das Fachwissen der internen Mitarbeiter unter Umständen vervollständigt. Als Beispiel für einen Dienstleister im Bereich der Industrial Safety kann das international agierende Unternehmen Pilz Ges.m.b.H genannt werden, welches sich durch seine Kernkompetenz, die Sicherheit von Automatisierungstechnik, für die vorliegende Problematik empfiehlt. Eine Partei, deren Anwesenheit gemäß Maschinenrichtlinie verpflichtend ist, stellt der Systemintegrator dar, der mit einem Experten vor Ort sein muss und alle notwendigen Informationen zur Anlage bereitstellt. Der Systemintegrator ist darüber hinaus verpflichtet, sämtliche Unterlagen, die in der Risikoanalyse entstehen, aufzubewahren und im Falle einer gerichtlichen Aufforderung zur Verfügung zu stellen. Die für den Betrieb zuständigen Experten in den Bereichen Safety und

Security sind ebenfalls zwingend in den Prozess der Risikoanalyse miteinzubeziehen.

Ein für die Risikoanalyse der Anlage sehr nützliches Dokument stellt die normierte Risikobeurteilung der einzelnen Komponenten, wie beispielsweise des Roboters, dar. Diese ist von jedem Hersteller verpflichtend durchzuführen und im Falle eines Unfalls an die untersuchenden Behörden zu übermitteln, jedoch nicht Teil der Dokumentation. Daher ist ein Hersteller nicht verpflichtet, diese Risikobeurteilung an den Anlagenbetreiber auszuhändigen. Es empfiehlt sich dennoch, im Zuge einer Bestellung explizit nach dieser zu fragen, da wichtige Informationen für die Risikobeurteilung auf höherer Ebene enthalten sind.[38]

Der praktische Teil dieser Masterarbeit wurde in der smartfactory der TU Graz durchgeführt. Es handelt sich hierbei um eine universitäre Forschungsfabrik, bei der sämtliche Verantwortlichkeiten klar geregelt und den entsprechenden Bereichen zugeteilt sind. Der Zentrale Informatikdienst (ZID) betreut die IT-Infrastruktur unter Einhaltung der einheitlich an der TU Graz festgelegten Richtlinien. Die Anlagen sind Großteiles in sich homogen, d.h. Steuerung und Anlage stammen von einem Lieferanten und weisen keine größeren Altersunterschiede auf. Die Recherche im Rahmen dieser Arbeit zeigt auf, dass im Gegensatz zur smartfactory vor allem in KMUs große Mischungen aus alten und neuen Anlagen bestehen. Hier ist es besonders wichtig, die entsprechenden Experten aus Security und Safety zusammenzuführen, um einen gemeinsamen Konsens zu finden, der zu einer maximalen Gesamtsicherheit der Anlage führt.

Für den Anwendungsfall der Fernwartung soll im Folgenden eine Risikobeurteilung gemäß der zuvor beschriebenen Vorgehensweise auszugsweise durchgeführt werden, um aufzuzeigen, welche Konflikte entstehen können und wie die Kooperation der beiden Bereiche realisiert werden kann. Zunächst werden die Risiken für den Menschen sowie die Anlage anhand der Gefährdungsübersicht aus der ISO 12100 erarbeitet. Es ist an dieser Stelle zu erwähnen, dass die Gefährdungen sehr stark vom Typus und Aufbau des MRK-Systems abhängt. Daher

[38] lt. Interview V.Malisa, AUVA am 09.04.2021

werden in dieser Arbeit nur Hauptgefährdungen, die sehr allgemein gehalten sind, untersucht. Bezogen auf einen speziellen Anwendungsfall, müssen sämtliche Gefährdungen bezüglich deren Relevanz neu bewertet werden. Ein Beispiel, wie diese Bewertung durchgeführt werden kann, ist Anhang A zu entnehmen.

Die Risiken für das Unternehmen und die diesbezüglichen Informationen können den Grundgefährdungen des IT-Grundschutzkompendiums entnommen werden. Die Auflistung enthält 47 Gefährdungen, die bereits eine Betrachtung enthalten, welche der Grundwerte der Informationssicherheit Vertraulichkeit (C - Confidentiality), Integrität (I - Integrity) und Verfügbarkeit (A - Availability) durch die jeweilige Gefährdung beeinträchtigt werden. Dabei versteht man unter Vertraulichkeit, dass Informationssysteme oder Daten ausschließlich von berechtigten Personen einsehbar und somit vor unbefugter Preisgabe geschützt sind. Verfügbarkeit bedeutet, dass das IT-System zu einem gewissen Zeitpunkt oder in einem gewissen Zeitraum zur Verfügung steht. Die Vollständigkeit und Unversehrtheit der Daten sind durch den Grundwert der Integrität beschrieben. [39] Der große Vorteil einer Gefährdungsanalyse auf Basis des IT-Grundschutz besteht darin, dass dieser im Gegensatz zu ISO-Normen frei verfügbar ist. Darüber hinaus wird dieser jährlich aktualisiert und somit an die neuesten Bedrohungen angepasst. In Anhang B werden die Gefährdungen hinsichtlich der Thematik Fernwartung untersucht und festgelegt, ob die jeweilige Gefährdung direkte, indirekte oder keine Einwirkung auf das System hat. Im BSI-Standard 200-3 werden diese drei Einwirkungen wie folgt definiert:

- „ „Direkt relevant“ bedeutet hier, dass die jeweilige Gefährdung auf das betrachtete Zielobjekt einwirken kann und deshalb im Rahmen der Risikoanalyse behandelt werden muss.
- „Indirekt Relevant“ meint hier, dass die jeweilige Gefährdung zwar auf das betrachtete Zielobjekt einwirken kann, in ihrer potenziellen Wirkung aber nicht über andere (allgemeinere) Gefährdungen hinausgeht. In diesem Fall muss die jeweilige Gefährdung für dieses Zielobjekt nicht gesondert im Rahmen einer Risikoanalyse behandelt werden.

[39] Vgl. Burgdorf, 2014, S. 310.

- „Nicht relevant“ heißt hier, dass die jeweilige Gefährdung nicht auf das betrachtete Zielobjekt im Rahmen der Risikoanalyse einwirken kann und deshalb für dieses Zielobjekt im Rahmen der Risikoanalyse nicht behandelt werden muss.“[40]

3.3.3 Zusammenhang von Sicherheitslevels

Wie bereits erwähnt, besitzen die Bereiche Safety und Security unterschiedliche Herangehensweisen, um eine Aussage über die Sicherheit einer Anlage zu erhalten. Beide Bereiche verfügen über Einteilungen, sogenannte Levels, in denen das jeweilige Schutzniveau definiert werden soll. Zwischen dem Sicherheits-Integritätslevel (SIL) aus dem Safety-Bereich und dem Security-Level (SL) aus dem Security-Bereich besteht kein unmittelbarer oder direkter Zusammenhang. Die Einteilung in die fünf Security-Levels SL 0 – SL 4 gemäß IEC 62443 erfolgt im Hinblick auf den Schutz gegen zufälligen oder absichtlichen Missbrauch unter Berücksichtigung der verwendeten Mittel, des Aufwands, der Fertigkeiten und der Motivation des Angreifers.[41] Das Sicherheits-Integritätslevel gemäß IEC 61508 mit den Werten SIL 1 – SIL 4 beruht auf einem numerisch definierten Ausfallgrenzwert, der abhängig von der Anforderungsrate der Sicherheitsfunktion, entweder die „Wahrscheinlichkeit eines gefahrbringenden Ausfalls bei Anforderung der Sicherheitsfunktion“ oder die „Häufigkeit eines gefahrbringenden Ausfalls der Sicherheitsfunktion“[42] beschreibt.

Da bei einer Risikobeurteilung auf höherer Ebene Parteien aus dem Safety- und Security-Bereich zusammen an einem Projekt arbeiten, muss eine einheitliche Sprache gewählt werden, die den IT-Spezialisten genau verstehen lässt, wie gefährlich ein potenzielles Safety Risiko zu bewerten ist. Gleiches gilt für den umgekehrten Fall, Safety Spezialist und Security Risiko. Die einfachste Möglichkeit ist hierbei die Verwendung einer von Rot nach Grün verlaufenden Farbskala. In diese Skala müssen die jeweiligen Risiken durch die zugehörigen Spezialisten eingestuft werden. Basierend auf dieser Zuordnung sollten im weiteren Verlauf

[40] BSI-Standard 200-3, 2017, S. 16.

[41] Vgl. Norm OVE EN IEC 62443-3-3, 2020, S. 78–79.

[42] Norm ÖVE/ÖNORM EN 61508-1, 2011, S. 36.

auch die entsprechenden Levels gewählt werden. Da alle involvierten Parteien unterschiedliche Interessen vertreten, sollte die Festlegung der nötigen Levels beider Bereiche in wechselseitiger Abstimmung aller Beteiligten erfolgen. Das Beispiel einer Drehzahlregulierung für die Spindel einer Drehmaschine verdeutlicht zuvor beschriebenes. Im Normalfall nimmt der Arbeiter vor Ort im Fehlerfall sofort auffällige Geräusche wahr und stoppt die Anlage manuell. Die Safety-Steuerung könnte daher theoretisch mit einem Wert SIL 2 - SIL 3 ausgestattet werden. Wird die Anlage an einen Fernwartungszugang angebunden, so lässt sich über eine Manipulation der Drehzahl schwerer Schaden an Maschine und Umgebung hervorrufen. Daher sollte hier den Maximalwert von SIL 4 erreicht werden.

3.3.4 Bewertung der Security-Risiken

Bei Betrachtung der in Kapitel 3.3.2 ausgearbeiteten Risiken fällt die Zuteilung in die Bereiche vermeintlich leicht. Die Risiken werden auf die beiden Bereiche verteilt, die jeweiligen Risikoanalysen getrennt voneinander durchgeführt, dabei entwickelte Maßnahmen und Gegenmaßnahmen abgeglichen und auf eine gegenseitige Einflussnahme geprüft.

Doch auch im IEC TR 63069 fehlt die Einteilung der Security Risiken unter Berücksichtigung der Safety. Abbildung 16 zeigt die beispielhafte Einteilung der Risiken in eine Matrix nach BSI-Standard 200-3, die sowohl die Eintrittshäufigkeit als auch die Schadenshöhe enthält. Für die Analyse der Security Risiken unter Berücksichtigung des Einflusses auf die Safety bietet sich an, die horizontale Achse durch die Beeinträchtigungsmöglichkeit von Safety-Komponenten zu ersetzen, wie es in Abbildung 17 dargestellt ist. Um die Gefährdungen richtig einzuteilen, sollten diese in beide Matrizen eingeordnet werden. Die endgültige Zuordnung in die jeweilige Risikokategorie sollte dann nach dem Maximumprinzip erfolgen.

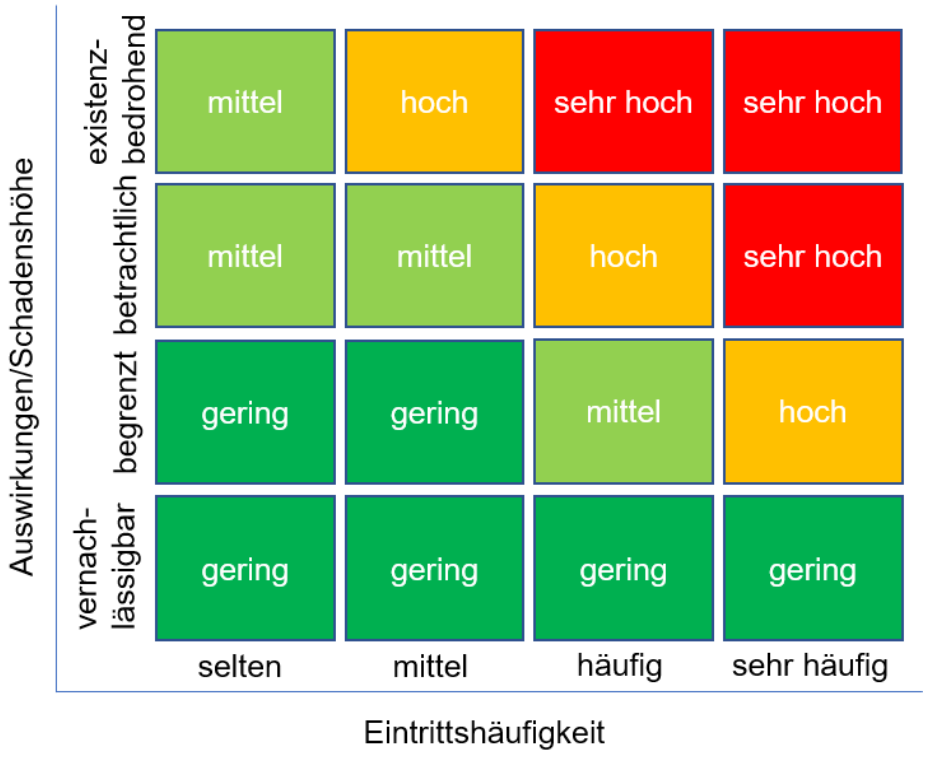

Abbildung 16: Matrix zur Einstufung von Risiken, Quelle: Bundesamt für Sicherheit in der Informationstechnik (2017), S.27

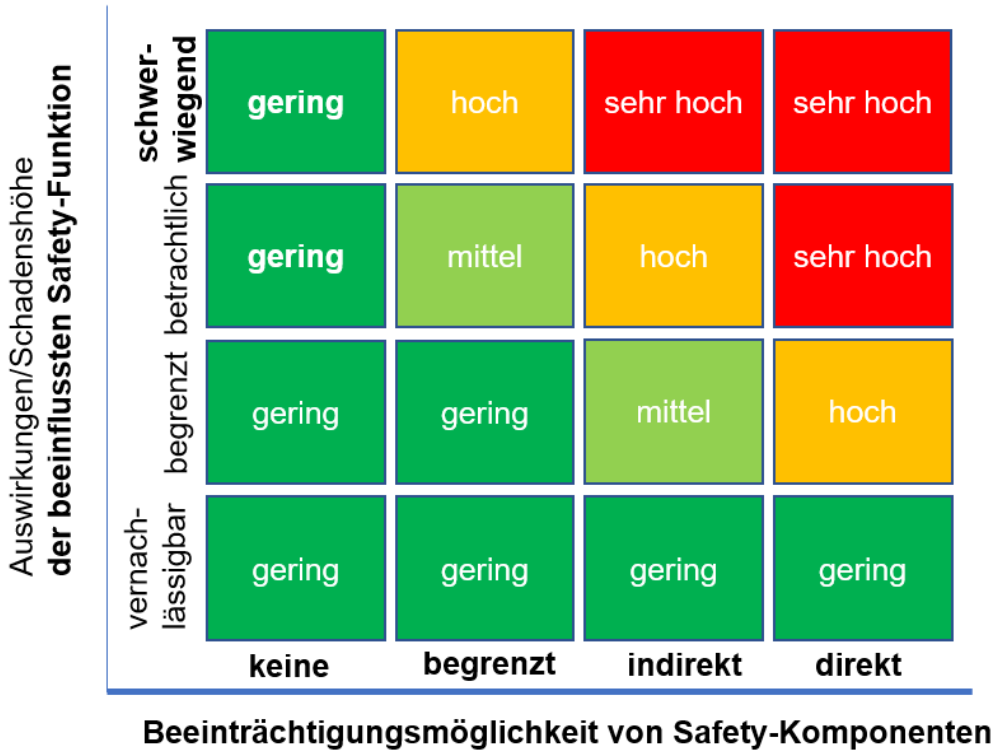

Abbildung 17: Matrix zur Einstufung von Risiken mit Safety-Berücksichtigung, **FETT** *zeigt die Änderungen zu Abbildung 16, Quelle: eigene Darstellung*

Während die Definitionen für die Eintrittshäufigkeit und Auswirkungen aus Abbildung 16 im BSI-Standard 200-3 definiert sind, muss die Definition für die beiden Achsen aus Abbildung 17 festgelegt werden. Tabelle 1 liefert einen Vorschlag, wie diese Definition aussehen könnte, um die entsprechenden Einteilungen abzugrenzen. Darüber hinaus muss eine Festlegung der Einteilung der Auswirkungen der beeinflussten Safety-Funktionen getroffen werden. Tabelle 2 enthält einen Vorschlag, wie diese Festlegung ausgeführt sein könnte. Anhang C zeigt, wie die Einteilung der Gefährdungen anhand der erarbeiteten Matrizen und Tabellen im Falle der Fernwartung aussehen könnte.

Tabelle 1: Definition der Beeinträchtigungsmöglichkeiten

Beeinträchtigungsmöglichkeiten von Safety-Komponenten	
keine	Durch die Gefährdung ist kein Zugriff auf Safety-Komponenten möglich
begrenzt	Durch die Gefährdung ist ein begrenzter Zugriff auf Safety-Komponenten möglich. Die Komponenten können erreicht werden, sind aber nochmals geschützt (z.B. Passwort)
indirekt	Durch die Gefährdung ist ein indirekter Zugriff auf Safety-Funktionen möglich, diese können geändert werden, aber ein zusätzlicher Mechanismus muss die Änderungen bestätigen.
direkt	Durch die Gefährdung besteht voller Zugriff auf Safety-Funktionen sofern nicht weitere Mechanismen vorgesehen sind.

Tabelle 2: Definition der Auswirkung/Schadenshöhe

Auswirkung/Schadenshöhe der beeinträchtigten Safety-Funktion	
vernachlässigbar	Geringste Materielle Schäden im Bereich bis maximal 10 €
begrenzt	Materielle Schäden bis maximal 100 €, kurzer Stopp der Anlage, keine große Reparatur notwendig
beträchtlich	Materielle, hochpreisige Schäden, die längere Ausfallzeiten und Reparaturen zur Folge haben
schwerwiegend	Irreparable hohe materielle Schäden oder gar Personenschäden

Das Ergebnis dieser Bewertung soll unter anderem eine Aussage sein, welche Komponenten einen besonderen Schutz während der Fernwartung erfordern. Es kann sich dabei um spezielle Hard- oder Softwarekomponenten, aber auch um Daten oder Anwenderprogramme handeln. Im zu behandelnden Fall handelt es sich beispielsweise bei der Hardware um das Endgerät, das die Fernwartung durchführt, z.B. ein Notebook, das Programm und die beteiligte Hardware zum Verbindungsaufbau sowie die Steuerung selbst.

3.3.5 Risikobeurteilung im Security-Bereich

Die Risikoanalyse des Security-Bereichs sollte gemäß IEC TR 63069, wie in Abbildung 15 dargestellt, nach der IEC 62443 ausgeführt werden. Da der bereits erwähnte BSI-Standard 200-3 eine sehr gute und vor allem frei verfügbare Alternative repräsentiert, wird in der vorliegenden Arbeit diese Risikoanalyse gemäß des BSI durchgeführt. Die einzelnen Schritte dazu sind in Abbildung 18 illustriert.

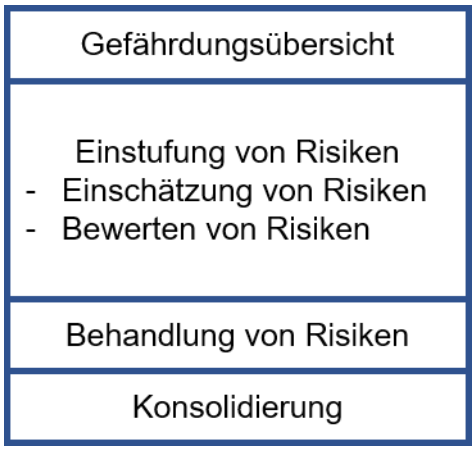

Abbildung 18: Schritte in der Security-Risikoanalyse, Quelle: BSI (2017), S.7

Die ersten beiden Schritte „Gefährdungsübersicht“ sowie „Einstufung von Risiken“ wurden bereits in den vorangegangenen Kapiteln durchgeführt. Das folgende Kapitel befasst sich daher mit der Behandlung der Risiken und der abschließenden Konsolidierung. Daher werden zunächst entsprechende Risikobehandlungsoptionen ausgewählt, die laut BSI 200-3 wie folgt aussehen könnten:

- Vermeidung des Risikos durch Ausschluss der Risikoursache
- Reduktion des Risikos durch Modifikation der Rahmenbedingungen, welche für die Risikoeinstufung verantwortlich sind.
- Transfer des Risikos (z.B. Outsourcing oder Abschluss einer entsprechenden Versicherung)
- Akzeptanz eines gewissen Restrisikos[43]

[43] Vgl. BSI-Standard 200-3, 2017, S. 34–36.

Abgesehen von den Risiken, welche in Anhang C als gering eingestuft wurden, muss diese Einteilung für alle restlichen Risiken durchgeführt werden. In Anhang D sind exemplarisch Maßnahmen aus dem IT-Grundschutz Kompendium für die Gefährdungen, welche als mittel, hoch oder sehr hoch eingestuft wurden, aufgelistet. Diese Maßnahmen stellen nur einen Auszug aus allen zu treffenden Maßnahmen dar, die im Zuge der Implementierung einer IT-Infrastruktur ergriffen werden sollten. Die für die Fernwartung wichtigsten Aspekte werden in Kapitel 4.2.3 beschrieben.

Den Abschluss des in Abbildung 18 dargestellten Prozesses bildet die Konsolidierung des Sicherheitskonzepts. Bezogen auf das Gesamtsystem muss die Eignung, das Zusammenwirken, die Benutzerfreundlichkeit sowie die Angemessenheit der Maßnahmen überprüft werden, bevor diese in das System integriert werden. Entsprechende Hilfestellung liefert auch hier der BSI Standard 200-3.[44]

[44] Vgl. BSI-Standard 200-3, 2017, S. 39–40.

3.3.6 Risikobeurteilung im Safety-Bereich

In der Norm ISO 12100 wird die Risikobeurteilung als iterativer Prozess betrachtet, der aus den Teilbereichen Risikoanalyse, Risikobewertung und der Kontrolle, ob das Risiko minimiert wurde, besteht. Der Bereich Risikoanalyse beinhaltet die Festlegung der Grenzen der Maschine, die Identifizierung der Gefährdungen und die Risikoeinschätzung.[45] Im folgenden Kapitel sollen Auszüge einer Risikoanalyse für die in Abbildung 19 dargestellte kollaborative Roboteranwendung, in der smartfactory@tugraz, die wesentlichen Sicherheitsmaßnahmen für die Fernwartung dieser Anlagen herausarbeiten.

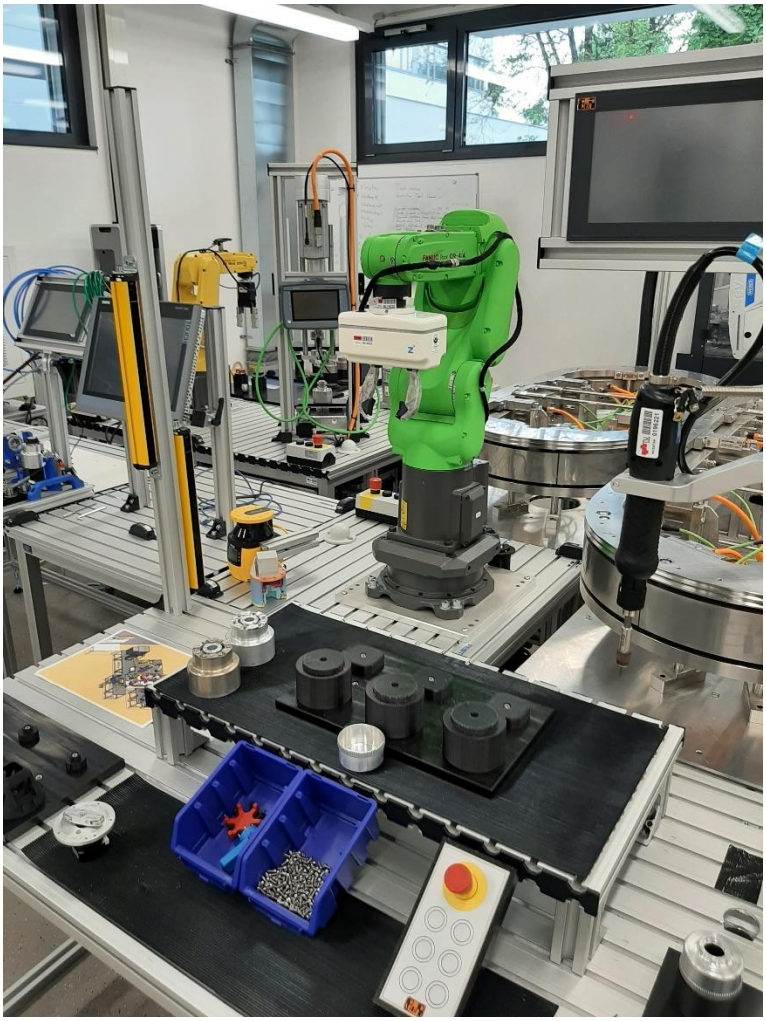

Abbildung 19: Kollaborative Roboteranwendung in der smartfactory@tugraz, Quelle: eigene Aufnahme

[45] Vgl. Norm DIN EN ISO 12100:2011-03, 2011.

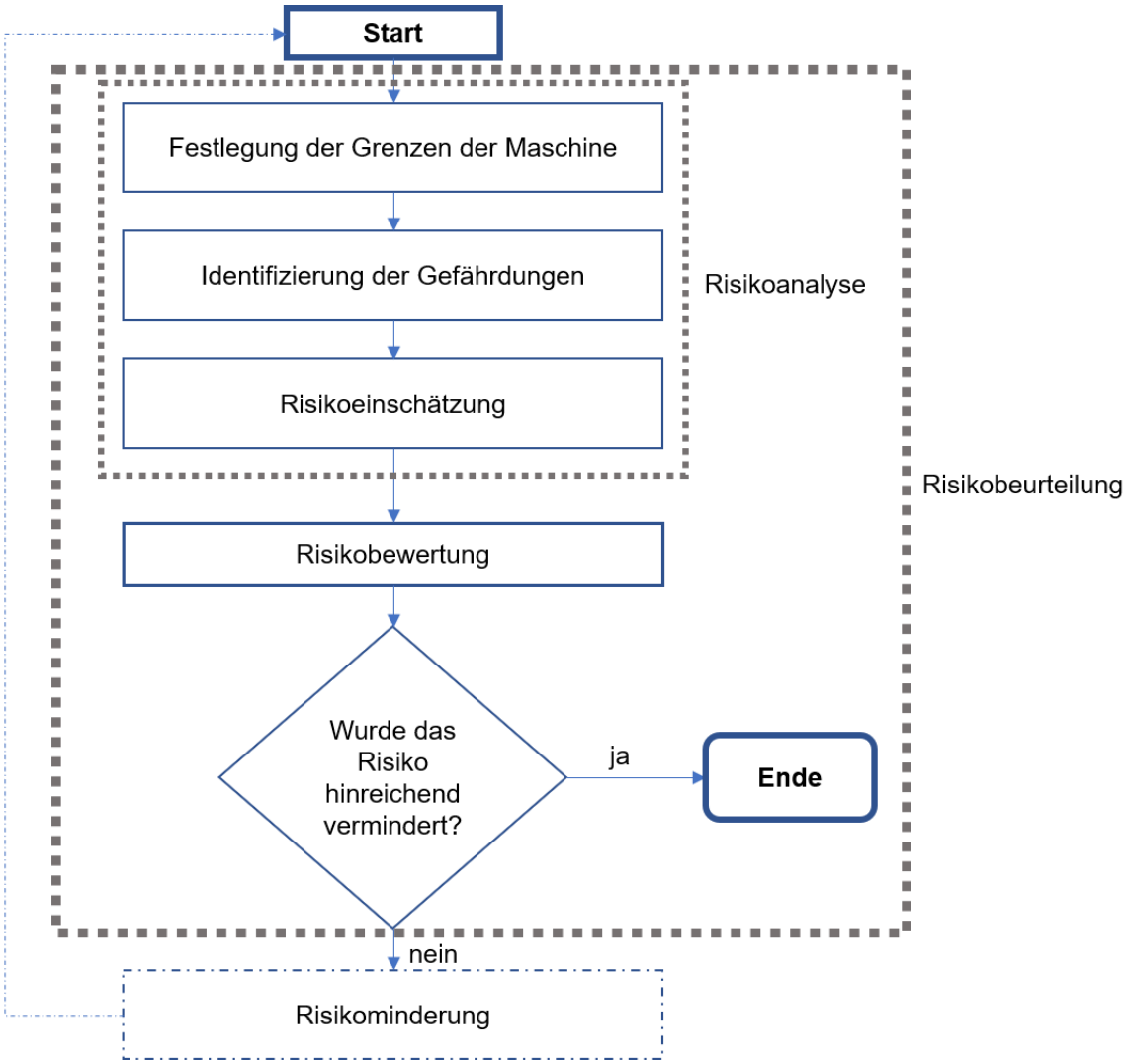

Abbildung 20: Iterativer Prozess der Risikobeurteilung. Quelle: DIN EN ISO 12100:2011-03 (2011)

Festlegung der Grenzen der Maschine

Zunächst werden für den Anwendungsfall der Fernwartung die Grenzen der Maschine festgelegt. Im ISO/TR 14121-2 wird als Ziel dieses Schrittes definiert, dass eine „anschauliche Beschreibung der mechanischen und physikalischen Eigenschaften, der Funktionsfähigkeit der Maschine, deren bestimmungsgemäße Verwendung und vernünftigerweise vorhersehbare Fehlanwendung sowie die Art der Umgebung, in der sie wahrscheinlich verwendet und gewartet wird“[46], existiert. Genau darin besteht auch eine der Schwierigkeiten der Risikobeurteilung von Anlagen mit Fernwartungszugängen. Laut Experten erweitert sich die Grenze der Anlage auf den Arbeitsplatz des Fernwartenden, was in der Analyse berücksichtigt werden sollte.[47]

In Abbildung 21 ist der Arbeits- bzw. Kollaborationsbereich der untersuchten Anlage dargestellt. Das größte Gefährdungspotenzial für Personen in der direkten Umgebung im Rahmen einer Fernwartung birgt dabei der Kollaborationsbereich. Die beiden Bereiche sind durch Lichtschranken getrennt, die den Roboter zum Stillstand bringen, wenn eine Person in den Arbeitsbereich eingreift. Im Kollaborationsbereich ist eine Kraft- und Momentenbegrenzung aktiv, zusätzlich bewegt sich der Roboter in diesem Bereich mit deutlich reduzierter Geschwindigkeit.

[46] Technical Report DIN ISO/TR 14121-2, 2013, S. 8.

[47] lt. Jonas Stein, Institut für Arbeitsschutz der DGUV (IFA), Webinar „Fernwartung von Industriesteuerungen“ am 08.03.2021

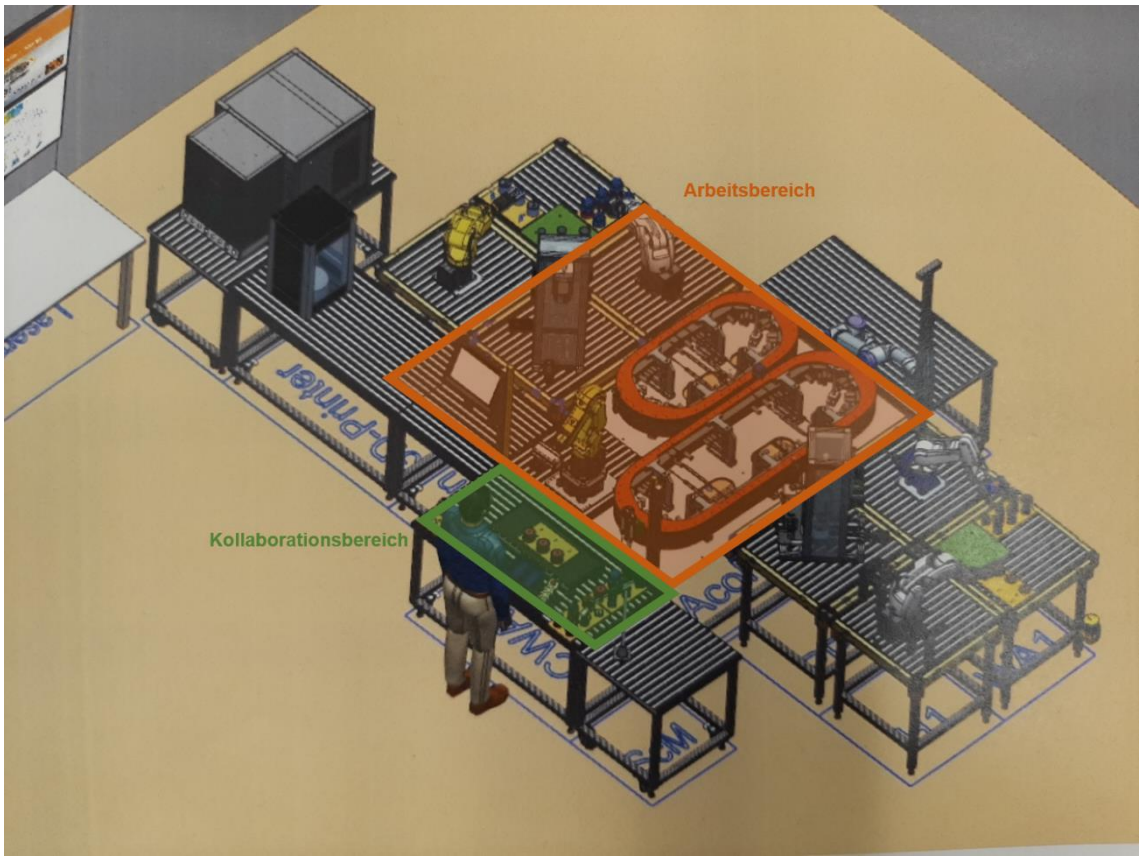

Abbildung 21: Kollaborations- und Arbeitsbereich der untersuchten Roboteranwendung, Quelle: smartfactory@tugraz

Tabelle 3: Beschreibung der Maschine

Beschreibung des Arbeitssystems
Bei dem Arbeitssystem handelt es sich um eine kollaborative Roboteranwendung, bestehend aus einem kollaborativen Roboter, der den Anforderungen der Normen ISO 10218-1 und ISO/TS 15066 entspricht und in eine Systemumgebung installiert ist, die der Norm ISO 10218-2 folgt. Im Zuge einer Fernwartung greift eine externe Person, welche sich nicht vor Ort befindet, mit Hilfe eines anwesenden Anlagenbedieners auf die Anlage über eine Kommunikationseinrichtung zu und erhält die Kontrolle über das gesamte System. Im Regelbetrieb besitzt der Roboter einen Greifer, mit dem Bauteile von einer Fördereinrichtung genommen und in den Kollaborationsraum übergeben

werden. Der Arbeiter fügt ein weiteres Bauteil hinzu und verschraubt es mit einem elektrischen Schrauber. Anschließend legt der Roboter das fertig verschraubte Bauteil an einer fest definierten Position ab.

Tabelle 4: Festlegung der Verwendungsgrenzen

Verwendungsgrenzen – **Bestimmungsgemäße Verwendung und vorhersehbare Fehlanwendung**
Die Anlage wurde einmalig installiert und im Rahmen einer Risikobeurteilung für den Regelbetrieb bewertet. Dabei sind Prozessparameter, technische Daten sowie Produkte festgelegt, die ohne eine erneute Risikoanalyse nicht geändert werden dürfen. Im Zuge der Fernwartung ist also zu beachten, welche Änderungen zulässig sind, ohne dass eine erneute Risikobeurteilung erforderlich ist. Die nachstehende Risikobeurteilung befasst sich nur mit dem Prozess der Fernwartung. Sämtliche weitere Lebensphasen, wie Betrieb/Produktion, Entsorgung, Reinigung sind nicht enthalten. a) Betriebsarten Im Regelbetrieb befindet sich die Anlage im „Automatikbetrieb“, ist im Zuge von Wartungs- oder Programmierarbeiten das Eingreifen einer Bedienperson erforderlich, so kann die Maschine in den „Manuellen Betrieb“ überführt werden, bei dem die Prozessschritte manuell getätigt werden müssen. Bei der Fernwartung muss sichergestellt sein, dass sich die Anlage im manuellen Betriebsmodus befindet und damit die Geschwindigkeit reduziert ist.

b) Einsatzbereich

Die Anlage steht in einer industriellen Umgebung und ist ausschließlich für den festgelegten Anwendungsfall bestimmt.

c) Qualifikation des Bedienpersonals sowie weiterer Personen, die den Gefährdungen im Zusammenhang mit der Anlage ausgesetzt sein können

Alle bei der Fernwartung involvierten Personen müssen eine entsprechende Ausbildung und Qualifikation vorweisen können. Zudem ist nachzuweisen, dass diese die Bedienungsanleitung der Anlage sowie die Fernwartungsvereinbarung gelesen und verstanden haben. Nicht zuletzt müssen sie mit dem Prozessablauf vertraut sein.

Alle beteiligten Personen müssen eine Einschulung erhalten und alle Personen im Umfeld auf die Fernwartung hingewiesen werden.

Tabelle 5: Räumliche Grenzen

Räumliche Grenzen
a) Bewegungsraum Der Bewegungsraum bei der Fernwartung kann von dem des Regelbetriebs stark abweichen. b) Platzbedarf für Personen, die mit der Maschine umgehen Für alle beteiligten Personen ist eine freie, unverstellte Fläche im Abstand von mind. 1 m von allen zugänglichen Seiten der Anlage sicherzustellen, um ein Ausweichen jederzeit zu ermöglichen. c) Mensch-Maschine-Schnittstellen Die Schnittstellen sollten durch Taster und visuelle Signale (z.B. Warnleuchte) realisiert sein. Während der Fernwartung kann ein direkter Kontakt zwischen Roboter und Bediener erforderlich sein.

Tabelle 6: Zeitliche Grenzen

Zeitliche Grenzen
Die Fernwartungswerkzeuge sollten während des gesamten Lebenszyklus der Anlage auf dem aktuellsten Stand gehalten werden. Dies bedeutet vor allem regelmäßige Updates für Soft- und Hardwareprodukte.

Identifizierung der Gefährdungen

Den nächsten Schritt bildet die Identifikation der Gefährdungen. Das Ergebnis sollte aus einer Liste von Gefährdungen, Gefährdungssituationen und Gefährdungsereignissen bestehen, die Aufschluss darüber gibt, wann eine Gefährdungssituation zu welchem Ausmaß eines Schadens führen kann.[48] Eine detaillierte Auflistung zu den Gefährdungen im Zusammenhang mit einer Fernwartung gemäß ISO TR 14121-2 ist aus Anhang E ersichtlich.

Tabelle 7: Eingreifen von Personen während der Fernwartung

Eingreifen von Personen während der Fernwartung
Es kann erforderlich sein, dass der Bediener durch händischen Eingriff im Zuge der Fernwartung Verklemmungen lösen, kleine Reparaturen wie z.B. Nachziehen von Schraubverbindungen, unter Anleitung des Fernwartenden, Handführung des Roboters oder Einstellungen im Gefährdungsbereich vornehmen muss. Bei Neustart der Anlage, der Inbetriebnahme nach Abschluss der Fernwartung und dem Aufbau der Verbindung ist ebenfalls ein Eingreifen vor Ort erforderlich. Der Gefährdungsbereich ist durch den kompletten maximalen Arbeitsbereich des ferngewarteten Roboters definiert.

[48] Vgl. Technical Report DIN ISO/TR 14121-2, 2013, S. 9.

Tabelle 8: Mögliche Betriebszustände der Anlage

Mögliche Betriebszustände der Anlage
a) Normalbetrieb der Fernwartung Die bei der Anlage befindliche Person steht an einem sicheren Ort in der Nähe der Anlage, hat das Teachpendant in der Hand und kann darauf die Handlungen des Fernwartenden verfolgen. Zusätzlich kann parallel eine telefonische Verbindung zum Servicetechniker bestehen, der durch Anweisungen den Anlagenbediener anleiten kann, um händische Eingriffe vorzunehmen. b) Fehlerfall Bemerkt der Anlagenbediener Auffälligkeiten, die durch die Fernwartung entstanden sind, oder gerät die Anlage außer Kontrolle muss dieser unverzüglich in der Lage sein, die Anlage stillzusetzen, beispielsweise durch das Betätigen eines Not-Aus-Tasters. Im Anschluss ist die Anlage neu zu starten und mittels Backups in den Zustand vor der Fernwartung zu überführen.

Tabelle 9: Möglichkeiten von Fehlverhalten oder -anwendung

Mögliche unbeabsichtigte Aktionen der Bedienperson
• Eine Person reagiert reflexartig auf eine Fehlfunktion oder Bewegung, die während der Fernwartung ausgeführt wird, beispielsweise das Entfernen von Hindernissen, auf die sich der Roboter zubewegt, um eine Kollision zu vermeiden • Verhalten von nicht beteiligten Personen, z.B. das Eintreten einer Person in den Arbeitsbereich des Roboters ohne Kenntnis über die Gefahrensituation der Fernsteuerung zu haben. • Verhalten, das durch Unachtsamkeit oder Konzentrationsmangel entsteht, beispielsweise falsche Eingabe von Parametern. Diese können um Zehnerpotenzen vom gewollten Wert abweichen.

Risikoeinschätzung

Den dritten Schritt der Risikoanalyse bildet die Risikoeinschätzung. Dazu wird im Folgenden das Verfahren mittels Risikograph gemäß ISO TR 14121-2 gewählt. Ziel ist es, einen Risikoindex, basierend auf die Risikoelemente Schadensausmaß, Häufigkeit und/oder Dauer der Gefährdungsexposition, Eintrittswahrscheinlichkeit eines Gefährdungsereignisses sowie Möglichkeit zur Vermeidung oder Minderung des Schadens, zu ermitteln.[49]

[49] Vgl. Technical Report DIN ISO/TR 14121-2, 2013, S. 17–18.

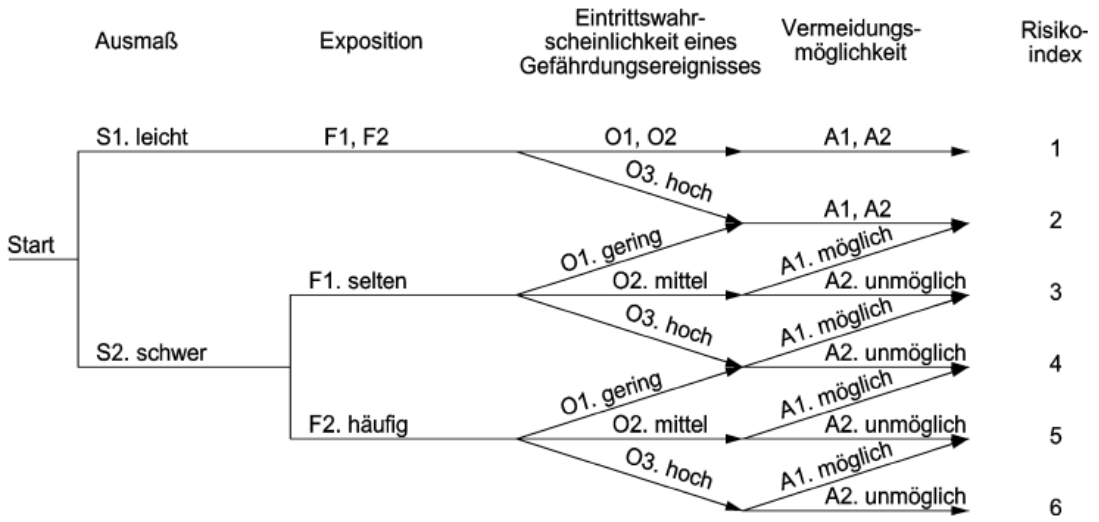

Abbildung 22: Risikograph zur Ermittlung des Risikoindex, Quelle: Technical Report DIN ISO/TR 14121-2 (2013), S.19

Abbildung 22 illustriert das zuvor angesprochene Verfahren zur Ermittlung des Risikoindex. Eine genaue Beschreibung der Kriterien ist der Norm ISO TR 14121-2 zu entnehmen. Der Risikograph liefert Anhaltswerte für die Vergabe der Indizes der einzelnen Kriterien, mit dessen Hilfe die Risikobewertung durchgeführt wird. Diese bemisst, inwiefern für gewisse Gefährdungssituationen eine Risikominderung erforderlich ist und ob die gewählten Maßnahmen zur Risikoreduzierung keine weiteren Gefährdungen oder Erhöhungen anderer Risiken hervorruft. [50] Die endgültige Risikominderung wird damit erreicht, dass festgelegt wird, wer dafür verantwortlich ist und wann die Maßnahmen, welche in den vorherigen Schritten erarbeitet wurden, realisiert werden. Bis zur Umsetzung der geplanten Maßnahmen darf die Anlage nicht in Betrieb genommen werden.

Anhang F zeigt exemplarisch für die zuvor beschriebene Anlage, wie die erarbeiteten Schritte tabellarisch durchgeführt werden könnten. Es ist an dieser Stelle wichtig zu erwähnen, dass die vorliegende Risikobeurteilung als Hilfestellung dient, um in Kapitel 4 Maßnahmen zur sicheren Fernwartung genauer zu beschreiben. Bezogen auf eine spezifische Anlage ist es unabdinglich, dass eine Bewertung von entsprechendem Fachpersonal (z.B. Pilz GmbH, TÜV, u.v.m.) durchgeführt wird. Als Beispiel kann hier eine Schweißapplikation genannt

[50] Vgl. Technical Report DIN ISO/TR 14121-2, 2013, S. 26.

werden, die eine gänzlich andere und auch sehr hohe Gefährdungssituation darstellt. Hier haben Schweißparameter einen sehr großen Einfluss auf die Qualität des Ergebnisses und vor allem auf die Safety, sodass eine Erreichbarkeit dieser Parameter aus dem Netzwerk nicht empfehlenswert, wenn nicht sogar fahrlässig ist. Dieses Beispiel verdeutlicht, warum es sich bei der zuvor durchgeführten Risikoanalyse nur um ein Muster handelt, das als Hilfestellung herangezogen aber nie deckungsgleich verwendet werden kann.

3.4 Beispiele für Fernwartungssysteme

In Kapitel 3.1 wurde bereits erwähnt, wie laut Norm ISO 10218-2 prinzipiell ein Fernzugriff auf Robotersysteme durchzuführen ist. In diesem Kapitel werden verschiedene Handhabungen von Fernwartungsabläufen vorgestellt, die entweder direkt vom Roboter- und Steuerungshersteller, vom Systemintegrator oder von Drittanbietern durchgeführt werden.

3.4.1 System ABB

ABB, ein Schweizer Konzern für Automatisierungstechnik, bietet Remote Access (Fernzugriff) im Rahmen des Connected Services Pakets an. Dieses umfasst neben der bereits angesprochenen Möglichkeit des Fernzugriffs auch noch Condition Monitoring und Diagnostics (Zustandsüberwachung und Diagnose), Backup-Management, Fleet Assessment (Beurteilung des Roboterbestands) und Asset Optimization (Systemoptimierung).[51]

In neuen Steuerungen ist bereits eine Möglichkeit zur Anbindung an das Netzwerk enthalten, bei älteren Anlagen kann das Connected Service Kit nachträglich installiert werden. Mittels WLAN-, 3G- oder Ethernet-Schnittstelle gelangt die Service-Box ins Internet. Wie in Abbildung 23 dargestellt, wird über das Internet ein VPN Tunnel zum Remote Server hergestellt, auf dem die Software für die Datenauswertung installiert ist. Da der Fernzugriff nicht nur Datenfluss von der Steuerung zum Server (outbound) sondern auch umgekehrt (inbound) erfordert,

[51] Vgl. ABB, 2021.

muss im Falle einer Fernwartung mittels physischen Schlüsselschalter an der Robotersteuerung ebendiese Inbound-Kommunikation zugelassen werden. Für die Fernwartung greift ABB auf das Tool eines Drittanbieters (Talk2M von eWON) zurück.[52]

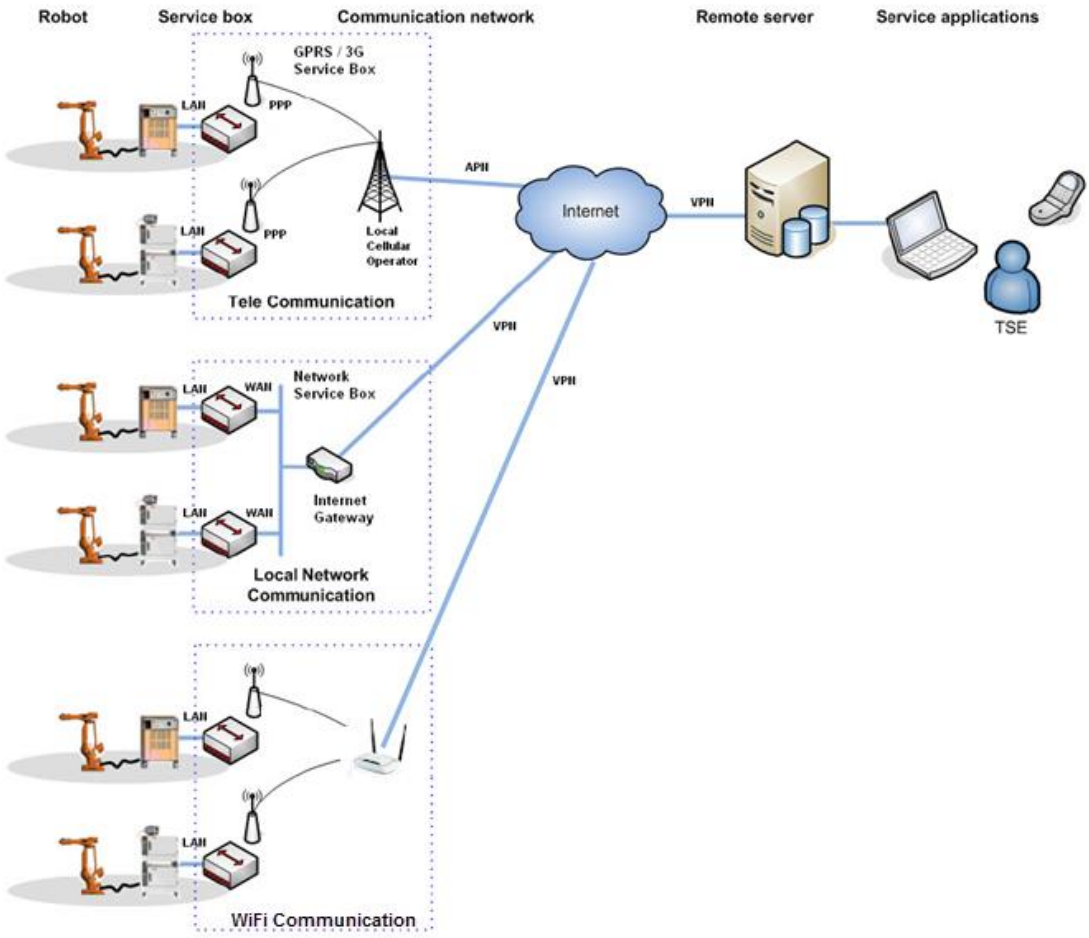

Abbildung 23: Übersicht der Verbindungsmöglichkeiten der ABB Service Box, Quelle: ABB (2017)

Der Service Talk2M besteht aus dem eCatcher Tool, das auf dem Laptop des Fernwartenden (z.B. ABB Servicetechniker) installiert ist. Abbildung 24 illustriert, dass auch die Servicebox der Steuerung mit der Cloud verbunden ist und die Verwaltung des Fernzugriffs über eine Web Browser Applikation stattfindet. Die Cloud ermöglicht eine volle Zugriffskontrolle, bei der der Roboterbetreiber bestimmten Usern, für einen festgelegten Zeitraum bestimmte Rechte erteilen kann. Eine Zwei-Faktor-Identifikation stellt sicher, dass es sich um die richtige Person

[52] Vgl. ABB, 2017, S. 85.

handelt, die einen Zugriff auf die Steuerung erhält. Die Personen, die Uhrzeit und die Dauer des Zugriffs werden mit Hilfe des Tools „Audit trail“ automatisch mitgeloggt. [53]

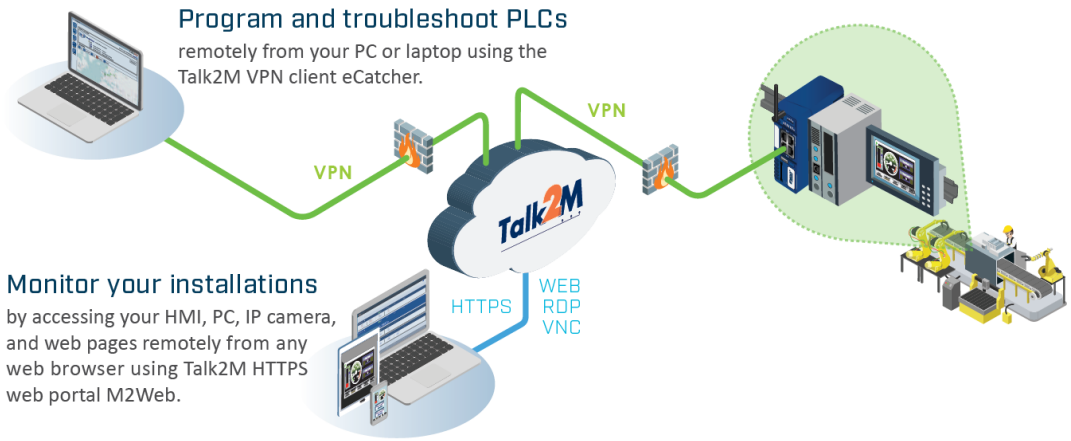

Abbildung 24: Überblick Verbindungsaufbau Talk2M, Quelle: Ewon (2020), Onlinequelle [03.02.2021]

Die zusätzlich benötigte Software („RobotStudio“), um Eingriffe an der Steuerung vornehmen zu können, erlaubt keine Deaktivierung von Sicherheitsvorkehrungen und soll so eine ausreichende Betriebssicherheit während der Fernwartung gewährleisten. Ein Überblick des erwähnten Ablaufs ist in Abbildung 25 ersichtlich. Mit Stand Juli 2020 greifen deutschlandweit lediglich 3-4 Kunden auf das Fernwartungstool von ABB zurück.[54]

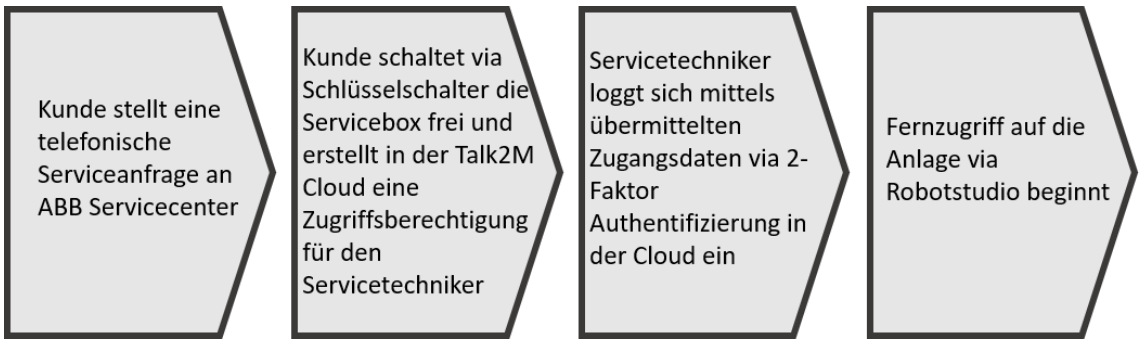

Abbildung 25: Ablauf des Beginns einer Fernwartung bei ABB

[53] Vgl. Ewon, 2020, S. 4.

[54] lt. Telefonat M. Burret, ABB am 28.07.2020

Vorteile:

+ Speziell auf die Steuerung abgestimmte Hardware
+ Ermöglicht Betriebsdatenerfassung
+ Starke Authentifizierungsmechanismen in der Talk2M Cloud
+ Automatisches Logging mittels „Audit trail“
+ Physischer Schlüsselschalter an der Steuerung erlaubt jederzeit die Verbindung zu beenden

Nachteile:

- Spezielle Software und Lizenzen werden benötigt
- Fernwartender hat keinen Überblick, ob sich Personen im Gefahrenbereich befinden
- Daten gehen über Server außerhalb des Unternehmens
- Vor Ort kein Einblick in die Aktivitäten des Fernwartenden

3.4.2 System Fanuc

Fanuc bietet mit seiner Software „iPendant Controls“ die Möglichkeit, mittels eines Windows Rechners auf die Robotersteuerung zuzugreifen. Dazu wird zunächst die Software auf einem Engineering PC installiert, welcher im weiteren Verlauf mittels Ethernet Kabel mit der Steuerung verbunden wird. Über einen Webbrowser (in diesem Fall Internet Explorer) kann die IP-Adresse des Roboters aufgerufen werden, daraufhin öffnet sich eine in Abbildung 26 dargestellte Weboberfläche. Dieses Interface ermöglicht es dem Bediener des Engineering PCs, gewisse Remote-Funktionen auszuführen. Das Tool „Monitor iPendant (ECHO)“ ermöglicht ein reines Spiegeln der Benutzeroberfläche des Bedienpanels. Es ist dabei keine Möglichkeit zur Steuerung via Engineering PC vorgesehen. Mit der Erweiterung „Jogging iPendant“ (ITP) kann der Roboter zur Gänze ferngesteuert werden, auch ein Verfahren der Roboterachsen ist möglich. Dazu muss sich dieser im Automatikmodus befinden, wodurch sichergestellt wird, dass alle Safety-

Funktionen, die im normalen Betrieb die Sicherheit gewährleisten sollen, aktiv sind.

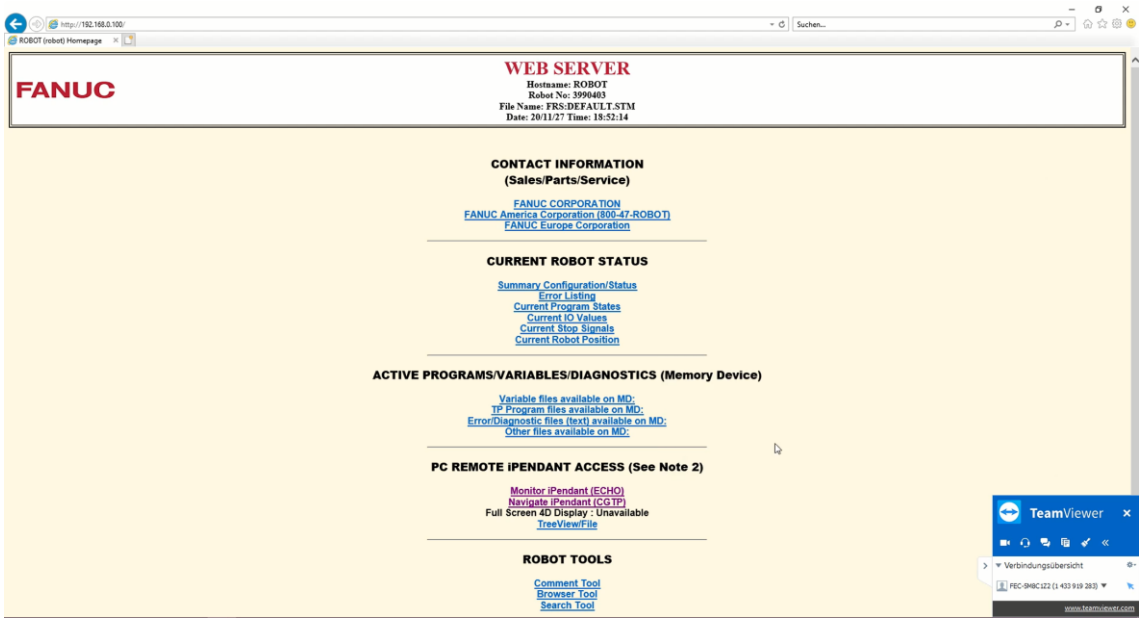

Abbildung 26: Weboberfläche FANUC iPendant Controls, Quelle: Screenshot (27.11.2020)

Im Rahmen dieser Arbeit wurde ein Testlauf durchgeführt, bei dem die Funktion „Navigate iPendant“ (CGTP) verwendet wurde. Diese erlaubt einen begrenzten Zugriff auf die Robotersteuerung und ist somit auch für Fernwartungen geeignet, da für gewisse Systemeingriffe vor Ort am Bedienpanel Bestätigungen erforderlich sind. Sämtliche im folgenden Abschnitt erwähnten Aspekte beziehen sich auf diese „Navigate iPendant“ Funktion.

Die zuvor genannten Funktionen erfordern, wie bereits erwähnt, eine direkte Verbindung per Ethernet Kabel vom Engineering PC zur Robotersteuerung. Um eine Fernwartung durchführen zu können, ist also noch eine Remote Verbindung des nicht vor Ort befindlichen Servicetechnikers auf den Engineering PC nötig. Im Rahmen dieses Testlaufs wurde hierzu der „TeamViewer“ gewählt. In Kapitel 3.2 werden die Möglichkeiten des Verbindungsaufbaus genauer erläutert.

Hat der Servicetechniker Zugriff auf den Engineering PC, kann er in der vorliegenden Konfiguration dieselben Tätigkeiten durchführen, als wäre er vor Ort. Beispielsweise kann im Fehlerfall der Fehlerspeicher ausgelesen und somit der Zustand des Roboters überprüft werden. Bei Bedarf können unter anderem

Registereinträge angepasst werden, die, falls sie im Programmablauf enthalten sind, diesen auch verändern können. Auch in der Sicherheitssteuerung können Adaptionen vorgenommen werden, jedoch erfordern alle sicherheitsrelevanten Änderungen einen Neustart, der vor Ort durchzuführen ist. Eine weitere Möglichkeit stellt der sogenannte „Background Modus“ dar, welcher ebenfalls über den Engineering PC aufgerufen werden kann. In diesem Modus ist es erlaubt, sowohl beim stehenden als auch beim arbeitenden Roboter Programme und Parameter zu verändern. Diese Änderungen werden nach einer Bestätigung in die laufenden Programme übernommen. Der für dieser Arbeit interviewte Servicetechniker rät aber von der Verwendung dieser Funktion im Rahmen einer Fernwartung ab. Das Starten von Programmen, Systemupdates, Deaktivieren von Sicherheitseinrichtungen (z.B. Lichtschranke) sowie das Durchführen eines Neustarts über den Engineering PC sind nicht möglich.

Ein wesentliches Element zur Gewährleistung der funktionalen Sicherheit stellt der DCS-Code zur Aktivierung dar. Nach dem Hochfahren des Roboters muss dieser mittels zuvor genannten Codes aktiviert werden, bevor ein Arbeiten möglich ist. Danach folgt eine Sicherheitsabfrage, bei der bestätigt werden muss, dass sowohl das richtige Werkzeug montiert ist, als auch eine visuelle Überprüfung stattgefunden hat, die bestätigt, dass sich niemand im Arbeitsbereich des Roboters befindet. Im Falle der Fernwartung muss zum einen dem Servicetechniker oder der Person vor Ort dieser Code bekannt sein, zum anderen muss sich der Servicetechniker auf den Mitarbeiter vor Ort verlassen können, um die Sicherheitsüberprüfung zu bestätigen.

Fanuc bietet in der Robotersteuerung eine Nutzerverwaltung an, die jedoch im Auslieferungszustand nicht aktiviert ist. Es empfiehlt sich generell, diese zu verwenden, besonders wichtig ist dies, wenn mehrere Personen, auch über Fernwartung Zugriff auf den Roboter haben. Es können Nutzerrollen, wie Operator, Programmer, Maintenance Technician, aber auch eigene Benutzerprofile angelegt werden. Diese passwortgeschützten Rollen haben unterschiedliche Zugriffsrechte und sollen sicherstellen, dass Bediener nur solche Änderungen durchführen können, für die sie auch ausgebildet sind.

Um den Zustand vor der Fernwartung zu konservieren, empfiehlt es sich ein Backup zu erstellen. Dies geschieht bei Fanuc per USB-Stick an der Steuerung. Nach Abschluss der Fernwartung kann ein weiteres Backup erstellt werden, dessen Differenz zum Backup vor der Fernwartung als Dokumentation dient. Darüber hinaus wird damit der Neuzustand dokumentiert.

Vorteile:

+ Keine spezielle Hardware nötig.
+ Software kann direkt vom Hersteller bezogen werden.
+ Überwachungsmöglichkeit vor Ort durch Kontrolle des Bildschirms und Dokumentationsmöglichkeit durch Bildschirmaufzeichnung.
+ DCS Code stellt zusätzliche Sicherheitsbarriere dar.
+ Sicherheitsrelevante Änderungen erfordern Neustart, der nur vor Ort durchführbar ist.
+ Nutzerverwaltung ermöglicht genaue Kontrolle, welcher Person welche Berechtigungen erteilt werden.

Nachteile:

- Änderungen in der Steuerung werden der Person zugeordnet, die am Engineering PC eingeloggt ist.
- Authentifizierung basiert auf persönlichem Vertrauen.
- Daten gehen über Server außerhalb des Unternehmens.
- TeamViewer stellt in vielen Firmennetzwerken ein IT-Risiko dar und muss richtig konfiguriert werden (siehe Kap. 4.2.14.1).
- „iPendant“ wird nur in Kombination mit einer Remote-Desktop-Applikation zu einem Fernwartungstool und ist daher nicht speziell für Fernzugriffe ausgelegt. Welche Änderungen verantwortbar sind, obliegt der Einschätzung des Fernwartenden.

3.4.3 System Fronius[55]

Das österreichische Unternehmen Fronius hat seinen Hauptsitz in Wels und ist in den Sparten Schweißtechnik, Solarenergie und Batterieladegeräte vertreten. Die neuesten Entwicklungen in den Bereichen Schweißtechnik und Automation greifen auch auf kollaborative Roboter zurück, da sich diese durch eine sehr einfache Programmierbarkeit auszeichnen. Der Betrieb der Schweißroboter ist aber nicht kollaborativ, da die zum Schweißen notwendigen Sicherheitsvorkehrungen einen kollaborativen Betrieb nicht zulassen, dennoch können aus diesem Beispiel wichtige Aspekte für Fernwartungen von MRK-Systemen herausgearbeitet werden. Für seine Kunden bietet Fronius die komplette Integration sowie den fortlaufenden Service der Anlage an. Bereits 2010 wurde entschlossen (in Kooperation mit „INSYS“) einen Router in jede ausgelieferte Anlage zu integrieren, der die Fernwartung ermöglicht. Der Ablauf einer Fernwartung bei Fronius wurde bereits in Kapitel 2.3.3 erörtert. Nachfolgend soll nur ein kurzer Überblick über die Verbindungsstruktur gegeben werden.

Abbildung 27 illustriert mit den Nummern von 1 - 6 die benötigten Schritte zum Verbindungsaufbau. Nachdem eine autorisierte Person den Schlüsselschalter aktiviert (1), führt der Router ein Dial-Out über das Kundennetz aus (2). Der VPN-Server, welcher bei Fronius stationiert ist, prüft das Zertifikat sowie den Schlüssel (3) und baut anschließend einen VPN-Tunnel auf (4). Sobald dieser Tunnel erfolgreich hergestellt wurde, sendet der Router automatisch eine E-Mailbenachrichtigung an einen Servicetechniker (5), der dann mit dem Zugriff beginnen kann (6). Die wichtigsten Komponenten sind der zuvor angesprochene Router in der Kundenanlage, der von „INSYS“ zur Verfügung gestellt wird, eine Internetanbindung, der VPN-Server bei Fronius sowie ein Remote-Techniker mit seinem Endgerät. Der Router kann via Mobilfunk, Intranet oder auch ISDN eine Verbindung herstellen. Das Modem kann so konfiguriert werden, dass es einen Zugriff auf Geräte im Anlagennetzwerk, FTP Servern zum Datenaustausch und Leitstandsrechnern ermöglicht. Der Fernwartende führt keine Änderungen durch, die eine erneute Risikoanalyse der Anlage zur Folge hätten, wie beispielsweise Eingriffe

[55] lt. Telefonat M. Mayr, Fronius am 18.02.2021

in die Sicherheitssteuerung. Ist dies notwendig, muss ein Servicetechniker von Fronius vor Ort sein.

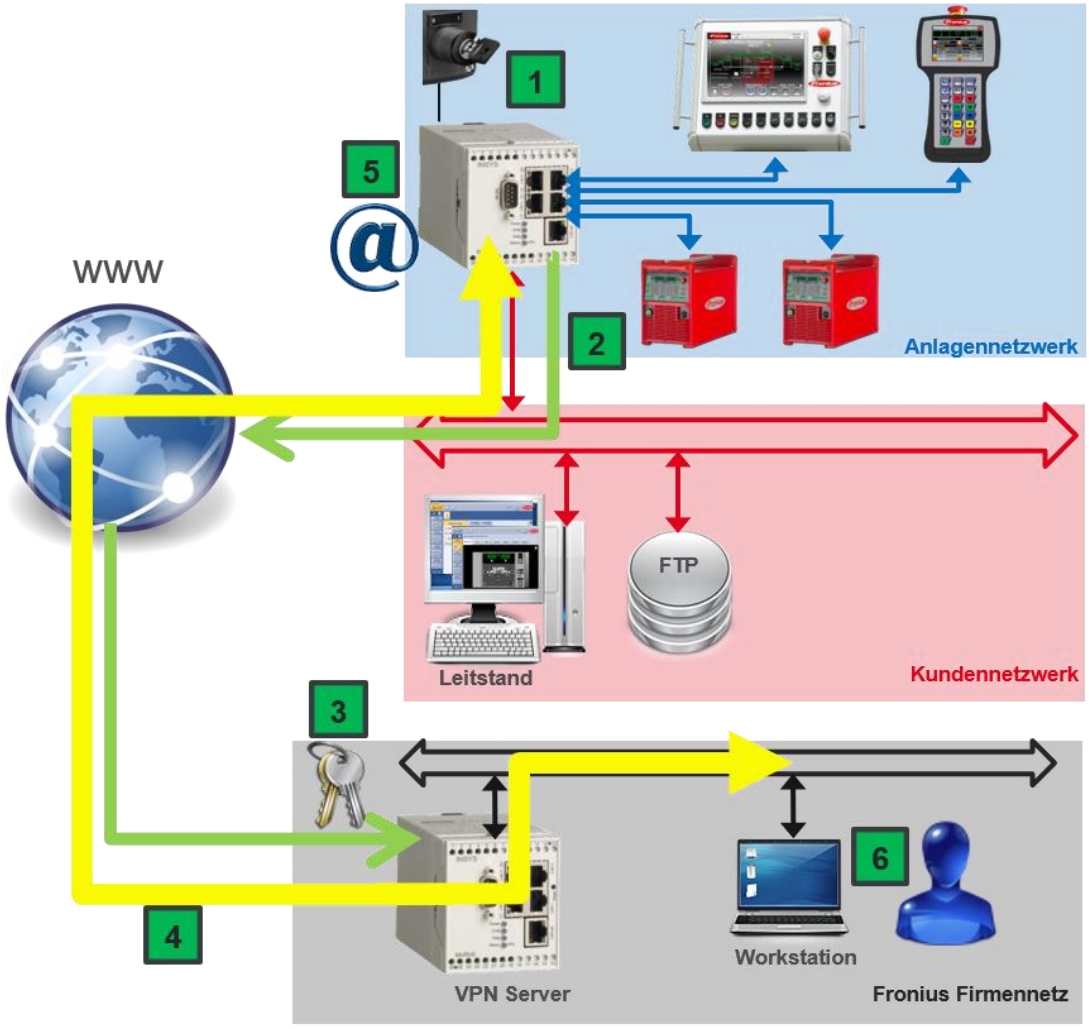

Abbildung 27: Verbindungsstruktur Fernwartung Fronius, Quelle: interne Unterlagen Fronius, Mayr Martin (2021)

Rechtlich sichert sich Fronius mit einer Fernwartungsvereinbarung ab, die vom Kunden unterzeichnet werden muss. Darin wird dem Anlagenbetreiber die Verantwortung vor Ort übertragen, solange Vorsatz bzw. grobe Fahrlässigkeit des Servicetechnikers ausgeschlossen werden kann. Ein Vertrag garantiert, dass von Seiten Fronius nur fachkundige und autorisierte Mitarbeiter Fernwartungszugriff erhalten. Die Dokumentationspflicht obliegt dem Kunden, der nach Abschluss der Fernwartung schriftlich an den Servicetechniker berichten muss. Im Fehlerfall liegt permanent eine Backupdatei des zuletzt freigegebenen Datenstandes bei Fronius vor, der jederzeit wieder auf die Anlage überspielt werden kann. Nach

Beendigung der Fernwartung muss die Anlage in die Grundstellung gefahren und der Schlüsselschalter in die Ausgangsposition gestellt werden, um den Regelbetrieb wieder aufzunehmen.

Hinsichtlich der von Fronius gebotenen Gesamtlösung verschafft sich das Unternehmen einen Vorteil gegenüber vergleichbaren Anbietern, von dem die Kunden aus der Security-Sichtweise profitieren. Der Schlüsselschalter, der nur eine einmalige, terminierte Verbindung herstellt und der VPN-Tunnel erlauben nahezu keinen Missbrauch. Aus Safety-Sicht muss der Bediener vor Ort auf seine Sicherheit und die der Umgebung achten. Spezielle Mechanismen, die dies gewährleisten, sind nicht vorhanden.

Vorteile:

+ Hardware ist bei Kauf der Steuerung bereits integriert.
+ Support direkt vom Systemintegrator.
+ Server ist bei Systemintegrator lokalisiert.
+ Schlüsselschalter stellt einmalig eine Verbindung her, selbst wenn dieser permanent im Fernwartungsmodus bleibt.
+ Update und Backup werden via Fernwartung ermöglicht.
+ Fernwartungs- und Onlineverträge schaffen eine gegenseitige vertragliche Absicherung.

Nachteile:

- Arbeitssicherheit der Personen vor Ort hängt vom Bediener vor Ort ab.
- Authentifizierung basiert auf persönlichem Vertrauen.
- Noch keine Betriebsdatenerfassung möglich.
- Keine eigenständigen Fernzugriffe innerhalb des Unternehmens möglich.

3.4.4 System Robotiq

Robotiq ist ein Privatunternehmen aus Kanada, das 2008 gegründet wurde und im Bereich der industriellen Automatisierung tätig ist. Die Spezialgebiete sind Greifer, Kraft-Momenten-Sensoren sowie das Monitoring von kollaborativen Robotern. Die Produkte sind mit den Robotern der Hersteller Aubo, Doosan Robotics, Hanwha, Omron TM, Techman Robot, Universal Robots und Yaskawa kompatibel.[56]

Das angebotene Softwarepaket „Insights“ beinhaltet unter anderem die Möglichkeit der Betriebsdatenerfassung und des Fernzugriffs. Es ist nur mit den Robotern UR3, UR5 und UR10 des Herstellers Universal Robots kompatibel. Über ein IIot Gerät wird der Roboter an den „Insights cloud service“ angebunden, über den die Kommunikation mit dem Anwender stattfindet. Die Verbindungstopografie ist in Abbildung 28 dargestellt. Im Regelbetrieb erlaubt das IIoT Gerät nur Outbound-Kommunikation, das heißt, es werden alle eingehenden Datenströme blockiert. Für die Fernwartung kann eine zeitlich begrenzte und verschlüsselte Verbindung aufgebaut werden, die auch eingehenden Datenverkehr erlaubt.[57]

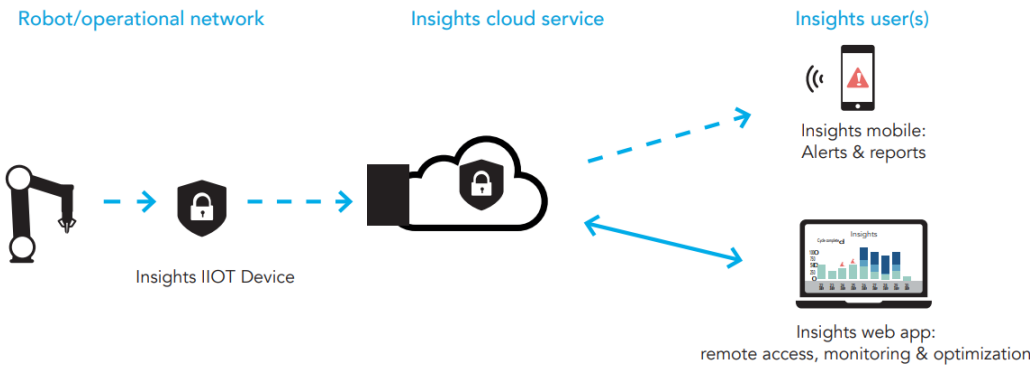

Abbildung 28: Topografie Netzwerkverbindung Robotiq, Quelle: Robotiq (2019), Onlinequelle [17.02.2021]

Der gewünschte Roboter muss zunächst mit einem Insights Account verknüpft werden, der auch die Benutzerverwaltung beinhaltet. Es gibt zwei Möglichkeiten des Fernzugriffs. Entweder der Inhaber des Accounts greift selbst auf den

[56] Vgl. Robotiq, 2021.

[57] Vgl. Robotiq, 2019, S. 1–2.

Roboter zu oder er übergibt einem weiteren Insights Nutzer die entsprechenden Berechtigungen. Über die Webapplikation wird ein Programm heruntergeladen, das auf einen USB-Stick transferiert werden muss. Dieser USB-Stick wird in weiterer Folge mit dem Teach-Pendant verbunden. Auf dem Pendant öffnet sich in weiterer Folge ein Remote Fenster, das einen Code generiert, welcher in der Benutzeroberfläche des Fernwartenden eingegeben werden muss. Der Fernwartende hat nun alle Funktionen und Möglichkeiten, die der Bediener vor Ort auch hätte inklusive Bewegung der Roboterachsen sowie Änderungen in Programmabläufen. Die Software beinhaltet die Möglichkeit, mehrere Webcams anzubinden, um so dem Fernwartenden eine visuelle Kontrolle der Roboterumgebung zu ermöglichen. Bei dem Softwarepaket handelt es sich um ein Lizenzprodukt, das jährlich zu bezahlen ist. Robotiq selbst führt nahezu keine Fernzugriffe durch. Das Ziel von „Insights“ ist es, Systemintegratoren ein Tool zur Verfügung zu stellen, das es ihnen ermöglicht, bei Bedarf auf die Anlagen ihrer Kunden zugreifen zu können.[58]

Abbildung 29 zeigt die Weboberfläche von „Insights“, aus der Sicht des Fernwartenden. Auf dem rechten Fensterabschnitt sind die Kamerabilder ersichtlich und auf dem linken Abschnitt das gespiegelte Teach-Pendant, auf dem das Fenster für den Fernzugriff noch geöffnet ist.

[58] lt. Interview P.Guerin, Applikationsingenieur bei Robotiq am 15.02.2021

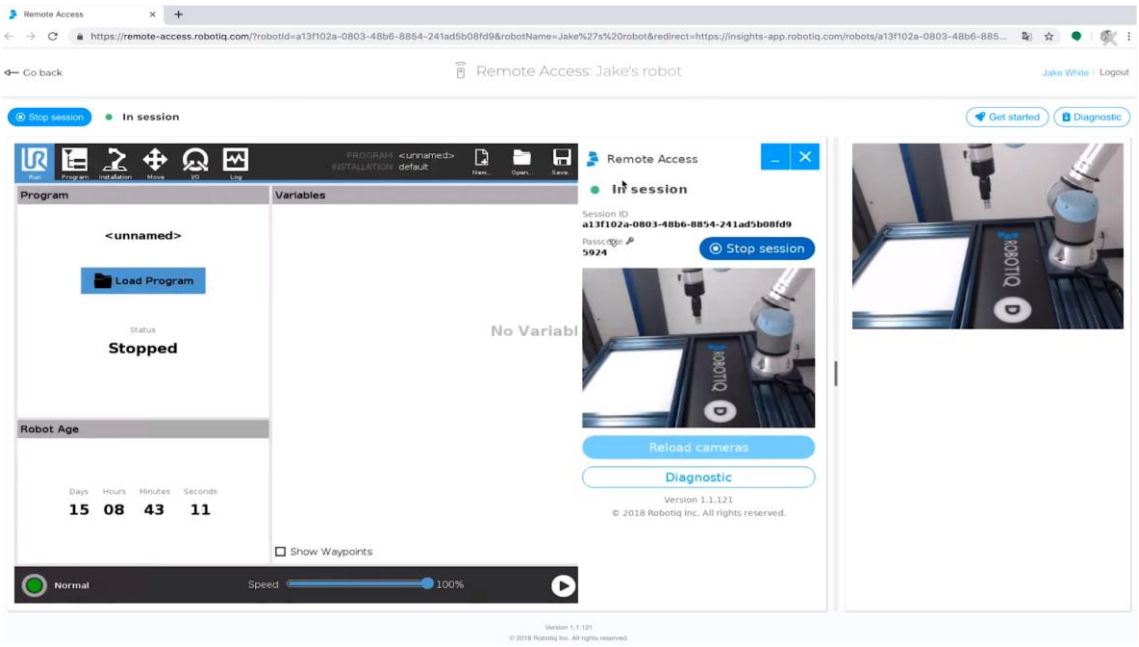

Abbildung 29: Weboberfläche „Insights“ mit Kameras (rechts) und gespiegeltem Teach-Pendant (links), Quelle: Robotiq (2021), Onlinequelle [17.02.2021]

Vorteile:

+ Gute Kompatibilität mit Universal Robots durch enge Zusammenarbeit.
+ Einfache Installation.
+ Ermöglicht Betriebsdatenerfassung.
+ Möglichkeit der visuellen Überwachung via Webcam.
+ Keine spezielle Software wird benötigt, da es eine Webapplikation ist.
+ Am Teachpendant können die Handlungen des Fernwartenden überwacht werden.

Nachteile:

- Safety und Security hängen von der Konfiguration des Roboters ab (z.B. Änderungen nur mit Passwort zulassen).
- Authentifizierung basiert auf persönlichem Vertrauen.
- Daten laufen über Server außerhalb des Unternehmens.

3.4.5 System Tosibox

Das Unternehmen Tosibox hat seinen Hauptsitz in Oulu, Finnland und verkauft seit 2012 Geräte für den Fernzugriff. Das in Abbildung 30 dargestellte System, besteht aus einem sogenannten „Lock“ und dem dazu passenden „Key“, der den Zugriff auf den Lock über das Internet erlaubt. Es handelt sich bei dieser Verbindung um eine direkte, sichere Punkt-zu-Punkt-Verbindung über einen VPN-Tunnel. Der Lock ist ein Router mit integrierter Firewall und patentierter Tosibox Plug&Go Technologie, welche das Koppeln von Anlage und Fernwartungsgerät ermöglicht. Die Kommunikation ist über WAN- sowie LAN-Anschlüsse, USB-Ports und je nach Ausführung mit integriertem WLAN und 4G Mobilfunk möglich. Für die Verwendung der Tosibox-Lösung auf Geräten von Drittanbietern kann der Lock auch als Softwarelösung ausgeführt sein, die auf der entsprechenden Hardware installiert wird. Der Lock bildet ein eigenes Netzwerk, an das die Geräte angebunden sind, die über das Internet erreichbar sein sollen.

Abbildung 30: Verbindungsübersicht Tosibox Quelle: Tosibox Oy (2021), Onlinequelle [30.01.2021]

Die Zugriffsrechte- und Netzwerkverwaltung findet über die Plattform „Tosibox Virtual Center Lock“ statt, die gemeinsam mit den Locks das in Abbildung 31 dargestellte, frei skalierbare Tosibox-Ökosystem bildet. Die Qualität dieser Konfiguration ist ausschlaggebend für die Security und Safety des gesamten Systems. Mit der Plattform VCL verfolgt das Unternehmen die Strategie, mit möglichst einfach bedienbarer Software unabhängig von der Qualifikation des Users hohe Security-Standards zu erreichen. Beispielsweise kann die User- und Geräte-Verwaltung per Drag&Drop durchgeführt werden. Zum Aufbau einer VPN-

Verbindung wird entweder eine Tosibox Softkey Software-Lizenz, ein Tosibox-App Mobile Client oder der physische Tosibox Key in Form eines USB-Sticks benötigt. Der Hintergrunddienst „MatchMaker“ dient dazu, den entsprechenden Lock zum verwendeten Key zu finden und die Verbindung aufzubauen. Ist diese erfolgreich hergestellt, besteht ein direkter VPN-Tunnel ohne Cloud oder weiteren Hintergrunddiensten.[59]

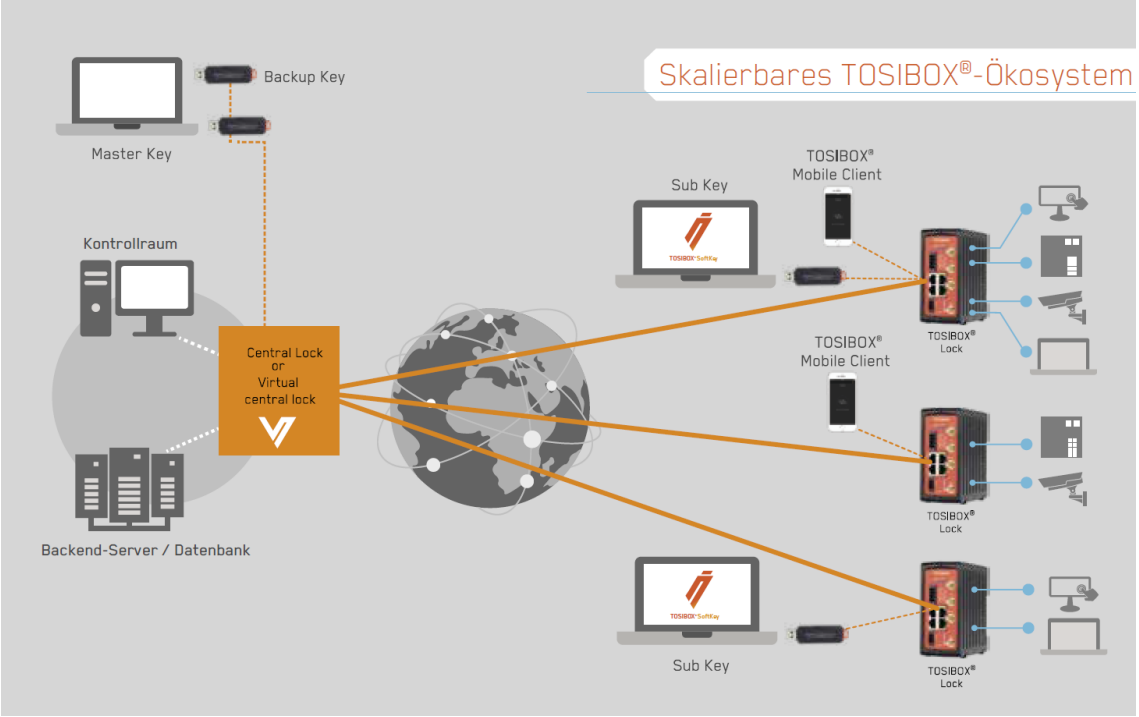

Abbildung 31: Skalierbares Tosibox-Ökosystem, Quelle: Produktfolder Tosibox Oy (2019)

In Abbildung 32 sind die verschiedenen Locks dargestellt, die je nach Einsatzgebiet auf die Umgebungsbedingungen angepasst sind. Preislich beginnen die Starter Kits, bestehend aus Lock, Key und Softkey bei 595 € für den Lock 150. Das Modell Lock 500i kostet im Starterkit 995 €. (Preise exkl. Mehrwertsteuer, Stand Jänner 2021)[60]

[59] Vgl. Tosibox Oy, 2021.

[60] Vgl. Tosibox Oy, 2021.

Abbildung 32: Übersicht der angebotenen Locks Quelle: Tosibox Oy (2021), Onlinequelle [30.01.2021]

Das System stellt eine sehr einfach zu bedienende, auch nachträglich installierbare Lösung dar. Dem steht der Nachteil gegenüber, dass der theoretisch uneingeschränkte Fernzugriff die korrekte Konfiguration der Steuerung, die über die Fernwartung erreicht werden soll, voraussetzt. Dies ist essenziell, um sicherzugehen, dass der Fernwartende nur solche Berechtigungen erlangt, die vom Bediener gewünscht und aus Safety-Sichtweise vertretbar sind. Bei allen nachträglichen Änderungen im Anlagenverbund empfiehlt sich generell, den Systemintegrator miteinzubeziehen, der die ursprüngliche Risikoanalyse unter Berücksichtigung der zusätzlichen Hardware erneut durchführt.

Vorteile:

+ Unbegrenzte Skalierbarkeit des Netzwerks.
+ Direkter VPN-Tunnel ohne Cloud.
+ Integrierte Security Mechanismen (z.B. Zwei-Faktor-Authentifizierung)
+ Ermöglicht Datenerfassung, Internet der Dinge und Operational Networks.

Nachteile:

- Safety hängt von der Konfiguration der Berechtigungen in der Steuerung ab.
- Kein Einblick in die Fernwartung vor Ort.
- Externer muss entsprechenden Key oder Software besitzen.

3.4.6 System Secomea

Secomea wurde 2008 gegründet und hat den Hauptsitz in Dänemark. Die angebotene Fernwartungslösung unterscheidet sich bezüglich der Hardware kaum von Tosibox, jedoch gibt es einen entscheidenden Unterschied in Bezug auf den in Abbildung 33 dargestellten Verbindungsaufbau.

Abbildung 33: Übersicht Verbindungsaufbau Secomea Quelle: Secomea (2020), Onlinequelle [31.01.2021]

Die Verbindung erfolgt nicht direkt über einen VPN-Tunnel, sondern über Access Management Server, die wahlweise von Secomea gehostet werden können, aber auch Lösungen via Amazon Server oder eigens im Unternehmen befindliche Server sind realisierbar. Es besteht darüber hinaus die Möglichkeit, eine Data Collection Cloud anzubinden, die eine Betriebsdatenerfassung ermöglicht.

Sitemanager 11XX/35XX	Sitemanager 15XX/35XX	Sitemanager Embedded

Abbildung 34: Überblick Sitemanager Secomea Quelle: Secomea 2020, Onlinequelle [31.01.2021]

Die Site Manager (Gateways) können, wie in Abbildung 34 dargestellt, als Hardware mit wahlweise WLAN und/oder 4G Antennen oder als Softwarelizenz ausgeführt sein. Je nach Art können so bis zu 100 Geräte mit dem Sitemanager verbunden werden. Abbildung 35 illustriert die benötigten Hard- und Softwareprodukte für einen Fernwartungszugriff. Neben dem zuvor erwähnten Site Manager wird eine Gate Manager Lizenz benötigt, in der die zentrale Verwaltung der Verbindungen und Berechtigungen stattfindet. Der Link Manager wird für das Endgerät benötigt, von dem aus der Zugriff auf ein System erfolgen soll. Die Kosten belaufen sich auf 440 - 885 € für den Sitemanager, 325 € für den Link Manager und 2070 € für den Gate Manager. (Preise exkl. Mehrwertsteuer, Stand Jänner 2021).[61]

[61] Vgl. Routeco GesmbH, 2020.

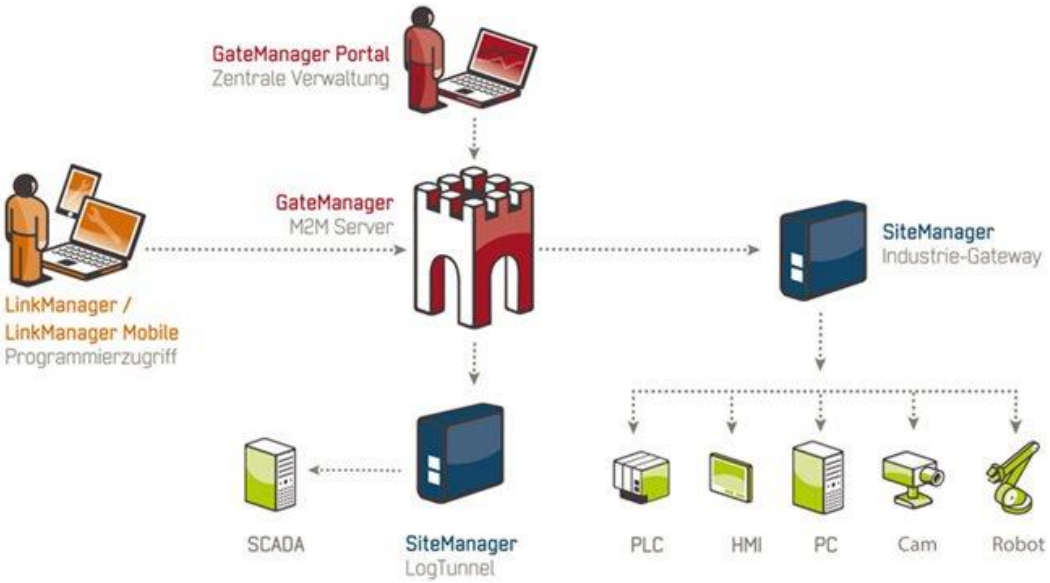

Abbildung 35: Übersicht Soft- und Hardware Secomea Fernwartung Quelle: Routeco 2020, Onlinequelle [01.02.2021]

Vorteile:

+ Überwachungsmöglichkeit der Verbindung am Gate Manager.
+ Sicherheitszertifizierter Anbieter
+ Integrierte Security Mechanismen
+ Ermöglicht Betriebsdatenerfassung
+ Updates und Sicherheit der Geräte werden von Secomea sichergestellt.

Nachteile:

- Safety und Security hängen von der Konfiguration des Site Managers ab.
- Kein Einblick in die Fernwartung vor Ort.
- Externer muss entsprechende Software besitzen.
- Daten passieren unter Umständen Server außerhalb des Unternehmens.

3.4.7 Analyse der Systeme

Bei genauerer Betrachtung der zuvor beschriebenen Systeme fällt auf, dass allen Anbietern von Fernwartungslösungen die Gefahr von Cyberangriffen bewusst ist. Vor allem Tosibox zeichnet sich trotz einfacher Handhabung durch einen hohen Sicherheitsstandard aus. Aber auch das System von Fronius ist aus Cybersecurity-Betrachtung heraus sehr positiv zu bewerten.

Im Bereich der Safety fällt auf, dass die Hersteller entweder komplett auf gewisse Funktionen verzichten, wie beispielsweise ABB, wo keine Bewegung des Roboters via Fernwartung ermöglicht wird, um so keine Gefährdungssituation zu erzeugen oder wie beispielsweise Fanuc die Verantwortung dem Anlagenbetreiber in Form von Verträgen und Hinweisen in der Bedienungsanleitung übertragen. Vor allem letzteres muss der Anlagenbetreiber bei der Implementierung einer Fernwartungslösung bedenken, denn bei Schäden an Mensch oder Maschine trägt er die Haftung. Robotiq versucht, den Grad der Safety durch visuelle Überwachung mittels Webcams zu erhöhen. Prinzipiell ist dieser Ansatz als gut zu bewerten, aber er setzt auch eine Internetverbindung mit sehr hoher Übertragungsrate und geringsten Verzögerungen voraus. Ist dies nicht gewährleistet und tritt eine Verzögerung zwischen Bild und Signalübertragung auf, trägt diese Funktion keinen entscheidenden Mehrwert zur Safety bei.

Die Problematik bei Lösungen von Drittanbietern ergibt sich aus der augenscheinlichen und beworbenen einfachen Installation, auch in bestehende Anlagen. Die Security ist durch etwaige Zertifizierungen gegeben, aber die Safety hängt von der Konfiguration und Architektur der Steuerung ab, in die die Fernwartungshardware integriert wird. Als einfaches Beispiel dient die Fragestellung, ob die SIS über die Fernwartungslösung erreichbar ist, also kein rückwirkungsfreier Betrieb der SIS vom Internet stattfindet. Dieser ist, sollte keine weitere Einschränkung vorgenommen werden, bei den Systemen von Tosibox und Secomea nicht gegeben. Experten raten aus aktueller Sicht ausdrücklich davon ab, dass eine SIS aus dem Internet erreichbar ist.[62]

[62] lt. Jonas Stein, Institut für Arbeitsschutz der DGUV (IFA), Webinar „Fernwartung von Industriesteuerungen“ am 08.03.2021

4. Maßnahmen zur sicheren Fernwartung eines MRK-Systems

Das bereits genannte Ziel dieser Arbeit ist es, Maßnahmen aufzuzeigen, die wie ein Handbuch für Anlagenbetreiber betrachtet werden können und eine sichere Fernwartung von MRK-Systemen ermöglichen. Basierend auf den vorherigen Kapiteln sollen in diesem Abschnitt Hinweise gegeben werden, wie mit möglichst einfachen Mitteln eine signifikante Verringerung von Risiken, sowohl im Safety- als auch Security-Bereich erreicht werden kann.

4.1 Safety relevante Aspekte

4.1.1 Sicherer Zustand eines MRK-Systems vor der Fernwartung

Die in Kapitel 3.1.1 zitierte Norm ISO 10218-2 fordert in Punkt k) einen „sicheren Zustand“ aller nicht für die Fernwartung benötigten Ausrüstungen, die eine Gefährdung verursachen können. Im folgenden Kapitel soll eine Checkliste erarbeitet werden, die es ermöglicht, zu evaluieren, ob der sichere Zustand zu Beginn der Fernwartung erfüllt ist.

Zunächst wird auf den Roboter selbst eingegangen, der laut Norm zwar nicht explizit im sicheren Zustand sein, sich aber trotzdem in einem Zustand befinden muss, aus dem heraus keine Gefährdung für die direkte Umgebung hervorgeht. Die Vorgabe hierzu lautet, dass der Roboter in der Grundstellung stehen und der Greifer geöffnet sein muss, damit keine Gefahr durch plötzlich herabfallende Gegenstände entsteht. Sämtliche Werkzeuge, wie Schraubendreher und -schlüssel müssen vom Roboter entfernt werden, damit von diesen keine Gefahr ausgehen kann. Es darf sich keine Person in unmittelbarer Nähe des Roboters befinden, dessen Betriebsmodus auf „manuell mit reduzierte Geschwindigkeit“ (T1)gestellt werden muss.

Für die Umgebung ist es schwierig, einen allgemeingültigen Ablauf zu definieren, der einen sicheren Zustand zur Folge hat, da sich die Systeme, in denen Roboter integriert sind, stark unterscheiden. Nachfolgend soll nur eine grobe Checkliste ausgearbeitet werden, die bei Spezialanwendungen (z.B. Schweißroboter) noch weitere Schritte benötigt (z.B. Abschalten der Schweißanlage), die

anwendungsspezifisch zu definieren sind. Folgende Checks sollten durchgeführt werden, um die Umgebung in den sicheren Zustand zu bringen, welcher nur dann gegeben ist, wenn alle nachstehenden Fragen mit JA beantwortet werden können.

- Sind die Not-Halt-Taster leicht zugänglich und sofort erreichbar?
- Ist der Arbeitsbereich, beispielsweise mit einer Kette, abgezäunt?
- Ist ein akustisches oder visuelles Signal, das die Fernwartung anzeigt, deutlich sicht- oder hörbar?
- Befinden sich nur geschulte Personen innerhalb des Arbeitsbereichs, die darüber in Kenntnis gesetzt sind, dass eine Fernwartung durchgeführt wird?
- Sind an der Fernwartung nicht beteiligte Anlagen im Arbeitsbereich ausgeschaltet oder zumindest gestoppt?
- Kann sich der Mitarbeiter jederzeit vom Robotersystem entfernen oder selbst befreien? Wird er durch die Absperrung evtl. behindert?
- Sind am Prozess beteiligte Materialien oder ggf. gefährliche Flüssigkeiten ausreichend gesichert?
- Wurde ein Backup der bestehenden Konfiguration erstellt und gesichert?

Es empfiehlt sich, einen Testdurchlauf einer Fernwartung bei Integration der Fernzugriffslösung durchzuführen und den sicheren Zustand mit Fotos in einem Bericht zu definieren und zu dokumentieren. Erst, wenn die in Abbildung 36 dargestellte Checkliste erfolgreich abgearbeitet wurde, ist es aus Safety-Betrachtung verantwortbar, einen Fernzugriff zu starten. Idealerweise könnte diese Checkliste in den Verbindungsprozess der Fernwartung integriert und beispielsweise am Teach-Pendant Schritt für Schritt angezeigt werden. Ist dies nicht möglich, muss auf jeden Fall sichergestellt sein, dass vor Beginn des Fernzugriffs diese Liste abgearbeitet wurde. Wichtig ist auch der Check, ob durch die Eingriffe in die Umgebung, welche nötig sind, um diese in den sicheren Zustand zu

überführen, der den des Roboters beeinflusst wurde. Beispielsweise wird für das Sichern eines Gegenstandes in der Umgebung ein Schraubendreher benötigt, der dann versehentlich auf dem Roboter abgelegt wurde. Der Roboter befindet sich daher nicht mehr im sicheren Zustand, da von einem herabfallenden Schraubendreher aus gewisser Höhe eine Gefahr ausgeht. Daher muss bei jedem Eingriff der komplette Check für Roboter und Umgebung wiederholt werden.

Ist es nicht möglich, das System in den sicheren Zustand zu überführen, sollte kein Fernzugriff erlaubt werden.

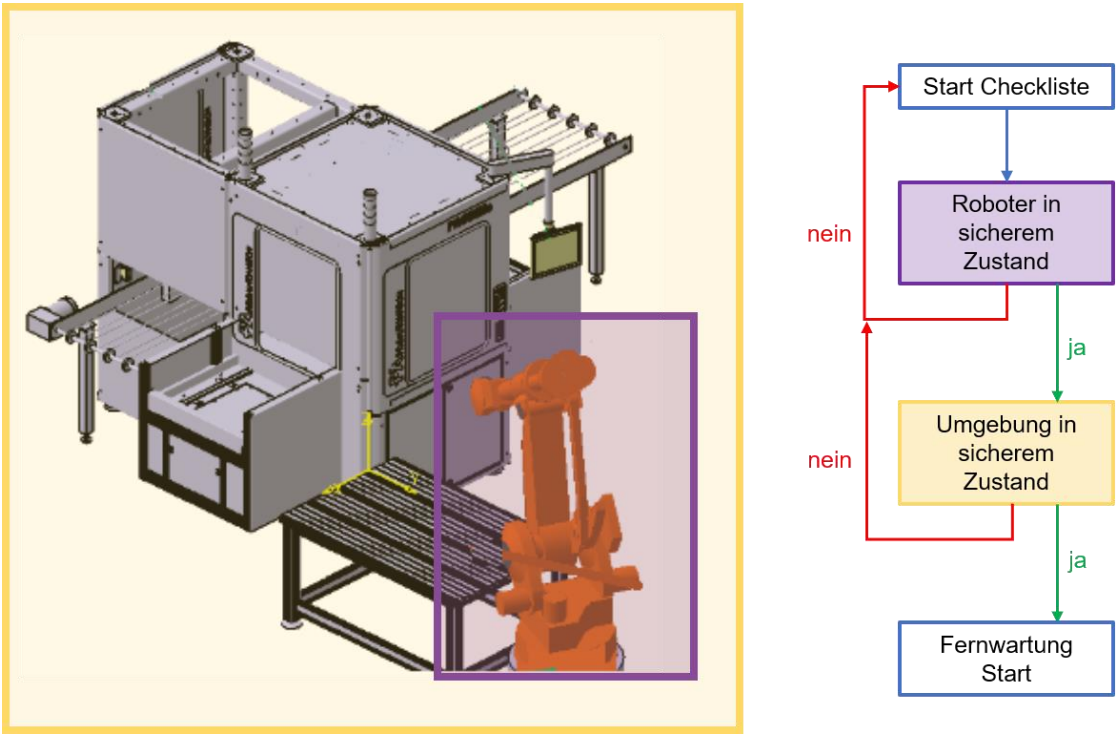

Abbildung 36: Ablauf der Checkliste vor einer Fernwartung, Quelle: eigene Darstellung

4.1.2 Sichere Architektur einer Anlage mit Fernwartungszugang

In Kapitel 3.3 wurden im Rahmen einer Risikoanalyse Maßnahmen entwickelt, die zur gewissen Architektur einer Anlage führen, welche über einen Fernwartungszugang verfügt. Nachfolgend wird exemplarisch eine kollaborative Roboteranlage beschrieben, die die wichtigsten Elemente enthält, damit eine sichere Fernwartung ermöglicht ist. Dazu ist in Abbildung 37 ein Vorschlag abgebildet, wie eine Architektur für eine sichere Fernwartung ausgeführt sein könnte.

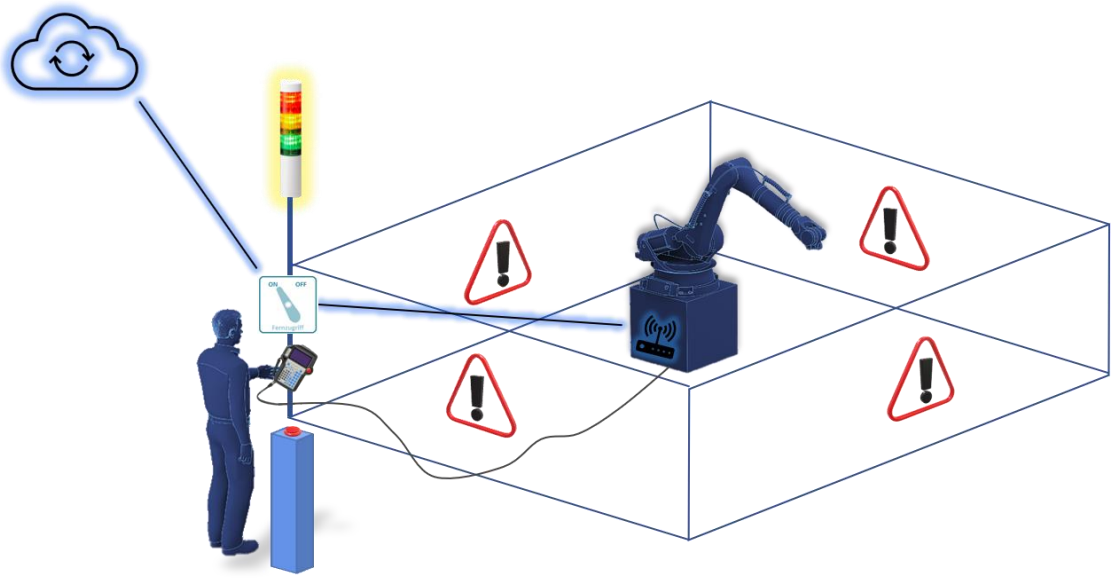

Abbildung 37: Architektur einer Anlage mit Fernwartungszugang, Quelle eigene Darstellung

Der rechteckig dargestellte Gefährdungsbereich der Anlage wird mit von allen Seiten klar sichtbaren Warnhinweisen versehen. Der Bediener vor Ort überwacht am Teach-Pendant die Handlungen des Fernwartenden und muss, damit der Fernwartende Bewegungen der Roboterachsen durchführen kann, einen Taster gedrückt halten, der sich ebenfalls außerhalb des Gefahrenbereichs befindet. Ein gut sichtbares visuelles Signal zeigt an, dass die Anlage gerade aus der Ferne gesteuert wird. Über einen Schalter, der ebenfalls außerhalb des Gefährdungsbereichs liegt, kann die Verbindung zum Internet und somit die Fernwartung lokal jederzeit unterbrochen werden. Falls es der Anbieter in der Steuerungslogik bereits programmiert hat, ist die Geschwindigkeit des Roboters bei Fernwartungen auf 250 mm/s limitiert. Andernfalls muss der Bediener vor Ort den Betriebsmodus „manuell mit reduzierte Geschwindigkeit“ (T1) wählen, sobald die

Fernwartungsverbindung aktiviert wird. Ist ein Eingreifen des lokalen Bedieners notwendig, so verlässt dieser seinen sicheren Platz und betritt die Gefährdungszone. Durch das Lösen des Bestätigungstasters sind keine Bewegungen des Roboters mehr möglich.

Das Aktivieren des Fernzugriffs impliziert darüber hinaus eine Deaktivierung von Eingaben am Teach-Pendant, um sicherzustellen, dass nur eine Bedienstation aktiv ist. Abbildung 38 illustriert eine Logik, die in der Steuerung hinterlegt sein sollte, um zu gewährleisten, dass die zuvor beschriebene Voraussetzung eingehalten wird. Die Aktivierung der Fernwartung darf nur lokal möglich sein. Eine selbstständige Herstellung der Verbindung zur Anlage darf nicht möglich sein. Alle genannten Maßnahmen, die in der Steuerungslogik hinterlegt werden müssen, könnten als Betriebsart „Fernwartung“ (siehe auch Kapitel 5.4) implementiert werden und somit klar den Zustand der Maschine definieren.

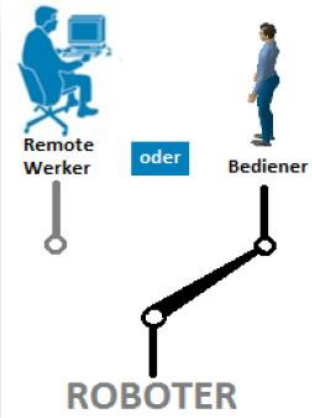

Abbildung 38: Hinterlegte Steuerungslogik zur Sicherstellung der Bedienung von einer Bedienstation, Quelle: Malisa (2019)

4.1.3 Inbetriebnahme nach der Fernwartung

Die Inbetriebnahme nach der Fernwartung besitzt ein ebenso hohes Risikopotential. Daher sollte bereits vor Beginn der Fernwartung sichergestellt werden, dass eine Person vor Ort ist, die die Anlage fachmännisch wieder in den Regelbetrieb versetzen kann. Durch die Fernwartung könnte es zu beabsichtigten und unbeabsichtigten Änderungen von Softwareparametern kommen, welche deutliche Auswirkungen auf den Bewegungsablauf des Roboters haben. Dadurch können Gefährdungssituationen entstehen, die im Rahmen einer fachgerechten Inbetriebnahme auszuschließen sind. Bestandteile einer fachgerechten Inbetriebnahme sollten sein:

- Trennung und Deaktivierung der Fernwartungsverbindungen/-zugänge
- Test des Programmablaufs bei stark reduzierter Geschwindigkeit
- Ggf. Überprüfung der vorgenommenen Änderungen
- Überprüfen der Dokumentation der Fernwartung
- Unterzeichnung eines Protokolls, das die Fernwartung und deren korrekte Durchführung bestätigt
- Über- und Freigabe der Anlage für den regulären Betrieb

Einen Sonderfall stellt die Inbetriebnahme nach einem ungeplantem Verbindungsabbruch oder ähnlichem Zwischenfall bei der Fernwartung dar. In diesem Fall sollte die Anlage keinesfalls in Betrieb genommen werden, bevor nicht der Softwarestand vor Beginn der Fernwartung wiederhergestellt wurde (z.B. mittels zuvor erstelltem Backups).

4.2 Security relevante Aspekte

4.2.1 Hinweise zur Fernwartung mittels „TeamViewer“

In Kapitel 3.2 wurde die Variante „Engineering-PC und Remote App“ bereits angesprochen. Die Recherchen für die vorliegende Arbeit haben ergeben, dass das Softwarepaket „TeamViewer“ ein sehr häufig verwendetes Hilfsmittel für Remote-Desktop Verbindungen darstellt. Nachfolgend werden einige Hinweise gegeben, die bei der Verwendung dieser Software berücksichtigt werden müssen.

Der Softwareanbieter „TeamViewer“ bietet sein Produkt zur privaten Nutzung als kostenlosen Service an. Wird diese Version im kommerziellen Umfeld benutzt, stellt es zum einen eine strafbare Urheberrechtsverletzung dar, zum anderen fehlen der kostenlosen Version wichtige Einstellungsmöglichkeiten, die die Security gewährleisten. Darüber hinaus besteht kein Servicevertrag, der einen Support durch „Teamviewer“ ermöglicht. Für die Fernwartung wichtige Funktionen, wie Geräte- und Benutzerzugriffsberichte, Festlegen von Geräterichtlinien und Benutzerverwaltung ist in der kostenlosen Version nicht möglich.[63] Das Unternehmen „Teamviewer“ selbst wies im Zuge der Recherche darauf hin, dass kostenlose private Lizenzen im industriellen Umfeld nicht nur gegen den EULA verstoßen, sondern auch mittels dem „Commercial Blocker“ regelmäßig deaktiviert und gesperrt werden. Dies bedeutet, dass die Verfügbarkeit des Fernwartungstools nicht gegeben sein kann, wenn es dringend benötigt wird.[64]

Die Möglichkeit, einen Computer aus der Ferne zu steuern, stellt ein sehr nützliches Feature dar. Jedoch sollte nicht außer Acht gelassen werden, dass der „TeamViewer“ nach erfolgreichem Verbindungsaufbau die Firewall gänzlich umgeht.[65] Aus mehreren, zuvor schon genannten Gründen ist es fahrlässig, den „TeamViewer“ als Privatlizenz im industriellen Umfeld zu verwenden. Die kommerzielle Version kann unter Einhaltung der nachfolgenden Aspekte eine

[63] Vgl. Teamviewer, 2021.

[64] lt. Interview Servicemitarbeiterin „Teamviewer“ am 17.02.2021

[65] Vgl. Groš, 2011, S. 103.

Alternative zu teuren Fernwartungslösungen darstellen, muss aber speziell mit der IT-Abteilung abgestimmt werden.[66]

- Der Modus „TeamViewer mit Windows starten“ sollte nicht aktiviert werden. Das bedeutet, dass der TeamViewer nur dann auf dem Rechner ausgeführt, wenn er auch benötigt wird. Nach Beendigung des Zugriffs sollte darauf geachtet werden, die Applikation am Rechner ebenfalls zu beenden. Gleiches gilt für den Modus „Einfachen Zugriff gewähren“, bei dem der Rechner ohne lokale Bestätigung aus einem „TeamViewer-Konto“ erreichbar ist.

- Bei der Einrichtung muss bedacht werden, wer Zugriff auf den Rechner haben soll. Befindet sich diese Person im selben Netzwerk, bietet der „TeamViewer“ die Möglichkeit, Verbindungen nur aus dem lokalen Netzwerk zuzulassen. Dies erschwert potenziellen Angreifern das ungewollte Eindringen über den „TeamViewer“.

- Für die Authentifizierung sollten Einmal-Passwörter generiert werden, es ist keinesfalls über längeren Zeitraum dasselbe Passwort zu verwenden.

- Die Anwendung muss so konfiguriert sein, dass sämtliche Verbindungen geloggt werden.

[66] Vgl. Groš, 2011, S. 106.

4.2.2 Verbesserung der IT-Security anhand der BSI-Bausteine

Um eine IT-Infrastruktur – gerade auch für die Fernwartung - möglichst sicher zu gestalten, können Standards des BSI zur Hilfe genommen werden. Der BSI Standard 200-2 beinhaltet Methodiken zur Strukturanalyse, eine Analyse des Schutzbedarfs der einzelnen Komponenten sowie Hilfestellungen zur Modellierung des Informationsverbunds. Sämtliche Teilaufgaben sind dem genannten Standard zu entnehmen und sollten prinzipiell beim Aufbau einer Netzwerkstruktur berücksichtigt werden. In Abbildung 39 ist ein Überblick der Modellierung illustriert, der die einzelnen Schritte vom ursprünglichen Informationsverbund bis zu Prüf- und Entwicklungsplan aufzeigt. Nachfolgend werden die einzelnen Bereiche kurz erläutert und aufgezeigt, dass die Modellierung mit Hilfe des BSI eine relativ einfache Methode ist, die Security in einem Unternehmen zu verbessern.

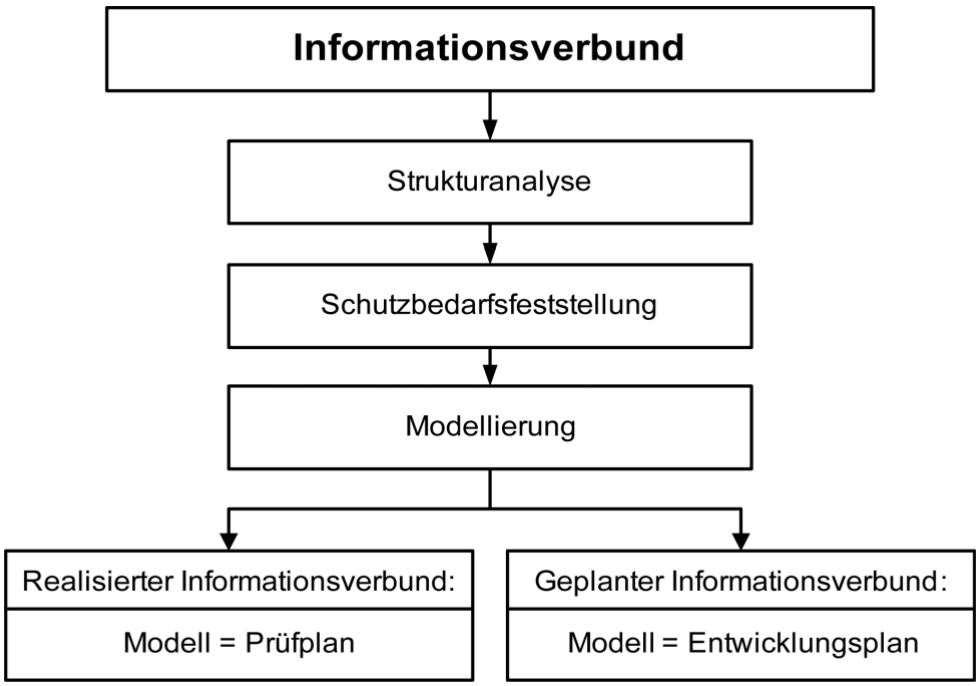

Abbildung 39: Ergebnis der Modellierung nach IT-Grundschutz, Quelle: BSI (2017), S. 135

Den ersten Schritt bildet die Strukturanalyse. Sie dient dazu, das Zusammenwirken von Geschäftsprozessen, Anwendungen und verwendeter Informationstechnik zu analysieren und dokumentieren.[67] Laut BSI sollten dabei folgende Aspekte berücksichtigt werden: [68]

1) Die „im Informationsverbund betriebene[n] Anwendungen und die dadurch gestützten Geschäftsprozesse,
2) Die organisatorischen und personellen Rahmenbedingungen für den Informationsverbund,
3) Im Informationsverbund eingesetzte vernetzte IT-Systeme, ICS- und Iot-Komponenten,
4) Die Kommunikationsverbindungen dazwischen und nach außen,
5) Die vorhandene Infrastruktur“

Bezogen auf die Thematik Fernwartung, können die zuvor genannten Aspekte wie folgt aussehen:

ad 1) Anwendungen im Informationsverbund können Softwareprodukte zur Roboterfernsteuerung, zum Verbindungsaufbau oder zur Dokumentation sein. Sie unterstützen den Geschäftsprozess Fernwartung, der zumindest einen von mehreren Geschäftsprozessen der gesamten Anlage darstellt.

ad 2) Um bei der Analyse alle notwendigen Fachabteilungen zu integrieren, müssen aus jeder entsprechende Vertreter daraus miteinbezogen werden. Dies sind neben den entsprechenden IT-Verantwortlichen die Bediener der Anlage, die bei der Fernwartung vor Ort sind, die Prozessverantwortlichen, die die Verantwortung über die Anlage haben sowie der Fernwartende, der sich von extern in die Anlage einwählt.

ad 3) Als Komponenten sind die jeweiligen Router zu berücksichtigen, sämtliche Hardware, die für den Verbindungsaufbau benötigt wird (z.B. USB-Sticks, Notebooks, Switches, Telefone) und darüber hinaus, jene Hardware, auf die über den Fernwartungszugang zugegriffen wird (z.B. SPS, SIS).

[67] Vgl. Bundesamt für Sicherheit in der Informationstechnik, 2017, S. 76–77.

[68] Bundesamt für Sicherheit in der Informationstechnik, 2017, S. 77.

ad 4) Es muss die verwendete Technologie untersucht werden, um zu eruieren, um welchen Typus von Kommunikationsverbindung es sich bei der vorliegenden Fernwartungslösung handelt. Möglichkeiten sind, wie in Kapitel 3.2 beschrieben, die Verbindung über Cloud-Server oder VPN-Tunnel.

ad 5) Bei der Analyse der vorhandenen Infrastruktur ist zu untersuchen, wo sich die jeweiligen an der Fernwartung beteiligten Personen befinden können. Beispielsweise kann der Fernwartende einen mobilen Arbeitsplatz haben oder von zu Hause arbeiten.

Im nächsten Schritt folgt die Schutzbedarfsfeststellung, die das Ziel hat, zunächst den Schutzbedarf der Geschäftsprozesse und Anwendungen zu bestimmen und daraus den der einzelnen IT-Systeme, Räume und Kommunikationsverbindungen abzuleiten. Das BSI definiert dazu die drei Schutzbedarfskategorien „Normal“, „Hoch“ und „Sehr hoch“. Auf den entsprechenden Anwendungsfall sind aber auch angepasste Kategorien möglich. Unter die Kategorie „Normal“ fallen jene Bereiche, bei denen die Schadensauswirkungen begrenzt und überschaubar sind. Die Kategorie „Hoch“ bedeutet beträchtliche Schadensauswirkungen und mit „Sehr hoch“ sind jene Bereiche zu kennzeichnen, bei denen die Auswirkungen ein existenziell bedrohliches Ausmaß erreichen können.[69]

Für jeden Geschäftsprozess und die zugehörigen Anwendungen muss eine Einteilung in Schutzbedarfskategorien durchgeführt werden, die den Einfluss des jeweiligen Elements auf die drei Grundwerte der Informationssicherheit, Vertraulichkeit (C - Confidentiality), Integrität (I - Integrity) und Verfügbarkeit (A - Availability) aufzeigt.

Tabelle 10 zeigt exemplarisch für den Geschäftsprozess „Fernwartung“, wie die Schutzbedarfsfeststellung gemäß BSI Standard 200-2 aussehen könnte. Analog erfolgt auf Basis der Feststellung für die Geschäftsprozesse und Anwendungen eine Schutzbedarfsfeststellung für alle beteiligten Elemente. Im Detail ist dies dem BSI-Standard 200-2 zu entnehmen.

[69] Vgl. Bundesamt für Sicherheit in der Informationstechnik, 2017, S. 104.

Tabelle 10: Schutzbedarfsfeststellung Geschäftsprozess Fernwartung gemäß BSI Standard 200-2

Beschreibung des Zielobjektes / der Gruppe der Zielobjekte	**Plattform/ Baustein**	**Vertraulichkeit**	**Begründung für die Vertraulichkeit**	**Integrität**	**Begründung für die Integrität**	**Verfügbarkeit**	**Begründung für die Verfügbarkeit**
Fernwartung	Fernwartung	Sehr hoch	Über einen Fernwartungszugang kann auf wichtige Daten zugegriffen werden	Sehr hoch	Falsch übermittelte Daten und Parameter können schwerwiegende Folgen für die Anlage haben	Normal	Sollte der Geschäftsprozess nicht durchführbar sein, entsteht kein nennenswerter Schaden

Aus der vollständigen Schutzbedarfsfeststellung ergibt sich, bezogen auf die jeweilige Kategorie, eine Schutzwirkung von Sicherheitsanforderungen nach dem IT-Grundschutz, die in Tabelle 11 illustriert ist. Daraus lässt sich schlussfolgern, ob und für welche Elemente eine Risikoanalyse durchgeführt werden muss und ob Elemente mit erhöhten Sicherheitsanforderungen in Sicherheitszonen konzentriert werden können.[70]

Tabelle 11: Schutzwirkung von Sicherheitsanforderunen nach IT-Grundschutz, Quelle BSI (2017) S. 130

Schutzwirkung von Sicherheitsanforderungen nach IT-Grundschutz	
Schutzbedarfskategorie „Normal“	Sicherheitsanforderungen nach IT-Grundschutz sind im Allgemeinen ausreichend und angemessen.
Schutzbedarfskategorie „Hoch“	Sicherheitsanforderungen nach IT-Grundschutz liefern eine Standard-Absicherung, sind aber unter Umständen alleine nicht ausreichend. Weitergehende Maßnahmen sollten auf Basis einer Risikoanalyse ermittelt werden.
Schutzbedarfskategorie „Sehr hoch“	Sicherheitsanforderungen nach IT-Grundschutz liefern eine Standard-Absicherung, reichen aber alleine im Allgemeinen nicht aus. Die erforderlichen zusätzlichen Sicherheitsmaßnahmen müssen individuell auf der Grundlage einer Risikoanalyse ermittelt werden.

[70] Vgl. Bundesamt für Sicherheit in der Informationstechnik, 2017, S. 132.

Den dritten und letzten Schritt bildet die Modellierung des Informationsverbunds mit Hilfe der im IT-Grundschutz-Kompendium enthaltenen Bausteine. Die in Kapitel 3.2 genannten Möglichkeiten des Verbindungsaufbaus erfordern für den Geschäftsprozess „Fernwartung“ die Berücksichtigung der in Tabelle 12 genannten Bausteine des IT-Grundschutzes. In diesen Bausteinen sind sowohl die Grundwerte enthalten, die durch den jeweiligen Grundbaustein gefährdet werden, als auch Maßnahmen, die die jeweiligen Gefährdungen reduzieren. Bei der Implementierung einer Fernwartungslösung sollten alle in den Bausteinen enthaltenen Maßnahmen getroffen werden. Sind gewisse Punkte nicht realisierbar, so muss anhand der Kreuzreferenztabelle analysiert werden, welche Gefährdung dadurch entsteht und es sind andere Maßnahmen zu finden, die die Gefährdung ausreichend reduzieren. [71]

Tabelle 12: Überblick der Bausteine aus dem IT-Grundschutz für die Fernwartung

Baustein Nummer	**Baustein Bezeichnung**
ORP.4	Identitäts- und Berechtigungsmanagement
OPS.1.2.5	Fernwartung
OPS.2.2	Cloud-Nutzung
SYS.3.1	Laptops
SYS.4.3	Eingebettete Systeme
SYS.4.4	Allgemeines IoT-Gerät
SYS.4.5	Wechseldatenträger
IND.1	Betriebs- und Steuerungstechnik
NET.3.3	VPN

[71] Bundesamt für Sicherheit in der Informationstechnik, 2020b.

Wie in Abbildung 39 dargestellt, kann das Ergebnis der drei zuvor genannten Schritte entweder ein Prüfplan oder ein Entwicklungskonzept sein. Abhängig ist dies von der Tatsache, ob es sich um einen bestehenden Informationsverbund, der mittels Soll-Ist-Vergleichs evaluiert werden soll oder um einen neuen Informationsverbund handelt, bei dem Sicherheitsanforderungen definiert werden.[72] Fernwartungslösungen sind oftmals nachträglich integrierte Konzepte, bei denen die zuvor beschriebenen Schritte sowohl einen Prüfplan für bestehende als auch ein Entwicklungskonzept für neu hinzugefügte Komponenten darstellt.

Sollte für gewisse Elemente eine Risikoanalyse notwendig sein, stellt das Bundesamt für Sicherheit in der Informationstechnik den Standard 200-3 zur Verfügung, der die Möglichkeit einer Risikoanalyse auf Basis der elementaren Gefährdungen des IT-Grundschutzes aufzeigt. Dabei handelt es sich um ein anerkanntes Vorgehen, das dem Unternehmen eine angemessene und zielgerichtete Steuerung der Informationssicherheitsrisiken ermöglicht.[73]

[72] Vgl. Bundesamt für Sicherheit in der Informationstechnik, 2017, S. 134.

[73] Vgl. BSI-Standard 200-3, 2017, S. 5.

4.2.3 Hinweise zu wesentlichen Security-Maßnahmen

Segmentierung des Netzwerks

Der Grundgedanke hinter der Segmentierung besteht darin, dem Angreifer den Zugang zum IACS Netzwerk über Schwachstellen im Unternehmensnetzwerk zu blockieren. Zudem trägt die Segmentierung dazu bei, dass sich Viren im Netzwerk nur dort ausbreiten, wo das infizierte Element Zugriff hat. Eine gängige Methode dazu stellt die Trennung von IACS und Unternehmensnetzwerk mittels einer industriellen Demilitarisierten Zone (DMZ) dar. Innerhalb der IACS Zone sollten weitere Unterteilungen, je nach Schutzbedarf des betroffenen Elements, vollzogen werden. [74]

Eine DMZ stellt einen Bereich dar, in dem sich die Systeme befinden, die direkt mit dem Internet kommunizieren müssen, wie VPN und E-Mail Gateways. Die VPN Gateways stellen in der Regel auch die Fernwartungszugänge dar und sollten die einzige Möglichkeit sein, wie von Extern auf das ICS zugegriffen werden kann.[75]

[74] Vgl. Cisco/Rockwell Automation, 2019, S. 2.

[75] Vgl. Obregon, 2015, S. 7.

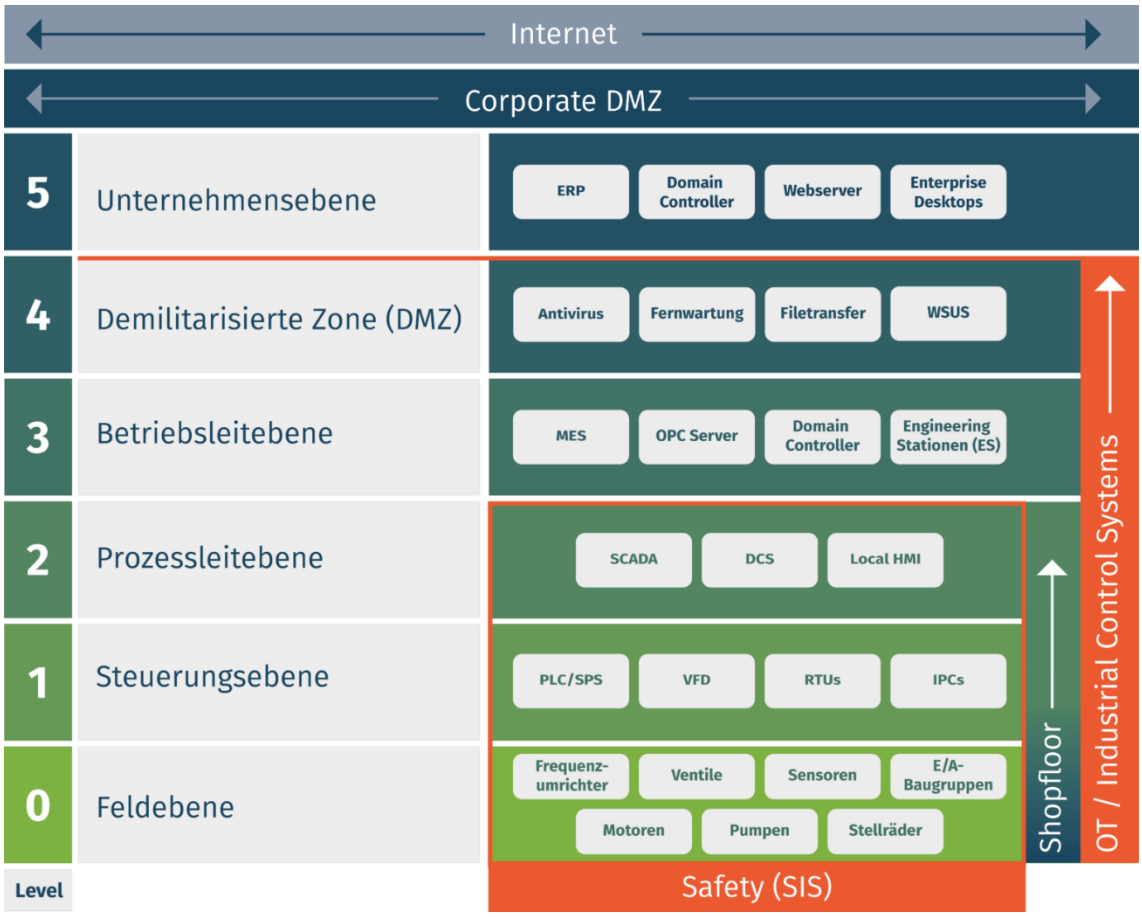

Abbildung 40: Purdue Reference Model für Industrielle Netzwerke, Quelle: Geiger (2018), Onlinequelle [05.03.2021]

Das in Abbildung 40 dargestellte Purdue Reference Model verfolgt ein zentrales Schema. Je geringer das Level, desto umfangreicher sind die Anforderungen an die Echtzeitfähigkeit und Verfügbarkeit der enthaltenen Systeme. Standardmäßig dürfen Systeme aus geringeren Levels keinen höheren Levels vertrauen.[76] Zwischen den einzelnen Ebenen findet eine genau überwachte Kontrolle der eingehenden und ausgehenden Kommunikation mittels Firewalls statt, um Auffälligkeiten sofort zu erkennen.[77] In Abbildung 41 ist ein Beispiel aufgeführt, wie das Purdue Model in einer Systemarchitektur realisiert werden kann. Es ist sowohl für bestehende Systeme als auch für Neuinstallationen realisierbar und schafft die Möglichkeit, durch einen Engineering-Arbeitsplatz auf den Einsatz von

[76] Vgl. Geiger, 2018.

[77] Vgl. Obregon, 2015, S. 16.

riskanten Service-Laptops zu verzichten. Eine vollständige Implementierung der in Abbildung 41 dargestellten Architektur ist nicht zwingend erforderlich.[78]

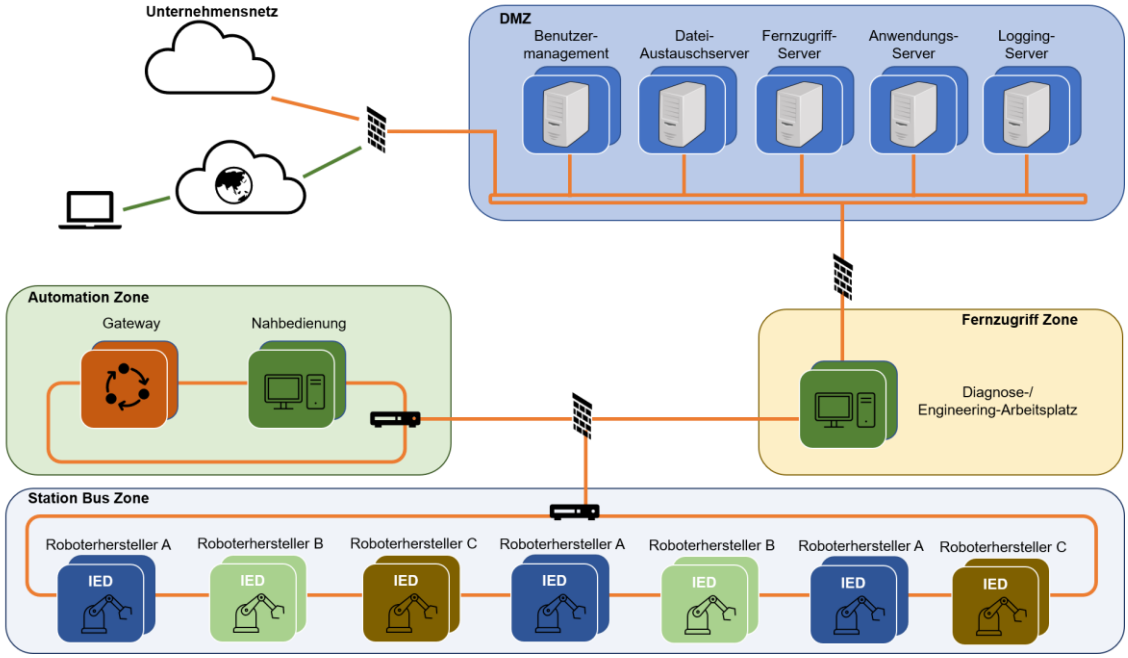

Abbildung 41: Sichere Systemarchitektur für den Fernzugriff, In Anlehnung an die Darstellung von: Harner (2019), Onlinequelle [08.03.2021]

Die Station Bus Zone kann als der Bereich betrachtet werden, in dem die Roboter und deren Steuerungen enthalten sind. Während es sich bei den in Abbildung 41 farblich unterschiedlich gekennzeichneten Bereichen um physisch oder logisch getrennte Netzwerke handelt, sollte der Bereich, in dem die Robotersteuerungen enthalten sind, nochmals virtuell unterteilt werden. Bei virtuellen Netzwerken handelt es sich um eine logische Verbindung von Elementen mehrerer Netzwerke.[79] Auch ein physisches Netzwerk kann in mehrere logische Netzwerke unterteilt werden. VLAN erlaubt somit, Geräte, die sich an einem Switch befinden, in einzelne Subbereiche zu unterteilen.[80] Im Hinblick auf die Fernwartung von Robotern in einer Fertigungsumgebung ist dies eine hilfreiche Möglichkeit, um sicherzustellen, dass einem Servicetechniker eines Roboterherstellers nur Zugriff auf die Anlage gewährt wird, die auch in dessen Zuständigkeitsbereich enthalten ist.

[78] Vgl. Harner, 2019, S. 10–11.

[79] Vgl. Rajaravivarma, 1997, S. 49.

[80] Vgl. Nyambayar, Davaadorj, et al., 2017, S. 78–79.

Trennung und Unabhängigkeit der SIS von der Umgebung

Diese Maßnahme ist Teil der zuvor beschriebenen Segmentierung. Während bei den beschriebenen Levels eine Unterteilung in virtuelle LANs ausreicht, sollten SIS physisch vom Umgebungsnetzwerk getrennt werden. Der BSI spricht von einem rückwirkungsfreien Betrieb der SIS von der Umgebung.[81]

Starke Authentisierungsmechanismen

Unter starken Authentisierungsmechanismen versteht man die Kombination von zwei oder mehr Authentisierungstechniken. Als Beispiel kann hier die Identifikation mittels Passwortes und Transaktionsnummer (Einmalpasswort) angeführt werden.[82] Generell sollten für Passwörter Richtlinien definiert werden, um die Sicherheit ebendieser zu garantieren. Diese definieren einen Zyklus, innerhalb dessen Passwörter regelmäßig geändert werden müssen und schreiben gleichzeitig die Form des Passwortes vor. Beispielsweise wird nebst der Mindestanzahl an Zeichen auch die Verwendung von Sonderzeichen, Groß- und Kleinbuchstaben sowie Zahlen verpflichtend. [83] Darüber hinaus empfiehlt sich eine Sensibilisierung der Mitarbeiter bezüglich der Thematik. Passwörter sollten nur in speziell dafür vorgesehenen und vom Unternehmen freigegebenen Tools gespeichert und keinesfalls in eigenständig geführten Excel Listen o.ä. niedergeschrieben werden.

[81] Vgl. Bundesamt für Sicherheit in der Informationstechnik, 2020a, S. 3 IND.2.7.

[82] Vgl. Bundesamt für Sicherheit in der Informationstechnik, 2020a, S. 11 Glossar.

[83] Vgl. Marouane/Rott, 2016, S. 122.

Vertraulichkeitsvereinbarung für den Einsatz von Fremdpersonal

Bevor externen Personen der Zugriff auf das System gewährt wird, muss eine Vertraulichkeitsvereinbarung geschlossen werden. In diesem Dokument müssen alle, zum Schutz der institutionsinternen Informationen nötigen Aspekte erfasst sein.[84] Im Rahmen einer Fernwartungsvereinbarung können diese integriert werden. Nachfolgende Auflistung zeigt auf, welche Punkte darüber hinaus enthalten sein sollten:

- Gegenstand der Vereinbarung
- Laufzeit und Kündigung
- Leistungsinhalt
- Vergütung, Kosten, Zahlungsbedingungen
- Allgemeine Pflichten Auftraggeber- und -nehmer
- Technische und organisatorische Sicherheitsmaßnahmen
- Haftung, Schadenersatz
- Anwendbares Recht, Gerichtsstand

Da bei diesen Verträgen eine juristisch korrekte Formulierung zwingend erforderlich ist, ist es empfehlenswert, entsprechendes juristisches Fachpersonal heranzuziehen, das mit den involvierten Security und Safety-Experten einen gültigen Vertrag aufsetzt.

[84] Vgl. Bundesamt für Sicherheit in der Informationstechnik, 2020a, S.3 ORP.2.

Regelungen zur mobilen Nutzung von Laptops

Das BSI empfiehlt eine Regelung der mobilen Nutzung von Laptops, die festlegt, welche Geräte mobil genutzt werden dürfen, wer diese mitnehmen darf und welche Sicherheitsmaßnahmen für diesen Gebrauch gelten.[85] Für ein Unternehmen, das Fernwartungsdienstleistungen von externem Personal in Anspruch nimmt, stellt dies einen schwer kontrollierbaren Aspekt dar. In der Regel ist keine Einflussnahme auf die Verwendung der mobilen Geräte der Fernwartungsdienstleister möglich. Mögliche Risiken dabei können sein:

- Fernwartender befindet sich in schlecht gesichertem, öffentlichen Internetzugang (z.B. auf Flughäfen)
- Notebook des Fernwartenden ist mit Virus infiziert
- Unbeteiligte Dritte erhalten Einblick in die Bildschirmaktivitäten

Um diese Risiken zu minimieren, sollten diese Aspekte zum einen in der Fernwartungsvereinbarung festgehalten werden (z.B. Verwendung öffentlicher Netzwerke untersagt) und zum anderen könnte eine Software in den Prozess des Verbindungsaufbaus integriert werden, die eine Überprüfung des Endgeräts vornimmt. Beispielsweise wird die Internetverbindung überprüft, ein Virenscan muss durchgeführt werden und der Ort des Fernwartenden muss bestätigt werden.

Kann nicht sichergestellt werden, dass es sich um ein sicheres Endgerät handelt, empfiehlt sich, im Rahmen der Fernwartung nur solche Aktionen zuzulassen, die unbedenklich sind, so wie z.B. eine reine Viewing-Sitzung, bei der der Fernwartende lediglich die Bedienoberfläche sieht, aber keine Befehle einspielen kann. Die Anleitung findet dann über telefonische Anweisung an den vor Ort befindlichen Anlagenbediener statt.

[85] Vgl. Bundesamt für Sicherheit in der Informationstechnik, 2020a, S. 3 SYS.3.1.

Absicherung integrierter Fernwartungssysteme

Bei der Beschaffung von neuen Steuerungen muss überprüft werden, ob diese bereits über entsprechende Hardware zur Fernwartung verfügen. Falls diese nicht verwendet werden, sind diese zu deaktivieren. Als Beispiel ist hier die Ethernet Schnittstelle einer Steuerung zu nennen. Ist diese vorhanden und frei zugänglich, so ist die Wahrscheinlichkeit durchaus hoch, dass im Laufe der Lebensdauer der Anlage eine Person diese nutzen möchte und ein entsprechendes Kabel dort anschließt. Aus diesem Grund sind nicht verwendete Schnittstellen zu sichern oder zu deaktivieren. Siemens bietet mit dem in Abbildung 42 dargestellten Port Lock System eine Hardware an, mit der Ethernet Schnittstellen gesperrt werden können. Werden die Systeme hingegen verwendet, ist zu beachten, dass die zuvor erwähnte Segmentierung durchgeführt wird. Es empfiehlt sich, die Funktionen der Fernwartungskomponente zu evaluieren und in die Risikoanalyse des Gesamtsystems miteinzubeziehen. [86]

Abbildung 42: Siemens Port Lock, Quelle: Siemens AG (2010), Onlinequelle [09.05.2021]

[86] Vgl. Bundesamt für Sicherheit in der Informationstechnik, 2020a, S. 6 OPS.1.2.5.

Verwaltung der Fernwartungswerkzeuge

Den Verantwortlichen im Unternehmen muss ein Überblick über alle in der gesamten Infrastruktur enthaltenen Fernwartungswerkzeuge vorliegen. Die Durchführung von Fernwartungen muss innerbetrieblich klar geregelt werden. Es empfiehlt sich hierzu eine Anleitung zu verfassen, die im Rahmen einer Schulung erörtert und jederzeit abrufbar ist. Regelmäßige Auffrischung der Schulungen, Testläufe sowie Sensibilisierung der Mitarbeiter bezüglich dieser Thematik sollten ebenso durchgeführt werden. Es sollte eine Person, die innerhalb des Unternehmens der zentrale Ansprechpartner für Fernwartungen ist, definiert werden.[87] Die Verwaltung der Werkzeuge muss darüber hinaus genaue Mechanismen enthalten, die definieren, wie im Falle der Ausmusterung der Anlage mit den Fernwartungszugängen und der entsprechenden Hardware umgegangen wird. Die Weitergabe oder unkontrollierte Weiterverwendung von für das Netzwerk konfigurierten Geräten ist zu vermeiden. Hier bietet der Hersteller nützliche Informationen, wie diese Geräte entsorgt oder zurückgesetzt werden können. Im Zweifelsfall empfiehlt sich, entsprechende Hardware zu vernichten.

[87] Vgl. Bundesamt für Sicherheit in der Informationstechnik, 2020a, S. 4-5 OPS.1.2.5.

4.2.4 Empfehlung zur Wahl der Verbindungstopologie

In Kapitel 3.2 wurden die drei wesentlichen Hautverbindungstypen und deren Vor- sowie Nachteile erwähnt, die hauptsächlich im Rahmen von Fernwartungen verwendet werden. Dieser Abschnitt soll eine Empfehlung abgeben, für welchen Zweck der jeweilige Verbindungstypus verwendet werden sollte.

Die Variante „Engineering PC und Remote App" erfreut sich vor allem aufgrund der einfachen Installation, sowie niedrigen Kosten großer Beliebtheit. Werden die in Kapitel 4.1 beschriebenen Hinweise berücksichtigt, stellt eine Remote App eine gute Variante für eine Fernwartung dar. Gespräche mit IT-Beauftragten der TU Graz zeigten, dass Remote Apps nicht prinzipiell abgelehnt werden, aber zwingend mit den IT-Verantwortlichen des Unternehmens abzustimmen sind. Für eine nachträglich installierbare Lösung stellt diese Variante eine gute Alternative dar, da keine spezielle Hardware und somit auch kein Eingriff in die Steuerung benötigt wird. Es setzt jedoch die Verwendung von Engineering-PCs voraus, deren IT-Anbindung mindestens die in Kapitel 3.3.5 erwähnten Anforderungen erfüllen muss.

Bei der Variante „Service-Box und Service-Cloud" ist zu unterscheiden in eine vom Hersteller bereits integrierte und eine von Drittanbietern nachträglich installierte Lösung. Vor allem letzteres ist aus Safety Betrachtung heraus genau zu untersuchen, am besten im Rahmen einer Risikoanalyse. Diese Möglichkeit bietet sich an, wenn ein Unternehmen viele Anlagen in unterschiedlichen Netzen besitzt, da jede Service-Box auch ohne lokale Netzwerkanbindung über das Internet kommunizieren kann. Wenn die Funktion der „Smart Maintenance", d.h. die vorausschauende Wartung durch laufende Betriebsdatenerfassung, verwendet werden soll, über die diese Geräte nahezu alle verfügen, bietet sich diese Lösung ebenfalls an, da die Hard- und Software somit die beiden Aspekte Fernwartung und Smart Maintenance abdeckt. Bei mehreren Anlagen empfiehlt sich, die benötigte Service-Cloud im eigenen Unternehmen zu hosten, um somit den Transfer von Daten über fremde Server zu verhindern. Bei wenigen Anlagen kann auch auf die Service-Cloud von einem Drittanbieter zurückgegriffen werden, wenn dieser die Grundanforderungen des eigenen Unternehmens in Bezug auf IT-Security garantieren kann.

Die Variante des „VPN-Tunnels“ mit dem VPN Konzentrator im eigenen Unternehmen bietet sich an, wenn mehrere Anlagen in ein Firmennetz integriert sind. Es setzt aber voraus, dass es sich um moderne Steuerungen mit Ethernet Schnittstellen handelt. Da es sich um eine direkte Ende-zu-Ende Verbindung handelt kann diese Verbindung aus Security Sicht als sehr sicher angesehen werden. Sie empfiehlt sich vor allem für Anlagen, die eine hohe Systemrelevanz innerhalb des Unternehmens haben und daher bestmöglich geschützt werden müssen.

5. Technische und organisatorische Aspekte zur Durchführung einer sicheren Fernwartung

5.1 Steigerung der Anlagensicherheit durch Grundlegende Maßnahmen

Die in den vorigen Kapiteln beschriebenen Maßnahmen sind oftmals mit hohem finanziellen und personellen Aufwand verbunden, der vor allem für KMUs eine große Hürde darstellt. Im Folgenden soll daher, basierend auf den erarbeiteten Inhalten, eine Prozessempfehlung für eine Fernwartung gegeben werden, die mit Hilfe von möglichst einfachen Maßnahmen eine dennoch essenzielle Steigerung der Anlagensicherheit im Zuge einer Fernwartung zur Folge hat.

In Abbildung 43 ist dazu ein Prozess dargestellt, dessen gewissenhafte Durchführung der einzelnen Schritte für eine hohe Gesamtsicherheit der Anlage sorgt.

1. Geschultes Personal für Fernzugriff: fern und lokal

   Es empfiehlt sich, regelmäßige Testläufe von Fernwartungen durchzuführen, um die beteiligten Personen mit dem neuesten Stand der Soft- und Hardware vertraut zu machen, Basisschulungen, welche im Rahmen der Anlagenintegration durchgeführt worden sind, sollten regelmäßig aufgefrischt werden.

2. Maschine und Produkt vorbereiten

   Die Anlage selbst und sämtliche in der direkten Umgebung befindlichen Objekte/Anlagen sind vor der Fernwartung immer in den sicheren Zustand überzuführen. Hilfestellung bietet dazu Kapitel 4.2.3. Zudem ist die Anlage gegen Zutritte Unbeteiligter zu sichern und muss akustisch oder optisch den Zustand Fernwartung anzeigen.

3. Backup von Steuerprogramm erstellen

   Bevor der Fernzugriff startet, empfiehlt es sich, ein Backup des Letztstandes der Software zu erstellen und dieses auch nach der durchgeführten Fernwartung zu verwahren.

4. Logs einschalten

Sämtliche zur Verfügung stehende Möglichkeiten des Loggings sollten genutzt werden. Beispiele hierfür können eine Bildschirmaufzeichnung, ein Verbindungslogfile oder eine Audioaufzeichnung sein. Diese bilden später einen wichtigen Bestandteil der Dokumentation.

5. Manuellen Betriebszustand herbeiführen

Der manuelle Betrieb stellt sicher, dass keine Programme im Automatikmodus aus der Ferne gestartet werden können. Daher sollte der Schalter der Steuerung vor Beginn der Fernwartung auf den manuellen Betrieb gesetzt werden.

6. Fernzugriff erlauben

Ein festgelegter Mechanismus, der den Fernzugriff erlaubt, kann nach Absolvierung der vorherigen Schritte gestartet werden. Die Steuerung des Fernzugriffs sollte so ausgelegt sein, dass dieser jederzeit von lokaler Seite abgebrochen werden kann.

7. Steuerprogramm ändern/Neue Funktionen implementieren

Je nach Zweck der Fernwartung werden in diesem Schritt die Handlungen aus der Ferne durchgeführt. Es empfiehlt sich, dass eine mit der Anlage vertraute fachkundige Person vor Ort den Prozess beobachtet. Gemeinsam mit dem Fernwartenden muss diese Person auch darüber entscheiden, ob die im Rahmen der Fernwartung durchgeführten Änderungen eine erneute Risikoanalyse der Anlage erfordern.

8. Dokumentation lesen, Einschulung vornehmen

Die im Rahmen der Fernwartung erstellte Dokumentation (siehe Kapitel 5.3) sollte unverzüglich nach Beendigung der Tätigkeiten für die Fernwartung erstellt werden. Gemeinsam mit dem Fernwartenden müssen die Punkte der Dokumentation besprochen und freigegeben werden. Der Bediener vor Ort muss vom Fernwartenden eine Einweisung in die Änderungen erhalten.

9. Testbetrieb besprechen und vornehmen

Bevor die Anlage in den Regelbetrieb übergeht, sollte gemeinsam mit dem Fernwartenden ein Testlauf durchgeführt werden, bei dem mit stark reduzierter Geschwindigkeit die Anlagenabläufe zu überprüfen sind.

10. Inbetriebnahme durchführen

Eine geschulte Person vor Ort kann die Anlage wieder in Betrieb nehmen. Hilfestellung dazu bietet Kapitel 4.1.3.

11. Änderungen aufgrund von Fernwartung dokumentieren und bei Bedarf in die Unterweisung aufnehmen

Ist es im Rahmen der Fernwartung zu Anpassungen gekommen, die das Verhalten der Anlage verändern, wie beispielsweise das Erhöhen einer Geschwindigkeit in einem gewissen Arbeitsschritt, so ist diese Änderung zu dokumentieren und in die Unterweisung für Anlagenbediener aufzunehmen.

12. In Automatikbetrieb umschalten

Erst, wenn alle zuvor erwähnten Aspekte gewissenhaft von einer geschulten Person durchgeführt wurden, darf die Anlage wieder in den Automatikmodus versetzt werden. Es empfiehlt sich, eine Checkliste zu erstellen, die abgearbeitet und mittels Unterschrift zu bestätigen ist, bevor die Anlage in den Automatikmodus versetzt wird.

13. Dokumentation über Fernzugriff lokal speichern

Wie später in Kapitel 5.3 genauer erläutert wird, müssen alle Dokumentationen von Fernzugriffen an einer gesammelten Stelle innerhalb des Unternehmens lokal abgespeichert und verwahrt werden.

Im gesamten Prozess gilt, den Systemintegrator bei Unsicherheiten miteinzubeziehen und keine Schritte zu überspringen, da dies im Fehlerfall zu schwerwiegenden Auswirkungen führen kann. Die zuvor genannten Punkte sollten auch für KMUs realisierbar und im finanziellen Rahmen sein. Im Regelfall reicht eine Person aus, die mit allen Anlagen vertraut und speziell auf Fernwartungen geschult ist. Diese Person ist verantwortlich für sämtliche Dokumentationen sowie Fernwartungszugänge und muss daher bei einer Fernwartung vor Ort sein. Das Risiko, dass bei Ausfall der Person keine Fernwartung möglich ist, kann durch eine zweite geschulte Person verringert werden. Dies ist jedoch mit finanziellem Mehraufwand verbunden, welcher in Gegenüberstellung mit den Folgen des Ausfalls der Fernwartung abgewogen werden muss.

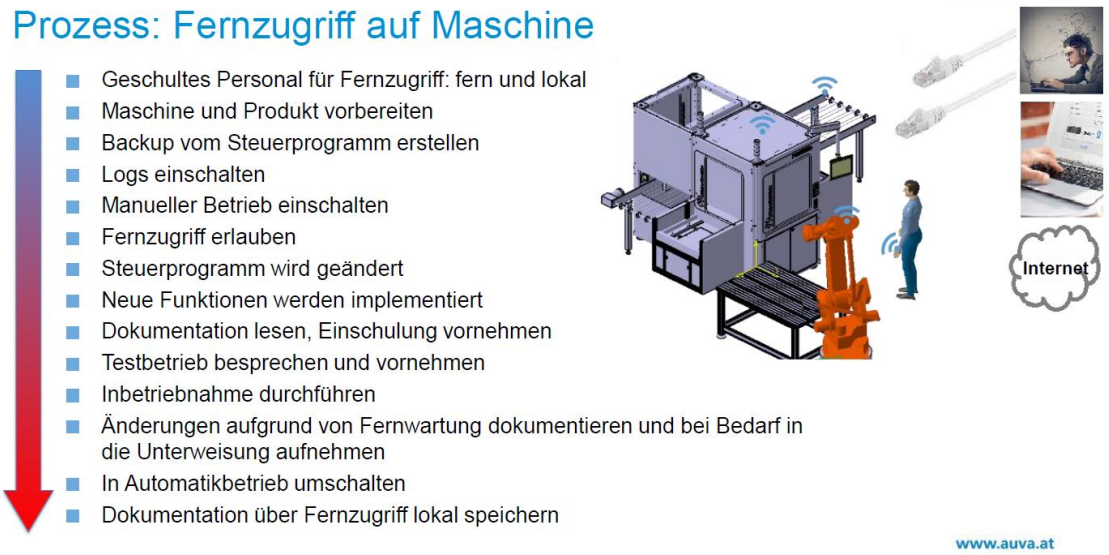

Abbildung 43: Prozessempfehlung Fernwartung, Quelle: Malisa (2019)

5.2 Bewertung der Aufgaben für die Fernwartung

In den vorherigen Kapiteln wurden Maßnahmen besprochen, die dazu beitragen sollen, eine sichere Fernwartung zu gewährleisten. Dabei stellt sich die Frage, bei welchen Aufgaben der Einsatz einer Fernwartung als sinnvoll erachtet werden kann. Nachfolgend sind daher Beispiele von Tätigkeiten aufgezeigt, die sinnvollerweise mittels Fernwartung durchgeführt werden können.

Prinzipiell sollten in der Fernwartung nur solche Tätigkeiten durchgeführt werden, die keine erneute Risikoanalyse zur Folge haben. Kommt es beispielsweise im Programmablauf zu Änderungen, die in der Risikoanalyse der ursprünglichen Konfiguration nicht berücksichtigt wurden, so ist diese erneut durchzuführen. Um dies sicherzustellen, sollten Eingriffe dieser Art nur vor Ort durchgeführt werden.

Wie in Kapitel 4.2.3 beschrieben, sollte die SIS so abgegrenzt werden, dass ein Erreichen über den Fernwartungszugang nicht möglich ist. Daher ist davon abzuraten, sämtliche Tätigkeiten, die ein Eingreifen in die SIS erfordern, via Fernwartung durchzuführen, auch wenn aufgrund der vorliegenden Konfiguration diese Möglichkeit besteht.

Die im Zuge dieser Arbeit durchgeführten Gespräche und Recherchen haben ergeben, dass die Fernwartung sehr erfolgreich im Zusammenhang mit User-Trainings eingesetzt wird. Das Unternehmen „Robotiq“ schafft dadurch eine Möglichkeit, kostengünstig und ohne Reisetätigkeiten ihren Kunden eine Schulung durch entsprechende Experten anzubieten.[88]

Für geplante Routinewartung, wie die Pflege von Hardware, Firmware und Software bietet sich die Fernwartung an, da diese Prozesse sehr gut planbar und innerhalb fest definierter Abläufe durchführbar sind. Wichtig ist hierbei, das Schutzziel der Verfügbarkeit zu berücksichtigen, da beispielsweise fehlerhafte Updates zu einem Ausfall der Anlage führen können. Die Analyse und Behebung von Fehlerfällen sowie die Konfiguration von Komponenten, die schnell realisiert werden muss, stellt ebenfalls einen beliebten Anwendungsfall einer Fernwartung dar. Da es sich hierbei um kurzfristig und meist ungeplante Aktivitäten handelt,

[88] lt. Interview P.Guerin, Applikationsingenieur bei Robotiq am 15.02.2021

ist es wichtig, eine einfach handzuhabende, ausreichend evaluierte und zuverlässige Fernwartungslösung im Unternehmen integriert zu haben. Hier ist vor allem das Schutzziel der Vertraulichkeit zu beachten, da unter Umständen externe Servicemitarbeiter Zugriff zu vertraulichen Daten erlangen können.[89]

Eine Besonderheit, die oftmals im direkten Zusammenhang mit Fernwartungstools steht, stellt die Betriebsdatenerfassung für Services, wie „Smart Maintenance“ dar. Hierbei ist darauf zu achten, dass im Regelbetrieb nur Outbound Kommunikation zugelassen und sämtliche Inbound Verbindungen über Fernwartungszugänge nur dann freigeschaltet werden, wenn diese erforderlich sind.

5.3 Dokumentation eines Fernwartungsvorgangs

Im vorherigen Kapitel wurde bereits die Dokumentation einer Fernwartung erwähnt. Im Folgenden sollen Hinweise gegeben werden, was die wichtigsten Inhalte einer solchen Dokumentation sind und wer diese aufzubewahren hat.

Neben den wichtigsten Daten eines Protokolls, wie Zeit, Dauer, Ort, beteiligte Personen, ferngewartete Hardware, sind darüber hinaus vor allem Verbindungsdaten wichtiger Bestandteil einer Dokumentation.

- Die übermittelte Datenmenge, während eines Fernwartungsvorgangs, gibt Aufschluss über die durchgeführte Tätigkeit und hilft, Unregelmäßigkeiten zu erkennen. Wurde beispielsweise bei einer Fernwartung, in der nur einzelne Parameter geändert werden sollen, eine sehr große Datenmenge übertragen, ist dies ein Indiz für eine Unregelmäßigkeit, die genauer untersucht werden muss.

- Die IP-Adresse der beteiligten Geräte gibt unter anderem Aufschluss über den Ort, an dem sich die beteiligten Personen befinden und ist somit ein wichtiger Bestandteil jeder Dokumentation.

[89] Vgl. Bundesministerium für Wirtschaft und Energie, 2016, S. 63–64.

- Es muss eine Gegenüberstellung von alten und neuen, im Rahmen der Fernwartung adaptierten Werten enthalten sein. Dies hilft, um im Falle eines späteren Zwischenfalls eruieren zu können, wer wann welche Parameter geändert hat. Es müssen nicht nur der neue Zustand, sondern auch die Änderungen dokumentiert werden.

- Idealerweise sollte eine Video- und Audiodokumentation des Fernwartungsvorgangs erstellt und lokal abgespeichert werden. Es empfiehlt sich, eine Bildschirmaufnahme zu erstellen, bei der die Handlungen des Fernwartenden klar ersichtlich sind.

In jedem Unternehmen sollte es eine Institution geben (ein Beauftragter/eine Abteilung), die diese Dokumentationen verwaltet und deren einheitliches Erscheinungsbild sicherstellt. Es empfiehlt sich, als Anlagenbetreiber diese Dokumentation über die gesamte Lebensdauer der Anlage zu verwahren.

5.4 Betriebsart Fernwartung

Die technische Dokumentation muss jede Betriebsart einer Anlage beschreiben. Somit sollte in dieser auch die Betriebsart „Fernwartung“ enthalten sein. Darin muss die Vorbereitung der Anlage für die Fernwartung eindeutig und ausführlich beschrieben sein. Für den Übergang in den Betriebsmodus „Fernwartung“ ist der in Kapitel 4.1.1 beschriebene sichere Zustand verpflichtend. Dieser dient als Freigabe für den Aufbau einer Fernwartungsverbindung. Ist es nicht möglich, diesen sicheren Zustand zu erreichen, muss die Wartung konventionell vor Ort beim Betreiber vorgenommen werden. Darüber hinaus sollen in der Beschreibung der Betriebsart weitere Aspekte enthalten sein:

- Anforderungen an die Ausbildung des Fernwartungsspezialisten und den lokalen Bediener

- Hinweise über Schulungen, die in regelmäßigen Abständen durchgeführt werden sollen, insbesondere im Fall von Software-Updates, Personalwechsel oder Hardwareänderungen. Es empfiehlt sich, Geräte und Software im Halbjahrestakt vor Ort zu überprüfen und zumindest einmal jährlich eine Evaluierung der Fernwartung mit einem Fernwartungsspezialisten durchzuführen.

- Hinweise zur Inbetriebnahme nach der Fernwartung

5.5 Zertifizierung eines Unternehmens nach ISO 27001

Um als Unternehmen unterschiedlicher Größe und Branche eine ausreichend hohe Datensicherheit unter der Berücksichtigung Vertraulichkeit, Verfügbarkeit und Integrität zu gewährleisten, stellt die Zertifizierung nach ISO 27001 einen sehr guten Anhaltspunkt dar. Durch Analyse der IST-Situation und Optimierung zur SOLL-Situation des IT-Systems werden Daten vor Hackerangriffen, Datenverlust oder missbräuchlichen Zugriffen geschützt. Darüber hinaus ist eine schnelle Wiederherstellung des Systems nach diesen Zwischenfällen gewährleistet.[90]

Die Zertifizierung führt zu einem Informationssicherheits-Managementsystem, das auf die Sparte des Unternehmens angepasst ist. Fernwartungen stellen ein Werkzeug dar, das einen großen Einfluss auf die IT eines Unternehmens hat und sollten daher im ISMS berücksichtigt werden. Als Anlagenbetreiber ist es wichtig, die Zertifizierung nach ISO 27001 zum einen im eigenen Unternehmen zu erhalten und diese zum anderen ebenso von jenen externen Unternehmen zu verlangen, die über Fernwartung Zugriff auf Anlagen innerhalb der eigenen Infrastruktur haben.

[90] Vgl. TÜV AUSTRIA CERT GMBH, 2018, S. 2.

6. Zusammenfassung

Die Untersuchungen zu dieser Masterarbeit haben gezeigt, dass Fernwartungen von Serienmaschinen, wie beispielsweise Spritzgießmaschinen oder standardisierten Werkzeugmaschinen bereits gut etabliert sind. Sondermaschinen, die meist nach Kundenwunsch konstruiert und individuell gefertigt werden, bestehen zum Teil aus Standardmodulen und Sonderanfertigungen. Auch Steuerungen und Anwendungsprogramme bestehen aus teilweise fertigen Bausteinen und neu geschriebener Software. Um die Kommunikation der diversen Elemente untereinander zu ermöglichen, werden diese mit Schnittstellen versehen, was zu einem vernetzten Gesamtsystem führt. Bei Sondermaschinen ist die Fernwartung daher ein komplexer, vor allem nicht standardisierter Prozess, der exakt auf die jeweilige Maschine abgestimmt sein muss. Es ist daher unabdinglich, auf ein sorgfältig entwickeltes Sicherheitsdesign und eine umfassend durchgeführte Risikoanalyse zu achten.

Das Thema Security im Zusammenhang mit Fernwartungen über das Internet spielt eine große Rolle und wird von allen Herstellern teilweise sogar mittels Zertifizierungen wie die ISO 27001 nachgewiesen. Das Thema Safety ist jedoch immer Sache des Anlagenbetreibers, der die ausreichende Arbeitssicherheit in Zusammenarbeit mit dem Systemintegrator gewährleisten muss. Es muss noch stärker das Bewusstsein geschaffen werden, dass nur eine Zusammenarbeit von Experten aus den Bereichen Safety und Security zu einer ausreichend hohen Gesamtsicherheit der Anlage führt. Die unterschiedlichen Herangehensweisen der beiden Bereiche führt naturgemäß zu Verständigungsproblemen, die die Zusammenarbeit nicht immer leicht machen. Es ist daher hilfreich, über regelmäßigen Kontakt eine gemeinsame Sprache und Arbeitsweisen zu entwickeln, damit die Anlagenbetreiber das bestmögliche gemeinsame Ergebnis, die maximale Anlagensicherheit auch bei Fernwartungen, erzielen können.

Um sowohl Rechts- als auch Arbeitssicherheit seiner Anlagen zu gewährleisten, sollte der Anlagenbetreiber auch den Überblick über Maßnahmen haben, die im Zuge einer Systemintegration ergriffen wurden. Der Systemintegrator spielt in diesem Zusammenhang eine entscheidende Rolle. Er ist verantwortlich für die Durchführung und die Aufbewahrung der Risikoanalyse, die im Fall eines

Zwischenfalls gerichtliche Verwertbarkeit besitzt. Als Betreiber einer Anlage empfiehlt es sich, dieser Risikobeurteilung beizuwohnen und das fertige Dokument auch selbst zu speichern.

Bei vielen Unternehmen zeigt sich, dass ihr Anlagenpark aus Maschinen verschiedenster Hersteller besteht, die dann bei einer standardisierten Anbindung an IT-Netze ohne weitere Maßnahmen zu Gefährdungssituationen führen können. Gerade hier empfiehlt es sich, externe Firmen zur Hilfe zu nehmen, die mit der Vernetzung von Anlagen gut vertraut sind.

Die Thematik Fernwartung besitzt großes Potenzial bei der Einsparung von Reisekosten, dem Ausgleich von fehlendem Fachpersonal und der schnellen Fehlerbehebung. Unter Beachtung der wichtigsten, in dieser Arbeit erörterten, Aspekte stellt die Fernwartung als Tool ein Produkt dar, das die Konkurrenzfähigkeit eines Unternehmens steigert. Jedoch besitzt es auch ein Gefahrenpotenzial, das bei der Installation berücksichtigt und so gut es geht minimiert werden muss, um folgenschwere Zwischenfälle zu verhindern. Die Digitalisierung bringt neben der unbeabsichtigten Fehlhandlung auch beabsichtigte Manipulationen in die Betrachtung von Anlagengefährdungen mit und muss daher sowohl im Safety als auch im Security Bereich präventiv berücksichtigt werden.

Es wird verdeutlicht, dass Schwachstellen in der Fernwartungstopologie oftmals einfach zu beheben sind, wenn ein Bewusstsein vorherrscht, dass diese bestehen. Mittels einer sorgfältig geplanten Infrastruktur, deren wichtigste Aspekte in dieser Arbeit enthalten sind, können auch KMUs mit überschaubarem Aufwand eine sichere Fernwartung durchführen. Grenzen, die der aktuelle Stand der Technik setzt, sind aus aktueller Sicht nicht überwindbar und müssen berücksichtigt werden.

Literaturverzeichnis

Bendel, Oliver (2018): *Pflegeroboter*, Springer Fachmedien Wiesbaden, Wiesbaden

Bundesamt für Sicherheit in der Informationstechnik (2020a): *IT-Grundschutz-Kompendium*, 1. Aufl., Unternehmen und Wirtschaft, Bundesanzeiger Verlag, Köln

Burgdorf, Milan (2014): *IT-Sicherheitsmanagement als Controlling-Instrument*, in: Controlling, Heft 6/2014, S. 309–313

Buxbaum, Hans; Kleutges, Markus; Sen, Sumona (2018): *Full-Scope simulation of human-robot interaction in manufacturing systems*, in: IEEE (Hrsg.). 2018 Winter Simulation Conference (WSC), Gothenburg, S. 3299–3307

Conti, Sal (2017), Fernüberwachung: Laufzeiten verbessern und Expertenwissen standortunabhängig bereitstellen, in: Dankl, Andreas/Isopp, Jutta (Hrsg.), dankl+partner consulting gmbh: *Jahrbuch*: *Instandhaltungstage 2017*, Leykam Buchverlag, Graz, S.43-45

Franke, Jörg, et al. (2019), in: Müller, Rainer (Hrsg.): *Handbuch Mensch-Roboter-Kollaboration*, Hanser, München

Groš, Stjepan (2011): *Security risk assessment of TeamViewer application*, in: IEEE (Hrsg.), *Proceedings of the ITI 2011*: *33rd International Conference on Information Technology Interfaces*, Curran Associates, Cavtat, S. 103–108

Marouane, Chadly; Rott, Benno (2016): *Mobile Authentisierung im Unternehmensalltag*, in: Informatik-Spektrum, Heft 2/2016, S. 122–130

Nyambayar, Davaadorj, et al. (2017): *Education Method for Simultaneous Achievement of Safety and Security in the IoT Era*, in: Metropolitan College (Hrsg.). Proceedings of the Third International Conference on Information Security and Digital Forensics, Thessaloniki, S. S.1-22

Preiss, Reinhard (2017): *Methoden der Risikoanalyse in der Technik*: *Systematische Analyse komplexer Systeme*, 2., überarbeitete und ergänzte Auflage, Edition TÜV Austria, Wien

Rajaravivarma, V. (1997): *Virtual local area network technology and applications*, in: IEEE (Hrsg.), *Proceedings The Twenty-Ninth Southeastern Symposium on System Theory*, The Twenty-Ninth Southeastern Symposium on System Theory, IEEE Comput. Soc. Press, Cookeville, S. 49–52

Rusch, Tobias; Ender, Hannah; Kerber, Florian (2020): *Kollaborative Robotikanwendungen an Montagearbeitsplätzen*, in: HMD Praxis der Wirtschaftsinformatik, Heft 6/2020, S. 1227–1238

ABB (2021): *ABB Ability™ Connected Services*: *Längere Roboter-Lebenszyklen und optimale Leistung*, https://new.abb.com/products/robotics/de/service/connected-services [Stand 03.02.2021]

AUVA (2019): *Auszug aus der Statistik 2018*, https://www.auva.at/cdscontent/load?contentid=10008.633448&version=1563531738 [Stand 17.09.2020]

Berghoff, Tim (2021): *Wasserwerk: Angriff per Fernwartung*, https://www.gdata.de/blog/wasserwerk-angriff-per-fernwartung [Stand 08.03.2021]

Bundesamt für Sicherheit in der Informationstechnik (2017): *BSI-Standard 200-2*: *IT-Grundschutz-Methodik*, https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/Standard202/ITGStandard202_node.html [Stand 29.01.2021]

Bundesamt für Sicherheit in der Informationstechnik (2020b): *Kreuzreferenztabellen zum IT-Grundschutz-Kompendium*, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/krt2020_Excel.html;jsessionid=E5936D8F24DF0151C6B552FE6776993C.1_cid500 [Stand 29.01.2021]

Bundesamt für Sicherheit in der Informationstechnik (2021): *IT Grundschutz*: *Umsetzungshinweise zum Baustein OPS.2.4 Fernwartung*, https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/Umsetzungshinweise/umsetzungshinweise_node.html [Stand 21.06.2021]

Bundesministerium für Wirtschaft und Energie (2016): *IT-Sicherheit für die Industrie 4.0*: *Produktion, Produkte, Dienste von morgen im Zeichen globalisierter Wertschöpfungsketten*, Berlin,

https://www.bmwi.de/Redaktion/DE/Publikationen/Studien/it-sicherheit-fuer-industrie-4-0.pdf?__blob=publicationFile&v=4 [Stand 23.03.2021]

Cisco; Rockwell Automation (2019): *Network Security within a Converged Plant-wide Ethernet Architecture*, https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/5-1/Network_Security/WP/CPwE-5-1-NetworkSecurity-WP.pdf [Stand 05.03.2021]

Di Pinto, Alessandro; Dragoni, Younes; Carcano, Andrea (2018): *TRITON: The First ICS Cyber Attack on Safety Instrument Systems*: *Understanding the Malware, Its Communications and Its OT Payload*, Black Hat USA, https://www.nozominetworks.com////downloads/US/Nozomi-Networks-TRITON-The-First-SIS-Cyberattack.pdf [Stand 01.02.2021]

Ewon (2020): *Talk2M Secure Cloud Service for Industrial Remote Solutions*, https://www.hms-networks.com/docs/librariesprovider10/ewon-english/brochures/talk2m-brochure---v-3-2.pdf?sfvrsn=6cf60fd7_2 [Stand 03.02.2021]

Geiger, Marcus (2018): *Purdue Model: Wie Sie komplizierte Automatisierungsnetze anschaulich überblicken können*, https://www.sichere-industrie.de/purdue-model-wie-sie-komplizierte-automatisierungsnetze-anschaulich-ueberblicken-koennen/ [Stand 05.03.2021]

Geiger, Marcus (2019): *TRISIS – Wenn IT-Sicherheitsmängel die Safety beeinträchtigen*, https://www.sichere-industrie.de/trisis-wenn-it-sicherheitsmaengel-die-safety-beeintraechtigen/ [Stand 02.02.2021]

Harner, Andreas (2019): *Anwendungshinweis für die Normenreihe IEC 62351*: *Informationssicherheit in der Netz- und Stationsleittechnik*, https://www.dke.de/resource/blob/1806462/2d569bd41f55c4b1726cf33f46be491b/informationssicherheit-in-der-netz--und-stationsleittechnik-download-data.pdf [Stand 08.03.2021]

Malisa, Viktorio (2018): *Arbeit in der Industrie 4.0 sicher und gesund gestalten*, https://www.researchgate.net/publication/325999580_Arbeit_in_der_Industrie_40_sicher_und_gesund_gestalten [Stand 31.07.2020]

Obregon, Luciana (2015): *Secure Architecture for Industrial Control Systems*, https://www.sans.org/reading-room/whitepapers/ICS/paper/36327 [Stand 05.03.2021]

Robotiq (2019): *Insights Security Sheet*, https://blog.robotiq.com/hubfs/Support%20Documents/Security%20Sheet/Security-Sheet-Insights-EN.pdf [Stand 17.02.2021]

Robotiq (2021): *Homepage*, https://robotiq.com/de [Stand 17.02.2021]

Routeco GesmbH (2020): *Homepage*, https://www.routeco.com/de-at [Stand 30.01.2021]

Schnabel, Patrick (2020): *RAS - Remote Access Service*, https://www.elektronik-kompendium.de/sites/net/0907081.htm [Stand 09.09.2020]

Schrade, Karl (2015): *Sichere Fernwartung*: *BSI-ACS-Themenquartal-ICS Security*, https://docplayer.org/3037097-Sichere-fernwartung-bsi-allianz-fuer-cybersicherheit-themenquartal-ics-security-public-click-here-to-select-the-date-if-applicable-status-approved.html [Stand 30.07.2020]

Siemens AG (2010): *Industry Online Support*: *Produkt Support*, https://support.industry.siemens.com/cs/document/45619913/auslauferkl%C3%A4rung-des-sinaut-isdn-w%C3%A4hlmodem-md4?dti=0&lc=de-WW [Stand 10.02.2021]

Sittner, Felix u. a. (2014): *Entwicklung eines adaptiven Bandbreitenmanagement- und Sicherheitssystems für die industrielle Fernwartung*, https://docplayer.org/41133967-Entwicklung-eines-adaptiven-bandbreitenmanagement-und-sicherheitssystems-fuer-die-industrielle-fernwartung.html [Stand 18.05.2021]

Springer, Matthias (2016): *Was ist der Unterschied zwischen Safety und Security?*, https://www.tuev-nord.de/explore/de/erklaert/was-ist-der-unterschied-zwischen-safety-und-security/ [Stand 17.09.2020]

Teamviewer (2021): *Produktbeschreibung*, https://www.teamviewer.com/de/product-descriptions/ [Stand 12.02.2021]

Tosibox Oy (2021): *Homepage*, https://www.tosibox.com/ [Stand 30.01.2021]

TÜV AUSTRIA CERT GMBH (2018): *ISO 27001*: *Informationssicherheit – mit einer Zertifizierung auf der sicheren Seite*, https://www.tuv.at/fileadmin/user_upload/Factsheet_27001_Web_2018.pdf [Stand 22.06.2021]

ABB (2017): *Product manual - Connected Services*, Revision: B

Bundesamt für Sicherheit in der Informationstechnik (Hrsg.) (2017) BSI-Standard 200-3: *Risikoanalyse auf der Basis von IT-Grundschutz*

Deutsches Institut für Normung e.V. (Hrsg.) (2011). Norm DIN EN ISO 10218-1: *Industrieroboter - Sicherheitsanforderungen*: *Teil 1: Roboter*

Deutsches Institut für Normung e.V. (Hrsg.) (2011). Norm DIN EN ISO 10218-2: *Industrieroboter – Sicherheitsanforderungen*: *Teil 2: Robotersysteme und Integration*

Deutsches Institut für Normung e.V. (Hrsg.) (2011). Norm DIN EN ISO 12100:2011-03: *Sicherheit von Maschinen- Allgemeine Gestaltungsleitsätze*: *Risikobeurteilung und Risikominderung*

Deutsches Institut für Normung e.V. (Hrsg.) (2013). Technical Report DIN ISO/TR 14121-2: *Sicherheit von Maschinen - Risikobeurteiklung*: *Teil2: Praktischer Leitfaden und Verfahrensbeispiele*

International Electrotechnical Commission (Hrsg.) (2019). Technical Report IEC TR 63069: *Industrial-process measurement, control and automation – Framework for functional safety and security*

ÖVE Österreichischer Verband für Elektrotechnik (Hrsg.) (2009). Norm IEC/TS 62443-1-1: *Industrial communication networks - Network and system security*: *Part 1-1: Terminology, concepts and models*

ÖVE Österreichischer Verband für Elektrotechnik (Hrsg.) (2011). Norm ÖVE/ÖNORM EN 61508-1: *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme*: *Teil 1: Allgemeine Anforderungen*

ÖVE Österreichischer Verband für Elektrotechnik (Hrsg.) (2011). Norm ÖVE/ÖNORM EN 61508-4: *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme*: *Teil 4: Begriffe und Abkürzungen*

ÖVE Österreichischer Verband für Elektrotechnik (Hrsg.) (2020). Norm OVE EN IEC 62443-3-3: *Industrielle Kommunikationsnetze – IT-Sicherheit für Netze und Systeme*: *Teil 3-3: Systemanforderungen zur IT-Sicherheit und*

VDMA (Hrsg.) (2017). VDMA 66418: *Industrial Security*: *Grundlegende Anforderungen an die Security von Maschinen*

Abbildungsverzeichnis

Tabellenverzeichnis

Anhang A

Gefährdungsüberblick nach EN ISO 12100

	Gefährdung	Relevanz		Ursache
		Ja	Nein	
1 – Mechanische Gefährdungen	1.1 – Überfahren werden		x	
	1.2 – Weggeschleudert werden		x	
	1.3 – Quetschen	x		rasche, unvorhergesehen Bewegungen des Roboters
	1.4 – Schneiden oder Abschneiden	x		scharfe Kanten am Greifer
	1.5 – Einziehen oder Fangen	x		rasche, unvorhergesehen Bewegungen des Roboters
	1.6 – Erfassen	x		Unzureichende oder deaktivierte Schutzeinrichtung
	1.7 – Reiben oder Abschürfen	x		rasche, unvorhergesehen Bewegungen des Roboters
	1.8 – Stoß	x		rasche, unvorhergesehen Bewegungen des Roboters
	1.9 – Eindringen von unter Druck stehenden Medien		x	
	1.10 – Scheren	x		rasche, unvorhergesehen Bewegungen des Roboters
	1.11 – Ausrutschen, Stolpern, Stürzen	x		Bodenbeschaffenheit, Kabel, Betriebsmittel
	1.12 – Durchstich oder Einstich		x	
	1.13 – Ersticken		x	
	1.14 – Sonstiges		x	

2 – Elektrische Gefährdungen	Gefährdung	Relevanz		Ursache
		Ja	Nein	
	2.1 – Vebrennung		x	
	2.2 – Chemische Reaktionen		x	
	2.3 – Auswirkungen auf medizinische Implantate		x	
	2.4 – Tödlicher Stromschlag		x	
	2.5 – Stürzen, Weggeschleudert werden		x	
	2.6 – Feuer	x		unerwartetes Brennen von Teilen
	2.7 – Herausschleudern von geschmolzenen Teilen		x	
	2.8 – (Elektrischer) Schlag	x		Ausführung der Maschine
	2.9 – Sonstiges		x	

3 – Thermische Gefährdungen	Gefährdung	Relevanz		Ursache
		Ja	Nein	
	3.1 – Vebrennung		x	
	3.2 – Dehydrierung		x	
	3.3 – Unbehagen		x	
	3.4 – Erfrierung		x	
	3.5 – Verletzungen durch Strahlung von Wärmequellen		x	
	3.6 – Verbrühung		x	
	3.7 – Sonstiges		x	

4 – Gefährdungen durch Lärm	Gefährdung	Relevanz		Ursache
		Ja	Nein	
	4.1 – Unbehagen		x	
	4.2 – Bewusstseinsverlust		x	
	4.3 – Gleichgewichtsstörung		x	
	4.4 – Bleibender Gehörverlust		x	
	4.5 – Stress		x	
	4.6 – Tinnitus (Ohrensausen)		x	
	4.7 – Ermüdung		x	
	4.8 – Sonstiges		x	

5 – Gefährdungen d. Vibration	Gefährdung	Relevanz		Ursache
		Ja	Nein	
	5.1 – Unbehagen		x	
	5.2 – Erkrankungen der unteren Wirbelsäule		x	
	5.3 – Neurologische Erkrankungen		x	
	5.4 – Knochengelenkschaden		x	
	5.5 – Wirbelsäulenverletzung		x	
	5.6 – Gefäßerkrankung		x	
	5.7 – Sonstiges		x	

6 – Gefährdungen d. Strahlung	Gefährdung	Relevanz		Ursache
		Ja	Nein	
	6.1 – Verbrennung		x	
	6.2 – Augen- und Hautschädigung		x	
	6.3 – Auswirkungen auf die Fortpflanungsfähigkeit		x	
	6.4 – Mutation		x	
	6.5 – Kopfschmerzen, Schlaflosigkeit		x	
	6.6 – Sonstiges		x	

7 – Gefährdungen d. Materialien od. Substanzen	Gefährdung	Relevanz		Ursache
		Ja	Nein	
	7.1 – Atembeschwerden, Ersticken		x	
	7.2 – Krebs		x	
	7.3 – Korrosion		x	
	7.4 – Auswirkungen auf die Fortpflanzungsfähigkeit		x	
	7.5 – Explosion		x	
	7.6 – Feuer		x	
	7.7 – Infektion		x	
	7.8 – Veränderung des Erbguts		x	
	7.9 – Vergiftung		x	
	7.10 – Sensibilisierung		x	
	7.11 - Sonstiges		x	

8 – Ergonomische Gefährd.	Gefährdung	Relevanz		Ursache
		Ja	Nein	
	8.1 – Unbehagen	x		Durchführen von nicht geplanten Aufgaben
	8.2 – Ermüdung		x	
	8.3 – Störung des Bewegungsapparates		x	
	8.4 – Stress		x	
	8.5 – Alle weiteren Probleme als Folge menschlichen Fehlverhaltens		x	
	8.6 – Sonstiges		x	

9 – Einsatzumgebung	Gefährdung	Relevanz		Ursache
		Ja	Nein	
	9.1 – Vebrennung		x	
	9.2 – Leichte Erkrankungen		x	
	9.3 – Ausrutschen, Stürzen	x		Bodenbeschaffenheit, Kabel, Betriebsmittel
	9.4 – Ersticken		x	
	9.5 – Sonstiges		x	

10 – Kombination	Gefährdung	Relevanz		Ursache
		Ja	Nein	
	10.1 – Dehydrierung		x	
	10.2 – Bewusstseinsverlust		x	
	10.3 – Hitzeschock		x	
	10.4 – Sonstiges		x	

Mögliche Gefährdungen speziell im Zusammenhang mit Maschinen

11 – Form/Oberflächenbeschaffenheit	Relevanz		Ursache
	Ja	Nein	
11.1 – Kontakt mit rauen Oberflächen		x	
11.2 – Kontakt mit scharfen Kanten und Ecken, vorstehenden Teilen	x		Greifer, Werkzeuge, Maschinenbett

12 – Bewegliche Teile	Relevanz		Ursache
	Ja	Nein	
12.1 – Zugang zu / Kontakt mit beweglichen Teilen	x		Bedieneingriff in Arbeitsbereich
12.2 – Kontakt mit rotierenden offenen Enden	x		Bedieneingriff in Arbeitsbereich

13 – Kinetische Energie	Relevanz		Ursache
	Ja	Nein	
13.1 – Herabfallen oder Ausstoß von Objekten	x		offener Eingreifbereich für Bedienperson, Druckabfall, Kollision

14 – Standfestigkeit	Relevanz		Ursache
	Ja	Nein	
14.1 – Verlust der Standfestigkeit		x	

15 – Mechanische Festigkeit	Relevanz		Ursache
	Ja	Nein	
15.1 – Bruch während des Betriebs	x		Kollision des Roboters mit Betriebsmittel

16 – Pneumatik/Hydraulik	Relevanz		Ursache
	Ja	Nein	
16.1 – Verschieben sich bewegender Teile		x	
16.2 – Herausspritzen von Flüssigkeiten unter hohem Druck		x	
16.3 – Ungesteuerte Bewegungen	x		Druckabfall in der Pneumatik des Greifers, ungewollte Eingriffe des Fernwartenden

17 – Elektrik	Relevanz		Ursache
	Ja	Nein	
17.1 – Direkter Kontakt		x	
17.2 – Durchschlag		x	
17.3 – Lichtbogen		x	
17.4 – Feuer		x	
17.5 – Indirekter Kontakt		x	
17.6 – Kurzschluss		x	

18 – Steuerung	Relevanz		Ursache
	Ja	Nein	
18.1 – Herabfallen oder Herausschleudern eines sich bewegenden Maschinenteils	x		offener Eingreifbereich für Bedienperson
18.2 – Herabfallen oder Herausschleudern eines in der Maschine festgeklemmten Werkstücks	x		offener Eingreifbereich für Bedienperson
18.3 – Ausfall von Einrichtungen zum Anhalten von sich bewegenden Teilen	x		Steuerungslogik, Eingriffe des Fernwartenden
18.4 – Maschinentätigkeit als Ergebnis der Wirkungslosigkeit von Schutzeinrichtungen	x		Steuerungslogik, Eingriffe des Fernwartenden
18.5 – Ungesteuerte Bewegungen	x		Steuerungslogik, Eingriffe des Fernwartenden
18.6 – Unbeabsichtiger / unerwarteter Anlauf	x		Steuerungslogik, Eingriffe des Fernwartenden
18.7 – Weitere Gefährdungsereignisse durch Ausfälle oder unzureichende Konstruktion der Steuerung		x	

19 – Materialien und Stoffe	Relevanz		Ursache
	Ja	Nein	
19.1 – Kontakt mit Objekten hoher oder geringer Temperatur	x		Teile des Roboters können heiß werden
19.2 – Emission eines Stoffes, der gefährdend sein kann		x	
19.3 – Emission eines Geräuschpegels, der gefährdend sein kann		x	
19.4 – Emission eines Geräuschpegels, der zu Störungen der Sprachkommunikation führen kann		x	
19.5 – Emission eines Geräuschpegels, der zu Störungen akustischer Signale führen kann		x	
19.6 – Emission eines Schwingungspegels, der gefährend sein kann		x	
19.7 – Emission von Strahlungsfeldern, die gefährden sein können		x	
19.8 – Raue Umgebungsbedingungen		x	

20 – Beschaffenheit des Arbeitsplatzes	Relevanz		Ursache
	Ja	Nein	
20.1 – Übermäßige Anstrengung		x	
20.2 – Menschlicher Fehler	x		Konzentration, Übermüdung
20.3 – Verlust der direkten Sichtbarkeit des Arbeitsbereiches	x		Ungeeigneter Ort für Bauteile, die Zugang erfordern, unzureichend gestaltete Zustimmungseinrichtungen
20.4 – Schmerzhafte und ermüdende Körperhaltungen	x		Wartung
20.5 – Sich in hoher Frequenz wiederholende Tätigkeiten		x	

21 – Kombination von Gefährdungen	Relevanz		Ursache
	Ja	Nein	
21.1 – jede andere Auswirkung einer Kombination von Gefährdungen und Gefährdungssituationen	x		Robotersystem soll von einer Person gestartet werden, dieser Vorgang wird jedoch von einer anderen Person nicht erwartet

Anhang B

	Elementare Gefährdung nach IT-Grundschutz-Kompendium	Relevanz	Begründung	Grund-wert
G0.1	Feuer	Nicht	Im Falle eines Feuers wird keine Fernwartung durchgeführt	A
G0.2	ungünstige klimatische Bedingungen	Indirekt	Führen bei der Maschine zu Schäden, die nicht mit der Fernwartung in den Zusammenhang zu bringen sind	I,A
G0.3	Wasser	Indirekt	Wasserschaden beschädigt die Maschine, kann aber nicht durch eine Fernwartung hervorgerufen werden	I,A
G0.4	Verschmutzung. Staub, Korrosion	Indirekt	Kann zu Ausfall von Systemkomponenten führen, die eine Fernwartung notwendig machen	I,A
G0.5	Naturkatastrophen	Indirekt	In diesem Fall kommt es vermutlich zum Ausfall der gesamten Produktion und eine Fernwartung wird nicht stattfinden	A
G0.6	Katastrophen im Umfeld	Nicht	siehe G0.5	A
G0.7	Großereignisse im Umfeld	Nicht	siehe G0.5	C,I,A
G0.8	Ausfall oder Störung der Stromversorgung	Direkt	Unterbricht die Fernwartung (es muss eine Unterscheidung gemacht werden, ob die Unterbrechung vor Ort an der Maschine oder beim Servicetechniker stattfindet)	I,A
G0.9	Ausfall oder Störung von Kommunikationsnetzen	Direkt	siehe G0.8	I,A

G0.10	Ausfall oder Störung von Versorgungsnetzen	Direkt	siehe G0.8	A
G0.11	Ausfall oder Störung von Dienstleistern	Direkt	siehe G0.8	C,I,A
G0.12	Elektromagnetische Störstrahlung	Indirekt	Kann die Verbindung der Maschine in das interne Netzwerk beeinflussen, stört aber schon vor einer potentiellen Fernwartung die Funktion der Maschine	I,A
G0.13	Abfangen kompromittierender Strahlung	Indirekt	Vorrichtungen, die das vermeiden, müssen generell getroffen werden. Das Risiko wird durch die Fernwartung nicht erhöht.	C
G0.14	Ausspähen von Informationen (Spionage)	Direkt	Durch den Fernwartungszugang kann auf interne Daten zugegriffen werden	C
G0.15	Abhören	Nicht	Daten, die zur Fernwartung übertragen werden haben nicht den Nutzen um den Aufwand des Abhörens zu rechtfertigen	C
G0.16	Diebstahl von Geräten, Datenträgern oder Dokumenten	Direkt	Diebstahl von Fernwartungsequipment kann dann problematisch werden, wenn es sich beispielsweise um einen USB Schlüssel handelt, der den Besitzer ermächtigt, auf die Anlage zuzugreifen	C,A

G0.17	Verlust von Geräten, Datenträgern oder Dokumenten	Direkt	Fernwartungsequipment ist fest in der Anlage verbaut, Verlust kann dann problematisch werden, wenn es sich beispielsweise um einen USB Schlüssel handelt, der den Besitzer ermächtigt, auf die Anlage zuzugreifen	C,A
G0.18	Fehlplanung oder Fehlende Anpassung	Direkt	Sowohl bei Planung, Durchführung und Dokumentation kann fehlerhafte Planung schwerwiegende Folgen haben	C,I,A
G0.19	Offenlegung schützenswerter Informationen	Direkt	Durch Fernwartungszugänge kann auf geschützte Bereiche innerhalb des Netzwerks zugegriffen werden	C
G0.20	Informationen oder Produkte aus unzuverlässiger Quelle	Direkt	verwendete Hard- und Software muss vertrauenswürdig sein	C,I,A
G0.21	Manipulation von Hard- oder Software	Direkt	Manipulation kann zu Ausfällen der Maschine führen	C,I,A
G0.22	Manipulation von Informationen	Direkt	Maschinendaten können manipuliert werden	I
G0.23	Unbefugtes Eindringen in IT-Systeme	Direkt	Fernwartungszugang öffnet ungewollte Zugänge	C,I
G0.24	Zerstörung von Geräten oder Datenträgern	Direkt	unsachgemäßer Umgang führt schon vor der Fernwartung zu Schäden und muss unterbunden werden	A
G0.25	Ausfall von Geräten oder Systemen	Direkt	Fernwartung kann im Fehlerfall zum Ausfall der gesamten Anlage führen	A

G0.26	Fehlfunktion von Geräten oder Systemen	Indirekt	Führen zum Ausfall der Anlage unabhängig einer Fernwartung	C,I,A
G0.27	Resourcenmangel	Direkt	zu wenige geschulte Mitarbeiter für eine Fernwartung vor Ort	A
G0.28	Software-Schwachstellen oder -Fehler	Direkt	Fehlerhafte Fernwartungssoftware	C,I,A
G0.29	Verstoß gegen Gesetze oder Regelungen (Policy)	Direkt	Regelungen für die Fernwartung müssen eingehalten werden	C,I,A
G0.30	Unberechtigte Nutzung oder Administration von Geräten und Systemen	Direkt	Fernwartungszugriff kann ungewünscht erfolgen, wenn ein einseitiges starten der Fernwartung möglich ist.	C,I,A
G0.31	Fehlerhafte Nutzung oder Administration von Geräten und Systemen	Direkt	Fernwartungszugänge müssen mit dezidierten Regeln versehen sein	C,I,A
G0.32	Missbrauch von Berechtigungen	Direkt	Berechtigungen, welche im Zuge der Fernwartung erteilt werden, werden missbraucht	C,I,A
G0.33	Personalausfall	Direkt	Fällt das geschulte Personal aus, kann niemand eine Fernwartung durchführen	A
G0.34	Anschlag	Indirekt	Schäden, die bei einem Anschlag entstehen übersteigen diejenigen, die bei einer Fernwartung entstehen können	C,I,A

G0.35	Nötigung, Erpressung oder Korruption	Indirekt	Zielt nicht auf Fernwartung ab	C,I,A
G0.36	Identitätsdiebstahl	Direkt	Ein angbelicher Servicetechniker kann sich als solcher ausgeben und mit falscher Identität die Fernwartung durchführen.	C,I,A
G0.37	Abstreiten von Handlungen	Direkt	Der Fernwartende kann abstreiten, Änderungen in der Anlage durchgeführt zu haben	C,I
G0.38	Missbrauch personenbezogener Daten	Indirekt	für Fertigunganlagen nicht relevant	C
G0.39	Schadprogramme	Direkt	Durch die Fernwartung können Schadprogramme in die Anlage eingespielt werden	C,I,A
G0.40	Verhinderung von Diensten (Denial of Service)	Direkt	Die Anlage kann komplett blockiert sein, wenn entsprechende Schadprogramme installiert sind	A
G0.41	Sabotage	Direkt	Bewusste Sabotage im Rahmen einer Fernwartung kann zum Ausfall von Systemen führen	A
G0.42	Social Engineering	Indirekt	Zielt nicht auf Fernwartung ab	C,I
G0.43	Einspielen von Nachrichten	Direkt	Falsche Nachrichten können im Zuge der Fernwartung zu Fehlern führen	C,I
G0.44	Unbefugtes Eindringen in Räumlichkeiten	Indirekt	Zielt nicht auf Fernwartung ab	C,I,A

G0.45	Datenverlust	Direkt	Anlagendaten können verloren gehen, wenn vor der Fernwartung kein Backup gemacht wird und es zu einem Fehler während der Fernwartung kommt	A
G0.46	Integritätsverlust schützenswerter Informationen	Indirekt	kann durch die Fernwartung nicht beeinflusst werden	I
G0.47	Schädliche Seiteneffekte IT-gestützter Angriffe	Direkt	durch Eingriffe in die Anlage können andere Komponenten der Anlage beschädigt werden	C,I,A

Anhang C

	Gefährdung	**Eintrittshäufigkeit** mittel (m), selten (s), häufig (h), sehr häufig (sh)	**Auswirkungen/Schadenshöhe** vernachlässigbar (ver), begrenzt (beg), beträchtlich (bet), existenzbedrohend (exi)	**Beispiele für Auswirkungen und Schäden**	**Einteilung Security** gering (g), mittel (m), hoch (h), sehr hoch (sh)	**Beeinträchtigungs-möglichkeit von Safety Komponenten** keine (k), begrenzt (beg), indirekt (ind), direkt (dir)		**Auswirkungen/ Schadenshöhe der beeinflussten Safety-Funktion** vernachlässigbar (ver), begrenzt (beg), betrachtlich (bet), schwerwiegend (sch)		**Einteilung Safety&Security** gering (g), mittel (m), hoch (h), sehr hoch (sh)		**Einteilung Gesamt** gering (g), mittel (m), hoch (h), sehr hoch (sh)
G0.8	Ausfall oder Störung der Stromversorgung	m	bet	Hardware kann durch plötzlichen Stromausfall defekt werden	**m**	k		ver		**g**		**m**
G0.9	Ausfall oder Störung von Kommunikations-netzen	h	beg	Fernwartung bricht ab, Maschine steht	**m**	k		ver		**g**		**m**
G0.10	Ausfall oder Störung von Versorgungsnet-zen	m	beg	siehe G0.8	**g**	k		ver		**g**		**g**
G0.11	Ausfall oder Störung von Dienstleistern	m	beg	Fernwartung bricht ab oder ist nicht mög-lich	**g**	k		ver		**g**		**g**
G0.14	Ausspähen von Infor-mationen (Spionage)	m	exi	Diebstahl von Daten und geistigem Eigen-tum	**h**	k		ver		**g**		**h**

G0.16	Diebstahl von Geräten, Datenträgern oder Dokumenten	s	bet	materieller Verlust, möglicher Zugang zu IT Infrastruktur	**g**	ind	Mit Geräten und Dokumenten kann Unbefugter Zugang zu Safety Einrichtungen erhalten	sch	Dieb verfolgt Ziel der maximalen Beschädigung	**sh**		**sh**
G0.17	Verlust von Geräten, Datenträgern oder Dokumenten	s	bet	siehe G0.16	**m**	ind	siehe G0.16	beg	entsprechende User und Hardware muss gesperrt werden	**m**		**m**
G0.18	Fehlplanung oder Fehlende Anpassung	m	exi	Zugang zu umgebender IT Infrastruktur	**h**	dir	durch falsche Konfiguration können Safety Einrichtungen leicht erreichbar sein	bet	Eindringling verfolgt das Ziel der Beschädigung der Anlage	**sh**		**sh**
G0.19	Offenlegung schützenswerter Informationen	m	exi	Reputationsverlust	**h**	k		ver		**g**		**h**
G0.20	Informationen oder Produkte aus unzuverlässiger Quelle	m	bet	Zugang zu IT Infrastruktur über zweifelhafte Hardware	**m**	dir	durch mangelhafte Produkte können Safety Einrichtungen leicht erreichbar sein	bet	siehe G0.18	**sh**		**sh**
G0.21	Manipulation von Hard- oder Software	m	bet	Funktionsausfall von Hard- und Software	**m**	dir	Hard- und Software kann so manipuliert werden, dass Safety Einrichtungen beeinflusst sind	sch	Manipulierte Safety Einrichtung kann zu massiven Auswirkungen führen	**sh**		**sh**
G0.22	Manipulation von Informationen	m	bet	siehe G0.21	**m**	dir	Parameter können so manipuliert werden, dass Safety Einrichtungen beeinflusst sind	sch	siehe G0.21	**sh**		**sh**
G0.23	Unbefugtes Eindringen in IT-Systeme	s	exi	Löschen, Manipulation und Auslesen von Daten	**m**	beg	Zugang zu gesicherten Safety Komponenten möglich	beg	Eingriffe müssen korrigiert werden	**g**		**m**
G0.24	Zerstörung von Geräten oder Datenträgern	m	bet	materieller Verlust	**m**	k		beg		**g**		**m**
G0.25	Ausfall von Geräten oder Systemen	m	beg	Ausfall der Anlage	**g**	k		beg		**g**		**g**
G0.27	Resourcenmangel	h	bet	stark verzögerte Verbindung durch Bandbreitenmangel	**h**	dir	Verzögerung der Übertragung führt zu Gefährdungssituationen	bet	Roboter kann kollidieren	**sh**		**sh**

G0.28	Software-Schwachstellen oder -Fehler	h	bet	ermöglicht Angreifern ein Eindringen	**h**	dir	Ermöglichen Zugang zu Safety Funktionen	bet	Roboter kann Fehlfunktionen ausüben	**sh**		**sh**
G0.29	Verstoß gegen Gesetze oder Regelungen (Policy)	m	bet	Strafrechtliche Konsequenzen	**m**	k		ver		**g**		**m**
G0.30	Unberechtigte Nutzung oder Administration von Geräten und Systemen	h	bet	Personen bekommen Zugriffe ohne Berechtigung	**h**	beg	Ungeschultes Personal kann Zugriff auf Safety Einrichtungen erhalten	beg	versehentliche Fehler können Schäden verursachen	**g**		**h**
G0.31	Fehlerhafte Nutzung oder Administration von Geräten und Systemen	h	bet	siehe G0.30	**h**	dir	Geräte erhalten zu hohe Berechtigungen und können Safety Einrichtungen beeinflussen	bet	eröffnet Möglichkeiten für Angreifer die das Ziel der Beschädigung verfolgen	**sh**		**sh**
G0.32	Missbrauch von Berechtigungen	m	bet	Weitergabe von Daten an Dritte	**m**	ind	Person kann Berechtigungen nutzen um Safety Einrichtungen zu manipulieren	bet	Ungewollte Einblicke in Safety Bereiche	**h**		**h**
G0.33	Personalausfall	sh	beg	Aktivitäten müssen aufgeschoben werden	**h**	k		ver		**g**		**h**
G0.36	Identitätsdiebstahl	s	exi	Fremde Personen erhalten Zugang zu IT System	**m**	beg	Fremde Person gibt sich als Techniker aus und erhält Zugang	sch	Verfolgt das Ziel der maximalen Beschädigung der Anlage	**h**		**h**
G0.37	Abstreiten von Handlungen	m	beg	Fehler müssen gesucht werden, da Mitarbeiter seine Handlungen vertuschen will	**g**	k		ver		**g**		**g**
G0.39	Schadprogramme	h	bet	Anlagen können stillgelegt werden	**h**	dir	Safety Funktionen können beschädigt werden	sch	keine Schutz mehr durch Safety Funktionen	**sh**		**sh**
G0.40	Verhinderung von Diensten (Denial of Service)	m	bet	Verdienstausfall	**m**	dir	Ausfall von Safety Einrichtung kann schwere Folgen haben	sch	siehe G0.39	**sh**		**sh**
G0.41	Sabotage	m	bet	Ausfall von Systemen	**m**	dir	siehe G0.40	sch	siehe G0.39	**sh**		**sh**
G0.43	Einspielen von Nachrichten	m	beg	Manipulation von Daten	**g**	beg	falsche Parameter können eingespielt werden	bet	Schäden an der Anlage	**m**		**m**

G0.45	Datenverlust	m	bet	Verlust von Entwicklungsarbeit	**m**	k		ver		**g**		**m**
G0.47	Schädliche Seiteneffekte IT-gestützter Angriffe	s	bet	durch Angriff auf Büronetzwerk kann gesamter Server beschädigt werden	**m**	k		ver		**g**		**m**

Anhang D

	Gefährdung	Einteilung Gesamt ohne Zusatzmaßnahme gering (g), mittel (m), hoch (h), sehr hoch (sh)	Zusatzmaßnahme	Einteilung Gesamt mit Zusatzmaßnahme gering (g), mittel (m), hoch (h), sehr hoch (sh)
G0.8	Ausfall oder Störung der Stromversorgung	**m**	Verwendung einer unterbrechungsfreien Stromversorgung	**g**
G0.9	Ausfall oder Störung von Kommunikationsnetzen	**m**	Akzeptanz	**m**
G0.14	Ausspähen von Informationen (Spionage)	**h**	Segmentierung des Netzwerks sichere Protokolle Absicherung der Schnittstellen starke Authentisierungsmechanismen	**g**

G0.16	Diebstahl von Geräten, Datenträgern oder Dokumenten	**sh**	Beaufsichtigung oder Begleitung von Fremdpersonen Vergabe von Berechtigungen Schutz von sensiblen Informationen am Arbeitsplatz Geräteverwaltung Betriebsmittelverwaltung Reaktion auf Verletzungen der Sicherheitsvorgaben Kontrollgänge Geregelte Verfahrensweise beim Weggang von Mitarbeitern Vertraulichkeitsvereinbarungen für den Einsatz von Fremdpersonal Überprüfung der Vertrauenswürdigkeit von Mitarbeitern Vergabe von Zutrittsberechtigungen Ordnungsgemäße Entsorgung von schützenswerten Betriebsmitteln und Informationen Sicherheitsrichtlinie zur Informationssicherheit auf Auslandsreisen Verwendung von Sichtschutz-Folien Verwendung der Bildschirm-/Code-Sperre Mitnahme notwendiger Daten und Datenträger Geeignete Auswahl und Nutzung eines mobilen Arbeitsplatzes Regelungen für mobile Arbeitsplätze Zutrittsregelung und -kontrolle Sichern von dienstlichen Unterlagen am häuslichen Arbeitsplatz Verlust- bzw. Manipulationsmeldung Personalauswahl für administrative Tätigkeiten Sensibilisierung und Schulung der Mitarbeiter im Umgang mit Mobiltelefonen Fernlöschung und Außerbetriebnahme von Endgeräten Einsatz einer geschlossenen Benutzergruppe Verhaltensregeln bei Sicherheitsvorfällen Regelungen zur mobilen Nutzung von Laptops Verwendung einer Festplattenverschlüsselung Verwendung der Anmeldeinformationsverwaltung Verhinderung der Ausführung von Betriebssystemkommandos	**m**

			Hardwaretausch betroffener IT-Systeme Sicherheitsüberprüfung von Administratoren Regelungen für Wartungs- und Reparaturarbeiten Geregelte Einstellung von IT-Administratoren Keine Speicherung von Daten zur automatischen Anmeldung Sicherheitsrichtlinien für Laptops Geeignete Aufbewahrung von Laptops Sichere Grundkonfiguration für mobile Geräte	
G0.17	Verlust von Geräten, Datenträgern oder Dokumenten	**m**	Maßnahmen für G0.16 reduzieren auch dieses Risiko	**g**

G0.18	Fehlplanung oder Fehlende Anpassung	**sh**	Übernahme der Gesamtverantwortung für Informationssicherheit durch die Leitungsebene Benennung eines Informationssicherheitsbeauftragten Integration der Informationssicherheit in organisationsweite Abläufe und Prozesse Kontrolle der Wirksamkeit der Benutzertrennung am IT-System bzw. Anwendung Vorgehensweise und Konzeption der Prozesse beim Identitäts- und Berechtigungsmanagement Nutzung zertifizierter Standardsoftware Festlegung benötigter Sicherheitsfunktionen der Individualsoftware Geeignete und rechtskonforme Beschaffung Vereinbarungen zum Informationsaustausch mit Externen Durchführung von Penetrationstests Planung des Einsatzes der Fernwartung Absicherung der Schnittstellen zur Fernwartung Regelungen zu Kommunikationsverbindungen Fachgerechte Installation Sichere Installation und Konfiguration von IoT-Geräten Auswahl und Beschaffung geeigneter Fernwartungswerkzeuge Erstellung einer Richtlinie für die Fernwartung	**m**
G0.19	Offenlegung schützenswerter Informationen	**h**	Sicheres Systemdesign (z.B. Segmentierung) Berücksichtigung von Compliance-Anforderungen Festlegung zulässiger Empfänger	**g**

G0.20	Informationen oder Produkte aus unzuverlässiger Quelle	**sh**	Absicherung integrierter Fernwartungssysteme Verwaltung der Fernwartungswerkzeuge Einsatzfreigabe Beschaffungskriterien für IoT-Geräte Application Whitelisting Auswertung von Informationen aus externen Quellen Zertifizierte Produkte	**m**
G0.21	Manipulation von Hard- oder Software	**sh**	Nachweisbarkeit von administrativen Tätigkeiten Zugangsbeschränkungen für administrative Zugänge Einsatz von mitgelieferten Systemfunktionen zur Detektion Einsatz zusätzlicher Detektionssysteme Zentrale Detektion und Echtzeitüberprüfung von Ereignismeldungen Echtzeiterfassung und Alarmierung von irregulären Vorgängen Zusätzliche Verhinderung der Ausbreitung bei der Ausnutzung von Schwachstellen Einsatz eines Produkts zum Schutz vor Schadsoftware	**m**
G0.22	Manipulation von Informationen	**sh**	siehe G 0.21	**m**
G0.23	Unbefugtes Eindringen in IT-Systeme	**m**	Akzeptanz	**m**
G0.24	Zerstörung von Geräten oder Datenträgern	**m**	Akzeptanz	**m**
G0.27	Resourcenmangel	**sh**	Entwicklung eines Redundanzkonzeptes für Anwendungen Ausreichende Ressourcen für den IT-Betrieb Tests und Notfallübungen Auswahl geeigneter Kabeltypen	**m**

G0.28	Software-Schwachstellen oder -Fehler	**sh**	Anwendung von Testverfahren Test- und Abnahmeverfahren für neue Software Penetrationstest und Revision Regelmäßige Audits Regelmäßige Aktualisierung	**m**
G0.29	Verstoß gegen Gesetze oder Regelungen (Policy)	**m**	Akzeptanz	**m**
G0.30	Unberechtigte Nutzung oder Administration von Geräten und Systemen	**h**	Einweisung des Personals in den sicheren Umgang mit IT Geeignete Auswahl von Identitäts- und Berechtigungsmanagement-Systemen Dokumentation von IT-Administrationstätigkeiten Festlegung von Rollen und Verantwortlichkeiten Erstellung einer Sicherheitsrichtlinie für die Cloud-Nutzung regelmäßige Passwortänderung	**m**
G0.31	Fehlerhafte Nutzung oder Administration von Geräten und Systemen	**sh**	Ansprechpartner zu Sicherheitsfragen Schulung der Verantwortlichen Zentrale Administration von Laptops Netzsegmentierung Erstellung einer Konfigurations-Checkliste für Hardware	**m**
G0.32	Missbrauch von Berechtigungen	**h**	Etablieren einer Berechtigungsverwaltung Prüfung und Überwachung von Berechtigungen Stärkere Abschottung der Zonen Einschränkung des Zugriffs für Konfigurations- und Wartungsschnittstellen	**m**
G0.33	Personalausfall	**h**	Vertretungsregelungen und Notfallvorsorge	**m**
G0.36	Identitätsdiebstahl	**h**	Mehr-Faktor-Authentisierung Schutz der Administrationsschnittstellen Einsatz von Netzzugangskontrollen	**m**

G0.39	Schadprogramme	**sh**	Backups Schutz externer Schnittstellen Security-Tests Absicherung eingehender Kommunikation vom Internet in das interne Netz Physische Trennung von Sicherheitssegmenten Auswahl eines Virenschutzprogrammes für Endgeräte Auswahl eines Virenschutzprogrammes für Gateways und IT-Systeme zum Daten-austausch Meldung von Infektionen mit Schadprogrammen	**m**
G0.40	Verhinderung von Diens-ten (Denial of Service)	**sh**	Absicherung von Datei-Uploads und -Downloads Überwachung des Netzverkehrs von IoT-Geräten Einsatz von zertifizierten Produkten Festlegen der Firewall-Regeln	**m**
G0.41	Sabotage	**sh**	Deaktivierung nicht genutzter Dienste Deaktivierung nicht genutzter Benutzerkonten Nutzung sicherer Protokolle für die Übertragung von Informationen Zweckgebundene Nutzung der Hard- und Softwarekomponenten Trennung und Unabhängigkeit des SIS von der Umgebung Sichere Übertragung von Engineering Daten auf SIS Anzeige und Alarmierung von simulierten oder gebrückten Variablen Absicherung der Daten- und Signalverbindungen	**m**
G0.43	Einspielen von Nachrich-ten	**m**	Verbesserung durch Maßnahmen der anderen Gefährdungen	**g**
G0.45	Datenverlust	**m**	Backups	**m**
G0.47	Schädliche Seiteneffekte IT-gestützter Angriffe	**m**	Akzeptanz	**m**

Anhang E

Ref.-Nr.	Aufgabe	Gefährdungsbereich	Unfallszenario	
			Gefährdung	Gefährdungssituation
1.3 1.5 1.6 1.7 1.8 1.10	Händisches Eingreifen bei der Fernwartung	maximaler Arbeitsbereich d. Roboters	Quetschen Einziehen oder Fangen Erfassen Reiben oder Abschürfen Stoß Scheren	Der Roboter quetscht den Bediener gegen ein im Arbeitsbereich befindliches Objekt. Dieser kann den Not-Aus Taster nicht mehr erreichen. Bediener nähert sich dem Roboter während der Fernwartung zu dicht und wird erfasst, da Sicherheitsmechanismen deaktiviert wurden.
1.4 1.11 9.3 11.2	Fernwartung	gesamter Arbeitsbereich und Anlagenumgebung	Schneiden oder Abschneiden Ausrutschen, Stolpern, Stürzen Kontakt mit scharfen Kanten und Ecken, vorstehenden Teilen	Beim Ausweichen als Reaktion auf eine Bewegung des Roboters findet ein Kontakt mit scharfen Kanten statt oder der Bediener stolpert über am Boden liegende Gegenstände
2.8 12.1 12.2 19.1	Fernwartung	gesamte Anlage	elektrischer Schlag Zugang zu/Kontakt mit beweglichen/rotierenden, heißen/kalten Teilen	Für die Fernwartung geöffnete Bereiche, die im Regelbetrieb geschlossen sind, exponieren gefährliche Gegenstände
13.1 16.3 18.1 18.2 18.5	Fernwartung	gesamter Arbeitsbereich und Anlagenumgebung	Herabfallen oder Ausstoß von Objekten Ungesteuerte Bewegungen	Druckabfall oder öffnen eines Greifers durch Eingriffe des Fernwartenden, die vor Ort nicht erwartet werden.
8.1 20.4	Händisches Eingreifen bei der Fernwartung	gesamte Anlage	Unbehagen Schmerzhafte oder ermüdende Körperhaltung	Im Zuge der Fernwartung kann durch nicht geplante Eingriffe ein Zugang zu schwer erreichbaren Orten erforderlich sein.

Ref.-Nr.	Aufgabe	Gefährdungsbereich	Unfallszenario	
			Gefährdung	Gefährdungssituation
2.6	Fernwartung	gesamte Anlage	Feuer	Plötzliches Brennen von Bauteilen aufgrund eines technischen Defekts
15.1 20.2	Fernwartung	gesamte Anlage	Bruch während des Betriebs menschliche Fehler	Der Roboter kollidiert mit einem Gegenstand aus dem Arbeitsbereich, da der Fernwartende eine Bewegung injiziert hat, die zu einer Kollision führt.
18.3 18.4	Fernwartung	maximaler Arbeitsbereich des Roboters	Ausfall von Einrichtungen zum Anhalten von sich bewegenden TeilenMaschinentätigkeit als Ergebnis der Wirkungslosigkeit von Schutzeinrichtungen	Für die Fehlerbehebung über die Fernwartung kann es manchmal nötig sein, dass Schutzeinrichtungen deaktiviert werden. Dabei können Zwischenfälle passieren, die sonst von Schutzeinrichtungen verhindert werden.
20.3	Fernwartung, händisches Eingreifen bei der Fernwartung	gesamte Anlage	Verlust der direkten Sichtbarkeit des Arbeitsbereichs	Wenn die Bedienperson vor Ort mit für die Fernwartung nötigen Eingriffen beschäftigt oder von dritten abgelenkt wird, verliert sie den Überblick über die Anlage.
18.6 21.1	Fernwartung	gesamte Anlage	unbeabsichtigter/unerwarteter Anlauf	Der Fernwartende kann, ohne dass die Person vor Ort dies erwartet, die Anlage starten und somit eine Gefährdungssituation hervorrufen.

Anhang F

Ref.-Nr.	Risikoeinschätzung (vorher)					Risikominderung (Schutzmaßnahme)	Risikoeinschätzung (nachher)					Risikominderung ausreichend
	S	F	O	A	RI		S	F	O	A	RI	
1.3 1.5 1.6 1.7 1.8 1.10	2	1	2	1	**2**	Bewegung des Roboters ist nur dann möglich, wenn der Bediener vor Ort an einem sicheren Ort steht und die Bewegung mit einem Taster freigibt. Ist dies nicht möglich, darf keine Freigabe zur Bewegung des Roboters aus der Ferne gegeben werden. Der Roboter befindet sich dann in einem sicheren Zustand und ist gegenüber Bewegungen gesperrt.	2	1	1	1	**2**	Ja
1.4 1.11 9.3 11.2	2	1	2	2	**3**	Die Umgebung der Anlage muss vor Beginn der Fernwartung in einen sicheren Zustand gebracht werden. Ein Bewegungsraum rund um die gesamte Anlage von mindestens einem Meter muss sichergestellt werden. Innerhalb dieser Fläche dürfen keine spitzen, losen oder sperrigen Gegenstände liegen. Ist dies nicht möglich, darf keine Bewegung des Roboters über die Fernwartung möglich sein.	2	1	1	1	**2**	Ja
2.8 12.1 12.2 19.1	2	1	2	1	**2**	Regelmäßige Schulungen bezüglich elektrischer Sicherheit und Sensibilisierung mit der Thematik von geöffneten Anlagen. Sämtliche Schaltschränke versperren und nur in Anwesenheit von entsprechendem Fachpersonal öffnen.	2	1	1	1	**2**	Ja
13.1 16.3 18.1 18.2 18.5	2	1	2	2	**3**	Bevor mit der Fernwartung begonnen werden darf, muss der Roboter und die Anlage in einen sicheren Zustand überführt werden. Im Greifer befindliche Teile müssen entfernt und der Roboter in die Grundstellung überführt werden. Ist dies nicht möglich, darf keine Bewegung möglich sein.	2	1	1	1	**2**	Ja

Ref.-Nr.	Risikoeinschätzung (vorher)					Risikominderung (Schutzmaßnahme)	Risikoeinschätzung (nachher)					Risikominderung ausreichend
	S	F	O	A	RI		S	F	O	A	RI	
8.1 20.4	2	1	2	2	**3**	Schulungen zu Ergonomie am Arbeitsplatz, beispielsweise wie schwere Lasten zu heben sind. Geräte, die regelmäßigen Zugriff erfordern müssen gut zugänglich sein.	1	1	1	1	**1**	Ja
2.6	1	1	2	1	**1**	Handfeuerlöscher an der Anlage anbringen.	1	1	1	1	**1**	Ja
15.120.2	1	1	2	2	**1**	Kein Abschalten von Sicherheitsmechanismen während der Roboterbewegung aus der Ferne. Alternativ muss die Bewegung mit dem Drücken eines Tasters vor Ort ermöglicht und nur in reduzierter Geschwindigkeit ausgeführt werden. Sobald der Taster losgelassen wird, stoppt die Bewegung des Roboters.	1	1	1	2	**1**	Ja
18.3 18.4	2	1	2	2	**3**	Kein Abschalten von Sicherheitsmechanismen während der Roboterbewegung aus der Ferne. Alternativ muss die Bewegung mit dem Drücken eines Tasters vor Ort ermöglicht werden. Sobald der Taster losgelassen wird, stoppt die Bewegung des Roboters.	2	1	1	2	**2**	Ja
20.3	1	1	2	1	**1**	Änderungen über die Fernwartungsschnittstelle dürfen nur mit lokaler Bestätigung ermöglicht werden. Darin muss die Übersicht der Anlage, sowie die Plausibilitätskontrolle der Änderung quittiert werden.	1	1	1	1	**1**	Ja
18.6 21.1	2	1	2	2	**3**	Kein Starten von Programmen über die Fernwartungsschnittstelle, Bewegung nur mit reduzierter Geschwindigkeit und lokaler Bestätigung.	2	1	1	2	**2**	Ja