

Sachgebiet Maschinen, Robotik und Fertigungsautomation – Themenfeld Sicherheitssteuerungen und -komponenten

Stand: 31.03.2022 ENTWURF

Durch Fernwartung von Maschinen beziehungsweise deren Steuerungskomponenten sollen Ausfallzeiten auf ein Minimum begrenzt und Einsätze von Wartungspersonal vor Ort reduziert oder vermieden werden, um Zeit und Kosten zu sparen, zum Beispiel für die Anfahrt. Um eine solche Fernwartung zu ermöglichen, muss zwangsläufig eine Verbindung der vernetzten Steuerungskomponenten aus dem Maschinennetzwerk mit dem entfernten Netzwerk des Fernwartungs-Dienstleistenden über das öffentliche Internet hergestellt werden. Dadurch erhöht sich das Risiko für die Sicherheit im Sinn der IT-Security als auch im Sinn der Safety, also der Arbeitssicherheit von Beschäftigten im Betrieb. Das Risiko muss über geeignete Maßnahmen so gering wie möglich gehalten werden. Bedingt durch die typischerweise vorhandene Netzwerkinfrastruktur und IT-Security-Maßnahmen stehen Kleinbetriebe dabei vor größeren Herausforderungen als mittelständische oder Großbetriebe, die in der Regel über gut aufgestellte Fachabteilungen für die „Industrial IT-Security“ verfügen. Unter Beachtung einiger Grundregeln lässt sich jedoch auch mit beschränkten Mitteln eine sichere Fernwartung realisieren.

Inhaltsverzeichnis

1	Zielgruppe	1
2	Risiken und Anforderungen	3
3	Schutzmaßnahmen-Konzept	5
4	Zusammenfassung und Anwendungsgrenzen.....	8

1 Zielgruppe

Die Handlungshinweise und Empfehlungen richten sich vor allem an Betreiber, aber auch an Hersteller von Maschinen, die Steuerungs- und Kommunikationskomponenten integriert haben, die einen Zugriff aus der Ferne über Schnittstellen aus dem lokalen Maschinennetzwerk heraus ermöglichen. Sie richten sich außerdem an Fernwartungsdienstleistende und an alle, die Fernwartungslösungen anwenden.

1.1 Definition Fernwartung

Der gebräuchliche Begriff Fernwartung bezeichnet den Zugriff auf lokale Mess-, Steuer- und Regelungstechnik (MSR) einer Maschine oder Anlage über (Netzwerk-)Schnittstellen von außen. In der „Electropedia“ der International Electrotechnical Commission (IEC) wird der Begriff „Fernwartung“ als „Wartung mit ferngesteuerten Geräten“ beschrieben oder als „über ein Kommunikationsnetz durchgeführte Softwarewartung“ (übersetzt aus dem englischen Original) definiert. [1] In Anbetracht der Definition von Wartung, wie Sie im Kontext der Indu-

strie verstanden wird, nämlich als „Maßnahmen zur Verzögerung des Abbaus des vorhandenen Abnutzungsvorrats“ [2], wäre der Begriff „Fernzugriff“ treffender. Der Begriff „Ferndiagnose“ wird in diesem Zusammenhang ebenfalls verwendet. Er ist nicht scharf abgegrenzt, beschreibt aber in den meisten Fällen einen ausschließlich lesenden Fernzugriff. Aufgrund der weiten Verbreitung und Geläufigkeit wird nachfolgend der Begriff „Fernwartung“ für den lesenden und schreibenden Zugriff aus der Ferne verwendet. Weitere, häufig bedeutungsgleich verwendete Begriffe, vor allem auch im internationalen Sprachgebrauch, sind „Remote Service“, „Remote Access“, „Teleservice“, „ferngesteuerte Instandhaltung“, „Remote-Instandhaltung“ oder „Remote Maintenance“ [3].

Der Begriff der Fernwartung kann weiter in die „Aktive Fernwartung“ und die „Passive Fernwartung“ unterteilt werden. Bei der aktiven Fernwartung findet ein aktiver Zugriff auf die Steuerungskomponenten und deren Konfiguration aus der Ferne statt. Parameter der Steuerung können dabei direkt vom Fernwartungspersonal aus der Ferne verändert werden. Dem steht die passive Fernwartung gegenüber, bei der das Fernwartungspersonal aus der Ferne dem sachkundigen Personal an der Maschine Anweisungen erteilt, zum Beispiel per Telefon, und das Szenario über eine Bildschirmübertragung verfolgt. Die aktive Handlung wird jedoch vom Wartungspersonal auf Seiten des Betreibers vorgenommen. Der Unterschied gegenüber der aktiven Fernwartung besteht darin, dass die Person in der Ferne keine aktiven Handlungen an der Maschine vornehmen kann, also maximal ein lesender Fernzugriff auf die MSR-Technik besteht.

Die passive Fernwartung wird in einem knappen Exkurs (vgl. Abschnitt 1.3) betrachtet. Die Schrift befasst sich primär mit der aktiven Fernwartung.

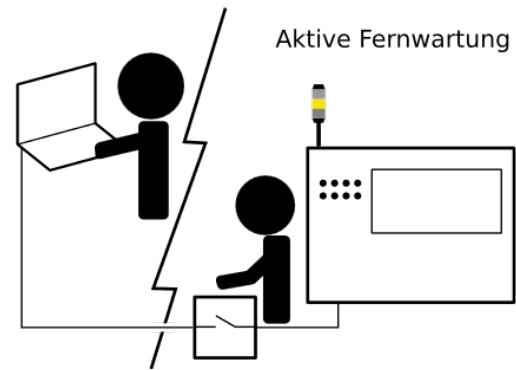


Abbildung 1 – Aktive Fernwartung – Der Betreiber hat Kontrolle über den Fernzugriff auf die Maschine, führt selbst aber keine Änderungen durch.

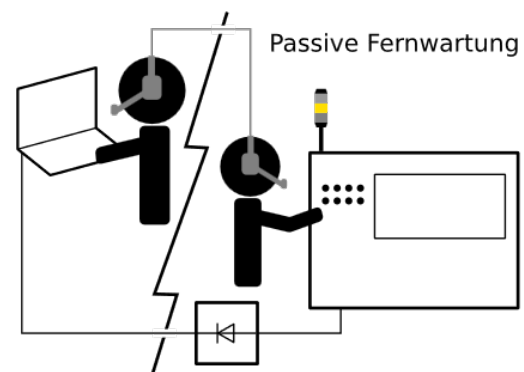


Abbildung 2 – Passive Fernwartung – Der Betreiber führt Wartung unter Anleitung eines Experten/einer Expertin (mit lesendem Zugriff auf die Maschine) durch.

1.2 Abgrenzung zur Ferndiagnose

Bei der Ferndiagnose, die es der Herstellfirma ermöglicht, im laufenden Betrieb der Maschine mit passiven Methoden, also ohne aktiven Eingriff auf die Maschinensteuerung, Daten zur Diagnose zu sammeln („Predictive Maintenance“ bzw. „Vorausschauende Wartung“, z. B. zur Früherkennung von Lagerschäden durch Analyse von Schwingungen an einer Welle), kann bei geschickter Hard- und Software-Architektur nur die Security, nicht jedoch die Safety, betroffen sein. Dazu können als „Daten-Dioden“ auch Optokoppler genutzt werden, die physikalisch eine Rückwirkung auf die Steuerungskomponenten ausschließen. Gelingt es, die Komponenten für die Ferndiagnose auf physikalischer Ebene so von den MSR-Komponenten der Maschine oder Anlage zu trennen, dass eine Rückwirkung sicher ausgeschlossen

werden kann, sind in Bezug auf die Arbeitssicherheit für den externen Zugriff keine Einschränkungen zu beachten.

1.3 Exkurs – passive Fernwartung

Bei der „Passiven Fernwartung“ (oft engl. als „Remote-Service“ bezeichnet) werden Informationen über den Zustand der Maschine oder der MSR-Komponenten (z. B. Video-Übertragung von Bildschirmhalten oder telefonische Übermittlung von gesetzten Parametern) ausschließlich „lesend“ an Fernwartungsdienstleistungen übertragen, ohne die Möglichkeit zu erhalten, aktiv (schreibend, verändernd) zuzugreifen zu können. Gleichzeitig erhält eine Person während der Instandhaltung an der Maschine von dieser Dienstleistungsfirma aus der Ferne Unterstützung und Instruktionen darüber, welche Änderungen aktiv vorgenommen werden sollen.[4] Die Übertragung der Instruktionen etc. kann zum Beispiel per Telefon, Videokonferenz oder Datenbrille erfolgen. Der Unterschied zur aktiven Fernwartung liegt darin, dass die Person in der Ferne keine aktiven Handlungen an der Maschine vornehmen kann. Sie muss aber die Person vor Ort sicher und kompetent anleiten, die Änderungen aktiv durchzuführen.

Wichtige Voraussetzungen zur sicheren Durchführung einer passiven Fernwartung:

Instand haltende Person

- kann falsche Anweisungen identifizieren,
- erkennt Gefährdungen bzw. Wechselwirkungen mit anderen Gefährdungen,
- kann sicher kommunizieren,
- beachtet ihre Sorgfaltspflicht.

Person mit Expertise in der Ferne (Remote)

- kennt Gefährdungen vor Ort,
- hat Aus- und Wechselwirkungen ihrer Instruktionen im Blick,
- hat Einblick in betriebliche Prozesse vor Ort,
- kennt die Qualifikation ihres Gegenübers,
- beachtet ihre erhöhte Sorgfaltspflicht.

Auch in diesem Fall gilt es, die Auswahl geeigneter Personen für die Durchführung von Instandhaltungstätigkeiten gemäß „Zusammenarbeit mehrerer Unternehmer“ (§ 6 DGUV Vorschrift 1) zu beachten. Weiterführende Informationen dazu gibt die Schrift FB HM 118 „Arbeitsschutzgerechter Einsatz von Datenbrillen“ im Abschnitt 4.1 „Exkurs: Assistenzsysteme und Verantwortung“.

2 Risiken und Anforderungen

2.1 Allgemeines

Beim Thema Fernwartung sind aus Sicht des Arbeitsschutzes sowohl Safety- als auch Security-Aspekte zu berücksichtigen. Die an Betreiber und Hersteller gerichteten gesetzlichen Anforderungen stehen sowohl in der Betriebssicherheitsverordnung und den zugehörigen Technischen Regeln, wie beispielsweise TRBS 1112, TRBS 1115 und TRBS 1115-1, als auch in der Maschinenrichtlinie beziehungsweise in der künftigen EU Maschinenverordnung, in der EU Verordnung über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik (EU Cybersecurity Act) und im angekündigten Gesetz über Cyberresilienz (EU Cyber Resilience Act).

Im Sinn des Arbeitsschutzes (Safety) darf es keine Möglichkeit geben, dass Steuerungskomponenten der Maschine durch Unbefugte manipuliert werden können. Bei der Fernwartung muss ein solcher unbefugter Zugriff von außen durch eine entsprechend starke Absicherung des Fernwartungszugangs (Security) verhindert werden. Die funktionale Sicherheit der Maschine darf nicht negativ beeinflusst werden. Daher gelten diese Anforderungen im Besonderen für Steuerungskomponenten, die in Sicherheitsfunktionen involviert sind. Sicherheitsrelevante Parameter, wie maximale Drehzahl eines CNC-Bearbeitungszentrums oder Grenzwerte für Druck und Temperatur, die die von Herstellfirmen festgelegten Grenzen überschreiten und deshalb zu einer Gefährdung

führen können, dürfen grundsätzlich nicht über Fernwartung verändert werden. Sollen im Ausnahmefall doch sicherheitsrelevante Parameter über einen Zugriff aus der Ferne verändert werden, ist ein Schutzmaßnahmenkonzept, wie in Abschnitt 3 beschrieben, erforderlich.

Die Anwendung von Fernwartung ist so zu begrenzen, dass sie nur für einen kurzzeitigen Zugriff auf die MSR-Komponenten eingesetzt wird. Die Fernwartung darf nicht regelmäßig oder dauerhaft als Zugriff auf MSR-Komponenten genutzt werden. Über eine Fernwartung findet keine Fernsteuerung statt. Außerdem sind über eine Fernwartung keine Aktionen erlaubt, die zu einer unmittelbaren Gefahr (Anlauf, unerwarteter Anlauf, Auslösen gefahrbringender Bewegungen, ...) an der Maschine oder Anlage führen könnten.[5]

2.2 Änderungen an Maschinen vor dem Hintergrund einer Fernwartung

In der Folge von Änderungen an Maschinen ergeben sich für die Beteiligten verschiedene Pflichten. Im Rahmen der Fernwartung sind dabei folgende Änderungen relevant:

- Änderung sicherheitsrelevanter Parameter
- Aufspielen einer neuen Software mit sicherheitsrelevanten Änderungen

Bei jeder Änderung einer Maschine ist zunächst zu bewerten, ob es sich um eine wesentliche Veränderung handelt (siehe Interpretationspapier des BMAS [6]). Wird die Schwelle zur wesentlichen Veränderung überschritten, wird die Person oder Institution, die die Änderungen vornimmt, zum neuen Hersteller der Maschine und muss ein neues Konformitätsbewertungsverfahren nach aktueller Maschinenrichtlinie durchführen.

Speziell zum Thema Software wird im „Blue Guide“ („Leitfaden für die Umsetzung der Produktvorschriften der EU 2022“) der Europäischen Kommission ausgeführt:

„Softwareaktualisierungen oder -reparaturen könnten Instandhaltungsarbeiten gleichgesetzt werden, sofern sie ein bereits auf dem Markt befindliches Produkt nicht so verändern, dass die Konformität mit den geltenden Anforderungen beeinträchtigt werden kann. Wie bei physischen Reparaturen oder Änderungen sollte ein Produkt als durch eine Softwareänderung wesentlich verändert angesehen werden, wenn i) die Softwareaktualisierung die ursprünglich vorgesehenen Funktionen, die Bauart oder die Leistung des Produkts verändert und dies bei der ursprünglichen Risikobewertung nicht vorhergesehen wurde, ii) sich aufgrund der Softwareaktualisierung die Art der Gefahr geändert oder das Risikoniveau erhöht hat und iii) das Produkt bereitgestellt wird (oder in Betrieb genommen wird, wenn dies durch die spezifischen Harmonisierungsrechtsvorschriften der Union geregelt ist).“

Bei Anhang-VI-Maschinen, wie Pressen der Metallverarbeitung mit Handbeschickung und/oder Handentnahme oder Kunststoffspritzgieß- und Kunststoffformpressmaschinen mit Handbeschickung oder Handentnahme, muss der Hersteller außerdem sicherheitsrelevante Änderungen vor dem Ausrollen an die Kundin mit der benannten Stelle abstimmen, wenn das Konformitätsbewertungsverfahren EG-Baumusterprüfung angewendet worden ist. Erfolgt in diesem Fall die Veränderung sicherheitsrelevanter Software-Parameter oder sicherheitsrelevanter Software ohne Freigabe durch die benannte Stelle, erlischt die Prüfbescheinigung der EG-Baumusterprüfung.

Liegt keine wesentliche Veränderung vor, gelten weiterhin die Anforderungen der Betriebssicherheitsverordnung. Der Betreiber muss dann beurteilen, ob die Änderungen eine Folgewirkung auf die Sicherheit der Maschine haben und ob es sich somit um prüfpflichtige Änderungen handelt. Nach TRBS 1201 ist das beispielsweise beim Aufspielen einer neuen Software mit sicherheitsrelevanten Änderungen der Fall oder bei Änderung von Betriebsparametern, durch die die Sicherheit beeinflusst wird. Die erforderlichen Prüfungen müssen von

einer dazu befähigten Person durchgeführt werden. Dazu gehören auch umfassende Funktionstests der Sicherheitsfunktionen nach dem Einspielen.

Die neue ISO 13849-1 erlaubt Änderungen an „safety-related Software“ per Fernwartung nur dann, wenn eine lokale Validierung durchgeführt wird. Kann eine Validierung vor Ort nicht sichergestellt werden, dürfen Änderungen an „safety-related Software“ per Fernwartung nicht möglich sein. [7]

3 Schutzmaßnahmen-Konzept

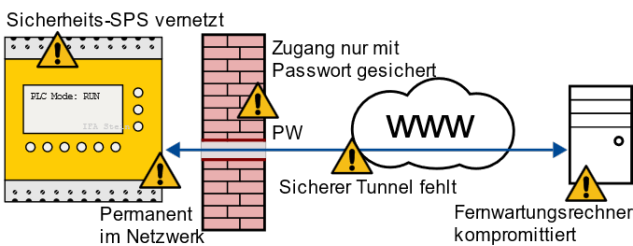


Abbildung 3 – Einige typische Schwachstellen einer Industriesteuerung mit Fernwartungslösung: programmierbare Sicherheitssteuerung verfügt über einen Netzwerkanschluss und ist über das Internet zur Fernwartung über einen fremden Rechner erreichbar

Das Schutzmaßnahmen-Konzept folgt der hierarchischen Anwendung des TOP-Prinzips. Demnach sind vorrangig technische Maßnahmen zu treffen und gegebenenfalls durch organisatorische und persönliche Maßnahmen zu ergänzen.

3.1 Technische Maßnahmen

Grundsätzlich ist es für eine Fernwartung nötig, eine Verbindung herzustellen: vom Hersteller-/vom Fernwartungsdienstleistenden in das interne Netzwerk des Betreibers, bis hinein in das Maschinennetzwerk auf der Steuerungs- und der Feldebene. Für den Aufbau des Netzwerks beim Betreiber ist eine Vielzahl möglicher Architekturen denkbar, wie Netzwerksegmentierungen, virtuelle Netzwerke etc.

Entsprechend vielfältig sind die Möglichkeiten, durch die jeweiligen Netzwerksegmente und Zonen hindurch eine Verbindung zur Fernwartung herzustellen. Daraus resultieren ebenso vielfältige Konstellationen in Bezug auf die Verantwortung der Hersteller, Fernwartungsdienstleister und Betreiber für die IT-Sicherheit und Pflege der einzelnen eingesetzten Komponenten. Sie sind daher im Einzelfall zu prüfen und entsprechend zu bewerten.

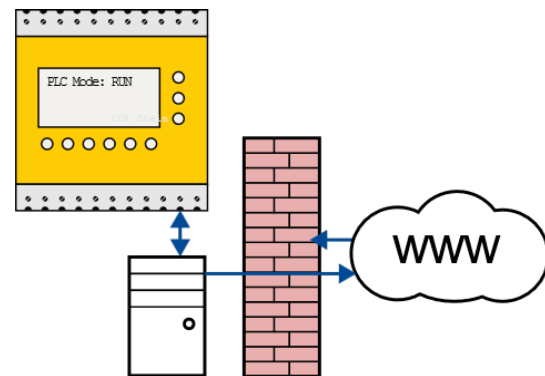


Abbildung 4 – Sicherheitssteuerung ist mit Rechner verbunden – innerhalb einer demilitarisierten Zone sind beide durch Firewall geschützt: Wird der Rechner durch eine Schadsoftware kompromittiert, kann ein Tunnel die Firewall öffnen und die Steuerung angegriffen werden.

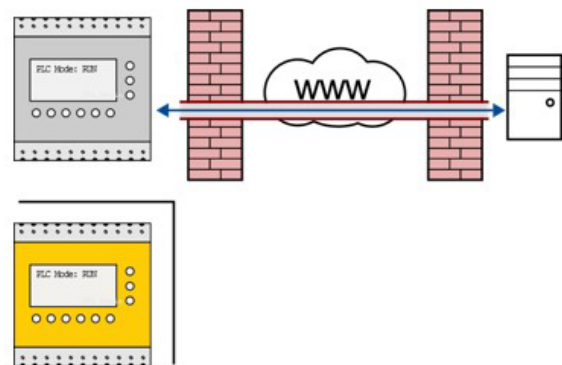


Abbildung 5 – Steuerung der Maschine rückwirkungsfrei von Sicherheitssteuerung in Fernwartungslösung integriert: Produktionsdaten können ausgelesen und Rezepte angepasst werden (Kriterium der wesentlichen Änderung nicht erfüllt), sicherer Tunnel verbindet Steuerung mit Fernwartungsrechner, der keine Verbindung zu anderen Netzen hat.

Der Betreiber richtet für die konkrete Fernwartung einen Zugang auf die Maschine mit einem Verfahren zur Authentifizierung und Autorisierung der fernwartenden Person ein. Dazu bietet sich ein Login mit Benutzername und Passwort oder Public-Private-Key-Verfahren an. In diesem Zusammenhang dürfen nur Zugangsverfahren genutzt werden, die auf dem Stand der Technik sind, also keine bekannten Schwachstellen haben, und eine Ende-zu-Ende Verschlüsselung nutzen.

Zusätzlich sollte nach dem Minimale-Rechte-Prinzip („principle of least privilege“) vorgegangen werden. Das bedeutet: Nur die zur Erfüllung der Fernwartungs-Aufgabe benötigten Berechtigungen auf dem Zielsystem dürfen an die fernwartende Person vergeben werden. Das setzt allerdings voraus, dass ein Rechte- und Rollensystem vorhanden ist, das detailliert konfiguriert werden kann.

Analog zum Minimale-Rechte-Prinzip muss auch das Zeitfenster, in dem Verbindungen möglich sind, durch Hardware- oder Softwarelösungen auf das notwendige Minimum reduziert werden. Das Beenden eines Fernwartungszugangs sollte klar definiert sein. Zur Beendigung werden eingerichtete Zugänge wieder geschlossen. Das bedeutet: Firewall-Regeln werden zum Beispiel zurückgesetzt oder Benutzeraccounts deaktiviert. Um das „Vergessen“ offener Zugänge zu vermeiden, sollte eine automatische Rücksetzung, zum Beispiel nach 30 Minuten Inaktivität, spätestens aber nach 8 Stunden, konfiguriert sein (automatisches Timeout). Außerdem sollte es nicht möglich sein, dass über die Fernwartung einer Maschine auf andere IT-Systeme oder Maschinen der Institution zugegriffen werden kann. [8]

Grundsätzlich sollte bereits eine möglichst sichere Netzwerkarchitektur vorliegen, also eine sinnvolle, aber restriktive Netzwerksegmentierung existieren, in der im Bedarfsfall eine Zone für die Fernwartung eingerichtet werden kann, die wiederum vom übrigen Netz-

werk durch eine Firewall abgeschirmt ist („Fernwartungszone“). Es bietet sich an, die Fernwartung per Rendezvous-Prinzip über „Kopplungsserver“ in einer demilitarisierten Zone (DMZ) des Unternehmensnetzwerks zu initiieren. Die fernwartende Person verbindet sich dabei von außen per VPN-Tunnel auf den Kopplungsserver und der Betreiber verbindet daraufhin die zu wartende Maschine per VPN-Tunnel mit dem Kopplungsserver. Alternativ kann, vor allem für kleinere Betriebe, die keine umfangreiche Netzwerk-Infrastruktur bereithalten können, der Einsatz von „Verschlüsselungs-Boxen“ (VPN) als Hardware ein geeignetes Mittel sein. Die Boxen könnten über vertrauenswürdige Dienstleistende für den temporären Fernwartungs-Einsatz bereits konfiguriert bezogen werden. Ein nützlicher Anhaltspunkt für die Auswahl geeigneter Hardware ist die Liste des Bundesamts für Sicherheit in der Informationstechnik (BSI) [9].

Der Verbindungsaufbau zur Fernwartung darf nur von der Betreiberseite aus initiiert werden können und sollte an der Maschine durch eine aktive Handlung bestätigt werden („von innen nach außen“). [10] Dadurch kann der Betreiber seinen gesetzlichen Pflichten nachkommen (z. B. Gefährdungsbeurteilung prüfen und ggf. anpassen, Prüfungen und Validierungen vornehmen) bevor die Maschine wieder in Betrieb genommen wird. Ein Fernwartungszugang über unmittelbar mit der Steuerung der Maschine verbundene, dedizierte Gateways (Mobilfunk-Router, separater Internetzugang), die nicht der permanenten Kontrolle des Betreibers unterliegen, ist grundsätzlich abzulehnen.

Die Fernwartung darf nur über Rechner mit einem Betriebssystem durchgeführt werden, das noch aktiv vom Hersteller mit Sicherheitsupdates versorgt wird und sich auf dem neuesten Update-Stand befindet. Ähnliches gilt für die übrigen Software-Komponenten des betreffenden Rechners. Deshalb muss gegebenenfalls das Einspielen von aktuellen security-relevanten Updates/Patches vor der Einrich-

tung von Fernwartungszugängen beachtet werden, um möglicherweise bestehende Lücken in der Absicherung zu schließen. Meldungen seitens der Hersteller oder CVE-Listen (Common Vulnerabilities and Exposures, siehe z. B. <https://www.cve.org/>) müssen deshalb beachtet werden. Es ist sicherzustellen, dass die eingesetzten Komponenten (Rechner, Datenträger, Virtuelle Maschinen, HMI, SPS, Gateways, ...) frei von Schadsoftware sind. Außerdem sollte der Wartungsrechner keine, für die Fernwartung unnötigen, Dienste und Programme installiert haben.

Zur Authentisierung/Authentifizierung der fernwartenden Person gegenüber dem zu wartenden System sollten keine einfachen Benutzername/Passwort-Verfahren zum Einsatz kommen, sondern Zwei-Faktor- beziehungsweise Multi-Faktor-Verfahren, zum Beispiel bestehend aus Smartcard und PIN, auf dem aktuellen Stand der Technik. Dadurch werden Angriffe, die durch gestohlene oder abgehörte Zugangsdaten möglich wären, durch einen weiteren Faktor (z. B. Besitz der Smartcard und Wissen über die dazugehörige PIN), verhindert. Unsichere Passwörter sind als Sicherheitsrisiko bekannt. Die Authentifizierung über ein Passwort kann durch kryptographische Hardware (z. B. Security-Token, HSM, Smart-Card) ersetzt werden.

Für die eindeutige Protokollierung sind personalisierte Zugänge zu nutzen, damit jederzeit nachvollzogen werden kann, wer zu welchem Zeitpunkt welche Änderung am Zielsystem vorgenommen hat. Die für die Protokollierung nötigen Log-Dateien werden zentral, außerhalb des Einflussbereichs der fernwartenden Person, gesammelt und gegebenenfalls automatisiert ausgewertet (permanentes Monitoring).[11]

3.1.1 Technische Beschaffenheitsanforderungen

Die technischen Maßnahmen für eine sichere Fernwartung:

- Vorhandensein einer sicheren, segmentierten Netzwerkstruktur
- Auswahl einer geeigneten Architektur für den Fernwartungszugang
- Einsatz einer kryptografisch abgesicherten Verbindung auf dem Stand der Technik
- Einsatz von anerkannten Verfahren zur Authentifizierung und Autorisierung auf dem Stand der Technik, möglichst mit zweitem Faktor
- Vorgehen nach dem Minimale-Rechte-Prinzip
- Die Fernwartung darf nur vom Betreiber initiiert werden können, im Idealfall direkt an der konkreten Maschine oder zumindest von einem Rechner in örtlicher Nähe zur Maschine und muss an der Maschine durch eine aktive Handlung bestätigt („von innen nach außen“) werden.
- Zeitliche Limitierung der Fernwartungszugänge; sie dürfen nicht permanent bestehen bleiben und sind durch ein initial definiertes Timeout zeitlich begrenzt.
- Zugangsberechtigungen müssen dokumentiert sein, sodass der Betreiber einen Überblick über alle bestehenden Zugänge hat.
- Fernwartungssitzungen müssen dokumentiert werden (Zeitstempel An- und Abmeldung, Benutzende, Maschine, ...)
- Durchgeführte Änderungen müssen nachvollziehbar sein (z. B. automatisierte Aufzeichnung).
- An der Maschine muss zwangsläufig signalisiert werden, wenn eine Fernwartung aktiv ist.
- Die betreffende Maschine muss eindeutig zur Fernwartung ausgewählt werden.
- Not-Halt und Sicherheitsfunktionen haben stets Vorrang vor Fernwartungs-Befehlen bzw. dürfen durch die Fernwartung nicht beeinflusst werden.
- Das Aussetzen oder Rücksetzen von Sicherheitsfunktionen und Schutzeinrichtungen darf nicht aus der Ferne möglich sein.

- Durch die Fernwartung dürfen weder die Steuerbefehle „Spannung ein“ noch „Betriebsartenwahl“ möglich sein.

3.2 Organisatorische Maßnahmen

Abseits von technischen Maßnahmen müssen als organisatorische Maßnahmen folgende Grundprinzipien beachtet werden:

- Die Fernwartung ist im Rahmen der Gefährdungsbeurteilung zu berücksichtigen.
- Eine Fernwartung findet nicht im regulären, produktiven Betrieb statt. Die Maschine ist zuvor in einen zur Fernwartung geeigneten, jedoch sicheren Zustand (Schutzeinrichtungen aktiv, Zugangsschutz, ...) zu versetzen.
- Die Maschine muss entsprechend gekennzeichnet sein, damit es auch für Dritte leicht zu erkennen ist, dass sie sich „in Fernwartung“ befindet. Ein Betreten der Gefahrenbereiche ist durch eine entsprechende Absicherung zu verhindern.
- Es muss während des Fernwartungsvorgangs permanent fachkundiges Personal vor Ort sein, das im Notfall eingreifen kann.
- Bei Beendigung der Fernwartung und Trennung der Verbindung erscheint eine entsprechende Meldung an der Maschine, die quittiert werden muss.
- Die Auswahl geeigneter Personen für die Durchführung von Instandhaltungstätigkeiten gemäß „Zusammenarbeit mehrerer Unternehmer“ (§ 6 DGUV Vorschrift 1) ist zu beachten und die Verantwortung der beteiligten Stellen ist zu klären.
- Je nach Situation sind weitere, über diese Auflistung hinausgehende, Maßnahmen zu treffen.

3.3 Persönliche Maßnahmen

Als persönliche Maßnahme muss, gemäß BetrSichV, eine Unterweisung der Beschäftigten durchgeführt werden:

- Es muss eine Betriebsanweisung für die Fernwartung (basierend auf der

Betriebsanleitung des Herstellers) erstellt werden, nach der die Beteiligten in die für sie geltenden Schutzmaßnahmen und das richtige Verhalten im Notfall unterwiesen werden.

4 Zusammenfassung und Anwendungsgrenzen

Unter Berücksichtigung technischer und organisatorischer Maßnahmen kann für Maschinen eine, sowohl im Sinn von „Safety“ als auch „Security“, sichere Fernwartung erreicht werden. Die Anforderungen aus diesen Maßnahmen sind essenziell für die Sicherheit und die Gesundheit, während der Arbeit mit Maschinen, auf die per Fernwartung zugegriffen werden kann.

Je nach Maschine oder Anlage (z. B. Maschinen in verfahrenstechnischen Anlagen) können gegenüber dieser Schrift weitergehende oder abweichende Anforderungen gelten. Beispielsweise wird in der hybriden Fernwartung mit einer Person vor Ort gemeinsam gearbeitet, wodurch sich das Risiko signifikant erhöht und noch mehr Maßnahmen, als hier beschrieben sind, erforderlich werden.

Diese „Fachbereich AKTUELL“ beruht auf dem zusammengeführten Erfahrungswissen vom Fachbereich Holz und Metall, vom Sachgebiet Maschinen, Robotik und Fertigungsautomation der Deutschen Gesetzlichen Unfallversicherung DGUV.

Die Schrift soll dazu dienen, sowohl Safety- als auch Security-Aspekte bei der Fernwartung von Maschinen und Anlagen zu berücksichtigen und notwendige Sicherheitsmaßnahmen umzusetzen und richtet sich gleichermaßen an Hersteller und Betreiber, die Anforderungen an die Gestaltung und die Anwendung von Fernwartung umzusetzen.

Die Bestimmungen nach einzelnen Gesetzen und Verordnungen bleiben durch diese Informationsschrift unberührt. Die Anforderungen

der gesetzlichen Vorschriften gelten uneingeschränkt. Um vollständige Informationen zu erhalten, ist es erforderlich, die infrage kommenden Vorschriftentexte einzusehen.

Diese „Fachbereich AKTUELL“ befindet sich in der Entwurfsfassung. Senden Sie bitte Ihre Stellungnahmen bis zum 25.05.2023 an die [Kommentaradresse](#).

Der Fachbereich Holz und Metall setzt sich unter anderem zusammen aus Vertretern und Vertreterinnen der Unfallversicherungsträger, der staatlichen Stellen, der Sozialpartner, der herstellenden und betreibenden Firmen.

Weitere DGUV-Kurzinformationen und Informationsblätter des Fachbereichs Holz und Metall stehen im Internet zum Download bereit. [12]

Literaturverzeichnis

[1]

<https://www.electropedia.org/iev/iev.nsf/display?openform&ievref=192-06-29>, abgerufen am 11.11.2022

[2] DIN 31051:2019-06 – Grundlagen der Instandhaltung, Beuth-Verlag, Berlin

[3] DIN EN 13306 :2018-02 Instandhaltung – Begriffe der Instandhaltung, Beuth-Verlag, Berlin

[4] BSI IT Grundschatz Kompendium Edition 2022 – vgl. OPS.1.2.5: Fernwartung, Bundesamt für Sicherheit in der Informationstechnik

[5] DIN EN ISO 14118:2018-07 Sicherheit von Maschinen – Vermeidung von unerwartetem Anlauf, Beuth-Verlag, Berlin

[6] Interpretationspapier zum Thema "Wesentliche Veränderung von Maschinen",

Bundesministerium für Arbeit und Soziales, 09.04.2015

[7] DIN EN ISO 13849:2016-06, Teil1, Sicherheit von Maschinen – Sicherheitsbezogene Teile von Steuerungen, Beuth-Verlag, Berlin

[8] BSI IT Grundschatz Kompendium Edition 2022, IND.2.4: Maschine, 3.1. Basis-Anforderungen, Bundesamt für Sicherheit in der Informationstechnik

[9] BSI-Schrift 7164: Liste der zugelassenen IT-Sicherheitsprodukte und -systeme

[10] TRBS 1115-1 Cybersicherheit für sicherheitsrelevante Mess-, Steuer- und Regeleinrichtungen, Abschnitt 4.5.2 Anforderungen an Cybersicherheitsmaßnahmen, Bundesanstalt für Arbeitsschutz und Arbeitsmedizin

[11] BSI IT Grundschatz Kompendium Edition 2022, IND.3.2.A13 i. V. m. OPS.1.1.2.A5

[12] Internet: www.dguv.de/fb-holzundmetall Publikationen oder www.bghm.de Webcode: <626>

Bildnachweis

Die gezeigten Bilder wurden freundlicherweise zur Verfügung gestellt von:

- Abbildungen 1-5 – Institut für Arbeitsschutz der DGUV (IFA)

Kommentaradresse

Fachbereich Holz und Metall
Sachgebiet Maschinen, Robotik und
Fertigungsautomation – Themenfeld
Sicherheitssteuerungen und -komponenten
Berufsgenossenschaft Holz und Metall
Vollmoellerstraße 11
70563 Stuttgart

Email: fb-holzundmetall@bghm.de

Die Fachbereiche der DGUV werden von den Unfallkassen, den branchenbezogenen Berufsgenossenschaften sowie dem Spitzenverband DGUV selbst getragen. Für den Fachbereich Holz und Metall ist die Berufsgenossenschaft Holz und Metall die federführende Unfallversicherungsträgerin und damit auf Bundesebene erster Ansprechpartnerin in Sachen Sicherheit und Gesundheit bei der Arbeit für Fragen zu diesem Gebiet.

An der Erarbeitung dieser Fachbereich AKTUELL haben mitgewirkt:

- BG ETEM
- BG N
- BG RCI
- IFA
- Phoenix Contact