BG ETEM
Energie Textil Elektro
Medienerzeugnisse

Fachtagung Digitale Arbeitswelt

Arbeitsschutz und Digitalisierung (Fernzugriff)

Dipl.- Ing. Klaus-Dieter Becker

02.09.2021

Erschreckende Nachrichten

Die Darkside-Gang erbeutete mit Randsomware-Angriffen mehr als **90 Millionen $** in den letzten neun Monaten

Security ist bereits ein Thema für alle Industriebetriebe

Bild: Fa. Pilz

Oktober 2019

Sämtliche IT Anwendungen wurden im Konzern lahmgelegt

- 2 Wochen Produktionsausfall
- Austausch von rund tausend Rechnern und hunderten von Datenträger weltweit

Motivation der Fernüberwachung (Anlagenüberwachung)

- Fernparametrierung (Veränderung einstellbarer Größen)
- Diagnose der Software (Erkennen von Fehlfunktionen)
- Software Updates (Aufspielen neuer Programme)
- Inbetriebnahme (Übertragung aller Software)
- Inspektion und Wartung (Auslesen von Fehlerspeichern, Betriebsstundenzählern, Programmwartung, etc.)
- Unterstützung der Instandsetzung / Umrüstung /Support
- Fehlfunktionsmanagement, Maschinendiagnose (Intelligente Fehlererkennung, Fehlercodes mit hinterlegten Maßnahmen)

Motivation der Fernüberwachung (Anlagenüberwachung)

- Fernauslösung (Starten von Fertigungsprozessen)
- Dokumentation (Erstellen von Auftragspapieren, Fertigungslogbücher für z.B. validierte Prozesse, etc.)
- Telemarketing (Ersatzteilversorgung, Feststellen gefertigter Stückzahlen, etc.)
- Teleteaching (z.B. Programmierungsunterstützung)
- Consulting / Beratung (z.B. Prozessoptimierung)

Europäische und nationale Rechtsgrundlagen für sichere Maschinen

Hersteller	**Betreiber**
Maschinenrichtlinie (98/37/EG bzw. 2006/42EG) ▪ Inverkehrbringen nach Artikel 95 EG Vertrag **(freier Warenverkehr)** ▪ Grundlegende Sicherheits- und Gesundheitsanforderungen zu Bau und Ausrüstung von Maschinen ▪ Umsetzung in nationales Recht in Deutschland durch Geräte- und Produktsicherheitsgesetz (9. Verordnung zum GPSG)	Arbeitsmittelbenutzungsrichtlinie (89/655/EWG) ▪ Benutzung von AM nach Artikel 138 EG Vertrag **(Arbeitnehmerschutz)** ▪ Mindestanforderungen an Arbeitsbedingungen in Bezug auf Sicherheit und Gesundheitsschutz ▪ Umsetzung in nationales Recht in Deutschland durch die Betriebssicherheitsverordnung (BetrSichV)

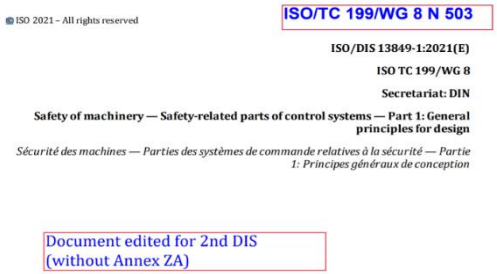
Entwurf Maschinenverordnung Anhang III

1.1.9 Schutz gegen Verfälschung

Das Maschinenprodukt muss so konstruiert und gebaut sein, dass der Anschluss einer anderen Einrichtung an das Produkt über eine beliebige Funktion der angeschlossenen Einrichtung selbst oder über eine mit dem Maschinenprodukt kommunizierende entfernte Einrichtung nicht zu einer gefährlichen Situation führt.

Ein Hardware-Bauteil für den Anschluss, das für die Übereinstimmung des Maschinenprodukts mit den einschlägigen Gesundheits- und Sicherheitsanforderungen von entscheidender Bedeutung ist, muss so konstruiert sein, dass es angemessen gegen unbeabsichtigte oder vorsätzliche Verfälschung geschützt ist.

Bild: it-daily.net



5.2.2.11 Fernzugriff

Ist eine Maschine für den **Fernzugriff ausgelegt**, muss das **SRP/CS** aktiviert bleiben. Alternative risikomindernde Maßnahmen können angewendet werden, wenn dies in der Benutzerinformationen angegeben ist.

Der Entwurf des **SRP/CS darf den Fernzugriff** auf eine Maschine nicht ohne besondere Maßnahmen zur Vermeidung von gefährliche Situationen zur Verfügung stellen, die durch die Anwesenheit von Personen in oder in der Nähe der Maschine entstehen können.

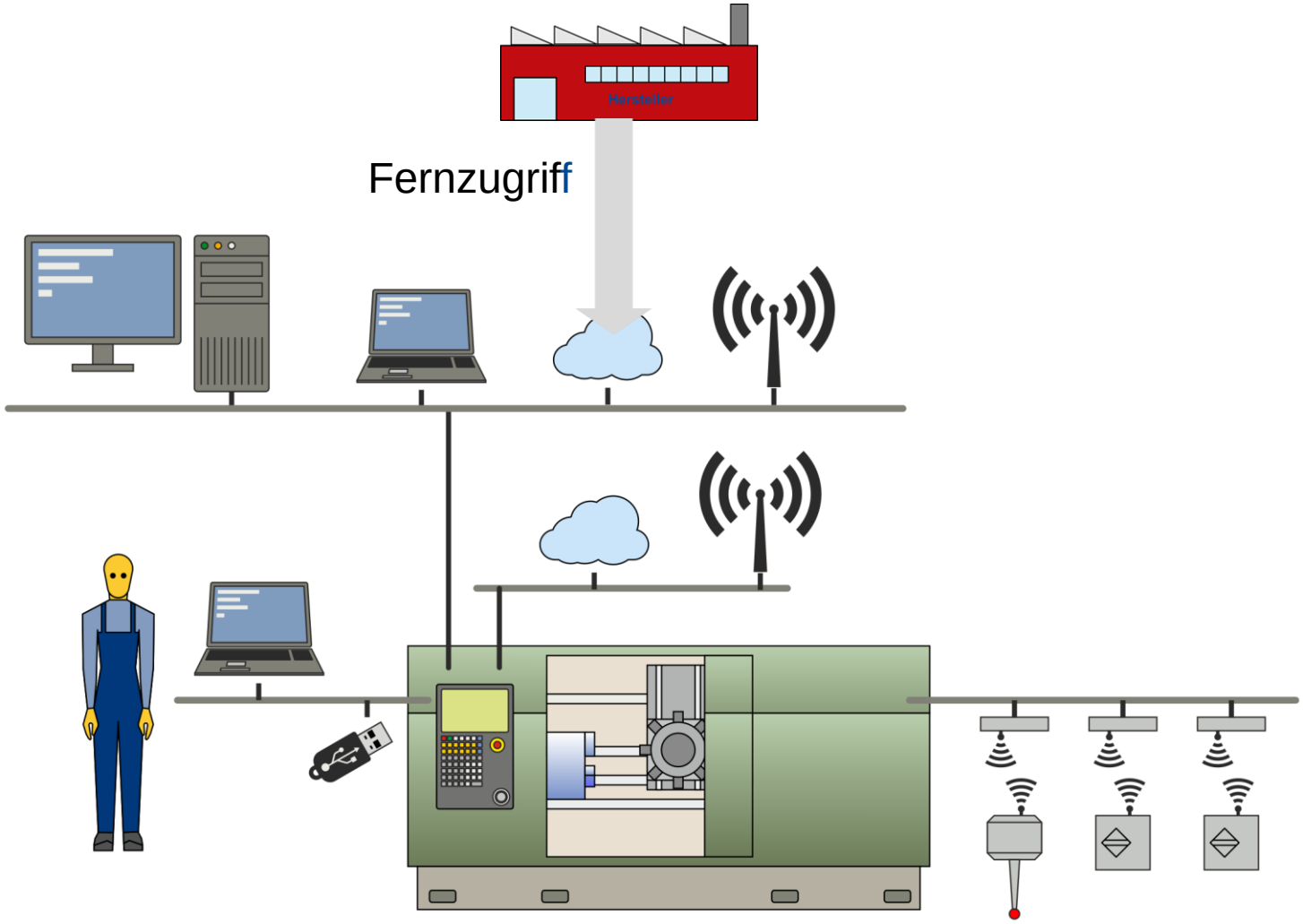
HINWEIS Ein **ferngesteuertes Anlaufen**, das von den an der Maschine arbeitenden Personen nicht vorgesehen wird, kann zu Verletzungen führen.

Betriebssicherheitsverordnung (BetrSichV)

§ 3 Gefährdungsbeurteilung

Der Arbeitgeber hat vor der Verwendung von Arbeitsmitteln die auftretenden Gefährdungen zu beurteilen (Gefährdungsbeurteilung) und daraus notwendige und geeignete Schutzmaßnahmen abzuleiten. Das Vorhandensein einer CE-Kennzeichnung am Arbeitsmittel entbindet nicht von der Pflicht zur Durchführung einer Gefährdungsbeurteilung.

Einfallstoren



Zusammenhang zwischen der Sicherheit und der IT- Sicherheit

IT Sicherheit (Security)

Bedrohung

Verwundbarkeit (Schnittstelle)

IT-Sicherheits- (Security) Risiko für die Maschine

Risikobeurteilung nach ISO 12100

Risikominderung durch Konstruktion

Schritt 1: Inhärent sicher Konstruktion

Schritt 2: Technische Schutzmaßnahmen

Schritt 3: Benutzerinformation

Verwundbarkeit: Schwachstelle bezüglich der Sicherheit eines IT-Systems, die durch eine Bedrohung ausgenutzt oder ausgelöst werden kann

Fehlfunktion in den SRP/CS

Beeinträchtigung oder Versagen von Schutzmaßnahmen

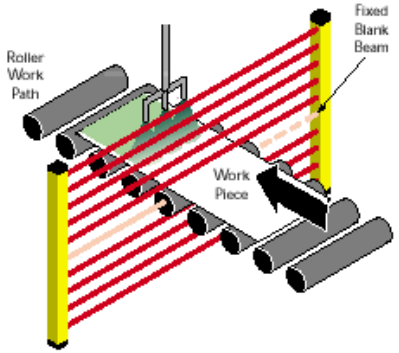
Unfall, Gesundheitsbeeinträchtigung

Maschine

Risikoanalyse im Kontext der (sicheren) Fernwartung

Die Umsetzung der IT-Maßnahmen dürfen nicht zum Verlust des Schutzes, der Regelung, der Beobachtungsmöglichkeit oder andere **wesentlicher Funktionen führen**.

Arbeitsschutz: Betrachtung resultierender Risiken, die sich auf Safety auswirken + potentielles Schadensmaß



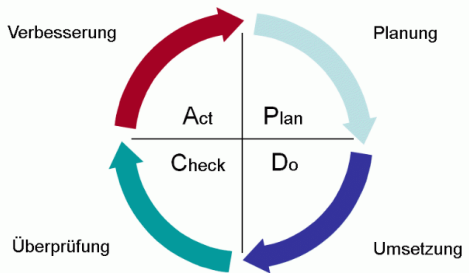
gemeinsame Risikobewertung von Safety und Security

während der **Projektierung/Konstruktion**

Risikoanalyse im Kontext der (sicheren) Fernwartung

- Identifikation der Maschinen/Komponenten (Welche Bedrohungen der IT- Sicherheit und Verwundbarkeiten bestehen)
- Betriebsmodi (Wartung, Reparatur usw.)
- Risikobewertung (Festlegung SL nach IEC 62443)
- Schützen (Entwickeln und Implementieren von geeigneten Gegenmaßnahmen zum Schutz der Maschine)

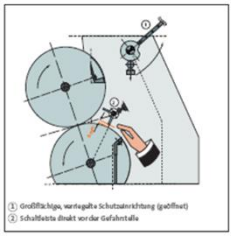
Geeignete Maßnahmen planen umsetzen und immer wieder nachprüfen



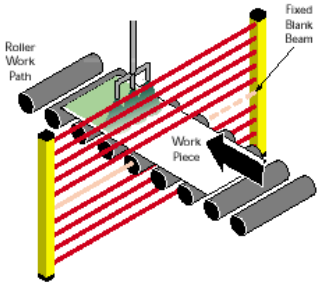
EN ISO 13849-1:2015

Ermittlung der notwendigen Sicherheitsfunktionen unter Berücksichtigung aller Betriebsarten, z.B.:

- Funktion zum Stillsetzen im Notfall (Not-Halt-Funktion)
- Sicherheitsbezogene Stoppfunktion (z.B. elektrisch verriegelte Schutzeinrichtungen)



- Verhinderung des unerwarteten Anlaufs
- Schleichgang
- Muting (vorübergehendes automatisches Überbrücken einer Sicherheitsfunktion)
- Lokale Steuerungsfunktionen (z.B. sicher reduzierte Geschwindigkeit oder Wegbegrenzung im Tippbetrieb)



- Sicherheitsbezogene Parameter (z.B. Temperatur, Gefahrstoffkonzentration, Strömungsrate)

Security Level	Beschreibung (IEC 62443)
SL 0	Keine besonderen Anforderungen oder Schutzmaßnahmen
SL 1	Schutz gegen gelegentlichen oder zufälligen Verstoß
SL 2	**Schutz gegen einen absichtlichen Verstoß mit einfachen Mitteln und geringem Aufwand, allgemeinen Fertigkeiten und geringer Motivation**
SL 3	Schutz gegen einen absichtlichen Verstoß mit raffinierten Mitteln und mittlerem Aufwand, automatisierungstechnischen Fertigkeiten und mittlerer Motivation
SL 4	Schutz gegen einen absichtlichen Verstoß mit raffinierten Mitteln und erheblichem Aufwand, automatisierungstechnischen Fertigkeiten und hoher Motivation

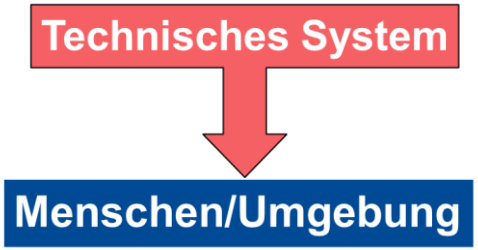
Gefahrenanalyse

Risiken

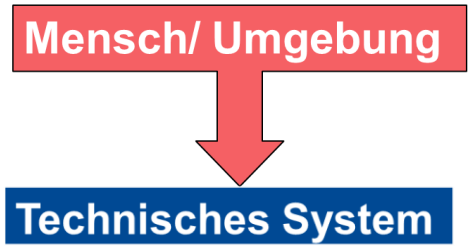
- der vereinbarte Verbindungsaufbau
- der unbeabsichtigte Verbindungsaufbau und
- der unberechtigte Verbindungsaufbau

Maschinensicherheit

Safety:
Schutz des Menschen bzw. der Umwelt vor Gefährdungen, die von einem (bekannten) technischen System ausgehen



Security:
Schutz eines technischen Systems vor Angriffen (prinzipiell unbekannt) und Störungen aus der Umgebung bzw. verusacht von Menschen



Vernetzte Steuerungssysteme schützen

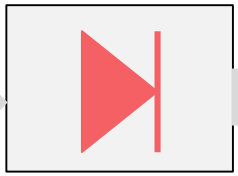
Alle Maschinen und Anlagen, die via Internet erreichbar sind, sind darüber prinzipiell aber auch angreifbar. Deshalb müssen die vernetzten Systeme vor eindringender Malware und unbefugten Zugriffen geschützt werden. Besonders hohen Sicherheitsbedarf haben natürlich Systeme, die kritische Infrastrukturen (KRITIS) oder andere Anlagen steuern, von deren fehlerfreier Funktion hohe Sachwerte oder gar Leben abhängen: z. B. Turbinen in Kraftwerken, chemische Fertigungsanlagen oder Industrieroboter in Produktionsstraßen.

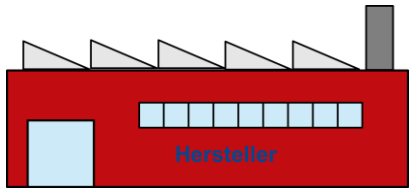
Betreiber

Maschine und Anlage

Datendiode

Betriebsdaten





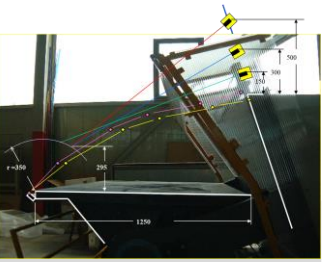
Statusmeldung OK / nicht OK

Verschlüsselung der Verbindung

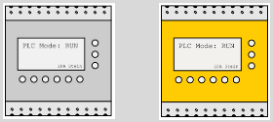
Die Fernwartung soll über eine kryptographisch abgesicherte Verbindung realisiert werden.

Ziel:

- Authentizität der Akteure
- Garantie der Vertraulichkeit der übermittelten Daten



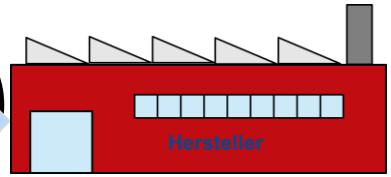
Maschine und Anlage



Betreiber

Betriebsdaten

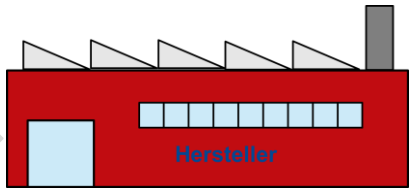
WWW



VPN Tunnel (Virtual Private Network)
SSH Secure Shell

Maschine und Anlage

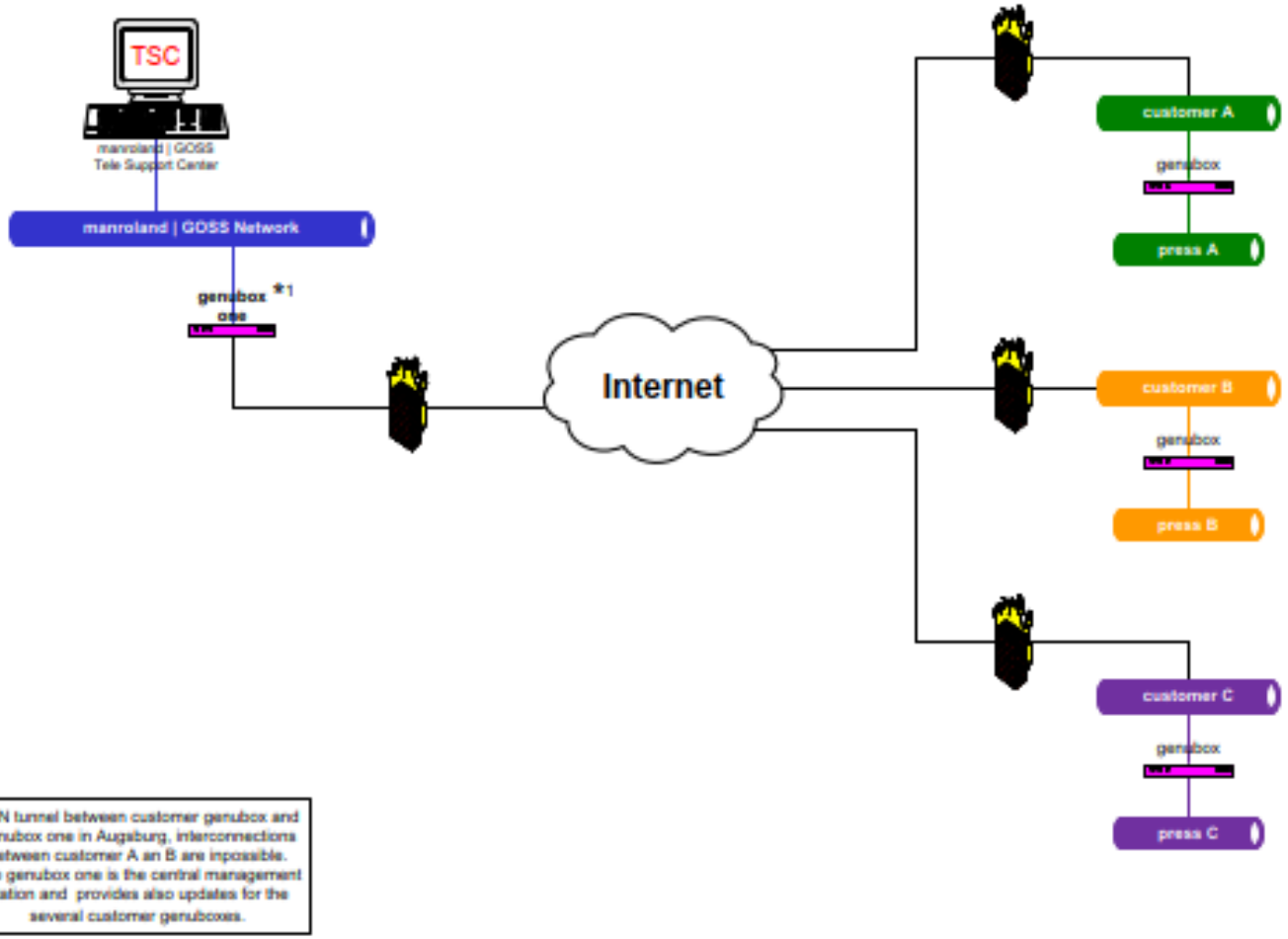
Betriebsdaten/Sicherheitsrelevanten Daten



Fernwartungs-Appliance genuebox der Fa. genua

Realisierte Sicherheitsmaßnahmen

- Punkt zu Punkt Verbindung
- Verschlüsselt Kommunikation über VPN (Virtual Private Network)Tunnel
- Verbindungsherstellung mit Kunden
- Zeitbegrenzt Gültigkeit des Datenflusses
- Validierung der Daten
- Automatische Unterbrechung des Daten Flusses


TSC
manroland | GOSS
Tele Support Center
manroland | GOSS Network
genubox *1
one
Internet
customer A
genubox
press A
customer B
genubox
press B
customer C
genubox
press C
*1 VPN tunnel between customer genubox and genubox one in Augsburg, interconnections between customer A an B are inpossible. The genubox one is the central management station and provides also updates for the several customer genuboxes.

Lösungsmöglichkeiten

Wie sieht es mit der **Security/Sicherheit** bei der Fernwartung aus? Bei einer Fernwartung ist es wichtig die Verbindung zwischen den beteiligten Komponenten abzusichern. Neben den rein **technischen Parametern** sollten **organisatorische Regelungen** bei dem Einsatz von Fernwartungssoftware eine Rolle spielen. Es muss ein Vertrauensverhältnis zwischen Sender und Empfänger bestehen. Zu empfehlen sind **vertragliche Vereinbarungen**, welche die Fernwartung regeln.

Bild: it-daily.net

Lösungsmöglichkeiten

Folgende Sicherheitsfeatures sind beispielhaft denkbar und können, je nach Sicherheitsstufe bzw. Sensitivität des zu steuernden Computers umgesetzt werden:

- Verschlüsselung der übertragenen Daten
- Authentifizierung der Administrator (Zwei-Faktor-Authentifizierung (BSI))
- Kundenvereinbarung (Bereitstellung einer Betriebsanleitung)
- Vereinbarung der Zugriffsprozesse
  - Betreiber muss der Fernwartung seines Rechners ausdrücklich vor Verbindungsaufbau zustimmen z.B. Betriebsartenwahlschalter „Fernwartung“
  - Priorisierung der Zuständigkeit (Zugriff Fernsteuerung oder Lokal)
  - Zeitfenster, d.h. zeitbegrenzte Gültigkeit der Fernwartung

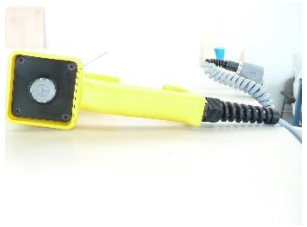
Bild: Fa. Eaton, Typ M22

Lösungsmöglichkeiten

- Fernwartung auf ein Wartungsobjekt beschränken
- die Einstellungen bzw. Konfiguration der verwendeten Fernwartungssoftware ist gesperrt und kann nur von Personen verändert werden, die mit dem Fernwartungsprozess zu tun haben
- der die Verbindung zur Fernwartung aufbauende Techniker muss sich authentifizieren
- Fernwartungssitzung wird revisionssicher protokolliert (Text-Protokoll)
- Fernwartungssitzung wird aufgezeichnet (Video-Protokoll)
- Sichere Trennung der Verbindung nach Ablauf des Zeitfensters (Rückwirkungsfrei Trennung) **Hardwaremäßiges Trennen**
- Übergänge zu anderen Netzen absichern
- Aktivierung bzw. Deaktivierung ist zu protokollieren
- Awareness

Bild: Fa.Eaton, Typ M22

Prozessbeobachtung bei laufender Maschine



- Aufgrund der komplexen Art des Fernzugriffs muss bei jedem Fernzugriff sichergestellt sein , dass die Bediener keiner gefahrbringender Bewegung oder keinen zusätzlichen Verletzungsrisikos ausgesetzt sind, und der Fernzugriff darf auf keinen Fall die festgelegten Sicherheitssysteme beeinträchtigen

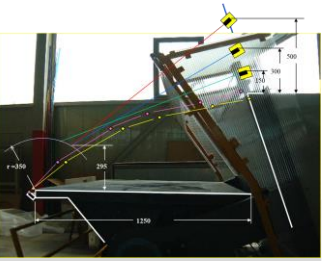
- Den Protokollen und Verfahren sollte von allen Beteiligen zugestimmt werden um die Integrität des Sicherheitssystems während und nach dem Abschluss des Fernzugriffs sicherzustellen.

- **Die sicherheitsgerichtete Reaktionszeit darf durch die Fernwartung nicht verändert werden**

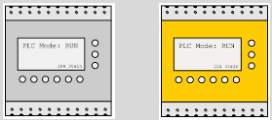
Softwareänderung durch Fernzugriff

Passwort, um das Sicherheitsprogramm zu bearbeiten:

Passwort: ****



Maschine und Anlage



Betriebsdaten

WWW

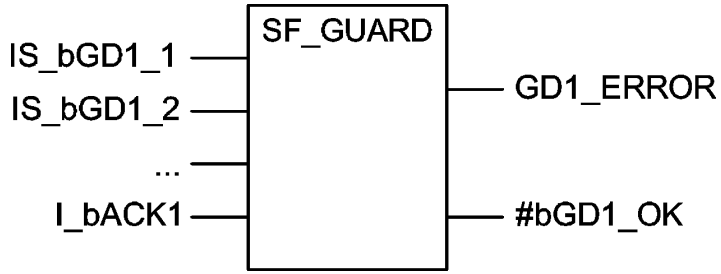
Hersteller

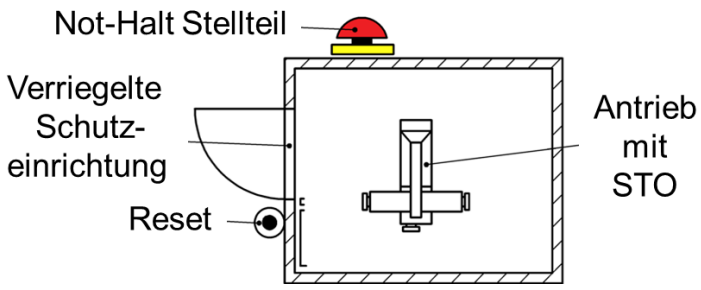
VPN Tunnel (Virtual Private Network)
SSH Secure Shell

Validierung der geänderte Softwareteils unter Berücksichtigung der EN ISO 13849-2 !!!

Sicherheitsfunktionen:

- Stoppfunktion eingeleitet durch Öffnen der verriegelten Schutzeinrichtung
- Nothaltfunktion





Nr.	Fehler	Reaktion	OK?

1	IS_bGD1_1 = LOW,
	IS_bGD1_2 = LOW
		#bGD1_OK = LOW,
		GD1_ERROR = LOW
			✓

2	IS_bGD1_1 = HIGH (permanent),
	IS_bGD1_2 = HIGH → LOW
		#bGD1_OK = LOW,
		GD1_ERROR = LOW → HIGH
			✓

3	IS_bGD1_1 = HIGH → LOW,
	IS_bGD1_2 = HIGH (permanent)
		#bGD1_OK = LOW,
		GD1_ERROR = LOW → HIGH
			✓

4	…	…	

Neue Frage Stellungen (Software Updates, KI und Cybersecurity)

Alte Welt (Nicht-digital)

- Umbau kann zu Herstellerpflichten führen?
- Bei wesentlicher Veränderung:
  - CE –Kennzeichnung für umgebaute und wesentlich veränderte Maschine

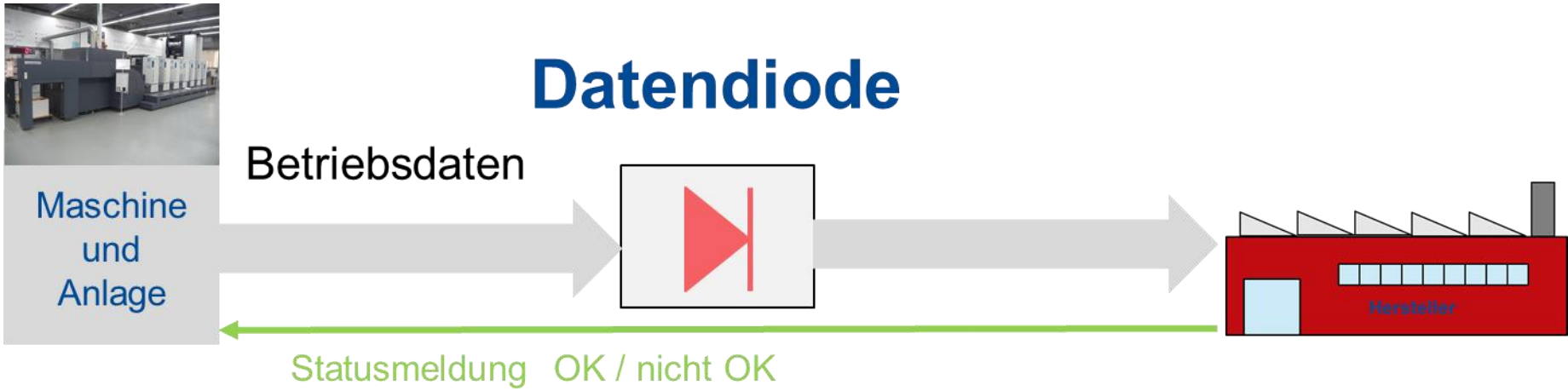
Digitale Welt“

- Software Update kann z.B. zu neuen Funktionen führen
  - Wenn Merkmale der wesentliche Veränderung erfüllt sind, besteht CE-Kennzeichnungspflicht

Nachrüstung von Fernwartungssystemen

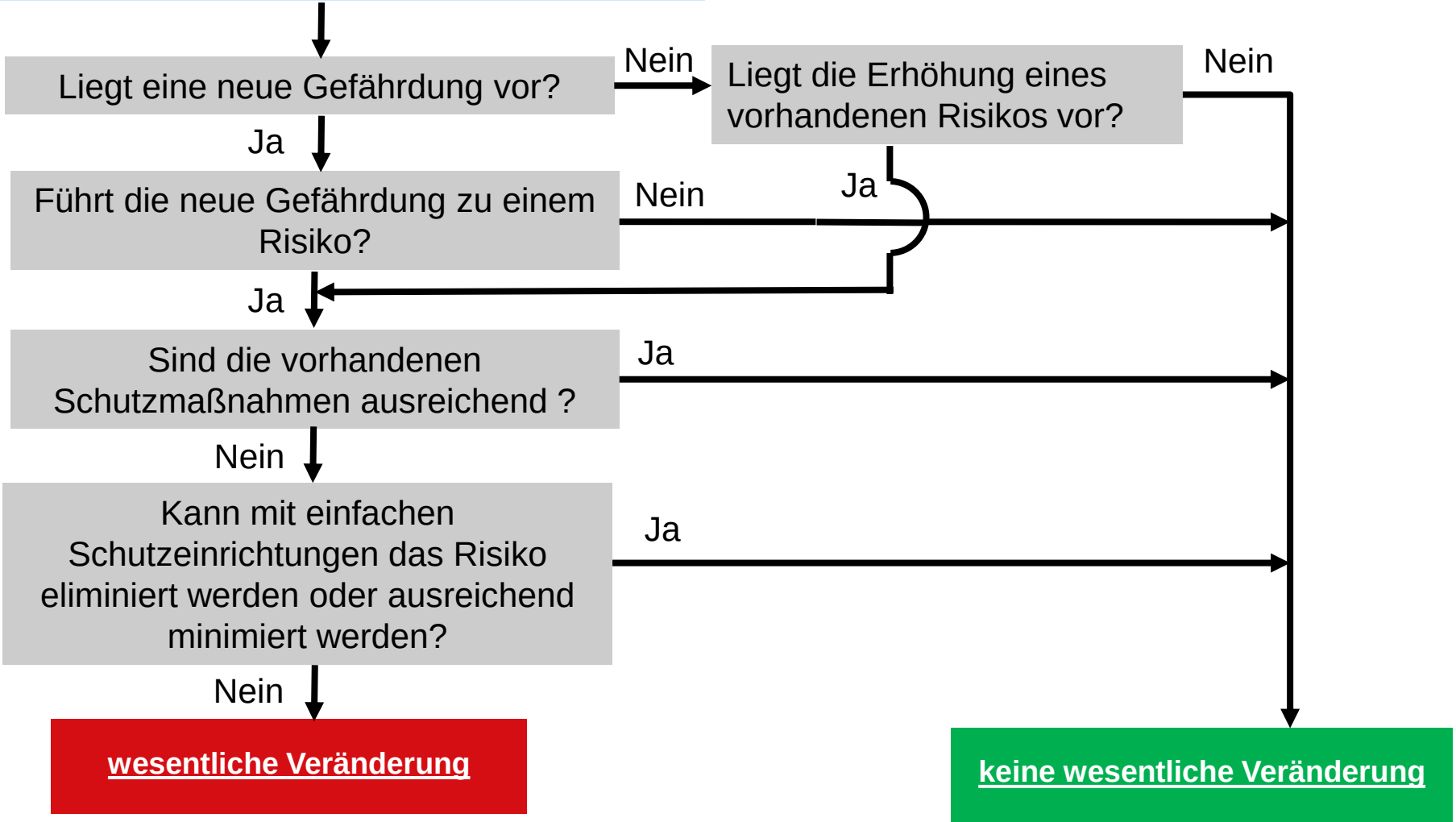
Frage:

Ist die nachträgliche Implementierung eines Fernwartungssystems als eine wesentliche Änderung der Maschine zu bewerten?



Maschine mit Fernwartung nachgerüstet

Interpretationspapier des BMAS „wesentliche Veränderung vom Maschinen“ vom 09. April 2015



BSI (Bundesamt für Sicherheit in der Informationstechnik):

- Empfehlung: Im IT Unternehmen
  Grundregeln zur Absicherung von Fernwartungszugängen (BSI-CS 054)

- Empfehlung: In der Produktion
  Fernwartung im industriellen Umfeld (BSI-CS 108)

Danke

für Ihre Aufmerksamkeit

如果你想一直快乐，你就必须经常变化 Wer ständig glücklich sein möchte, muss sich oft verändern.

Konfuzius (551 v. Chr-479 v. Chr)