Arbeit in der Industrie 4.0 sicher und gesund gestalten

Viktorio Malisa
FO: Industrie 4.0
Tel: +43 5 93 93 - 21767
E-Mail: viktorio.malisa@auva.at

Inhalt

- Begriffe und Motivation
- Cyber-Attacken und Security
- Sicherheit in der Industrie 4.0
- Forschungsprojekte

Begriffe der Industrie 4.0

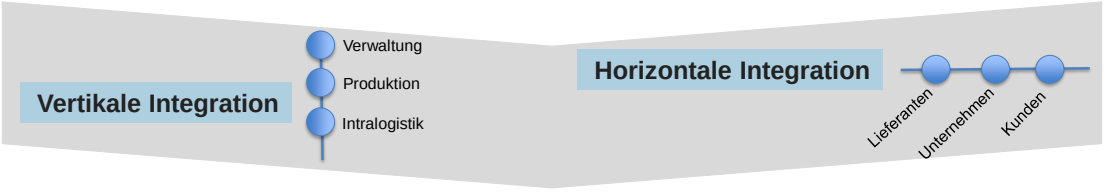
(~1975) **CIM**
Intelligent Manufacturing Systems

Digitale Zwillinge
Augmented Reality
Wearable Computing
Kommunikation 4.0
Vertikale Integration
Mensch-Maschine-Kollaboration
Virtuelle Inbetriebnahme
Virtuelle Realität
Predictive Maintenance
Safety & Security
IIoT
Digitale Fabrik
Industrie 4.0
Arbeit 4.0
Smart Manufacturing
Drohnen
Mobile Roboter
B i g D a t a
Selbstorganisierende Systeme
Vernetzung
Internet der Dinge
Arbeit 4.0
Gesellschaft 4.0
Cloud Computing
Selbstfahrende Autos
Psychische Belastung
Maschine-Maschine-Kommunikation
Bildung 4.0
3 D / 4 D - D r u c k e r
Cyber-Physical Systems
Serviceroboter
Flexible Arbeitszeit
Prävention 4.0
Horizontale Integration
Losgröße 1

www.auva.at

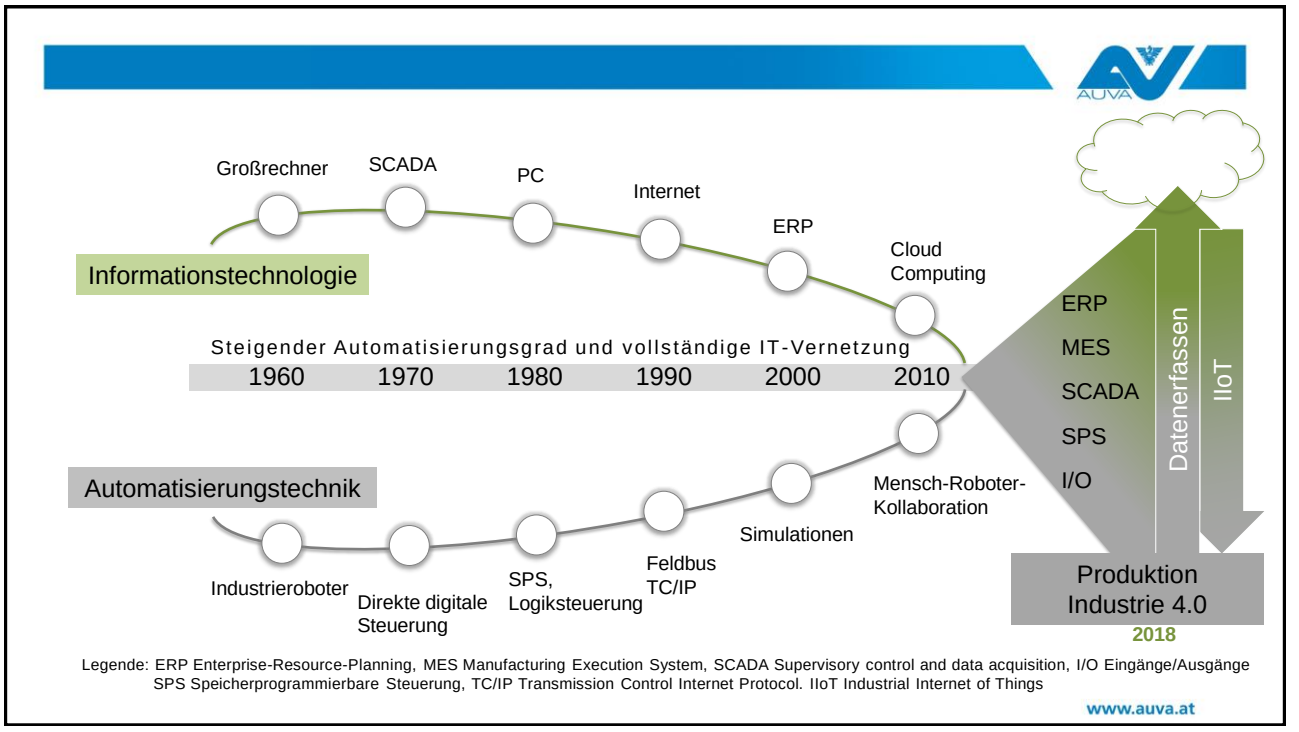
Definition Industrie 4.0

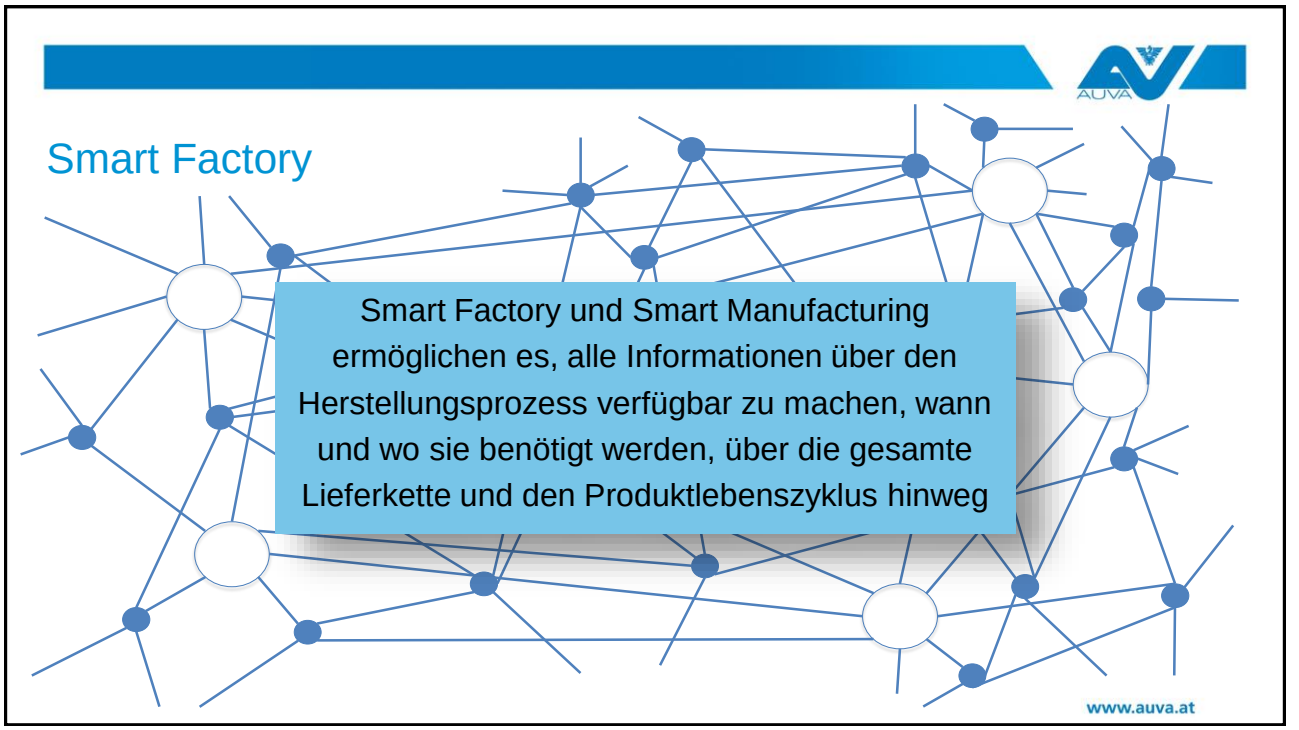
Industrie 4.0 ist ein **Begriff der deutschen Bundesregierung** und ein gleichnamiges Projekt in der Hightech-Strategie 2011 worin die industrielle **Produktion** mit moderner **Informations- und Kommunikationstechnik** verzahnt wird.



Definition angepasst: Industrie 4.0 - technischer Bereich - bezeichnet **bestimmte Technologien** verbunden mit der modernen Informations- und Kommunikationstechnik, die seit 2011 den Einzug in die Industrie gefunden haben und in großem Umfang **erforscht** bzw. **standardisiert** sind.

www.auva.at

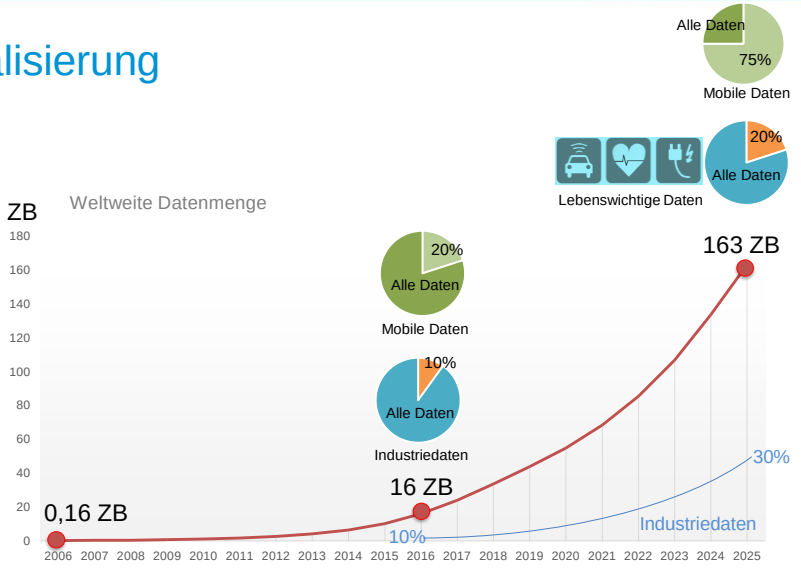

Großrechner
SCADA
PC
Internet
ERP
Cloud Computing
Informationstechnologie
Steigender Automatisierungsgrad und vollständige IT-Vernetzung
1960
1970
1980
1990
2000
2010
Automatisierungstechnik
Industrieroboter
Direkte digitale Steuerung
SPS, Logiksteuerung
Feldbus TC/IP
Simulationen
Mensch-Roboter-Kollaboration
ERP
MES
SCADA
SPS
I/O
Datenerfassen
IIoT
Produktion Industrie 4.0
2018
Legende: ERP Enterprise-Resource-Planning, MES Manufacturing Execution System, SCADA Supervisory control and data acquisition, I/O Eingänge/Ausgänge SPS Speicherprogrammierbare Steuerung, TC/IP Transmission Control Internet Protocol. IIoT Industrial Internet of Things
www.auva.at


Smart Factory
Smart Factory und Smart Manufacturing ermöglichen es, alle Informationen über den Herstellungsprozess verfügbar zu machen, wann und wo sie benötigt werden, über die gesamte Lieferkette und den Produktlebenszyklus hinweg
www.auva.at

Treibende Kraft der Smart Factory

- Produktion: Wandlungsfähigkeit, Flexibilität und steigende Effizienz
- Intelligente Interaktion aller Ressourcen in allen Lebensphasen der Produktion
- Intelligente Produkte jederzeit lokalisierbar und identifizierbar
- Flexible Arbeitsformen im Einklang mit den privaten Bedürfnissen und der Arbeit
- Bedarf an robusten und sicheren Kommunikationsnetzen
- Schnelle Distribution für kleine Losgrößen = Produktionsstandorte bei Kunden
- Maschine als Dienstleistung (Servization)
- Nachhaltigkeit: weniger Energie und Material

Digitalisierung



10^3	kB	kilobyte
10^6	MB	megabyte
10^9	GB	gigabyte
10^{12}	TB	terabyte
10^{15}	PB	petabyte
10^{18}	EB	exabyte
10^{21}	**ZB**	**zettabyte**
10^{24}	YB	yottabyte

$163*10^{21}$ Byte
40 Trillionen DVDs
100 Mil. Mal Erde-Mond-Erde

4.800 Daten/Tag/Person

Quelle: Online http://blog.wiwo.de/look-at-it/2017/04/04/weltweite-datenmengen-verzehnfachen-sich-bis-zum-jahr-2025-gegenueber-heute/, Zugriff am 11.6.2018

Sicherheit

Begriffe: Safety & Security

Safety

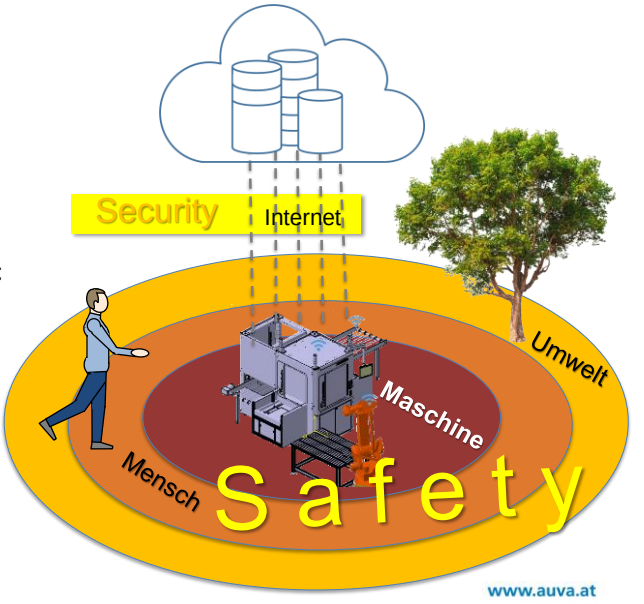
Betriebssicherheit bzw. Funktionale Sicherheit schützt Mensch, Maschine und Umwelt

Security / IT-Sicherheit / Informationssicherheit

Security soll die Maschinen vor der Umgebung schützen, mit dem Ziel Verfügbarkeit, Integrität und Vertraulichkeit der Daten abzusichern.

Fazit

Kombination aus funktionaler Sicherheit und Informationssicherheit bestimmt die **Gesamtsicherheit** der Anlage.



Security: Vertraulichkeit sicherstellen

Familienfoto der G20-Staats- und Regierungschefs und der geladenen G20-Teilnehmer

Bei G20 in Hamburg stand zur Verfügung:

- Planung durch internationale Experten
- Modernste Geräte und Software
- Umsetzung durch hervorragende Spezialisten
- Absperrungen
- Polizeikontrollen
- Sicherheitspersonal
- …

*) IMSI (International Mobile Subscriber Identity)
Internationale Mobilfunk-Teilnehmerkennung
ist auf SIM-Karte gespeichert

Quelle: BSI News

Lauschabwehr

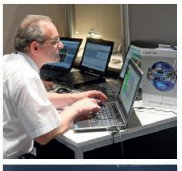


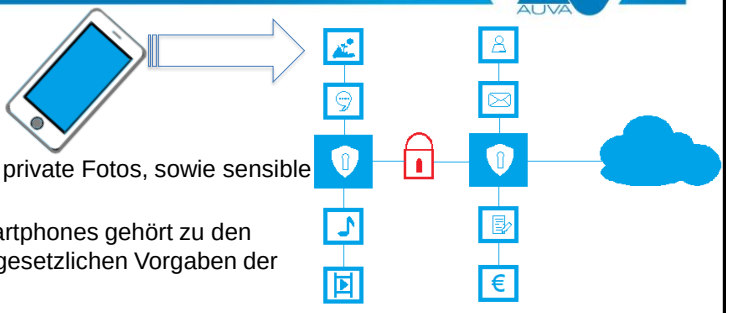
Bild links: Messungen am IT-Netzwerk hinsichtlich Auffälligkeiten mit einem speziellen Analysator

Bild rechts: BSI-Arbeitsplatz zur Überprüfung des Hochfrequenzspektrums, auch hinsichtlich Mobilfunkaktivitäten und IMSI-Catchern, im Konferenzbereich

Bild links: Im Messfahrzeug wurden die Sendeaktivitäten durch Mitarbeiter des BSI überwacht und hinsichtlich Auffälligkeiten bewertet

Bild rechts: Die Dolmetscher/-innen wurden gebeten, ihre Mobiltelefone außerhalb der Dolmetscherkabinen zu deponieren, sodass damit keine vertraulichen Gespräche aufgezeichnet oder nach außen übermittelt werden konnten

Dienst-Handy



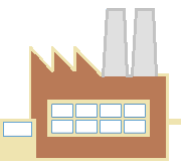
Auf einem Dienst-Handy:

- **Persönliche Daten**: Kontakte, E-Mails, private Fotos, sowie sensible **Daten des Unternehmens**
- Verlust eines gewerblich genutzten Smartphones gehört zu den größten Risiken bei der Einhaltung der gesetzlichen Vorgaben der DSGVO
- DSGVO sieht vor, dass ein Datenverlust (**Dienst-Handy Verlust**) innerhalb von **72 Stunden** gemeldet werden muss.

Datenverlust (Smartphone) bedeutet Datenschutzverletzung

- Sicherheitssoftware (zB. Samsung-Knox): verlorene Geräte zu orten und bei Diebstahl oder unwiederbringlichem Verlust darauf gespeicherte Daten zu löschen
- **Persönliche** und **geschäftliche** Daten, laut DSGVO, werden voneinander **getrennt** gespeichert
- per Fernzugriff viele Mobilgeräte gleichzeitig konfigurierbar
- Hardwarebasierte **Verschlüsselung**

Automatisierungspyramide



Legende: ERP Enterprise-Resource-Planning, MES Manufacturing Execution System, SCADA Supervisory control and data acquisition, SPS Speicherprogrammierbare Steuerung, E/A Eingänge/Ausgänge

Top 10 Bedrohungen

Zu den Top Bedrohungen für Industrial Control Systeme (ICS) im Jahr 2016 gehören:

Platz	Bedrohung	Handlungsfelder
1	Social Engineering und Phishing	**Mensch**, Prozesse
2	Einschleusen von Schadsoftware über Wechseldatenträger und externe Hardware	Prozesse, Technik
3	Infektion mit Schadsoftware über Internet und Intranet	Netzwerk, Technik
4	Einbruch über Fernwartungszugänge	Prozesse, Netzwerk
5	Menschliches Fehlverhalten und Sabotage	**Mensch**, Prozesse
6	Internet verbundene Steuerungskomponenten	Netzwerk, Technik
7	Technisches Fehlverhalten und höhere Gewalt	Technik
8	Kompromittierung von Extranet und Cloud-Komponenten	Netzwerk, Technik
9	(Distributed) Denial of Service Angriffe	Netzwerk, Robustheit
10	Kompromittierung von Smartphones im Produktionsumfeld	**Mensch**, Prozesse, Technik

Quelle: BSI Bundesamt für Sicherheit in der Informationstechnologie, https://www.bsi.bund.de

Cyberkriminalität

- 72 Prozent aller Unternehmen **in Österreich** waren in den letzten 12 Monaten Opfer einer Cyberattacke
- Jedes zweite Unternehmen hatte Unterbrechung der Geschäftsprozesse
- Angriffsmethoden: 90% Malware/Ransomware, 89% Phishing, 47% Social Engineering: Sorglosigkeit von Mitarbeitern wird ausgenutzt!
- 31 % aller Cyberangriffe werden gemeldet
- Cyberrisiken werden in 3 von 4 Unternehmen (74 %) auf oberster Ebene diskutiert
- Trend: 23% aller Angriffe sind gezielte Angriffe auf Unternehmen, Angriffe auf kritische **IT-Infrastrukturen** und vertrauliche **Daten**

Fazit der Studie: Es kann und wird jeden treffen. Unternehmen aller Branchen und Größenordnungen waren von Cyber-Angriffen betroffen.

Studie „Cyber Security in Österreich“, mit 240 österreichischen Cybersicherheitsexperten, KPMG Austria GmbH Wirtschaftsprüfungs- und Steuerberatungsgesellschaft, Wien, 2017

Daten gestohlen …

Live Cyber-Attacken

Cyber-Attacken, Live Ticker: http://map.norsecorp.com/#//

https://threatmap.checkpoint.com/ThreatPortal/livemap.html

news ORF.at

TVthek Radio Debatte Österreich Wetter IPTV Sport News

China stahl Pläne für US-U-Boot-Rakete

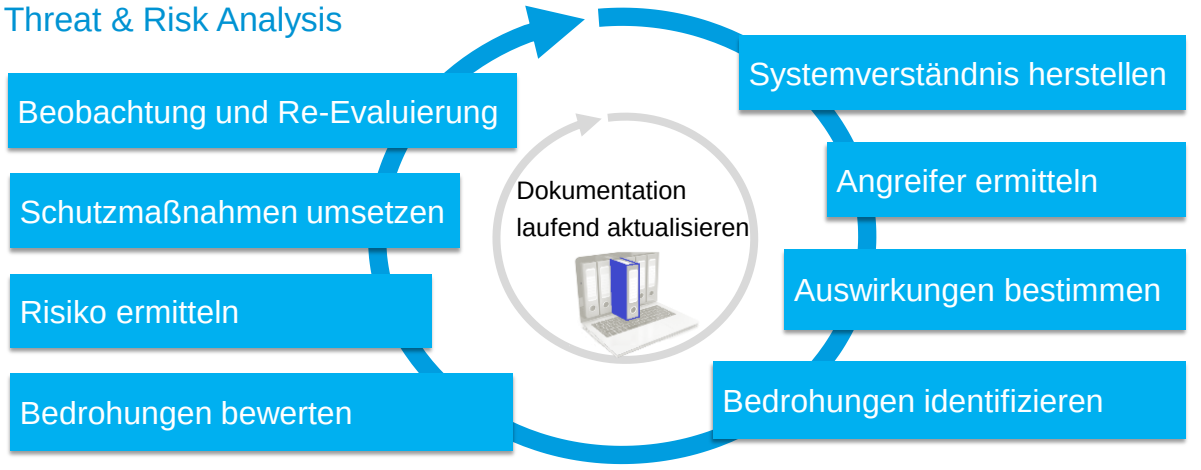
614 Gigabyte an geheimen Daten

Chinesische Hacker sollen im staatlichen Auftrag militärische Geheimnisse der USA gestohlen haben, wie die „Washington Post" mit Verweis auf die Ermittler am Freitag berichtet hat. Insgesamt sollen 614 Gigabyte sensible und geheime Daten gestohlen worden sein - darunter etwa die Pläne für eine Überschall-U-Boot-Rakete, ein Geheimcodesystem und das so gut wie unbekannte Programm „Sea Dragon" über neue Anwendungsfelder für bereits existierende Militärtechnologien.

Quelle: ORF.at, online: http://orf.at/stories/2442117/. Zugriff am 9. Juni 2018

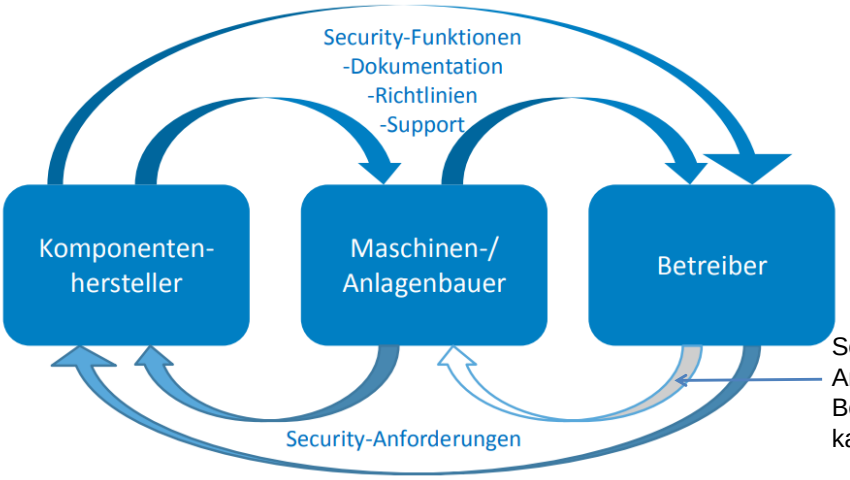
Risikoanalyse

Threat & Risk Analysis



Geändert nach Quelle: https://www.limessecurity.com/wp-content/uploads/2016/05/Limes_Security_Security_Forum_2016.pdf, Zugriff am 10.5.2018

Security Life Cycle



Security-Anforderungen vom Betreiber werden kaum aufgestellt !

IEC/TS 62443-1-1 Rev, Industrial communication networks – Network and system security – Part 1-1: Terminology, concepts and models

Safety & Security

- Sicherheitsvertrauenspersonen (SVP)
- IT-Abteilung => Person zuständig für Maschinensteuerungen (ICS)
- **Kommunikation SVP => IT ICS**
- Liste an Geräten im Ind. IT Netz: Accesspoint, Router, Switch, Personal Devices, Sensoren mit W-Lan, IT-Netz-Anschluss, Kameras, Drucker, PCs, SPS, …
  - Kritische Infrastruktur
  - Update !?
  - Austausch wenn veraltet (kein Update, Gerät ausgelaufen, Firma existiert nicht mehr, …)

- Digitale Sicherheit ist problematisch
- IT - Sicherheitsanalyse laufend
- Cyber-Attacken & Cyber-Security = großer Wirtschaftszweig
- Cyber-Attacken => Gefahr für Menschen (Arbeitssicherheit, Konsumenten)

Kleinere Firmen

Wenn einziger IT-Spezialist ausfallen sollte:

- Unternehmen ist von Angriffen nicht mehr geschützt
- Kein nahtloser Übergang: Verlust an wichtigen Informationen über IT-Infrastruktur und anstehende Schritte
- Zuständige Person für laufende Updates fehlt
- Spezialisten weltweit gesucht: Mitarbeitersucher kann sehr viel Zeit in Anspruch nehmen
- Neue Mitarbeiter braucht Einarbeitungszeit

Empfehlung:
- Vertrag mit IT-Spezialisten über Verschwiegenheit auch nach dem Ausscheiden!
- Vertrag mit einem Dienstleister für Fall der Fälle abschließen!
- Setzten Sie den Dienstleister für laufende Audits ein um im Kontakt zu bleiben!

Komponenten in der Produktion

- SPS, PC-Steuerungen
- IT-Netz, Router, Accesspoint,…
- Embedded Komponenten
- Datenbank
- Software Tools
- …

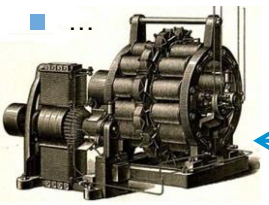
Liste eingesetzte Komponenten und Versionen führen!

Updates laufend durchführen und dokumentieren

Technische Dokumentation:
Manche Maschinenhersteller erlauben keine Updates!?

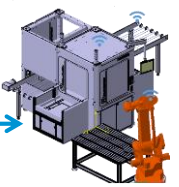
Anwendungsprogramm überprüfen!

Bei neuen Maschinen Security Anforderungen stellen!



Alte Maschine

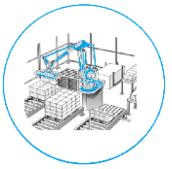
Kommunikation schützen !



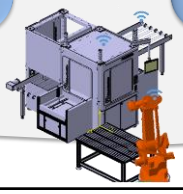
Neue Maschinen

Neue Berufe:
- Spezialist für Industrienetze
- Maschinendaten Engineer

Industrie 4.0 vereinfacht

1	2	3	4	5
Smarter Mensch	Cloud-Internet	Künstliche Intelligenz	Digitale Fabrik	Roboter
				
Human Machine Interface, Wearable Computing Personal Devices	Cloud Computing, Internet der Dinge, M2M, Fernwartung	Künstliche Intelligenz, Assistenzsysteme, Machine Learning	Virtuelle Realität, Augmented Reality Virtuelle Inbetriebnahme	MRK, Mobile Roboter, autn. Fahrzeuge

ICS - Industrial Control System

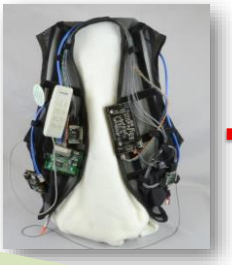


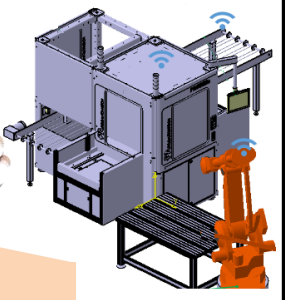
ICS-Security: Informationssicherheit

www.auva.at

Mensch in der Produktion

1





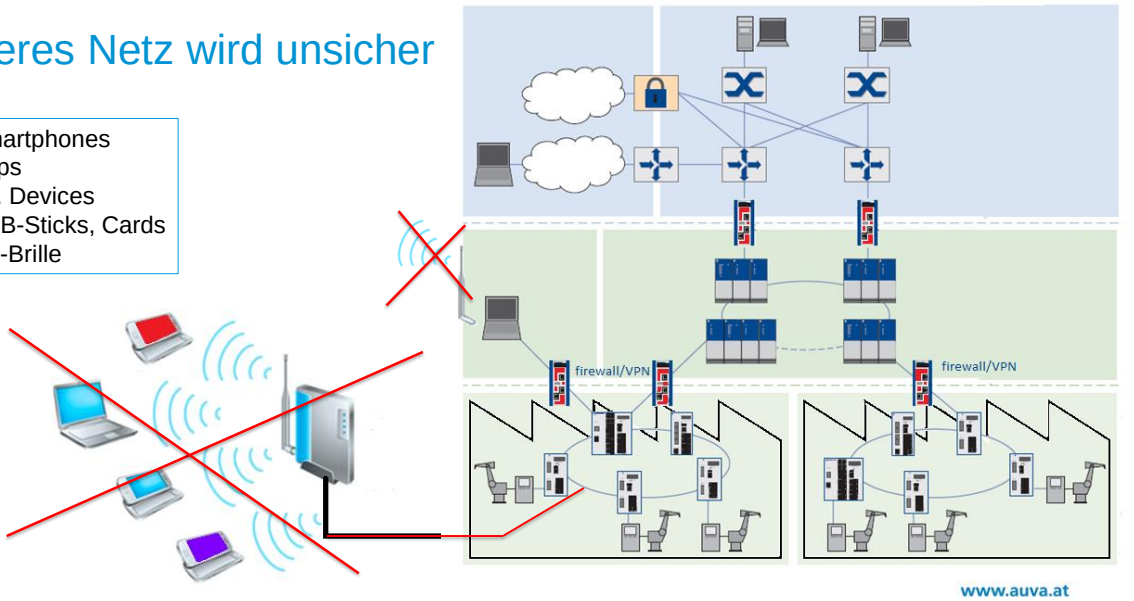
\+
- Körperhaltung regulierend
- Informationsgehalt erhöhend
- Effizienz steigernd
- Fehler reduzierend
- schnelle Einarbeitung

\-
- Überforderung
- Sicht-Einschränkung
- Ablenkung
- Personen Tracking

www.auva.at

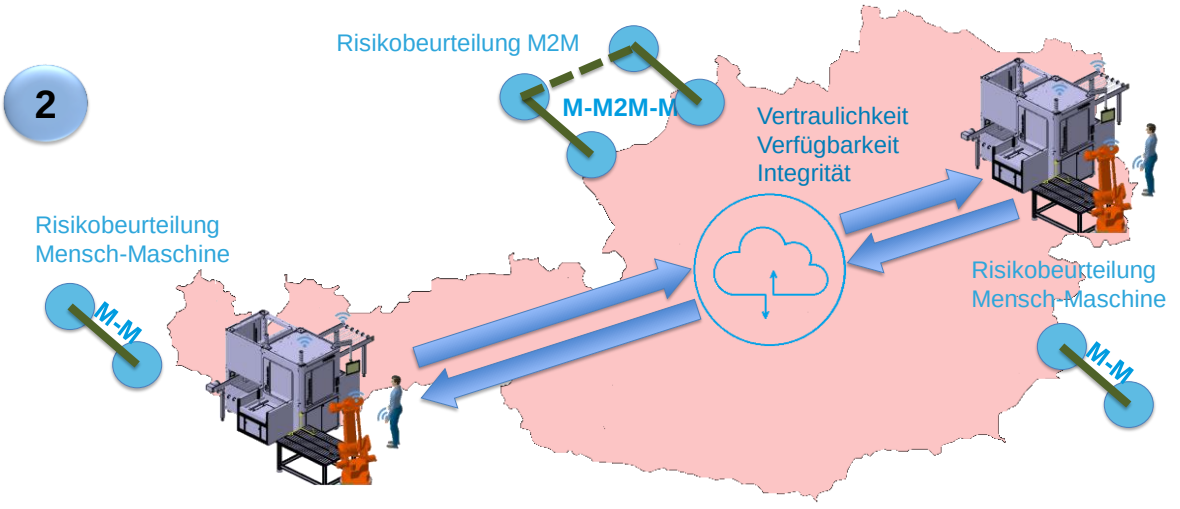
Sicheres Netz wird unsicher

- Smartphones
- Apps
- div. Devices
- USB-Sticks, Cards
- VR-Brille



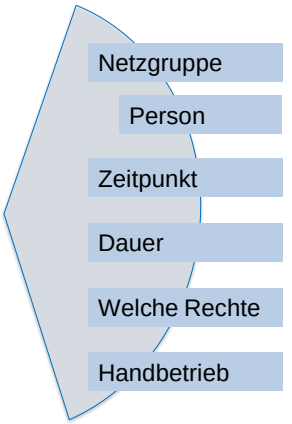
www.auva.at

Cloud-Internet: Maschine-Maschine Kommunikation



www.auva.at

Dokumentation über Fernzugriff



Die Betriebsanleitung muss Informationen enthalten, **welche Nutzergruppen** Fernzugriff auf die Maschinen erhalten, zu **welchem Zeitpunkt**, für **welchen Zeitraum** und mit **welchen Rechten** sie ausgestattet sind.

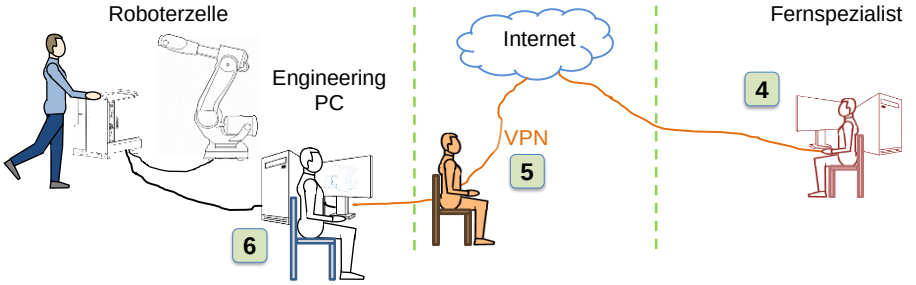
Es muss **ausgeschlossen** werden, dass der Fernzugriff zu einem Zeitpunkt erfolgt, in dem die Maschine **kritische Funktionen** ausführt.

VDMA 66481:2017: Industrial Security – Grundlegende Anforderungen an die Security von Maschinen, Anlagen und deren Komponenten

Fernwartung

1 Fernwartung: in der Maschinendokumentation beschrieben?

2 **Anwender** ⇨ **Vertrag** ⇦ **Hersteller/Dienstleister**



7 Beim Anwender wird Durchführung der Fernwartung überwacht, aufgezeichnet (Bild und Ton) und archiviert!

Künstliche Intelligenz

3

Künstliche Intelligenz (KI) ist ein Forschungsgebiet der sich mit der Automatisierung intelligenten Verhaltens bzw. Nachbildung menschenähnlichen Entscheidungsstrukturen und dem Maschinenlernen befasst. Meistens handelt sich um einfache Algorithmen die Maschine steuert um konkrete Anwendungsprobleme intelligent zu lösen.

Machine Learning

Optimierungsalgorithmen

Deep Learning

- Daten zum Einlernen
- Validierungsdaten
- Testdaten

Über Einlerndaten wird Modell generiert

Mit Validierungsdaten wird Modell überprüft

Leistung verbessern mit mehr Daten und verschiedenen Funktionalitäten

Modell nutzen für neue Daten

Eigenschaften überprüfen mit Testdaten

Data Mining

Mustererkennung

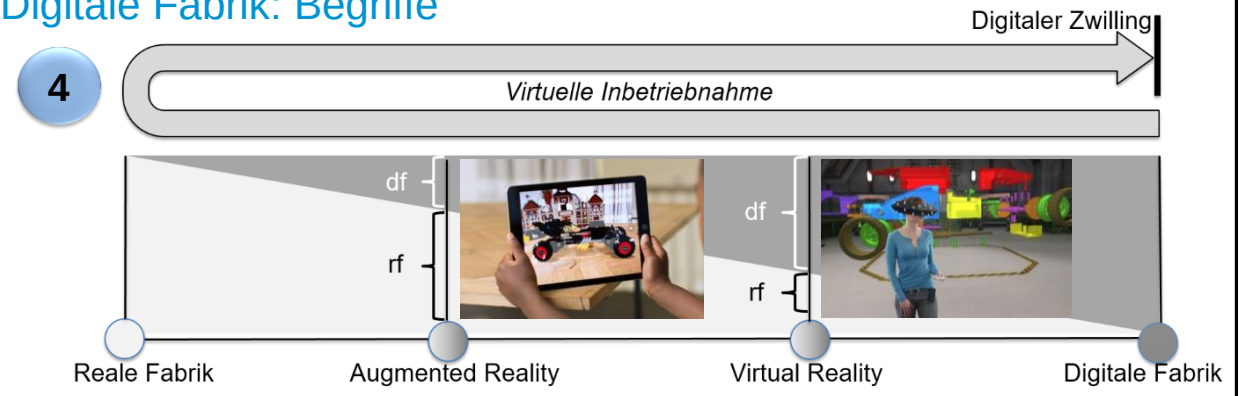
Prozess-Kennzahlen verfolgen !

Prozessabhängige Tests definieren !

www.auva.at

Digitale Fabrik: Begriffe

4

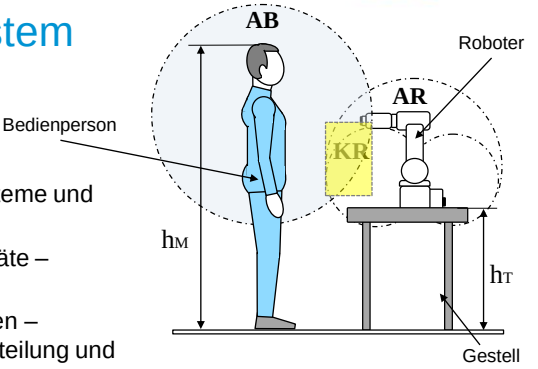


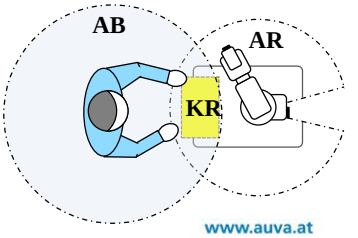
www.auva.at

Mensch-Roboter-Kollaborationssystem (MRK)

5

- EN ISO 10218-1:2012 Industrieroboter — Sicherheitsanforderungen Teil 1: Roboter
- EN ISO 10218-2:2012 Industrieroboter — Sicherheitsanforderungen Teil 2: Robotersysteme und Integration
- ISO/TS 15066:2016 Roboter und Robotikgeräte – Kollaborierende Roboter
- EN ISO 12100:2013 Sicherheit von Maschinen – Allgemeine Gestaltungsleitsätze - Risikobeurteilung und Risikominderung
- + Applikationsspezifische Normen

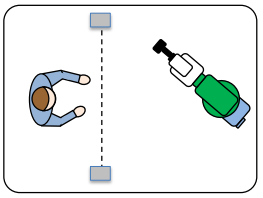




AB – Arbeitsbereich der Bedienperson
AR – Arbeitsbereich des Roboters
KR – Kollaborationsraum
h_M – Menschengröße
h_T – Tischhöhe

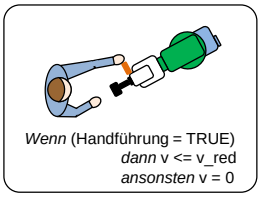
Betriebsart der Kollaborierenden Robotersysteme

1



SICHERHEITSGERICHTETER STOPP

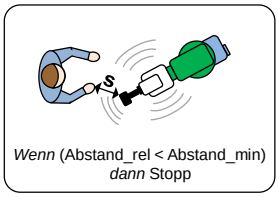
2



Wenn (Handführung = TRUE)
dann v <= v_red
ansonsten v = 0

HANDFÜHRUNG

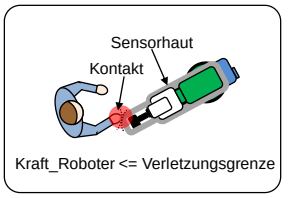
3



Wenn (Abstand_rel < Abstand_min)
dann Stopp

GESCHWINDIGKEITS- UND ABSTANDSÜBERWACHUNG

4



Kraft_Roboter <= Verletzungsgrenze

LEISTUNGS- UND KRAFTBEGRENZUNG

ISO 10218-2, ISO/TS 15066

Persönliche Schutzmaßnahmen 4.0

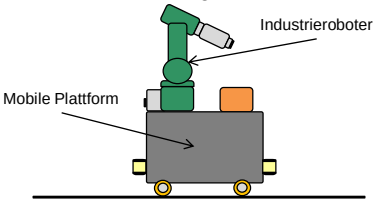
- Passwort alle 3 Monate ändern, bzw. wenn Mitarbeiter ausscheiden. Passwort aus Klein-, Großbuchstaben, Sonderzeichen und Zahlen zusammenstellen (IhkKu2N, MOi95-mF48)
- Passwort, wenn erforderlich, in einem Tresor aufbewahren
- Virenschutz verwenden, Einsatz auf Maschinensteuerungen problematisch
- Hardwarefirewall verwenden
- Standard Passwörter an Devices ändern, Passwörter nicht auf Maschinen aufschreiben
- Software sämtliche Hardware so bald verfügbar, updaten
- Surfen: nicht lange auf unsicheren Webseiten verbleiben
- Mails: unbekannte Links nicht anklicken, Anhang nicht aufmachen
- PC abdrehen wenn nicht verwendet wird
- Smartphone: nicht benötigte Apps deinstallieren
- Maschinen nicht ans Internet anschließen oder nur zeitweise wenn notwendig

Mobile Roboter

Kooperation

Selbständiges Fahren

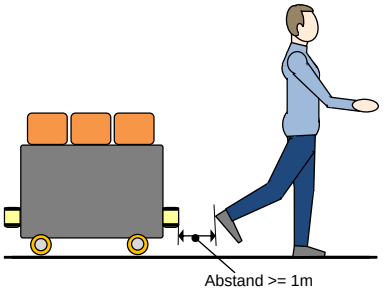
- unterwegs nach meinem Auftrag
- Anteil an Autonomie
- unterwegs zu mir
  - beauftragt von der Prozesssteuerung
  - beauftragt von anderen Person
- am Stand Aufträge bearbeiten



Kollaboration

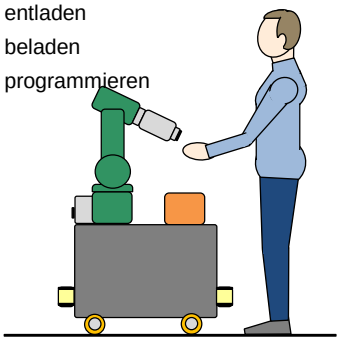
Personen folgen

- unterwegs nach meinem Auftrag
- unterwegs zu mir
- führt Aufträge aus
- Kollaborationsraum: Arbeitsbereich des Menschen



Arbeiten am Stand

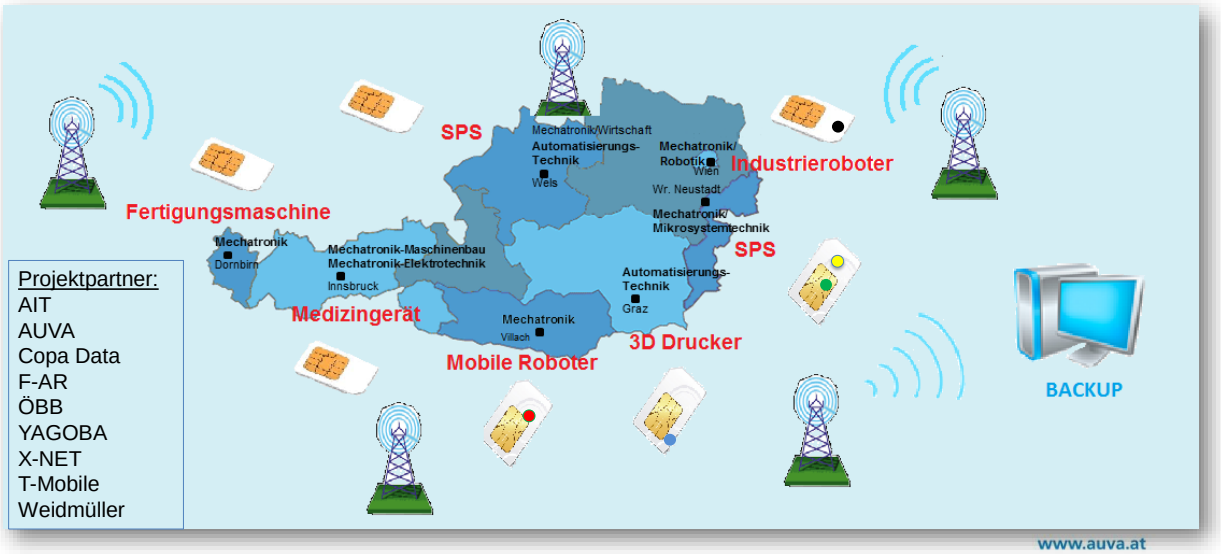
- Kollaborationsraum: Betriebsbereich des Manipulators
- gemeinsames Bearbeiten
- entladen
- beladen
- programmieren



Forschungsaktivitäten

Thema	Kooperationspartner	Jahr	Ziele
Mensch-Roboter-Kollaboration (MRK)	Joanneum Research Robotics	2017/18	• Merkblatt für Bediener „Arbeiten mit kollaborativen Robotern“ • Merkblatt für Systemintegratoren „Integration kollaborativer Robotikanwendungen“
MRK, Safety & Security	TU Graz, IFT	2018/20	• Auswirkung von Security auf Safety
Samrt Factory	AUVA, BGN, INAIL, Suva	2018/20	• Arbeitssicherheit 4.0
Safety in verteilten Systemen	Mechatronik Plattform, T-Mobile, AIT, X-net	2017/20	• Auswirkung von Security auf Safety über Cloud verbundene Systeme

Projekt: Verteilte Systeme MP / Labor+ MP



Verteilte Systeme

Ziele

- Testen von Sicherheit-Algorithmen und Kryptographie
- Maschinen- und Arbeitssicherheit bei M2M-Kommunikation
- Rollenwechsel Master-Slave
- Test von IoT-Dienste
- IT-Security und Auswirkung auf Safety
- Maschinen- und Arbeitssicherheit in den verteilten Systemen
- Sichere Produktionsplanung
- Zusammenlegung von Funktionalitäten
- Risikomanagement ISO/IEC 27001 für verteilte Systeme (Einbeziehung lokalen, verschiedenen ISMS)
- Risikoanalyse der verteilten Produktionssysteme

Arbeitssicherheit 4.0

- Personal soll zum Thema Security mehr sensibilisiert werden!
- Besucher, Gruppenführungen => keine Handys, USB-Sticks, elektronische Devices
- Infotafeln für Informationen zum Thema Cyber-Security nutzen!
- Schnittstelle und Kommunikation SVP – IT ist sehr wichtig!
- Neue Technologien nutzen für ergonomisch gerechte Arbeitsplätze!
- Neue Technologien können Sicherheit (Safety) am Arbeitsplatz erhöhen!
- AUVA ist Ihr Ansprechpartner für „Sicherheit in der Industrie 4.0“

Neue Seminare
im AUVA-Schulungsprogramm ab 2018/19

- Mensch-Roboter-Kollaborationssysteme
  - Graz, 11.10.2018, Anmeldung
  - Salzburg, 13.12.2018, Anmeldung
  - Stockerau, 19.03.2019, Anmeldung
  - Tiefgraben/Mondsee, 08.05.2019, Anmeldung
- Sicherheit in der Industrie 4.0
  - Wien, 29.11.2018, Anmeldung
  - Salzburg, 28.02.2019, Anmeldung
- Digitale Fabrik: Virtuelle Inbetriebnahme
  - Innsbruck, 22.11.2018, Anmeldung
  - Graz, 31.01.2019, Anmeldung

2018/2019

www.auva.at

Danke für Ihre Aufmerksamkeit!

www.auva.at