OTTO VON GUERICKE
UNIVERSITÄT
MAGDEBURG

LEHRSTUHL
PSA
PRODUKTIONSSYSTEME
und –AUTOMATISIERUNG

STIFTUNG

RISIKOMANAGEMENT FÜR DIE SMARTE FABRIK

Potenziale der
Digitalisierung erschließen
– Risiken aktiv managen

SMARTE WERTSCHÖPFUNG BRAUCHT SMARTES RISIKOMANAGEMENT

„Weshalb die Vision der Industrie 4.0 ihre Potenziale noch nicht voll entfaltet hat? Weil wir die Risiken, die mit neuen Digitalisierungs- und Automatisierungstechnologien einhergehen, bisher nicht systematisch betrachtet haben!“

Prof. Dr. Julia Arlinghaus, Leiterin Fraunhofer-Institut für Fabrikbetrieb und –automatisierung IFF

LEHRSTUHL PSA

OTTO VON GUERICKE UNIVERSITÄT MAGDEBURG

Fraunhofer IFF

Gefördert durch:

funk STIFTUNG

Herausgeber:
Lehrstuhl für Produktionssysteme und -automatisierung
Otto-von-Guericke-Universität Magdeburg
Universitätsplatz 2, 39106 Magdeburg
Autoren: Julia Arlinghaus, Falko Bendik, Yazgül Fidan, Melanie Kessler, Laura Reinecke
Telefon: +49 391 4090–477
E-Mail: julia.arlinghaus@ovgu.de

Gefördert durch die Funk Stiftung.
In Zusammenarbeit mit dem Fraunhofer Institut für Fabrikbetrieb und -automatisierung IFF.
Wenn Sie uns zitieren möchten: Arlinghaus, J.; Bendik, F.; Fidan, Y.; Kessler, M.; Reinecke, L. (2021): Risikomanagement für die Smarte Fabrik.
Online verfügbar unter https://www.psa.ovgu.de/iniaf_media/Risikomanagement_Smarte_Fabrik.pdf

DIPL.-BETRIEBSWIRT (BA)
HENDRIK F. LÖFFLER
Funk Stiftung

Liebe Leserinnen und Leser,

vor zehn Jahren weckte der Begriff Industrie 4.0 erstmals große Hoffnungen auf langfristige Wettbewerbsfähigkeit am Hochlohnstandort Deutschland. Tatsächlich revolutionieren Digitalisierung und Automatisierung derzeit die industrielle Wertschöpfung. Neue Produktions- und Kommunikationstechnologien – von Sensorik, über Roboter und autonome Systeme bis hin zu sogenannten Wearables wie Datenhandschuhe oder Datenbrillen – locken noch immer mit großen Potenzialen. Verbesserte Vorhersagen von Kundenbedarfen, reduzierter Wartungs- und Instandhaltungsaufwand, niedrigere Lagerkosten und höhere Qualität bei deutlich verkürzten Time-to-Market-Zyklen sowie Entwicklungskosten sind nur einige Beispiele.

2021 ist der Zeitpunkt, an dem auch kleine und mittelständische Unternehmen die Phase der Leuchtturmprojekte verlassen. Aus digitalen Einzelprojekten werden digitale Unternehmen, digitale Lieferketten und digitale Ökosysteme. Dieser Netzwerkeffekt wird weitere Potenziale freisetzen. Damit diese Potenziale schnell realisiert werden können, braucht es ein neues Risikomanagement: Ein Risikomanagement für die smarte Wertschöpfung.

Die Studie Risikomanagement für die Smarte Fabrik zeigt, wie neue Technologien auch die Risikosituation von Unternehmen – jenseits von Cyberrisiken – verändern. Außerdem werden Risikofaktoren für Technologien, Technologiebündel sowie erfolgreiche Mitigationsstrategien aufgezeigt.

Anfang 2021 hat die EU eine neue Vision der industriellen Wertschöpfung aufgezeigt. Der Begriff Industrie 5.0 steht für eine Industrie jenseits von Effizienz und Produktivität als alleinige Zielsetzungen. Industrie 5.0 hebt die Rolle des Menschen und den Beitrag der industriellen Produktion zur Gesellschaft hervor. Die mensch-zentrierte Gestaltung von Technologien und Produktionssystemen wird so zum Schlüssel langfristiger Wettbewerbsfähigkeit europäischer Unternehmen. Auch die Studie Risikomanagement für die Smarte Fabrik hebt den Menschen im Zentrum der industriellen Wertschöpfung hervor. Verzerrte Entscheidungsprozesse und mangelndes Digitalisierungs-Know-how sind echte Risikofaktoren für die Fabrik der Zukunft und müssen deshalb aktiv gemanagt werden. Die Autoren zeigen dafür Wege auf.

Wir freuen uns, dass die Funk Stiftung den Leser durch diese Studie einen leichten Einstieg in das Thema Risikomanagement in der Fabrik der Zukunft geben kann.

Viel Spaß beim Lesen!

Hendrik Löffler
Vorstandsvorsitzender
Funk Stiftung


STATOR
s/n: 3941501
Gear 7-38 1:2.75
Trans.Gear 1:3.25
s/n: 3941501

INHALT

06 INDUSTRIE 4.0 – GAMECHANGER?

08 RISIKOFAKTOREN VON INDUSTRIE 4.0-ANWENDUNGEN

10 FORSCHUNGSDESIGN

14 NEUE TECHNOLOGIEN – DIE ENABLER DER SMARTEN FABRIK

22 NEUE TECHNOLOGIEN – NEUE RISIKEN – NEUE MITIGATIONSANSÄTZE

36 FAKTOR MENSCH

38 AUSGEWÄHLTE RISIKEN UND MITIGATIONSANSÄTZE DER KERNTECHNOLOGIEN

42 DER DIGITAL QUICK CHECK

44 HANDLUNGSEMPFEHLUNGEN FÜR EIN ZUKUNFTSORIENTIERTES RISIKOMANAGEMENT

46 ÜBER UNS

INDUSTRIE 4.0 – GAMECHANGER?

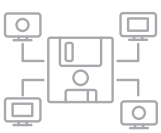
INDUSTRIE 4.0 BRAUCHT RISIKOMANAGEMENT 4.0

Industrie 4.0 – mit diesem Begriff verbinden Unternehmen in Industrie, Handel und Dienstleistung große Potenziale. Neben der Steigerung von Effizienz, Flexibilität, Lieferservice und Qualität entstehen entlang der Wertschöpfungsnetze ganz neue Produkte, Services und datenbasierte Geschäftsmodelle. Der Einsatz neuer Technologien und die Vernetzung in Fabriken und Gebäuden, Anlagen und Produkten bringt aber auch bisher unterschätzte Risiken mit sich.

WERTSCHÖPFUNGS-
NETZWERKE

FABRIKEN &
GEBÄUDE

ANLAGEN &
PRODUKTE



DATEN &
GESCHÄFTSMODELLE

Industrie 4.0 steht für die Digitalisierung und Vernetzung der industriellen Wertschöpfung. Die reale und die virtuelle Welt verschmelzen in der rasanten Technologieentwicklung in den Bereichen der Sensorik, Datenspeicherung, -verarbeitung und -analyse sowie Cloud-Computing. Kernelemente sind die Cyber-physischen-Systeme, verbunden über das Internet der Dinge und Services. Der erhoffte Effizienzsprung von bis zu 45 Prozent in der Smarten Fabrik wäre die vierte industrielle Revolution. Die Vision der selbststeuernden, adaptiven Fabrik zieht folglich immer mehr Unternehmen in ihren Bann. Im globalen Wettbewerb sichern dann höherer Lieferservice und verbesserte Qualität, steigende Produktivität und sinkende Kosten für Wartung, Instandhaltung und Lagerung sowie kürzere und effizientere Entwicklungsprozesse langfristig die Marktposition.

Zehn Jahre nach der Einführung des Begriffes Industrie 4.0 zeigt sich, dass viele Potenziale noch nicht realisiert wurden. Denn **Risiken im Zusammenhang mit Industrie 4.0-Projekten** werden oft nicht systematisch gemanagt. Der Projektfokus liegt häufig auf den vielfältigen Vorteilen und Potenzialen, während zahlreiche Risikofaktoren die Projekte zum Scheitern bringen. Es gilt also Adaptionsrisiken, Risiken aus menschlichem, technischem und organisatorischem Versagen genauso aktiv zu managen wie Risiken aus gezielten und ungezielten Cyber-Angriffen.

Insbesondere die zunehmende Vernetzung der Wertschöpfungsketten über Unternehmensgrenzen hinweg erfordert daher ein **angepasstes Risikomanagement** entlang der gesamten Supply Chain, um neben den unternehmensbezogenen Risikoquellen auch Risiken aus dem Umfeld und der Branche zu betrachten.

Ein leistungsfähiges Risikomanagement steht weit oben auf der strategischen Managementagenda vieler Unternehmen. Denn Industrie 4.0-Technologien sichern Prozesse ab, identifizieren Störungen und erlauben eine effektive Reaktion. Aber gleichzeitig tragen sie Risiken in die Unternehmen ein. Durch die Corona-Krise angetrieben, intensivieren jetzt auch kleine und mittelständische Unternehmen ihre Digitalisierungsprojekte. Diese Studie will Entscheidern in klein- und mittelständischen wie in großen Unternehmen eine **Orientierung** bieten, um die neuen Risikoherausforderungen zu meistern. Die Studie hilft Risiken zu erkennen und diese proaktiv zu managen.

Über 350 Industrie 4.0-Projekte aus 24 Branchen und mehr als 50 ausführliche Experteninterviews bilden die Basis der vorliegenden Studie. Anhand von zwölf Kerntechnologien werden hier die wichtigsten Risikofaktoren in der Smarten Fabrik identifiziert und wirksame **Mitigationsstrategien** vorgestellt.

RISIKOFAKTOREN VON INDUSTRIE 4.0-ANWENDUNGEN

UMFELDBEZOGEN

POLITISCHE/RECHTLICHE IMPLIKATIONEN
Datenschutzbestimmungen

HÖHERE GEWALT
Stromausfall, Feuer, Überschwemmung

BRANCHENBEZOGEN

WETTBEWERBSUMFELD
Alternativlösung zu verbreitetem Branchenbestand

BESCHAFFUNGS-/ABSATZMÄRKTE
> Abhängigkeit von bestimmten technischen Komponenten
> Beschränkte Schnittstellen zu Supply Chain-Partnern

Fokus dieser Studie sind insbesondere die unternehmensbezogenen Risiken: Über die Probleme der Adaption und Organisation insbesondere in der Implementierungsphase der Industrie 4.0-Anwendungen, über Fehler durch Versagen von Mensch, Technik oder der Organisation bis hin zur Risiken durch Angriffe. Ebenfalls finden sich Einblicke in Risiken aus politischen und rechtlichen Implikationen.

UNTERNEHMENSBEZOGEN

PROBLEME DER ADAPTION UND ORGANISATION

UNZUFRIEDENHEIT/ ABLEHNUNG DURCH MITARBEITENDE

UNERWARTETE OPPORTUNITÄTS-KOSTEN

DURCH FEHLER

MENSCHLICHES VERSAGEN
> Bedienungsfehler
> Programmierfehler

TECHNISCHES VERSAGEN
> Fehlfunktion/Ausfall
> Datenverlust

ORGANISATORISCHES VERSAGEN
> Unzureichende Wartung
> Fehlende Updatevorgänge

DURCH ANGRIFFE

GEZIELTE ANGRIFFE
> Datendiebstahl
> (Cyber)-Angriffe auf (IT)-Infrastruktur

UNGEZIELTE ANGRIFFE
> Phishing
> Terroranschläge
> Malware

FOKUS DER STUDIE

FORSCHUNGS-DESIGN

Die vorliegende Studie kombiniert das Wissen aus einer umfangreichen Literaturrecherche mit der Analyse von 359 Industrie 4.0-Anwendungsfällen und mehr als 50 Expertengesprächen.

Die in dieser Studie ausgewerteten Industrie 4.0-Anwendungsfälle stammen aus der Datenbank „Plattform Industrie 4.0“. Hierbei handelt es sich um eine Austauschplattform für Industrie 4.0-Use Cases.

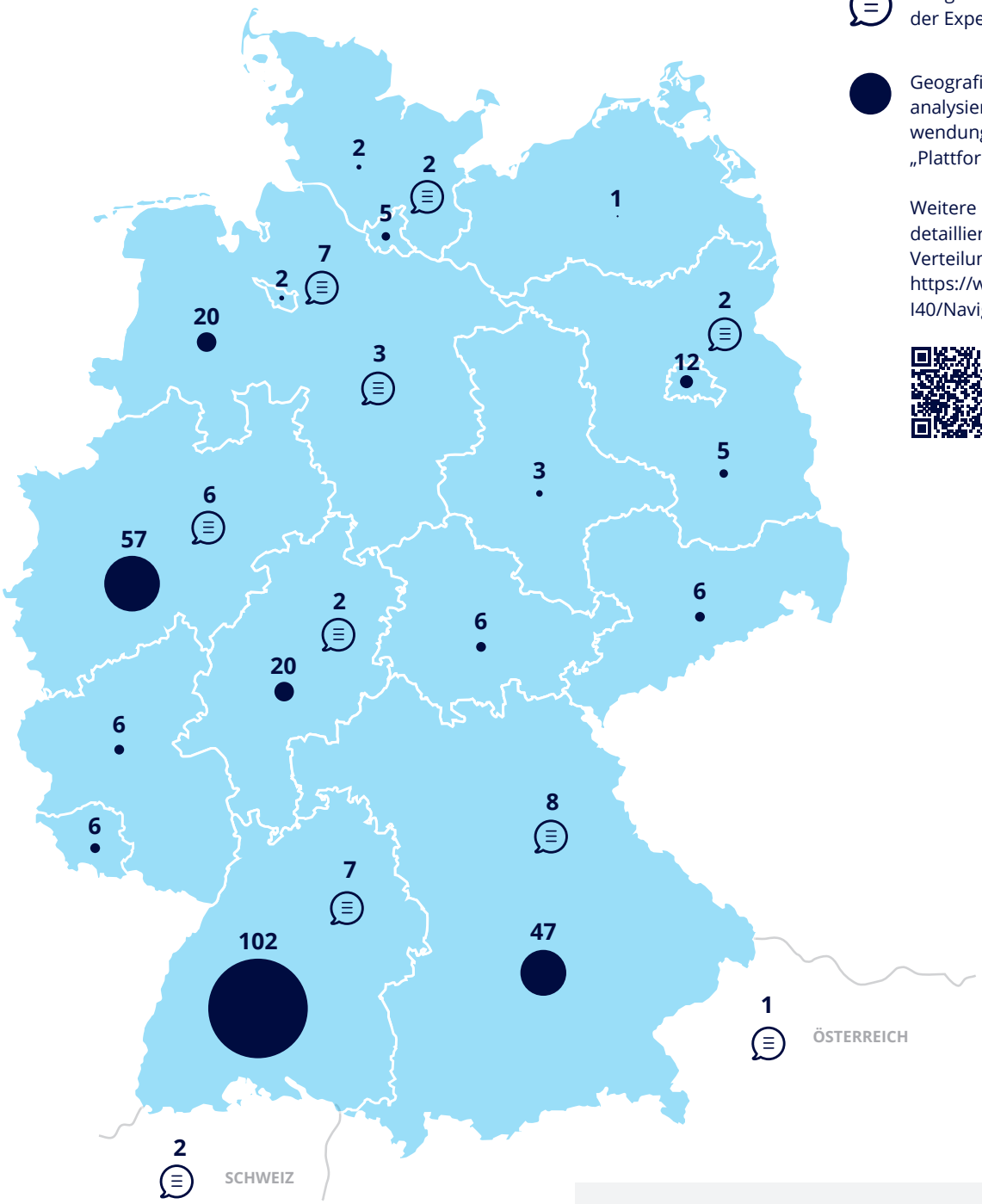
Initiiert durch die deutsche Bundesregierung hat sie das Ziel, Wissen, Erfahrungsberichte und Best Practices zu bündeln und der breiten Öffentlichkeit zur Verfügung zu stellen. Unternehmen beschreiben hier anhand eines strukturierten Erfassungsbogens ihre Industrie 4.0-Projekte und teilen spezifische Erfahrungen. Aus den dort im März 2019 als Rohdaten erfassten 359 Use-Cases konnten 300 vollständig ausgewertet werden. Auf ihrer Basis konnten zwölf Technologiekategorien gebildet und die damit einhergehenden Nutzenpotenziale und Herausforderungen für die jeweilige Industrie 4.0-Technologie analysiert werden.

Dieses Wissen wurde ergänzt um Erkenntnisse aus 54 geführten Experteninterviews. Während 14 der Interviews dem Hintergrund des Forschungsbereiches und der allgemeinen Systematisierung dienten, wurden 40 Interviews gezielt mit Anwendern und Technologieanbietern verschiedener Branchen und aus Unternehmen verschiedener Größe geführt. Die Experten wurden in einem fragebogenbasiertem, halbstrukturiertem intensiven Interview zu Technologieauswahl und -kombination, zu Nutzenpotenzialen und Herausforderungen im Projektablauf befragt. Insbesondere konnte die Bedeutung des Faktors Mensch beleuchtet werden.

Die Interviews wurden zwischen November 2018 und März 2019 durchgeführt, aufgezeichnet, transkribiert und den Expertinnen und Experten zur Durchsicht zur Verfügung gestellt.

Die Plattform Industrie 4.0 bündelt Wissen, bietet Handlungsempfehlungen und Best Practices auch für kleine und mittelständische Unternehmen und stellt diese auf einer interaktiven „Industrie 4.0 Landkarte“ als Anwendungsbeispiele von Industrie 4.0-Umsetzungen dar.
Als Datenbasis dieser Studie wurden 300 Datensätze im Jahr 2019 aus der Datenbank der Plattform ausgewertet.

(Plattform Industrie 4.0, 2021)



Geografische Verteilung der Experteninterviews

Geografische Verteilung der analysierten Industrie 4.0-Anwendungsfälle auf Basis der „Plattform Industrie 4.0“.

Weitere Informationen und detaillierte geographische Verteilung verfügbar unter: https://www.plattform-i40.de/I40/Navigation/Karte

N=300, Stand März 2019, Datenbasis: Analyse der Fallbeispiele,
Ergänzt um N=40, Datenbasis: Interviews

Ergänzend auf der Karte dargestellt ist die geografische Verteilung der 40 Experteninterviews, die mit Unternehmensvertretern in Deutschland und im deutschsprachigen Ausland geführt wurden.

HINTERGRÜNDE ZU DEN EXPERTENINTERVIEWS

FRAGENKOMPLEXE IN DEN EXPERTENINTERVIEWS

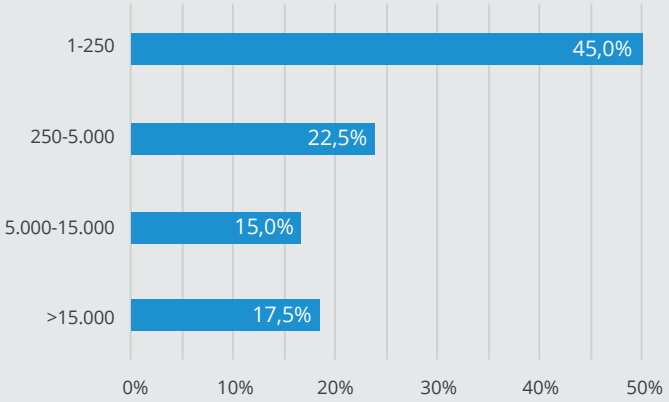
Teil 1: Industrie 4.0-Anwendungen
Anwendungsbereiche und betroffene Prozesse, Mitarbeitende, Ziele der Anwendung und Technologiekomponenten

Teil 2: Herausforderungen und Risikofaktoren in der Implementierung und Umsetzung

Teil 3: Reaktive und proaktive Risiko-managementstrategien und Mitigation in Implementierung und Umsetzung

GRÖSSE DER UNTERNEHMEN

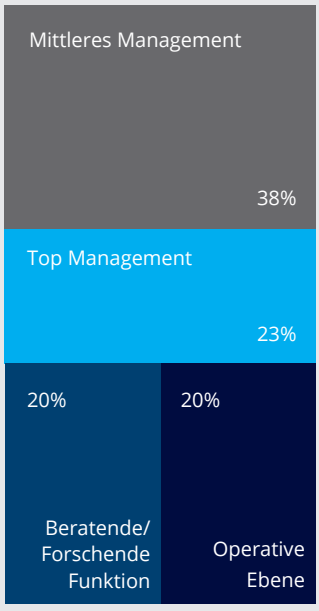
Nach Anzahl der Mitarbeitenden



N = 40, Mehrfachnennungen normalisiert | Datenbasis: Interviews.

POSITIONEN DER EXPERTEN

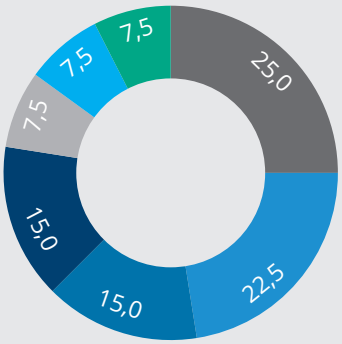
in Prozent



N = 40 | Datenbasis: Interviews.

BRANCHEN

in Prozent



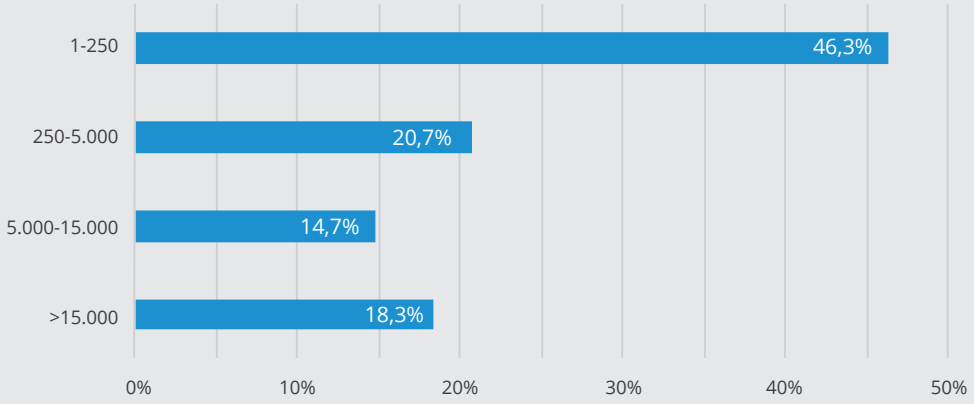
- EDV / IT / Kommunikation
- Anlagenbau / Automatisierungstechnik
- Maschinenbau
- Metalltechnik / Elektrotechnik
- Bildungseinrichtung / Forschung / Entwicklung
- Dienstleistungen / Beratung / Handwerk
- Verkehr / Logistik

N = 40, Mehrfachnennungen normalisiert | Datenbasis: Interviews.

STATISTISCHE AUSWERTUNG DER INDUSTRIE 4.0-FALLBEISPIELE

GRÖSSE DER UNTERNEHMEN

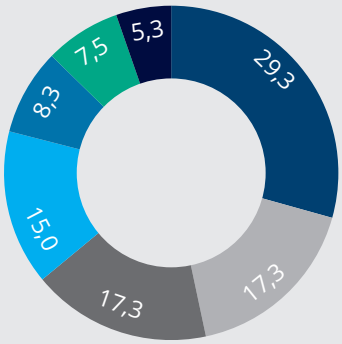
Nach Anzahl der Mitarbeitenden



N = 300, Mehrfachnennungen normalisiert | Datenbasis: Analyse der Fallbeispiele.

BRANCHEN

in Prozent

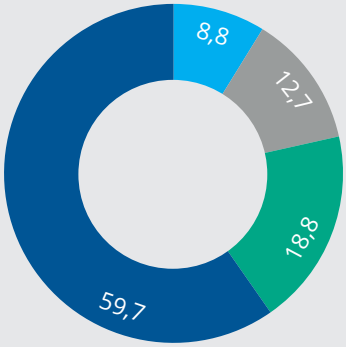


- EDV / IT / Kommunikation
- Anlagenbau / Automatisierungstechnik
- Maschinenbau
- Metalltechnik / Elektrotechnik
- Bildungseinrichtung / Forschung / Entwicklung
- Dienstleistungen / Beratung / Handwerk
- Sonstige Branchen

N = 300, Mehrfachnennungen normalisiert | Datenbasis: Analyse der Fallbeispiele.

REIFEGRAD

in Prozent



- Umsetzung durch erste Forschungs- und Entwicklungsergebnisse
- Prototypen (Demonstrator)
- Umsetzung im eingeschränkten Bereich des Anwendungsumfeldes
- Umsetzung in vollem Umfang des Anwendungsumfeldes

N = 300, Mehrfachnennungen normalisiert | Datenbasis: Analyse der Fallbeispiele.

NEUE TECHNOLOGIEN – DIE ENABLER DER SMARTEN FABRIK

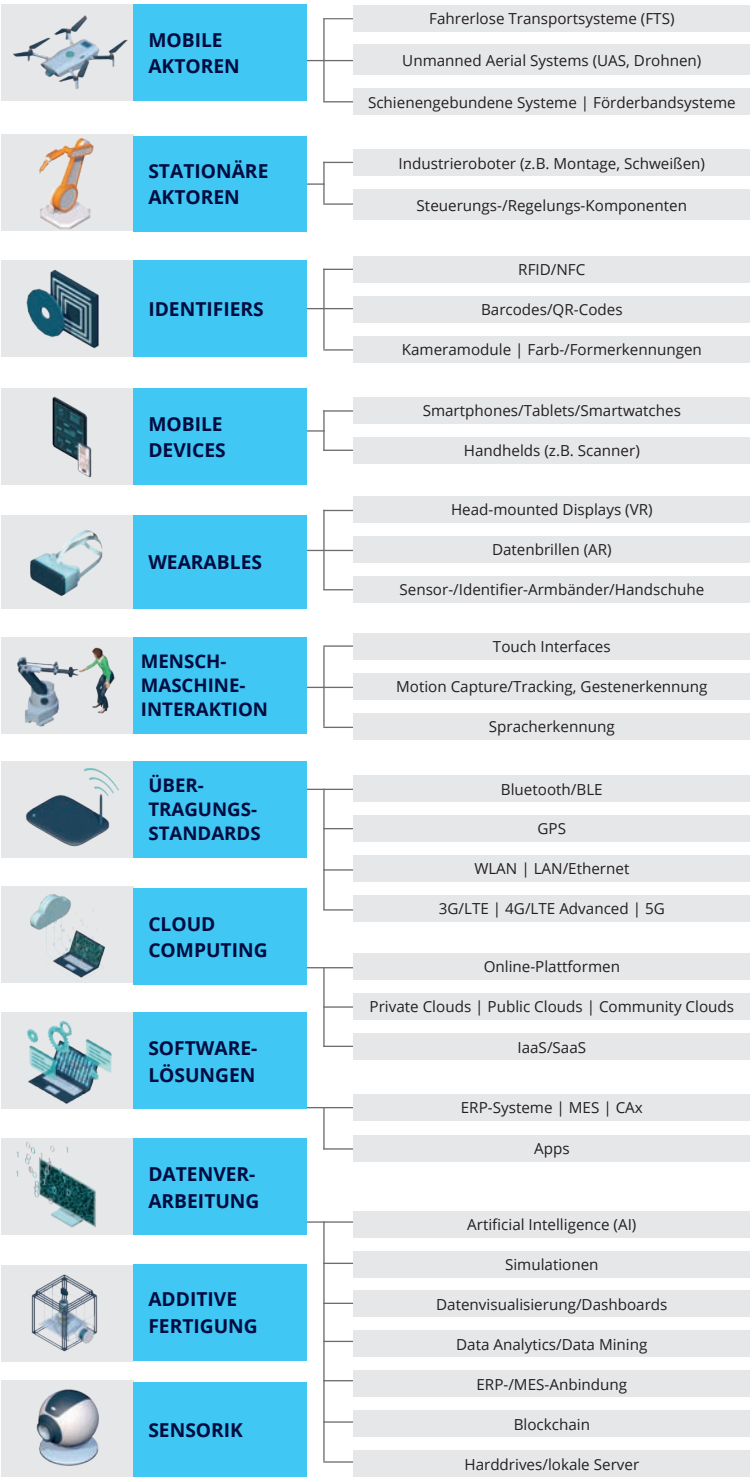
In der Fabrik der Zukunft liefern Fahrerlose Transportsysteme Material. Der Mensch wird bei komplexen Montage-, Planungs- und Steuerungsaufgaben digital unterstützt. Intelligente Objekte kommunizieren untereinander über die Cloud. Daten werden kontinuierlich gesammelt und ausgewertet. Alternative Zukunftsszenarien werden entworfen und bewertet, um noch bessere Entscheidungen zu treffen. So kommen Störungen im Prozess gar nicht erst vor oder werden automatisiert flexibel gehandhabt. Die Smarte Fabrik: Durchgängige Automatisierung, größte Adaptivität und Resilienz.

Neue Produktions- und Kommunikationstechnologien revolutionieren die Wertschöpfung

Das Internet der Dinge revolutioniert die Arbeitswelt in der Fertigung. In den Smarten Fabriken der Zukunft herrscht eine völlig neue Produktionslogik. Die Vision der vierten industriellen Revolution lässt dabei Produktion und IT zunehmend verschmelzen. Intelligente Werkstücke kennen ihre Historie, ihren derzeitigen Zustand und ihren Endbestimmungsort und steuern ihren Weg dorthin selbst. Dabei sind die Produkte auf ihrem Weg durch die Fabrik jederzeit identifizierbar und lokalisierbar. Die Maschinen und Logistiksysteme von Unternehmen sind innerhalb von Produktionsnetzwerken entlang der gesamten Supply Chain miteinander verknüpft und kommunizieren in Echtzeit miteinander. Durch den Einsatz modernster Kommunikationstechnologien entsteht eine völlig neue Art der Zusammenarbeit zwischen Mensch und Maschine.

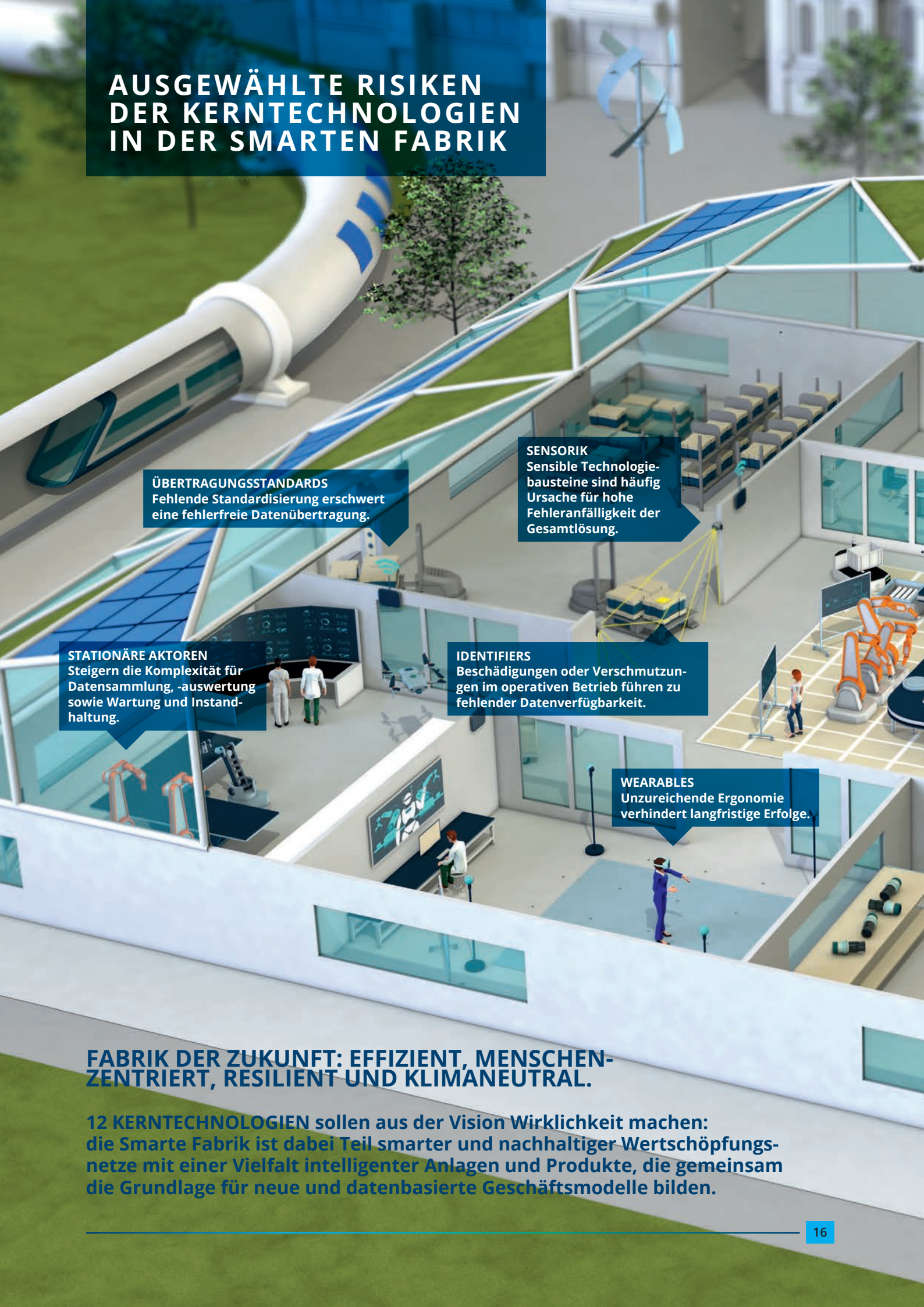
Digitale Technologien sind dabei die wichtigsten Elemente der Smarten Fabrik. 41 Basistechnologien wurden im Rahmen der Studie in zwölf Hauptkategorien gruppiert. Für jede Gruppe wurden die wichtigsten Begleittechnologien und die assoziierten Risiken und Mitigationsstrategien identifiziert.

BETRACHTETE TECHNOLOGIEGRUPPEN IN DER STUDIE



RFID: Radio-Frequency Identification | NFC: Near Field Communication | QR-Code: Quick Response Code | VR: Virtual Reality| AR: Augmented Reality | BLE: Bluetooth Low Energy | GPS: Global Positioning System | WLAN: Wireless Local Area Network | LAN: Local Area Network | LTE: Long Term Evolution | IaaS: Infrastructure-as-a-Service | SaaS: Software-as-a-Service | ERP: Enterprise-Resource-Planning | MES: Manufacturing Execution System | CAx: Oberbegriff für computergestützte Prozesse (Computer-Aided)

AUSGEWÄHLTE RISIKEN DER KERNTECHNOLOGIEN IN DER SMARTEN FABRIK



FABRIK DER ZUKUNFT: EFFIZIENT, MENSCHEN-ZENTRIERT, RESILIENT UND KLIMANEUTRAL.

12 KERNTECHNOLOGIEN sollen aus der Vision Wirklichkeit machen: die Smarte Fabrik ist dabei Teil smarter und nachhaltiger Wertschöpfungs-netze mit einer Vielfalt intelligenter Anlagen und Produkte, die gemeinsam die Grundlage für neue und datenbasierte Geschäftsmodelle bilden.


CLOUD COMPUTING
Mangelndes Know-how führt zu Unsicherheit bei Fragen der IT-Integration und Sicherheit.
SOFTWARELÖSUNGEN
Fehlende Schnittstellen und Standards erzeugen Übertragungsfehler und schon kurzfristig erhebliche Mehraufwände.
DATENVERARBEITUNG
Unstrukturierte Daten erschweren Auswertung und Weiterverarbeitung.
MOBILE DEVICES
Mangelhafte Interoperabilität durch zahlreiche notwendige Schnittstellen.
MOBILE AKTOREN
Oft unterschätzte Unfallgefahr.
MENSCH-MASCHINE-INTERAKTION
Oft unterschätzte zeit- und kosten-intensive Entwicklungsprozesse.
ADDITIVE FERTIGUNG
Fehlendes Know-how im Technologieumgang führt mittelfristig zu Qualitätsproblemen.

TECHNOLOGIEN

MOBILE AKTOREN

- Fahrerlose Transportsysteme (FTS)
- Unmanned Aerial Systems (UAS, Drohnen)
- Schienengebundene Systeme | Förderbandsysteme

Transportieren Güter unter Verwendung kabelloser Technologie, meist über eine Funkverbindung gesendete Signale.
Begleitende Technologien: Übertragungsstandards, Softwarelösungen, Datenverarbeitung

STATIONÄRE AKTOREN

- Industrieroboter (z.B. Montage, Schweißen)
- Steuerungs-/Regelungs-Komponenten

Beeinflussen Systeme und andere Aktoren auf Basis eingehender Signale.
Begleitende Technologien: Übertragungsstandards, Softwarelösungen, Datenverarbeitung

IDENTIFIERS

- RFID/NFC
- Barcodes/QR-Codes
- Kameramodule | Farb-/Formerkennungen

Machen ein Objekt, mit dem sie verknüpft sind, eindeutig identifizierbar.
Begleitende Technologien: Übertragungsstandards, Softwarelösungen, Datenverarbeitung, Sensoren

RFID: Radio-Frequency Identification | NFC: Near Field Communication | QR-Code: Quick Response Code | VR: Virtual Reality| AR: Augmented Reality

MOBILE DEVICES

- Smartphones/Tablets/Smartwatches
- Handhelds (z.B. Scanner)

Dienen der mobilen Daten-, Sprach- und Bildkommunikation oder Navigation.
Begleitende Technologien: Mensch-Maschine-Interaktion, Übertragungsstandards

WEARABLES

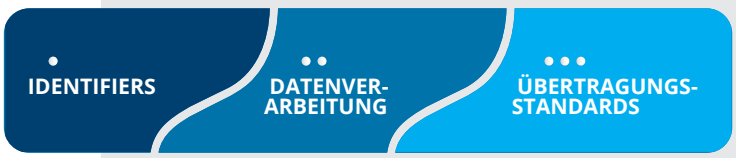
- Head-mounted Displays (VR)
- Datenbrillen (AR)
- Sensor-/Identifier-Armbänder/Handschuhe

Unterstützten direkt am Körper getragen die Arbeitsabläufe des Trägers.
Begleitende Technologien: Mobile Devices, Mensch-Maschine-Interaktion

MENSCH-MASCHINE-INTERAKTION

- Touch Interfaces
- Motion Capture/Tracking, Gestenerkennung
- Spracherkennung

Schnittstelle zwischen menschlicher Handlung und kooperierender Maschine.
Begleitende Technologien: Mobile Devices, Wearables



EINE TECHNOLOGIE KOMMT SELTEN ALLEIN – TECHNOLOGIEBÜNDEL:

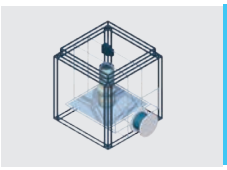
In der Praxis werden die einzelnen Basistechnologien oftmals in Kombination eingesetzt und bedingen sich teilweise gegenseitig. Beispielsweise benötigt ein RFID-Tag aus der Technologiekategorie der Identifier immer auch Übertagungsstandards und hat eine Datenverarbeitung zur Folge. Für eine detaillierte Risiko-Nutzenanalyse ist es daher wichtig, die Technologiebündel gesamthaft zu betrachten.

TECHNOLOGIEN

ÜBER-TRAGUNGS-STANDARDS

- Bluetooth/BLE
- GPS
- WLAN | LAN/Ethernet
- 3G/LTE | 4G/LTE Advanced | 5G

Überträgt Daten standardisiert unter Verwendung kabelloser Technologie.
Begleitende Technologien: Datenverarbeitung



ADDITIVE FERTIGUNG

Formt computergesteuert aus flüssigen oder festen Werkstoffschichten ein vorgegebenes Werkstück
z.B. Metalldruck, Kunststoffdruck
Begleitende Technologien: Datenverarbeitung

SENSORIK

Erfasst bestimmte Eigenschaften der Umgebung qualitativ und/oder quantitativ und gibt diese als elektrisches Signal weiter.
Begleitende Technologien: Identifiers, Übertragungsstandards

BLE: Bluetooth Low Energy | GPS: Global Positioning System | WLAN: Wireless Local Area Network | LAN: Local Area Network | LTE: Long Term Evolution | IaaS: Infrastructure-as-a-Service | SaaS: Software-as-a-Service | ERP: Enterprise-Resource-Planning | MES: Manufacturing Execution System | CAx: Oberbegriff für computergestützte Prozesse (Computer-Aided)

CLOUD COMPUTING

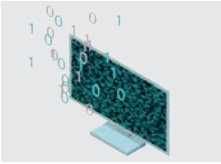
- Online-Plattformen
- Private Clouds | Public Clouds | Community Clouds
- IaaS/SaaS

Stellt Speicherplatz, Rechenleistung oder Anwendungssoftware als Dienstleistung über das Internet bereit.
Begleitende Technologien: Datenverarbeitung, Softwarelösungen

SOFTWARE-LÖSUNGEN

- ERP-Systeme | MES | CAx
- Apps

Dient der Lösung konkreter Probleme des Softwareanwenders durch eine Anwendungssoftware.
Begleitende Technologien: Datenverarbeitung



DATENVERARBEITUNG

- Artificial Intelligence (AI)
- Simulationen
- Datenvisualisierungen/Dashboards
- Data Analytics/Data Mining
- ERP-/MES-Anbindungen
- Blockchain
- Harddrives/lokale Server

Verarbeitet Datenmengen, die auf herkömmliche Weise kaum auswertbar sind.
Begleitende Technologien: Übertragungsstandards

NEUE TECHNOLOGIEN – NEUE RISIKEN – NEUE MITIGATIONSANSÄTZE

Warum es ein neues Risikomanagement braucht. Neue Technologien bringen neben großen Potenzialen neue und veränderte Risiken. Nur mit einem angepassten Risikomanagement kann die Erschließung dieser Nutzenpotenziale kurz-, mittel- und langfristig gelingen. Auch 2021 scheitern noch zu viele Projekte in der Implementierungsphase, denn der zu starke Fokus auf den Nutzen hemmt die Sicht auf die Fehlerabhängigkeit einzelner Systeme, die fehlende Verfügbarkeit benötigter Daten, mangelndes Know-how späterer Nutzer und fehlende Zeit- und Personalkapazitäten im Tagesgeschäft. Eine systematische Risikobetrachtung trägt maßgeblich zum Projekt- und zum Umsetzungserfolg bei.

Neue Technologien – das zweischneidige Schwert von Nutzen & Risiko

Digitale und vernetzte Wertschöpfung baut auf der Grundlage exzellenter Prozesse auf. So steigern bereits Computerisierung und Konnektivität signifikant die Produktivität. Mitarbeitende werden aktiv unterstützt und von repetitiven Aufgaben entlastet. Verknüpfte IT-Systeme orientieren sich operativ an exzellenten Wertschöpfungsprozessen und bilden somit die Grundlage für ein digitales Management im Sinne der Vision Industrie 4.0. So können Prozesse und Strukturen dynamisch sichtbar gemacht werden und in Echtzeit Managemententscheidungen unterstützen.

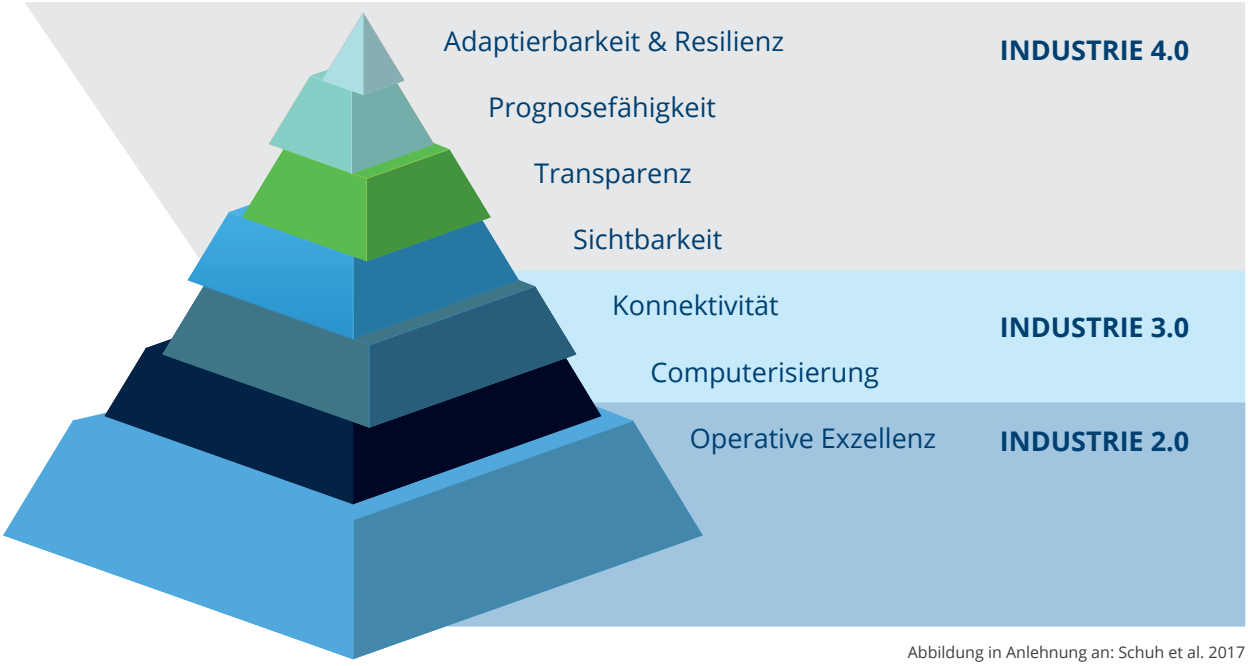
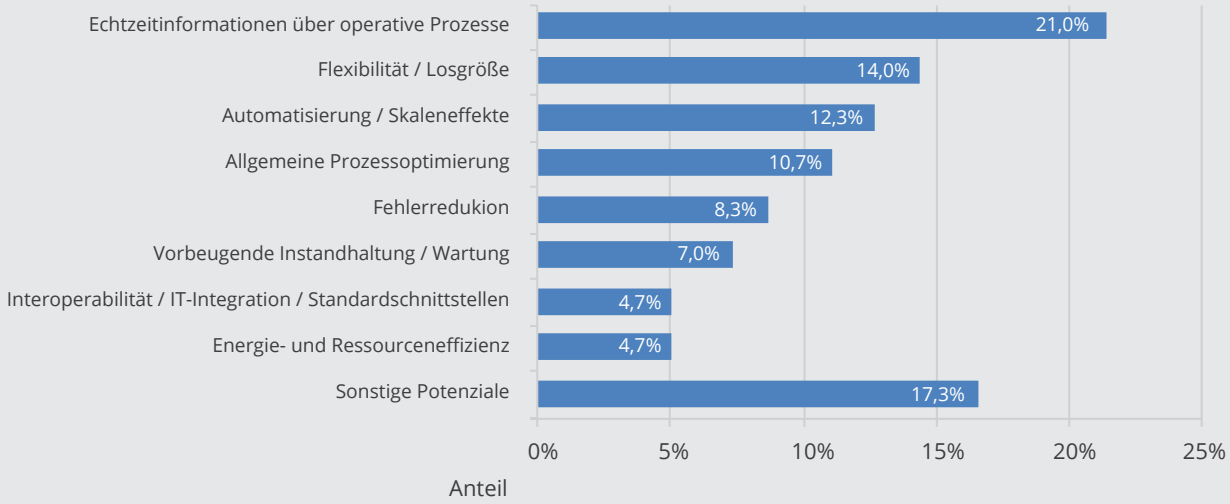


Abbildung in Anlehnung an: Schuh et al. 2017

Potenziale der Industrie 4.0-Anwendungen



N = 300, Mehrfachnennungen möglich. Antworten kategorisiert | Datenbasis: Analyse der Fallbeispiele

Die aufeinander aufbauende Logik der Potenziale der geschilderten Entwicklung zur Industrie 4.0 hin spiegelt sich auch in der Analyse der Nutzenpotenziale wider. So liegt die Hauptmotivation der analysierten Industrie 4.0-Fallbeispiele in der Verfügbarkeit von Echtzeitinformationen über operative Prozesse. Durch das Schaffen von Echtzeit-Wissen über Zustände und laufende Prozesse auf Anlagen-, Produkt-, Fabrik- und Supply Chain-Ebene wird somit die Grundlage für bessere Entscheidungen mit direktem Einfluss auf Produktions- und Lieferperformance ebenso wie auf die Produktivität und Kostensituation gelegt. Auch die Flexibilisierung und Anpassungsfähigkeit der eigenen Produktion an die volatilen Kundenbedarfe motivieren zu einem stärker digital geprägten Management.

Kurzfristig überschatten Potenziale die Risiken. Neben diesen großen Potenzialen kommt in der Diskussion oft eine systematische Betrachtung der vielfältigen Risiken dieser Technologien zu kurz. Die Gründe dafür sind zahlreich, dazu gehört oftmals das Fehlen von zeitlichen und finanziellen Ressourcen gerade in kleinen und mittelständischen Unternehmen. Die Risiken, die Projekte zum Scheitern bringen, haben häufig banale Ursachen und wären durch wenige, kostengünstige und ohne großen Aufwand mögliche Gegenmaßnahmen zu bewältigen. Zu einem späteren Zeitpunkt führen solche Ursachen jedoch zu hohen Kosten, die durch nachfolgende Verzögerungen, Ablehnung, Unfälle, Daten- und Qualitätsprobleme entstehen.

Fallstudie

Eine herbe Enttäuschung

In einem Produktionsunternehmen, das erstmals Fahrerlose Transportsysteme in der Getriebesteuerungs-Fertigung eingeführt hat, wurde das fehlende Risikomanagement zum Problem. Erst nach der Beschaffung und bei der eigentlichen Technologieinstallation wurde bemerkt, dass die zahlreichen Rampen in der Produktionshalle den Einsatz der beschafften Systeme unmöglich machen. Erhebliche Kosten, interne Personalkapazitäten und viel Frust belasten das Budget und mindern die Begeisterung für weitere Digitalisierungsprojekte.

RISIKOSCHWERPUNKTE IN DER IMPLEMENTIERUNG

In der Frühphase von Industrie 4.0-Projekten ist aktives Risikomanagement am wirksamsten. Vorausschauende Analysen der eingesetzten Technologien und der Abgleich mit potentiellen Problemen in den Bereichen Know-how, Investition, Recht, Adaptation und Integration in die Prozess- und IT-Landschaft hilft, um typische Probleme zu vermeiden.

Das größte Risiko in der Implementierungsphase ist die Ablehnung der neuen Technologie und Prozesslösung durch einzelne Mitarbeitergruppen. Schon aus vielen Jahren Veränderungs- und Entwicklungsforschung und -praxis bekannt, streben Mitarbeitende und auch Führungskräfte im Rahmen von Industrie 4.0-Projekten häufig danach Bekanntes zu erhalten, Neuerungen prinzipiell abzulehnen und den Status-Quo zu erhalten. Die Betriebsräte werden oft erst im Projektverlauf einbezogen, nicht aber in der Projektplanungsphase. In der Folge verlängern sich Lernkurven und die Produktivität sinkt auch im Alltagsbetrieb. Ein Trial-und-Error-Vorgehen bei der Veränderung hin zu einer für die Mitarbeitenden akzeptablen und produktiven Lösung führt zu Verzögerungen, Kostensteigerungen und Motivationsverlust. Dies wiederum kann eine Digitalisierungsstrategie als Ganzes gefährden. Folglich kommt es auch aus Investitionssicht zu immer mehr Problemen. Unklare Investitionskosten und ein unklarer Nutzen der Technologie mit oft unbekanntem ROI lassen auch Controlling und Top-Management das Bewährte präferieren. Nicht harmonisierte Prozess- und IT-Landschaften zeigen im Rahmen von Industrie 4.0-Projekten ihre ganze Problematik. Da diese nicht kurzfristig zu beseitigen sind, wird auch hier auf zeitlich und finanziell unplanbare Trial-and-Error-Lösungen zurückgegriffen. Besonders verheerend: um in einer fortgeschrittenen Projektphase doch noch einen Kurzfrist-Erfolg realisieren zu können, kommt es heute häufig zu Stand-Alone-Lösungen. Diese verschärfen sofort die Schnittstellenproblematik im Unternehmen und verhindern damit mittelfristig die weitere Digitalisierung.

Aber es geht anders: Problemorientierung und klare Zielorientierung schaffen schon in der Projektplanung Transparenz für alle Beteiligten. Betriebsräte und betroffene Mitarbeitende sind schon vor Projektstart einzubeziehen, zu qualifizieren und für die Lösungsgestaltung als Wissensgeber zu nutzen. Gerade in der Implementierung muss fehlendes Wissen notfalls auch durch externe Hilfe geschaffen werden.
Insbesondere gilt es Legacy Systeme (eigenentwickelte Systeme, oft unzureichend dokumentiert, mit veralteten Betriebs- und Entwicklungsumgebungen, vielen Schnittstellen und mit hoher

ROI: Return on Investment

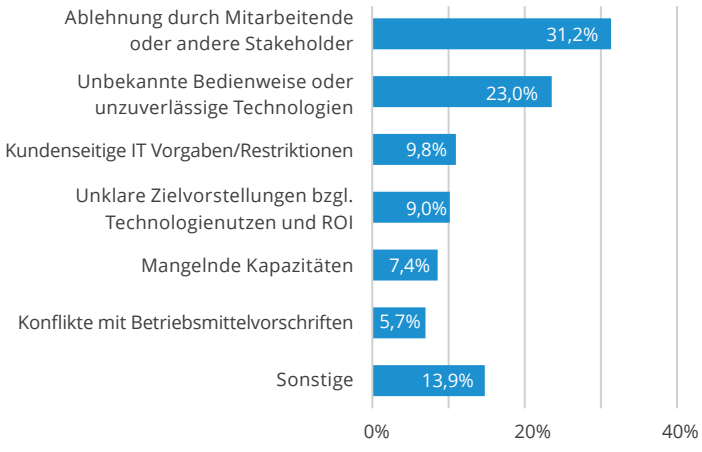
Komplexität) zu vermeiden und abzulehnen. Eigenschaften dieser Systeme erschweren zwar ihre Ablösung, fordern dies aber auch im Hinblick auf die IT-Sicherheit besonders stark. Stattdessen gilt es unternehmensweit und langfristig vorauszuschauen: Größere Veränderungen in der IT-Landschaft, beispielsweise durch die Aktualisierung der ERP-Systeme o.ä. können zum Ausgangspunkt für Projekte werden. Dies mag manchem wie ein kurzfristiger Rückschritt erscheinen, langfristig steigert der frühe Blick auf die Schnittstellen bei der Projektauswahl und -gestaltung jedoch den Projekterfolg.

Fallstudie

Basis für die Implementierung schaffen

Die Implementierung von digitalen Technologien ist verbunden mit einem erheblichen Investitionsaufwand. Insbesondere klein- und mittelständische Unternehmen sind dabei einem hohen Innovationsdruck ausgesetzt, um mit dem digitalen Fortschritt der Großunternehmen mithalten zu können. Häufig werden jedoch digitale Lösungen einfach übernommen, ohne dabei die unternehmenseigene IT- und Prozesslandschaft zu berücksichtigen, wie ein Berater für Industrie 4.0-Lösungen berichtet. Dies bestätigt auch der Fall eines KMUs, welches einen Industrieroboter für bislang manuell ausgeführte Materialveredelungsschritte einsetzen wollte. Auch wenn die Lichtverhältnisse in der ursprünglichen Arbeitsumgebung für das menschliche Auge bislang ausreichend waren, so waren sie für die Robotekamera eindeutig zu dunkel.

Risiken in der Implementierungsphase



N= 40, Mehrfachnennungen möglich, Antworten kategorisiert | Datenbasis: Interviews

RISIKOSCHWERPUNKTE IM OPERATIVEN BETRIEB

Die Betriebsphase von Industrie 4.0-Projekten fordert kontinuierliche Risikoüberprüfung. Der operative Betrieb muss sichergestellt sein. Dafür muss das Risikomanagement sowohl den Menschen als Risikofaktor betrachten als auch Fragen nach Cyberkriminalität, nach rechtlichen Risiken und nach durch die Technologienutzung geschaffenen Abhängigkeiten stellen.

In der Betriebsphase neuer Industrie 4.0-Lösungen ist eine Beeinträchtigung des operativen Unternehmensbetriebs unter allen Umständen zu vermeiden. Typische Trial-and-Error Ansätze, um über geringe Technologiereifegrade und Komplikationen in der Implementierung hinwegzutäuschen, sind leider bis heute übliche Vermeidungsstrategien. Neue Technologien und Prozesse erzeugen neue Abhängigkeiten: insbesondere sind Obsoleszenz regelmäßig zu betrachten. Nachlässigkeiten aus der Implementierung schlagen in dieser Phase voll durch. Hohe Zeit- und Kostenaufwände durch fehlende Schnittstellen und fehlende technische Komponenten und Services gefährden die Lösung selbst und das ganze System.

Zahlreiche aktuelle Beispiele zeigen, wie die zunehmende Cyberkriminalität die Arbeit von Produktions-, Handels- und Dienstleistungsunternehmen ebenso wie von Behörden und Kommunen einschränkt und gefährdet. Fehlendes Wissen und Fehleinschätzungen lassen viele Mitarbeitende auf die Sicherheit der vorhandenen Schutzeinrichtungen wie Firewalls vertrauen, sodass Phishing, Social Engineering, Datenmanipulationen und Hacking immer wieder erfolgreich sind. Auch durch unabsichtliche Bedienfehler, beabsichtigtes Umgehen existierender Standards sowie Manipulation der Technologiekomponenten entstehen Risiken. So entstehen auch rasch Compliance-Verstöße, die Konflikte mit dem Betriebsrat und sogar Klagen von intern und extern nach sich ziehen können. Die reine Adressierung in Betriebsvereinbarungen reicht hier nicht aus.

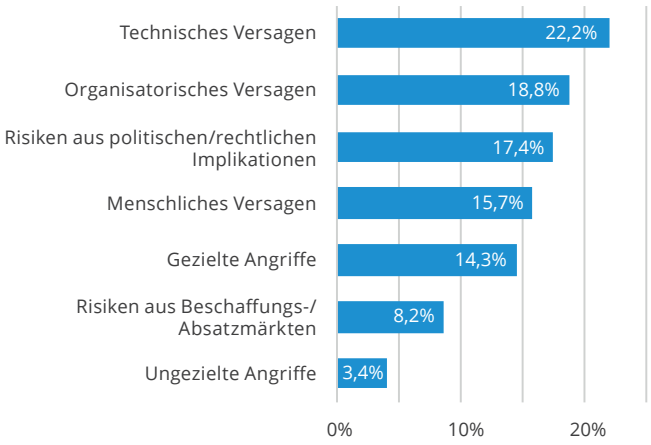
Experten sind sich einig, dass kein System absolut sicher sein kann. Dennoch trägt die Sensibilisierung und Schulung der Mitarbeitenden ganz maßgeblich zur Widerstandsfähigkeit gerade bei ungezielten Angriffen bei. White-/Blacklisting, technische Maßnahmen wie IDS und IPS, Segmentierung von Netzwerken und Backup-Strategien helfen, Cyberrisken zu minimieren.

Schon im Rahmen der Verbreitung des Lean Management-Ansatzes sind technische und organisatorische Kontrollmaßnahmen zur Fehlervermeidung bekannt geworden. Poka Yoke-Lösungen (versehentliche Fehler (poka) vermeiden (yokeru) lassen Fehler durch geschickte Prozessgestaltung gar nicht erst entstehen. Feedback- und kontinuierliche Verbesserungsprozesse (KVP) beteiligen Mitarbeitende an der schrittweisen Aufdeckung von Prozessrisiken.

IDS/IPS: Intrusion Detection Systems/Intrusion Prevention Systems | KVP: Kontinuierliche Verbesserungsprozess

"White-/Blacklisting, technische Maßnahmen wie IDS/IPS, Segmentierung von Netzwerken und Backup-Strategien helfen, Cyberrisken zu minimieren."

Risiken in der Betriebsphase



N= 40, Mehrfachnennungen möglich, Antworten kategorisiert | Datenbasis: Interviews

Fallstudie

Mittels Fernwartung Zugriff auf Daten von Mitarbeitenden

Vorausschauende Instandhaltung birgt riesige Potenziale. Einige Anbieter von sogenannten Predictive Maintenance-Lösungen bieten auch Fernwartungen an. Dies erfordert Datenzugriffe von extern. So zeigt sich im Fall eines mittelständischen Maschinenbauers erst Monate nach der Einführung der Lösung, dass deutlich mehr als die relevanten Verschleiß- und Nutzungsdaten übertragen worden sind. So wurden auch Fertigungsdaten zu Aufträgen und personenbezogene Daten zu Mitarbeiten übermittelt. Das Unternehmen reagierte umgehend und etablierte ein entsprechendes Risikomanagement mit regelmäßigen IT-Compliance-Audits.

RISIKOSCHWERPUNKTE IN DER PROJEKTIMPLEMENTIERUNG	TYPISCHER AKTUELLER UMGANG	AUSGEWÄHLTE MITIGATIONSANSÄTZE
UNZUREICHENDES TECHNOLOGIE-KNOW-HOW		
• Fehlendes Wissen zu Anwendungsarten • Unklare Lage auf Anbietermärkten • Fehlende interne/externe Erfahrungswerte	• Ablehnung von Projekten, Beibehaltung des Status Quo	• Screening von Anbietermärkten • Rückgriff auf externe Beratungsleistungen • Proof-of-Concept • Sukzessiver Rollout
INVESTITIONSRISIKEN		
• Unklare Investitionskosten, Nutzen schwer zu beziffern • Unbekannter ROI der meisten Lösungen	• Ablehnung von Projekten, Beibehaltung des Status Quo	• Opportunitätskosten einbeziehen • Vergleichbare Projekte zur Nutzenabschätzung nutzen, Risiken ermitteln und bewerten
RECHTLICHE RISIKEN		
• Compliance-Verstöße • Widerstände durch Betriebsrat	• Konsultierung des Betriebsrates im Rahmen der Einführung	• Einbezug Betriebsrat • Anpassung von Arbeitsverträgen • Techn. Anpassung, Zertifizierung
ADAPTION DER MITARBEITENDEN		
• Hohe anfängliche Widerstände • Flache Lernkurven, Produktivitätseinbußen	• Trial-and-Error	• Einbezug betroffener Mitarbeitender • Qualifizierungsmaßnahmen • Intuitives Lösungsdesign
INTEGRATION IN PROZESS- UND IT-LANDSCHAFT		
• Abweichende IT-Schnittstellen • Störungen der bestehenden IT-Infrastruktur durch Integration neuer Komponenten • Betriebsverzögerungen durch notwendige Anpassung von etablierten Prozessen	• Trial-and-Error • Vermeidung von IT-Integration und Schnittstellenproblematik durch Stand-Alone-Lösungen	• Ablösung von Legacy-Systemen • Schnittstellen als Auswahlkriterium • Synergien durch Technologie-Push nutzen/einplanen • Isolierter Pilotbetrieb

IDS/IPS: Intrusion Detection Systems/Intrusion Prevention Systems; KVP: Kontinuierliche Verbesserungsprozess; ROI: Return on Investment

RISIKOSCHWERPUNKTE IM OPERATIVEN BETRIEB	TYPISCHER AKTUELLER UMGANG	AUSGEWÄHLTE MITIGATIONSANSÄTZE
CYBERKRIMINALITÄT		
• Phishing, Social Engineering • Hacking • Datenmanipulation • Datendiebstahl	• Blindes Vertrauen auf vorhandene Schutzmaßnahmen wie Firewalls	• Sensibilisierung/Schulung der Mitarbeitenden, White-/Blacklisting • Techn. Maßnahmen wie IDS/IPS • Segmentierung von Netzwerken • Backup-Strategien • Berechtigungsmanagement
RECHTLICHE RISIKEN		
• Compliance-Verstöße, Klagen intern/extern • Konflikte mit Betriebsrat • Konflikte bezüglich Personendaten	• Adressierung in Betriebsvereinbarungen	• Anpassung von Compliance-Richtlinien durch Experten • Vertragliche Absicherungen • Selektive und verschlüsselte Datenübertragung • Datenklassifizierung
RISIKOFAKTOR MENSCH		
• Unabsichtliche Bedienfehler • Missbrauch und absichtliche Workarounds	• Einführung durch Technologieanbieter im Rahmen des Vertriebs	• Technische/organisatorische Kontrollmaßnahmen, Poka Yoke • Feedbackprozesse/KVP
DIREKTE UND INDIREKTE ABHÄNGIGKEIT		
• Rasche Obsoleszenz von Hard-/Software • Keine Schnittstellenstandards verfügbar • Verfügbarkeit techn. Komponenten/Services	• Trial-and-Error	• Auswahl substituierbarer Technologie-Produkte • Leasingmodelle/ Pay-per-X
BEEINTRÄCHTIGUNG DES OPERATIVEN BETRIEBS		
• Komplikationen mit industriellem Umfeld • Operative Beeinträchtigungen durch geringen Reifegrad/Usability	• Trial-and-Error	• Pilotbetrieb voranstellen • Evaluation der Basisprozesse vor Einführung unterstützender Technologien

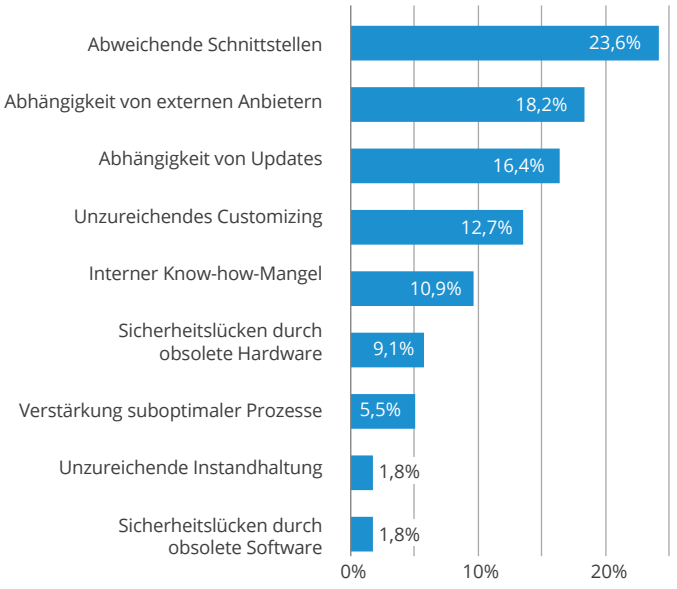
Datenquelle: Interviews, Workshop, Literatur

SPEZIELLE RISIKEN

Risiken aus organisatorischem Versagen

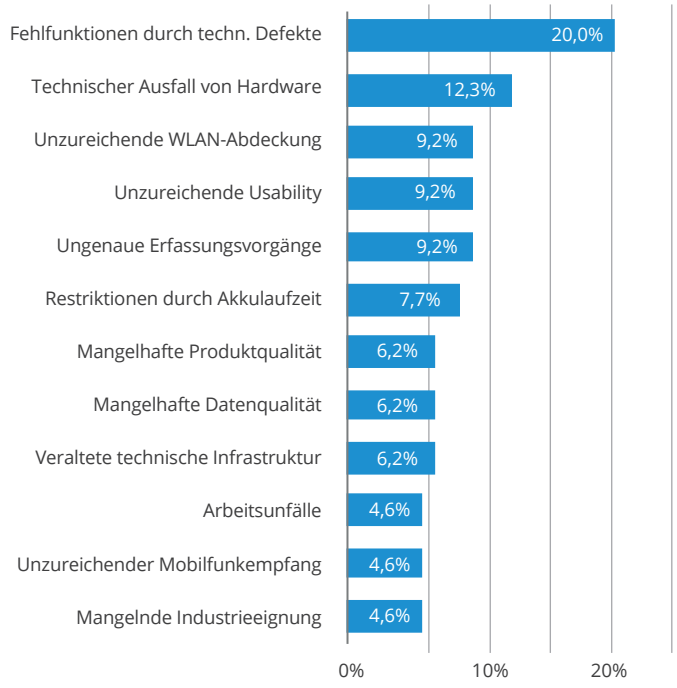
Auch wenn menschlich und technologisch bedingte Risiken durch eine gute Organisation abgefangen werden können, stellt eine nicht geeignete Organisation selbst ein Risiko für den Erfolg eines Industrie 4.0-Projekts dar. Die Mehrheit der untersuchten Technologien erzeugt gegenseitige Abhängigkeiten, die abzusichern sind. Beispielsweise gehört dazu die Abhängigkeit von Programmierern oder externen Dienstleistern, aber auch von Software- und Hardwarelieferanten. Der Einsatz komplexer Soft- und Hardware stellt darüber hinaus Anforderungen an eine gute Organisation des Updatemanagements, um Sicherheitslücken und Fehlfunktionen der Systeme zu vermeiden. Von den Experten wurden auch Risiken in den Fokus gerückt, die durch eine ungenügende Anpassung der Industrie 4.0- Technologien an die individuellen Bedürfnisse des Unternehmens entstehen. Am häufigsten wurden aber Probleme durch nicht zusammenpassende Schnittstellen als Folgen organisatorischen Versagens benannt, die den reibungslosen Ablauf innerhalb von Lieferketten gefährden können.

Risiken aus organisatorischem Versagen



N= 40, Mehrfachnennungen möglich,
Antworten kategorisiert | Datenbasis: Interviews

Risiken aus technischem Versagen



N= 40, Mehrfachnennungen möglich,
Antworten kategorisiert | Datenbasis: Interviews

Risiken aus technischem Versagen

Häufigstes technisches Risiko sind Fehlfunktion durch einzelne technische Defekte, gefolgt vom Ausfall ganzer Hardware-Systeme. Redundanzen im System führen schnell zu Problemen im operativen Betrieb. Längere Nicht-Verfügbarkeit der Systeme oder Daten- bzw. Wissensverlust können die Folge sein. Daneben bringen erfahrungsgemäß veraltete technische Infrastrukturen, die mangelnde Industrieeignung oder eine mangelhafte Produktqualität der Technologiekomponenten ein technologisch bedingtes Risiko mit sich. Auch eine unzureichende WLAN-Abdeckung oder ein unzureichender Mobilfunkempfang, sowie eine zu ungenaue und unzuverlässige Datenübertragung kann schwerwiegende Fehler erzeugen. Begünstigt werden diese technisch bedingten Risiken durch organisatorische Risiken, wie unflexible und veraltete Abläufe in IT-Abteilung, die insbesondere im Moment des Technologiewechsels ihr größtes Momentum erzeugen.

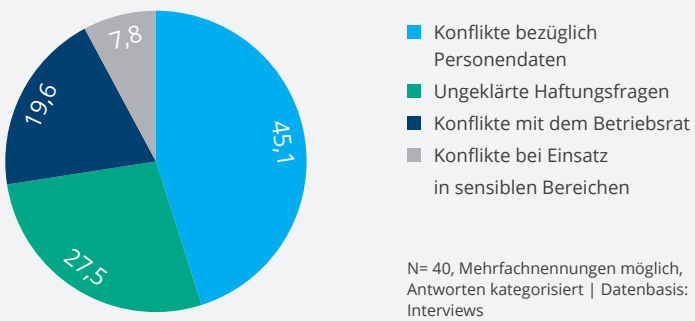
Risiken aus politischen und rechtlichen Implikationen

Smarte Technologien wie Motion Capture, Smartphones oder Datenhandschuhe sind in der Lage, ein hohes Maß an personenbezogenen oder personenbeziehbaren Daten zu generieren. Aus diesen Daten können Rückschlüsse auf Mitarbeitereffizienz, sowie An- und Abwesenheitszeiten abgeleitet werden. Das wirft die Frage auf, ob dadurch eine unrechtmäßige Mitarbeiterüberwachung entsteht. Es verwundert daher nicht, dass dieses Konfliktpotenzial das am häufigsten genannte Risiko im Bereich der rechtlichen und politischen Implikationen ist. Nicht selten resultiert aus diesen Umständen auch ein Konflikt mit dem Betriebsrat.

Viele Technologien müssen zur Sicherung der Grundfunktionalitäten aber personenbezogene Daten verarbeiten. So lässt sich beispielsweise bei einer Spracherkennungssoftware die Erfassung, Verarbeitung und Übertragung persönlicher Sprachinhalte nicht vollständig vermeiden. Wird eine externe Cloudlösung auch für die Verarbeitung von personenbezogenen Daten von KundInnen oder GeschäftspartnerInnen genutzt, entstehen dadurch zusätzlich auch noch unklare Haftungsfragen, die bereits in der Projektplanungsphase adressiert werden müssen.

Risiken aus politischen und rechtlichen Implikationen

in Prozent

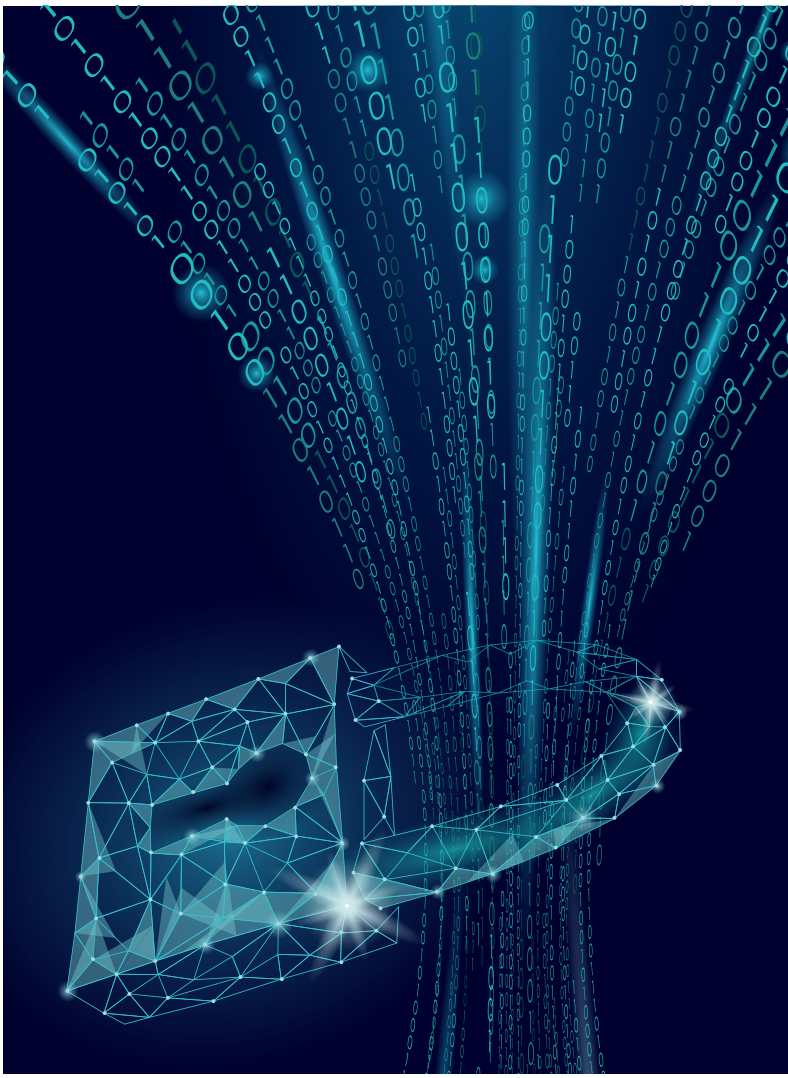


N= 40, Mehrfachnennungen möglich, Antworten kategorisiert | Datenbasis: Interviews

INDUSTRIE 4.0 CYBERRISIKEN

Management von Cyberrisiken – eine Aufgabe für das Top-Management

Risikoabwägungen in Digitalisierungsprojekten beschränken sich oft auf die so genannten Cyberrisiken. Durch die, wie eine Analyse der Funk Gruppe aus dem Jahr 2019 zeigt, ein jährlicher Gesamtschaden von mehr als 20 Milliarden Euro in Deutschland entsteht (Funk Gruppe GmbH, 2019). Dies bringt auch große volkswirtschaftliche Brisanz mit sich. Mehr als 70% von Industrieunternehmen haben bereits Erfahrungen mit Industriespionage, Sabotage oder Datendiebstahl gemacht. Fast die Hälfte aller Unternehmen wurde bereits Opfer eines Cyber-Angriffs mit finanziellen Schäden, etwa in Form von Imageschaden, Ermittlungs- und Aufklärungskosten, durch Patentrechtsverletzungen und Betriebsunterbrechungen.

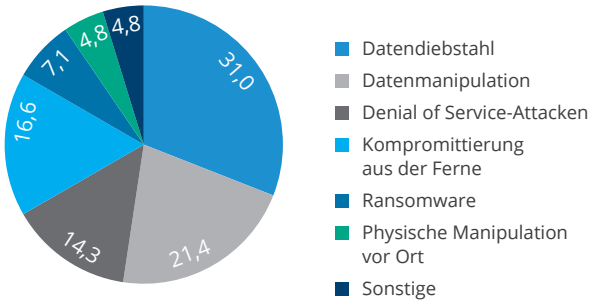


Neue Technologien und insbesondere der unsachgemäße Umgang damit bieten neue Einfallstore, die sich durch ein besseres Verständnis der Zusammenhänge von Technologien, Begleittechnologien und Mititgationsstrategien helfen, Cyberrisiken einzuschränken.

Das Risiko für gezielte und ungezielte Angriffe auf Unternehmensnetzwerke kann sich durch den Einsatz der Industrie 4.0-Technologien vergrößern. Besonders begünstigt wird dies, wenn eine zentrale Datenhaltung oder neue IT-Infrastruktur aufgebaut werden muss.
Die Experten fürchten dabei sowohl Datendiebstahl als auch Datenmanipulation im Unternehmen. Als Angriffsszenarien sehen sie ihr Unternehmen besonders durch Ransomware, (Distributed) Denial of Service-Attacken (DDoS) oder indirekte Methoden wie Phishing oder Malware gefährdet.

Risiken aus gezielten Angriffen

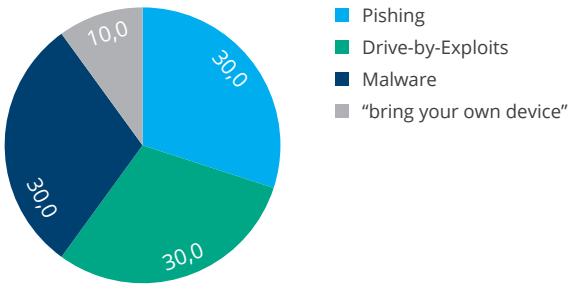
in Prozent



N= 40, Mehrfachnennungen möglich, Antworten kategorisiert | Datenbasis: Interviews

Risiken aus ungezielten Angriffen

in Prozent



N= 40, Mehrfachnennungen möglich, Antworten kategorisiert | Datenbasis: Interviews

Fallstudie

Risiko: Hacking über IT-Dienstleister

Kaseya bietet Softwareprogramme für Firmen, welche ihren Kunden administrative und organisatorische Arbeiten abnehmen. Nach dem Hackerangriff auf diesen IT-Dienstleister im Juni 2021 wurde bekannt, dass bis zu 1500 Unternehmen in 17 Ländern von der Attacke betroffen waren. Die Hackergruppe REvil soll das Desktop-Management-Tool VSA (Virtual System Administrator) von Kaseya gekapert und ein schadhaftes Update aufgespielt haben. Dabei wurden Abrechnungssysteme mit Ransomware infiziert und durch Verschlüsselung der Hacker blockiert. In Schweden war die Störung am stärksten zu spüren. Hunderte von Supermärkten mussten schließen, weil ihre Kassen nicht funktionierten. Die Hackergruppe REvil hat ca. 70 Millionen Dollar für die Wiederherstellung aller Daten gefordert. Es wurde ein Lösegeld direkt an REvil bezahlt.

(Manager Magazin, 2021)

FAKTOR MENSCH

Der HUMAN FACTOR – die Schlüsselressource in Industrie 4.0-Projekten

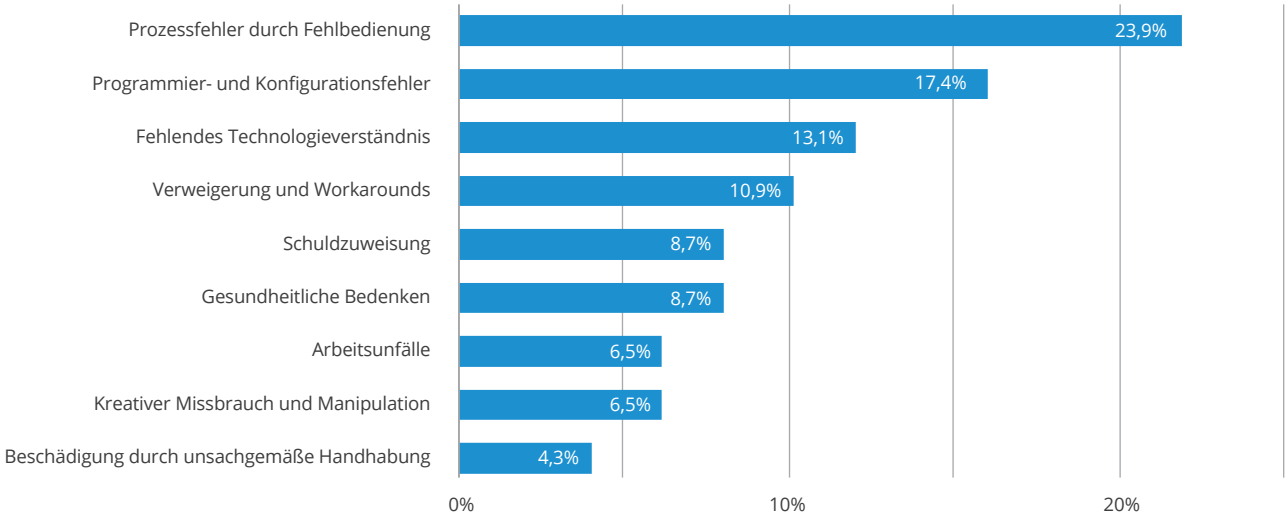
Der Mensch ist die Schlüsselressource im digitalen Zeitalter – trotz zunehmender Automatisierung. Die EU hebt die menschen-zentrierte und resiliente Produktion unter dem Begriff Industrie 5.0 derzeit prominent hervor (European Commission, 2021). Insbesondere als Nutzer und Manager von neuen Technologien nimmt der Mensch dabei eine bedeutende Rolle in der erfolgreichen Umsetzung von digitalen Projekten und der Gestaltung der Transformation ein. Für eine vollständige Realisierung der Nutzenpotenziale bedarf es daher eines systematischen Risikomanagements von menschlichen Fehlerquellen.

Fallstudie

Gut gemeint. Schlecht umgesetzt.

Ein Fertigungsleiter berichtet von der Einführung von RFID gesteuerten Kleinladungsträgern in der Logistik. Zur automatischen Identifikation und Lokalisierung müssen diese ein RFID-Antennentor in der Halle passieren. Immer wieder kam es jedoch zu Abweichungen von diesem Standard:
Werden die Materialien in den Kleinladungsträgern in der Fertigung dringend benötigt, entnahmen Mitarbeitende diese bereits vor dem Gate. Der RFID-Tag wurde entfernt und die angestrebte, vollständige Nachverfolgbarkeit war nicht mehr gegeben. Mit dem Ziel den Prozess kurzfristig zu beschleunigen, werden so mittelfristig große Probleme geschaffen. Der Gesamterfolg des Projekts konnte nicht erzielt werden.

Risiken aus menschlichem Versagen



N= 40, Mehrfachnennungen möglich, Antworten kategorisiert | Datenbasis: Interviews

Der Mensch selbst trägt Risiken in die smarte Fabrik ein. So entsteht eine Vielzahl von Herausforderungen wie Bedien-, Programmier- und Konfigurationsfehlern. Fehlendes Technologieverständnis und Workarounds gefährden ebenfalls Projekterfolge und den operativen Betrieb. Die Expertengespräche zeigen, dass mit der Digitalisierung einhergehenden Risiken in den Unternehmen bekannt sind. Kommt es zum konkreten Projekt, werden diese aber regelmäßig für das eigene Unternehmen als irrelevant eingestuft. Erst auf Nachfrage bei den Projektverantwortlichen zeigt sich, dass sich hinter diesem „Bekanntsein" oft nur wenig konkrete Vorstellungen von Gefahren abseits von plakativem „Hacking" verbergen. Industrie 4.0-Projekte werden z.B. oft als klassische IT-Projekte verkannt. Implizite Risiken werden gar nicht erst gesucht und daher auch nicht aktiv gemanagt. In der Folge werden bestehende Schutzmaßnahmen nicht an neue Prozesse und Technologien angepasst.

Technologien aus dem Endkonsumentenbereich mit hoher Anziehungskraft

Technologien aus dem Endkonsumentenbereich, wie Smartphones, Tablets, Smartwatches usw. haben einen hohen Reifegrad, geringe Kosten, und zahlreiche Substitute am Markt. Gerade in der Frühphase von Digitalisierungsinitiativen werden diese gerne in Industrielösungen integriert und bspw. zum Datenaustausch an existierende IT-Systeme angebunden. Mit Verbreitung und Reifegrad von Technologien steigen jedoch auch Anzahl und Reifegrad der zugehörigen Bedrohungen – die nun auch technologiegestützte Prozesse unmittelbar gefährden.

Compliance – Anfangs wichtig, zum Ende vergessen

Die Experten heben die große Relevanz von Compliance-Risiken hervor - insbesondere bei der Sammlung, Speicherung und Verarbeitung von Daten eigener Mitarbeitenden und von Supply Chain-Partnern. Sobald die Anfangsphase der Projekte jedoch überwunden ist, steht vor allem der operative Betrieb im Fokus. Funktioniert eine Industrie 4.0-Lösung im operativen Betrieb, enden häufig Compliance-Überlegungen.

Ohne entsprechendes Know-how enden Lösungen minimalinvasiv, stand-alone und dezentral

Insbesondere in klein- und mittelständischen Unternehmen scheuen Projektverantwortliche integrative Lösungen. Hier fehlt es häufig an Know-how, um Kosten und Nutzen der häufig suboptimalen Lösungen einzuschätzen.

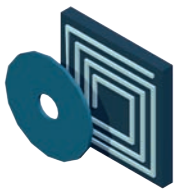
Die unbedingte Vermeidung zeitweiser operative Einschränkungen bei der Inbetriebnahme führen zur Inanspruchnahme „minimalinvasiver" Stand-alone-Lösungen.

Ohne Anbindung an vorhandene IT-Systeme oder M2M-Schnittstellen mit Zugängen über Web-Client und Apps werden so Lösungen geschaffen, deren Risiken spätestens mittelfristig den Nutzen überschatten werden.

Ebenso versuchen Projektverantwortliche die Nutzung von Cloud-Lösungen zu vermeiden. Eine unternehmenseigene und häufig lokale Datensicherung (mit entsprechendem Sicherheitskonzept) wird typischerweise ohne genauere Analyse bevorzugt, wenngleich Praxiserfahrungen zeigen, dass Clouddienste aufgrund standardisierter Sicherheitskonzepte On-Premise-Lösungen oftmals überlegen sind.

M2M: Machine-to-Machine

Ausgewählte Risiken und Mitigationsansätze der Kerntechnologien

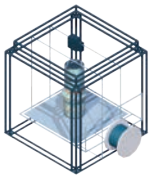
	TOP 5 RISIKEN	TOP 5 MITIGATIONSANSÄTZE
MOBILE AKTOREN 	1. Unbekannte Basistechnologie und Bedienweise 2. Abhängigkeit von externen Anbietern 3. Konflikte bezüglich Personendaten 4. Arbeitsunfälle 5. Physische Manipulation vor Ort	1. Poka-yoke/Safety-by-Design nutzen 2. Austauschgeräte vorhalten und bereitstellen 3. Mitarbeitende einbeziehen 4. Selektive und verschlüsselte Datenübertragung 5. Screening von Anbietermärkten
STATIONÄRE AKTOREN 	1. Absichtliche Workarounds 2. Abweichende Schnittstellen 3. Technischer Ausfall von Hardware 4. Sicherheitslücken durch obsolete Hardware 5. Unbekannte Basistechnologie und Bedienweise	1. Hardwareoffene Ausgestaltung 2. Mitarbeitende schulen 3. Begleitung durch Technologie-anbieter 4. Einbezug des Betriebsrates 5. Fallback-Prozesse
IDENTIFIERS 	1. Ablehnung durch Mitarbeitende 2. Verstärkung suboptimaler Prozesse 3. Datenmanipulation 4. Fehlfunktionen durch technische Defekte 5. Malware	1. Proof-of-Concept und sukzessiven Rollout einplanen 2. Fallback-Prozesse 3. Mitarbeitende schulen 4. Aufbau von Redundanzen 5. Berechtigungsmanagement

Neben den vorgestellten Implementierungs- und Betriebsrisiken, lassen sich die in den Expertengesprächen genannten Risikofaktoren auch einzelnen Technologiegruppen zuordnen. Diese Übersicht zeigt einen Auszug dieser Risikofaktoren und bewährter Praktiken des Risikomanagements.

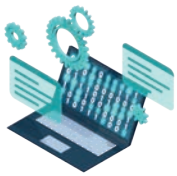
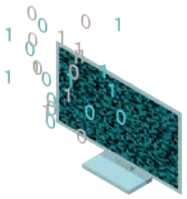
	TOP 5 RISIKEN	TOP 5 MITIGATIONSANSÄTZE
MOBILE DEVICES 	1. Ablehnung durch Mitarbeitende 2. Fehlfunktionen durch technische Defekte 3. Beschädigung durch unsachgemäße Handhabung 4. DoS/DDoS 5. Konflikte mit dem Betriebsrat	1. Aufbau von Redundanzen 2. Einsatz lokaler Server 3. Fallback-Prozesse 4. Rechtlichen Rahmen schaffen 5. Proof-of-Concept und sukzessiven Rollout einplanen
WEARABLES 	1. Ablehnung durch Mitarbeitende 2. Ergonomische Beeinträchtigung durch Dauereinsatz 3. Restriktionen durch Akkulaufzeit 4. Rasche Hardware-Obsoleszenz 5. Gesundheitliche Bedenken	1. Hardwareoffene Ausgestaltung 2. Mitarbeitende schulen 3. Begleitung durch Technologieanbieter 4. Einbezug des Betriebsrates 5. Fallback-Prozesse
MENSCH-MASCHINE-INTERAKTION 	1. Ablehnung durch Mitarbeitende 2. Kundenseitige IT Vorgaben / Restriktionen 3. Unbekannte Basistechnologie und Bedienweise 4. Konflikte bezüglich Personendaten 5. Prozessfehler durch Fehlbedienung	1. Mitarbeitende schulen 2. Proof-of-Concept und sukzessiven Rollout einplanen 3. Poka-yoke/Safety-by-Design nutzen 4. Begleitung durch Technologieanbieter 5. Mitarbeitende einbeziehen

DoS/DDoS: Denial of Service/Distributed Denial of Service | Kein Anspruch auf Vollständigkeit

Ausgewählte Risiken und Mitigationsansätze der Kerntechnologien

	TOP 5 RISIKEN	TOP 5 MITIGATIONSANSÄTZE
ÜBER-TRAGUNGS-STANDARDS 	1. Unzureichende Signal-Abdeckung 2. Kundenseitige IT Vorgaben / Restriktionen 3. Datenmanipulation 4. Datendiebstahl 5. Ablehnung durch Mitarbeitenden	1. Netzwerke segmentieren 2. Fallback-Prozesse 3. Berechtigungsmanagement 4. Aufbau von Redundanzen 5. Klassifizierung erfasster und gespeicherter Daten
ADDITIVE FERTIGUNG 	1. Unzureichende Usability 2. Datenmanipulation 3. Fehlendes Technologie-verständnis 4. Unklare Rollenverteilung im Supply Chain / Kooperations-probleme 5. Konflikte mit Betriebsmittel-vorschriften	1. Mitarbeitende schulen 2. Poka-yoke/Safety-by-Design nutzen 3. Revision bestehender Schutzmaßnahmen 4. Auditierung sowie Zertifizierungen prüfen und anpassen 5. Einsatz lokaler Server
SENSORIK 	1. Fehlfunktionen durch technische Defekte 2. Ungeklärte Haftungsfragen 3. Konflikte bezüglich Personendaten 4. Kundenseitige IT Vorgaben / Restriktionen 5. Unzureichender Mobilfunkempfang	1. Technischen Support organisieren 2. Eingeschränkten Offline-Modus anbieten 3. Anpassung des Haftpflicht-Versicherungsschutzes 4. Fallback-Prozesse 5. Softwareoffene Ausgestaltung

Weiterführende Informationen zur ausführlichen Einschätzung Ihrer Risiken und korrespondierende Mitigationsstrategien finden Sie auf der folgenden Seite.

	TOP 5 RISIKEN	TOP 5 MITIGATIONSANSÄTZE
SOFTWARE-LÖSUNGEN 	1. Konflikte bezüglich Personendaten 2. Abhängigkeit von Updates 3. Abweichende Schnittstellen 4. Unzureichendes Customizing 5. Abhängigkeit von Betriebssystem	1. Rechtlichen Rahmen schaffen 2. Screening von Anbietermärkten 3. Auditierung sowie Zertifizierungen prüfen und anpassen 4. Definition fixer Schnittstellen 5. Einbezug des Betriebsrates
CLOUD-COMPUTING 	1. Datendiebstahl 2. DoS/DDoS 3. Datenmanipulation 4. Phishing 5. Ablehnung durch Mitarbeitende	1. Umzug auf zertifizierte Cloudlösungen 2. Revision bestehender Schutzmaßnahmen 3. Berechtigungsmanagement 4. Einsatz lokaler Server 5. Selektive und verschlüsselte Datenübertragung
DATENVER-ARBEITUNG 	1. Konflikte bezüglich Personendaten 2. Ungeklärte Haftungsfragen 3. Interner Know-how-Mangel 4. Phishing 5. Ablehnung durch Mitarbeitende	1. Rechtlichen Rahmen schaffen 2. Mitarbeitende schulen 3. Selektive und verschlüsselte Datenübertragung 4. Mitarbeitende einbeziehen 5. Screening von Anbietermärkten

DoS/DDoS: Denial of Service/Distributed Denial of Service | Kein Anspruch auf Vollständigkeit

FINDEN SIE RISIKEN IN DIGITALEN PROZESSEN UND IN DER SMARTEN FABRIK

Risikoanalyse in wenigen Minuten. Mit den webbasierten Tools aus der Digital Quick Check-Familie können Sie schnell, kostenlos und sicher eine erste Einschätzung Ihrer Risikosituation vornehmen – in der Fabrik und entlang der gesamten Lieferkette.

Der Digital Quick Check

Egal ob Anwender, Technologieanbieter oder einfach am Thema interessiert – der webbasierte Digital Quick Check hilft Industrie 4.0 Anwendungsszenarien systematisch zu betrachten. Basierend auf den Detailergebnissen der Studie zu Risikoprofilen einzelner Technologien in unterschiedlichsten Anwendungsfeldern erhalten Sie Ihre individuelle Risikoanalyse. Grenzen Sie die aufgezeigten Risiken weiter ein, erhalten Sie detaillierte Informationen und lassen Sie sich geeignete Mitigationsstrategien vorschlagen. Nutzen Sie das Tool um sich, Kollegen und Mitarbeitende für Risiken und die Sorgfaltspflichten bei der industriellen Digitalisierung zu sensibilisieren.

Auch Interessierte können durch das breit angelegte Nutzerprofil von diesem Tool profitieren. Je nach Nutzerprofil werden die zu durchlaufenden Schritte angepasst, um so ein individuelles Risiko- und Mitigationsergebnis zu erhalten.

Der Zeitaufwand ist gering: Für die qualitative, aber aussagekräftige Analyse benötigt das Tool weder sensible noch umfangreiche Unternehmensdaten. Das Schwester-Tool Supply Chain Quick Check liefert schnell eine Informationsgrundlage für die Risikobewertung in Ihrer Lieferkette. Ständig aktuell durch die Verknüpfung mit einer Vielzahl von Informationsquellen zu Naturgefahren, Transportrisiken, Infrastrukturen, politischer Stabilität, Bildung und Nachhaltigkeit und vielen weiteren Aspekten erhalten Sie individuelle Analysen zu umwelt-, industrie- und unternehmensbezogenen Risiken Ihrer Lieferkette.

Speichern Sie jederzeit Ihre Zwischenergebnisse lokal und sicher. Laden Sie aussagekräftige Grafiken zu Ihren Analysen herunter und schaffen Sie so eine Diskussionsgrundlage zum Thema Risiko in der Fabrik und entlang der Supply Chain!

SUPPLY CHAIN
QUICKCHECK

Finden Sie Risiken in Ihrer Lieferkette!

Durch die Globalisierung werden Firmen Teil einer immer größer werdenden Lieferkette ...

https://supplychain.risk-quickcheck.de/de/

DIGITAL
QUICKCHECK

Finden Sie Risiken in digitalen Prozessen und Ihrer smarten Fabrik!

Im Zeitalter von Industrie 4.0 halten digitale Technologien Einzug in Unternehmen ...

https://risk-quickcheck.de/digital/tool/

Inhaltliche Ergänzung

Querverlinkung

HANDLUNGS-EMPFEHLUNGEN

FÜR EIN ZUKUNFTSORIENTIERTES RISIKOMANAGEMENT

Mit neuem Risikomanagement die Potenziale von Digitalisierung und Automatisierung erschließen!

OPERATIVE EXZELLENZ.

Sie bildet die Basis für Computerisierung und Vernetzung. Durch den Abbau von Schnittstellen, die Standardisierung von Prozessen und Harmonisierung der IT-Landschaft schaffen Sie die Voraussetzungen für weitere Potenziale und begegnen Risiken bereits an der Wurzel. Einer der Hauptgründe für das Scheitern von Digitalisierungsprojekten liegt in der hohen Komplexität, der fehlenden Flexibilität und mangelnden Interoperabilität der zugrundeliegenden Prozesse.

FAKTOR MENSCH.

Handlungsdruck klar kommunizieren. Unsicherheit, Unwissenheit über Projektziele und Motivation, fehlendes Know-how und fehlende Übung im Umgang mit neuen Technologien lassen Projekte scheitern. Führungskräfte und Mitarbeitende frühzeitig einbeziehen. Bedarfsgerechte Schulungen, Feedbacks sowohl in der Implementierung und im operativen Betrieb sind wesentliche Aspekte der Risikobewältigung.

RESSOURCEN BEREITSTELLEN.

Tagesgeschäft und Wettbewerbsdruck verschlingen dringend benötigte Ressourcen für Vorüberlegungen, Pilotierung und Vorbereitung. Ohne ausreichende Personal-, IT- und finanzielle Ressourcen fehlt die ganzheitliche Betrachtung. Kurzfristige Projektinitiativen führen so nicht zur langfristigen Erschließung von Potenzialen. Zu lange Entwicklungszeiten führen zu Störungskaskaden im Projekt, zu Kostensteigerungen und Motivationseinbrüchen. Ohne ausreichende Schulung der Nutzer fehlen Vertrauen, Sicherheit und Qualität.

TECHNOLOGIEREIFEGRAD PRÜFEN.

Ausreichend Zeit und Ressourcen für Technologieauswahl, Pilotierung und Behebung von Kinderkrankheiten einplanen. Die Fehleranfälligkeit von Technologien und Prozessen ist der größte Risikofaktor für den Erfolg von Digitalisierungs- und Automatisierungsprojekten.

DATENGRUNDLAGE SCHAFFEN.

Fehlende Prozesstransparenz, unklare Schnittstellen und fehlende Daten müssen idealerweise vor Pilot- und Implementierungsbeginn spätestens aber im Operativbetrieb vorhanden sein. Noch immer scheitern zu viele Industrie 4.0-Projekte an fehlenden und unverknüpften Datenmengen.

KOOPERATION.

Potenziale entfalten sich in besonderen Maße entlang der Lieferkette. Durch Standards, definierte Schnittstellen und neue Technologien Potenziale erschließen, durch Transparenz und integrierte Planung und Steuerung Resilienz erhöhen und gemeinsam schneller auf Störungen reagieren.

LEHRSTUHL PRODUKTIONSSYSTEME UND AUTOMATISIERUNG

PROF. DR. OEC.
JULIA C. ARLINGHAUS
Lehrstuhl-
inhaberin

YAZGÜL FIDAN
Wissenschaftliche
Mitarbeiterin

MELANIE KESSLER
Wissenschaftliche
Mitarbeiterin

FALKO BENDIK
Wissenschaftlicher
Mitarbeiter

LAURA REINECKE
Wissenschaftliche
Mitarbeiterin

Der Lehrstuhl für Produkionssysteme und Automatisierung sucht nach Lösungen für das Management komplexer, dynamischer und vernetzter Produktions- und Logistikprozesse. Digitalisierung und Automatisierung im Sinne der Vision der Industrie 4.0 stehen dabei ebenso im Fokus wie Nachhaltigkeit, Resilienz und Mensch-Zentrierung im Sinne der Vision der Industrie 5.0. Wir kombinieren Grundlagenforschung und angewandte Forschung und schaffen so eine inspirierende Atmosphäre für individuelle Lehre und akademische Beratung.

Unsere Mission ist es, Unternehmen bei der Digitalisierung und Automatisierung der Produktions-, Planungs- und Steuerungsprozesse sowie ihrer Geschäftsmodelle zu unterstützen. Dies ist eine interdisziplinäre Herausforderung. Wir arbeiten an der Schnittstelle von Management, Ingenieurwissenschaften, Produktion, Logistik und Informatik. Wir kooperieren eng mit Wissenschaftlern und Praktikern aus einer Vielzahl von Industrien und Forschungsrichtungen, u.a. Informatik, Mathematik, Psychologie und Biologie.

Gerne kooperieren wir in den folgenden Themenfeldern mit Ihnen:

- Risiko- und Reputationsmanagement in der smarten Fabrik und in globalen Lieferketten
- Planung und Steuerungssysteme in der smarten Fabrik
- Digitale und nachhaltige Wertschöpfungsnetzwerke
- Produktion und Logistik in und für Entwicklungsländer

Mehr Informationen finden Sie auf unserer Website: http://psa.ovgu.de/forschung.html

OTTO VON GUERICKE UNIVERSITÄT MAGDEBURG

LEHRSTUHL PSA

FUNK STIFTUNG

Mit den Fördermitteln der Funk Stiftung soll dazu beigetragen werden, das Bewusstsein für einen methodischen und analytischen Ansatz zur Risikobeurteilung und -bewältigung weiterzuentwickeln. Zu diesem Zweck konzentriert sich die Funk Stiftung auf Forschungs- und Praxisprojekte aus dem Bereich Risikomanagement. Im Vordergrund stehen hierbei die Entwicklung von Risikobewertungsmodellen und Tools, multinationale Projekte, die Förderung von Risikoforschung sowie die Weiterentwicklung des Risikobewusstseins. **www.funk-stiftung.org/de/die-stiftung**

Referenzen

- European Commission, 2021, A. Industry 5.0 - Towards a sustainable, human-centric and resilient European industry, 1st Edition [online], https://op.europa.eu/en/publication-detail/-/publication/468a892a-5097-11eb-b59f-01aa75ed71a1/, Zugriff am 06.07.2021.
- Plattform Industrie 4.0, 2021, FAQ [online], https://www.plattform-i40.de/PI40/Navigation/DE/Plattform/FAQ/faq.html, Zugriff am 18.06.2021.
- Funk Gruppe GmbH, 2019, Funk Cyber-Schadenspiegel 2019 [online], https://www.funk-gruppe.de/de/themen-blog/risikomanagement/funk-cyber-schadenspiegel-2019, Zugriff am 18.06.2021.
- Manager Magazin, 2021, Hackergruppe Revil erpresst bis zu 1500 Unternehmen [online], https://www.manager-magazin.de/unternehmen/tech/revil-hacker-erpressen-bis-zu-1500-unternehmen-a-154d0c68-7df0-4981-b802-40170b99db52, Zugriff am 06.07.2021.
- Schuh, G., Anderl, R., Gausemeier, J., ten Hompel, M., & Wahlster, W. (Hrsg.), 2017. Industrie 4.0 Maturity Index: Die digitale Transformation von Unternehmen gestalten (acatech Studie), München: Herbert Utz Verlag.

LEHRSTUHL PSA
PRODUKTIONSSYSTEME und –AUTOMATISIERUNG

OTTO VON GUERICKE UNIVERSITÄT MAGDEBURG

Fraunhofer IFF

Gefördert durch:

funk STIFTUNG

Wenn Sie uns zitieren möchten:
Arlinghaus, J.; Bendik, F.; Fidan, Y.; Kessler, M.; Reinecke, L. (2021):
Risikomanagement für die Smarte Fabrik.