

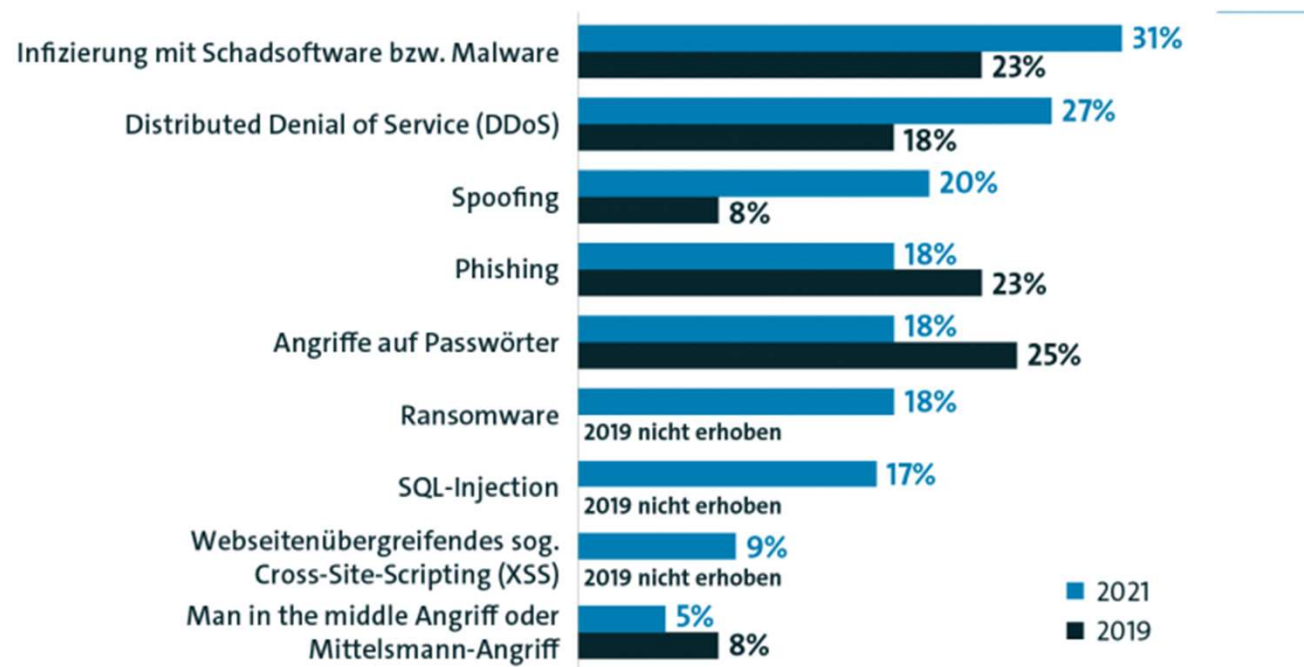
The background is a dark blue field filled with white binary code (0s and 1s) of varying sizes and orientations, creating a sense of digital data flow. In the center, there is a circular pattern of concentric lines, and within this, a dense, glowing cluster of small white dots, resembling a data visualization or a network hub.

Sicherheitsrisiken in der Smart-Factory

Max Rapp, Till Ptassek

Cyberangriffe betreffen nahezu 9 von 10 Unternehmen

Welche der folgenden Arten von Cyberangriffen haben innerhalb der letzten 12 Monaten in Ihrem Unternehmen einen Schaden verursacht?



Cyberangriffe haben bei

86%

der Unternehmen einen Schaden verursacht – 2019 waren es erst 70%.

Basis: Alle befragten Unternehmen (2021: n=1.067; 2019: n=1.070); Mehrfachnennungen in Prozent, 2017 und 2019: innerhalb der letzten zwei Jahre
Quelle: Bitkom Research 2021

bitkom

IT-Sicherheit

IT-Sicherheit als zentrales Risiko in der Smart Factory



IT-Sicherheit bedeutet **größtes technisches Risiko** in der Smart Factory



Zunahme von Cyber-Attacken gegen Unternehmen und Privatpersonen



Hohe finanzielle Schäden durch mangelnden Datenschutz & Datensicherheit



Hemmung neuer Geschäftsmodelle und Cloud-Lösungen durch Cybergefahren

IT-Sicherheit

Ursachen & Herausforderungen in der Produktions-IT

Ursachen

- Hoher Vernetzungsgrad durch **CPS-Systeme** (Cyber-Physical Systems)
- **Autonome & zeitkritische** Kommunikation zwischen Systemen
- **Veraltete** Produktionssysteme („Legacy-Systeme“)
- „Never touch a running system“-Mentalität
- **Fehlende Sicherheitswartung** durch Hersteller

= veraltete Systeme + hohe Vernetzung + fehlende Updates

Herausforderungen

- **Sicherheitslücken** in alten Systemen → leichtes Ziel für Angriffe
- Gegensätzliches Zielsystem:
 - Produktion will maximale **Verfügbarkeit**
 - IT will maximale **Sicherheit**
- **Mangelndes Identitäts- und Zugriffsmanagement**
→ keine Passwörter oder Berechtigungen, um Produktion nicht zu stören
- **Abhängigkeit von alten Infrastrukturen**
→ erschwert Integration moderner Schutzmaßnahmen

= Balance zwischen Betriebssicherheit & IT-Sicherheit finden

IT-Sicherheit

Maßnahmen zur Erhöhung der Sicherheit



- Absicherung der internen Kommunikation gegen Störungen & Manipulation
- Schutz der Daten vor Diebstahl und Missbrauch
- Abwehr von Angriffen wie DoS-Attacken und Schadsoftware

Wichtige Sicherheitsmaßnahmen im IoT-Umfeld:

- Leistungsfähiges Identitäts- & Zugriffsmanagement
- Verschlüsselung aller Datenübertragungen über das Internet
- Einrichtung von Firewalls
- Robuste Angriffsschutzsysteme
- Regelmäßiges Software- & Patchmanagement

Datenschutz



Datenschutz

- Schutz personenbezogener Daten vor Missbrauch
- „Datenschutz ist Personenschutz“



Unterschied zur IT-Sicherheit

- IT-Sicherheit schützt Systeme und Daten allgemein
- Datenschutz schützt Privatsphäre und Persönlichkeitsrechte



Rechtliche Grundlagen

- **Bundesdatenschutzgesetz** regelt Umgang mit personenbezogenem Daten in DE
- **Europäische Datenschutzkonvention** internationaler Vertrag zum Schutz & Datenaustausch in EU



Menschlicher Risikofaktor

- Gefahr durch Mitarbeiter mit legalem Datenzugriff
- Technisch kaum zu verhindern
- Prävention durch gutes Betriebsklima

Organisatorische Risiken



Change-Team oder **Change-Abteilung** notwendig
→ unterstützt Mitarbeiter bei neuen Aufgaben & Prozessen

Fehlendes Change-Management führt zu:

- Neophobie (Angst vor Neuem)
- Kritische Haltung gegenüber Veränderungen
- Sinkender Mitarbeiterzufriedenheit

Neue Technologien verändern Berufsprofile

- Mehr Bedarf an hochqualifiziertem Fachpersonal
- Weniger Arbeitsplätze für gering qualifizierte Tätigkeiten

Herausforderungen für Unternehmen

- Mitarbeiter müssen neue Technologien verstehen & anwenden können
- Förderung von lebenslangem Lernen
- Anpassung von Arbeitsorganisation, Teamstrukturen & Wissensmanagement

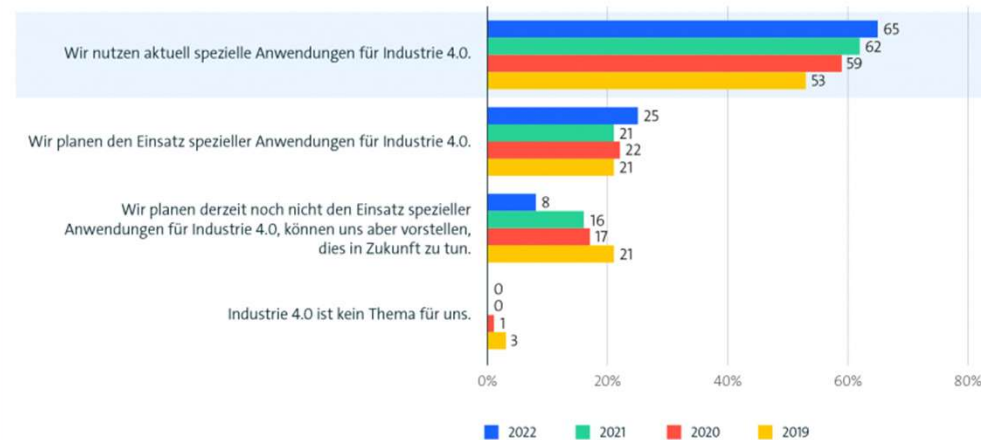
Wirtschaftliche Risiken



- **Investitionsbereitschaft oft gering**, trotz sinkender Einstiegskosten in Industrie 4.0
- **Fehlende Transparenz des wirtschaftlichen Mehrwerts**
→ Schwierige Abschätzung zukünftiger Anforderungen und Nutzen
- **Unternehmen erkennen zwar die Relevanz**, handeln aber oft zögerlich
- **Notwendigkeit ausreichender Investitionen & Ressourcen**
→ Umsetzung der Smart Factory erfordert langfristige Planung

9 von 10 Unternehmen setzen auf Industrie 4.0

Welche Bedeutung hat Industrie 4.0 für Ihr Unternehmen? (in Prozent)



Basis: Industrieunternehmen ab 100 Beschäftigten in Deutschland (2022: n=553; 2021 n=551; 2020: n=552; 2019: n=555) | an 100 Prozent fehlende Prozentwerte: »Weiß nicht / k. A.«
Quelle: Bitkom Research 2022

90%
nutzen oder planen
in diesem Jahr
Anwendungen
für Industrie 4.0
2021: 83%
2020: 81%
2019: 74%

bitkom

Investitionsvolumen in Deutschland (2025):
→ **50–70 Milliarden € jährlich** (Bitkom-Studie)

Wirtschaftliche Risiken

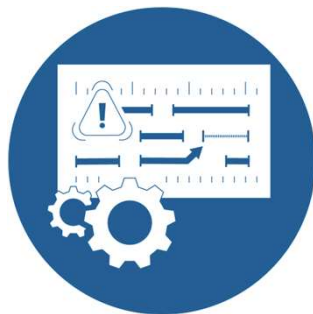


- **Risiko Arbeitsplatzverlust** durch Automatisierung einfacher Tätigkeiten
- **Starke Schwankungen im Personalbedarf** → Erfordert **flexiblen Personaleinsatz**
- **Steigende Qualifikationsanforderungen:**
 - Förderung von **akademischen Berufen** (MINT-Fächer)
 - **Weiterbildung** in Mechatronik & Automatisierungstechnik
 - **Interne Aus- & Weiterbildung** für technologische Kompetenz
- **Selbstorganisation & Eigenverantwortung** der Mitarbeiter
- **Strukturelle Marktveränderungen:**
 - Neue Marktteilnehmer & Start-ups verdrängen etablierte Unternehmen
- **Forschung als kritischer Erfolgsfaktor:**
 - Deutschland investiert gut, aber **China & Japan investieren stärker**
- **Ohne Berücksichtigung dieser Faktoren keine wettbewerbsfähige Industrie 4.0**

Standardisierung

Fehlende Standards & Herausforderungen

- **Keine internationalen Standards oder Normen** für Industrie 4.0 vorhanden
→ Erschwert Vernetzung und wirtschaftliches Potenzial
- **Abhängigkeit kleinerer Unternehmen:**
 - Zulieferer müssen sich an Standards großer Unternehmen anpassen
 - Weniger Handlungsspielraum für KMU
- **Risiko hoher Investitionskosten**, wenn Firmen auf nicht zukunftsfähige Technologien setzen
- **Standardisierung** ist Voraussetzung für Interoperabilität zwischen Systemen
- **Effiziente Kommunikation** entlang der Wertschöpfungskette

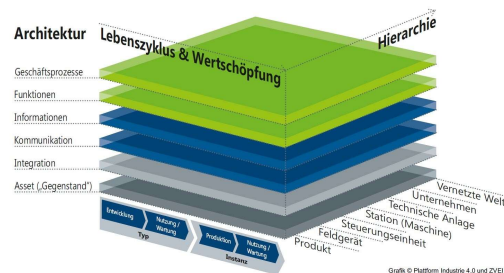


Lösungsansätze – RAMI 4.0 & OPC UA

Referenzarchitekturmodell Industrie 4.0 (RAMI 4.0)

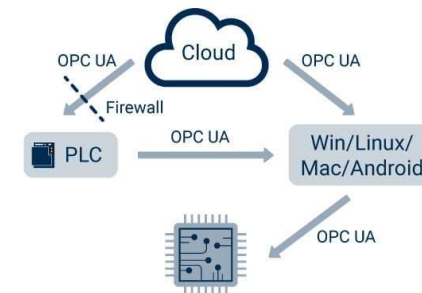
- Grundlage zur **Standardisierung** von Smart Factories
- Schafft **gemeinsames Verständnis** über notwendige **Standards, Use Cases und Normen**
- Ziel: **Einfaches, anschauliches Architekturmodell** mit **minimalem Einsatz verschiedener Standards**

Referenzarchitekturmodell Industrie 4.0 (RAMI 4.0)



OPC UA (Open Platform Communications Unified Architecture)

- **Standard-Kommunikationsprotokoll** für Industrie 4.0
Unterstützt **Maschine-zu-Maschine (M2M)** und **PC-zu-Maschine-Kommunikation**
- Überträgt **Maschinendaten** und beschreibt sie **semantisch maschinenlesbar**
- Bietet **hohe Interoperabilität** und ist **zentrale Voraussetzung** für vernetzte Produktion



Handlungsvorgabe des BMWi

- BMWi → Bundesministerium für Wirtschaft und Technologie
- Prämisse → deutsche Wirtschaft unterstützen bei:
 - Fragen der Sicherheit
 - Nationalen & internationalen Angriffen
- Gefahren können entstehen wenn bestimmte Einrichtungen der Wirtschaft ausfallen → besondere Gefahr geht von Personen aus, welche dort tätig sind
- Hat Initiative „IT-Sicherheit in der Wirtschaft“ eingerichtet
- Ziel der Initiative:
 - Unternehmen für IT-Sicherheit zu sensibilisieren
 - IT-Sicherheitsniveau verbessern



Bundesministerium
für Wirtschaft
und Technologie

Handlungsvorgabe des BMWi

Die zehn wichtigsten Punkte für die Initiative „IT-Sicherheit in der Wirtschaft“

1. IT-Systeme, mobile Geräte und Dienste sollen stets aktuell sein und regelmäßig auf Viren überprüft werden.
2. Sicherheitsrichtlinien und IT-System-Notfallpläne sollen gut verständlich erstellt werden
3. Verwendung von qualifizierter elektronischer Signatur, verschlüsseln bei sensiblen Daten und Achtsamkeit beim Verschicken und Speichern.
4. Verwendung eines eindeutigen und qualifizierten Berechtigungssystems
5. Regelmäßige räumlich getrennte Datensicherung mit Hinblick auf jederzeitige Verfügbarkeit

Handlungsvorgabe des BMWi

Die zehn wichtigsten Punkte für die Initiative „IT-Sicherheit in der Wirtschaft“

6. Kooperation nur mit vertrauenswürdigen IT-Dienstleistern oder Softwareanbietern die nach europäischen Datenschutzstandards arbeiten
7. Unternehmenskritische Daten in der Cloud nur in Organisationsformen (z.B. Private Cloud) die erhöhte Sicherheit inkl. Verschlüsselung bieten.
8. Bei IT-Geräten stets verschlüsselte Übertragungswege wie VPN und Proxy-Server, die keine Nutzerdaten speichern verwenden.
9. Den Mitarbeiter Richtlinien im Umgang mit sozialen Netzwerken vorgeben
10. Die Belegschaft regelmäßig für das Thema IT-Sicherheit schulen und aufmerksam machen.

VDMA-Handlungsleitfaden



- VDMA: **V**erband **D**eutscher **M**aschinen- und **A**nlagenbauer
 - Größte Netzwerkorganisation und wichtigstes Sprachrohr im Maschinenbau
 - Unterstützt seine Mitglieder u.a. in den Gebieten:
 - Beruf und Bildung, Forschung, Innovation, Recht, Normung und allgemeinen Fragen zu Gesellschafts- und Wirtschaftspolitik
 - Daraus Bildung des VDMA-Forums Industrie 4.0
 - Besteht aus interdisziplinärem Team von VDMA-Experten
 - Sieht sich als Partner und Dienstleister
 - Unterstützt Mitgliedsunternehmen in den Industrie 4.0 Handlungsfeldern
- [VDMA über die Bedeutung der Digitalisierung im Bereich Industrietechnik \(DE\)](#)

VDMA-Handlungsleitfaden

- IT-Sicherheit in Hinsicht für die Industrie 4.0 überlebensnotwendig
- Akteure müssen kontrolliert identifiziert und sämtliches Wissen über Produkte, Maschinen und Anlagen geschützt werden
- Zeitfaktor der Umstellung ebenfalls ausschlaggebend
 - Um nicht von anderen Branchen überholt zu werden
 - Um Innovations- und Marktführer in einem globalen und technischen Marktumfeld bleiben zu können

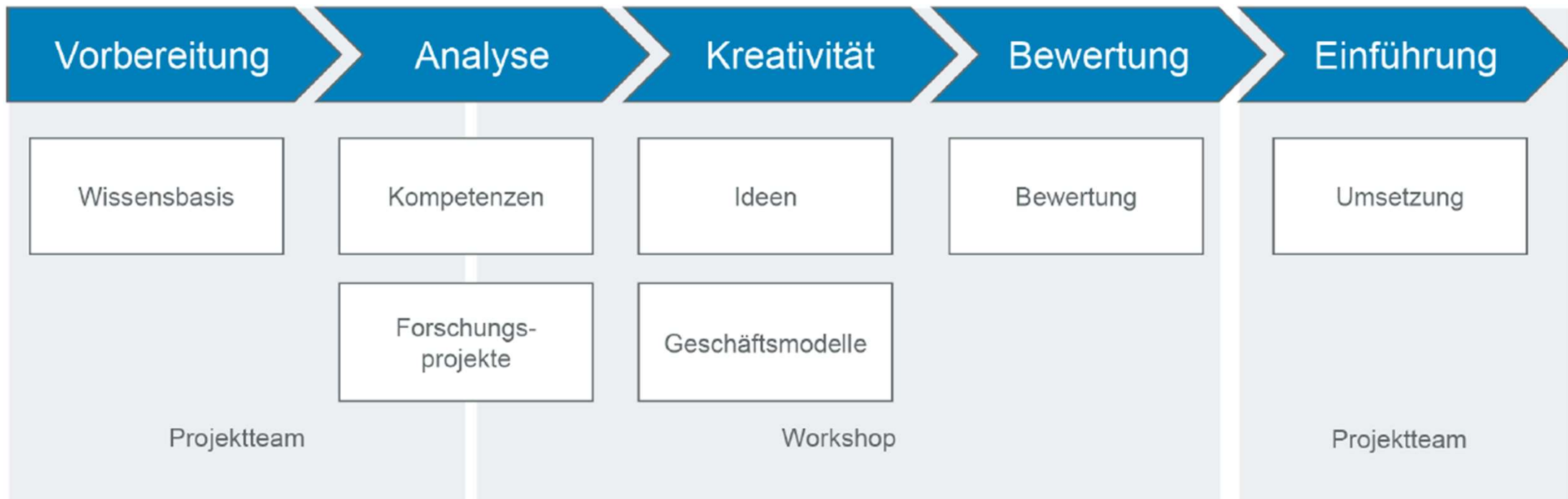
VDMA-Handlungsleitfaden

- VDMA stellt dafür Handlungsleitfaden bereit
 - Soll Unternehmen Unterstützung und Führung zur raschen Einführung von Geschäftsmodellen geben
 - Reduziert Visionen der Industrie 4.0 auf realisierbare Entwicklungsstufen
 - Vorstellung eines Konzepts von unternehmensinternen Workshops welche Ziele verfolgen und mit Kreativitätstechniken neue Lösungen generieren sollen
 - Lösungen Beispiele:
 - Ideenfindung für neue Geschäftsmodelle
 - Verbesserte Produktion

Werkzeugkasten & Workshops

- Konzept bedient sich am „Werkzeugkasten Industrie 4.0“
- Werkzeugkasten wird untergliedert in:
 - Produkte
 - Produktion
- Ziel: Know-how verschiedener Fachbereiche zusammenbringen
- Angesehen als zentrale Elemente für die kreative Einarbeitung von Konzepten für Geschäftsmodelle
- Ergebnisse werden nach Erarbeitung in reale Projekte überführt

VDMA-Handlungsleitfaden



VDMA-Handlungsleitfaden

Produktion

Daten- verarbeitung in der Produktion					
	Keine Verarbeitung von Daten	Speicherung von Daten zur Dokumentation	Auswertung von Daten zur Prozessüberwachung	Auswertung zur Prozessplanung / -steuerung	Automatische Prozessplanung / -steuerung
Maschine- zu- Maschine- Kommunikation (M2M)					
	Keine Kommunikation	Feldbus-Schnittstellen	Industrial Ethernet-Schnittstellen	Maschinen verfügen über Zugang zum Internet	Webdienste (M2M-Software)
Unternehmensweite Vernetzung mit der Produktion					
	Keine Vernetzung der Produktion mit anderen Unternehmensbereichen	Informationsaustausch über Mail / Telekommunikation	Einheitliche Datenformate und Regeln zum Datenaustausch	Einheitliche Dateiformate und abteilungsübergreifend vernetzte Datenserver	Abteilungsübergreifende, vollständig vernetzte IT-Lösungen

IKT- Infrastruktur in der Produktion					
	Informationsaustausch über Mail / Telekommunikation	Zentrale Datenserver in der Produktion	Internetbasierte Portale mit gemeinsamer Datennutzung	Automatisierter Informationsaustausch (z.B. Auftragsnachverfolgung)	Zulieferer / Kunden sind vollständig in Prozessgestaltung integriert
Mensch- Maschine- Schnitt- stellen					
	Kein Informationsaustausch zwischen Mensch und Maschine	Einsatz lokaler Anzeigergeräte	Zentrale / dezentrale Produktionsüberwachung/-steuerung	Einsatz mobiler Anzeigergeräte	Erweiterte und assistierte Realität
Effizienz bei kleinen Losgrößen					
	Starre Produktionsmittel und geringer Anteil von Gleichteilen	Nutzung von flexiblen Produktionsmitteln und Gleichteilen	Flexible Produktionsmittel und modulare Baukästen für die Produkte	Bauteilgetriebene, flexible Produktion modularer Produkte im Unternehmen	Bauteilgetriebene, modulare Produktion in Wertschöpfungsnetzen

VDMA-Handlungsleitfaden

Produkte

Integration von Sensoren / Aktoren					
	Keine Nutzung von Sensoren/Aktoren	Sensoren/Aktoren sind eingebunden	Sensordaten werden vom Produkt verarbeitet	Daten werden vom Produkt für Analysen ausgewertet	Das Produkt reagiert auf Basis der gewonnenen Daten eigenständig
Kommunikation / Connectivity					
	Keine Schnittstellen am Produkt	Das Produkt sendet bzw. empfängt I/O-Signale	Das Produkt verfügt über Feldbus-Schnittstellen	Das Produkt verfügt über Industrial Ethernet-Schnittstellen	Das Produkt verfügt über Zugang zum Internet
Funktionalitäten zu Daten-speicherung und Informations-austausch					
	Keine Funktionalitäten	Möglichkeit zur eindeutigen Identifikation	Produkt verfügt über passiven Datenspeicher	Produkt mit Daten-speicher zum autonomen Informationsaustausch	Daten- und Informationsaustausch als integraler Bestandteil

Monitoring					
	Kein Monitoring durch das Produkt	Detektion von Ausfällen	Erfassung des Betriebszustands zur Diagnose	Prognose der eigenen Funktionsfähigkeit	Selbstständige Maßnahmen zur Steuerung
Produkt-bezogene IT-Services					
	Keine Services	Services über Online-Portale	Service-Ausführung direkt über Produkt	Selbstständige Ausführung von Services	Vollständige Eingliederung in IT-Service-Infrastruktur
Geschäftsmodelle um das Produkt					
	Gewinne durch Verkauf der Standardprodukte	Verkauf und Beratung zum Produkt	Vorkauf, Beratung und Anpassung des Produktes an Kundenwünsche	Zusätzlicher Verkauf produktbezogener Dienstleistungen	Verkauf von Produktfunktionen

Zusammenfassung

Risiken der Smart Factory:

- Spionage und Sabotage durch Anbindung an das öffentliche Internet
 - durch kriminelle Handlungen von internen Mitarbeitern
- BMWi will Unternehmen bei Thematik IT-Sicherheit unterstützen

Resultat:

- Konkrete Handlungsvorschläge um Risiken zu vermeiden
- Handlungsleitfaden für schnelle Umsetzung der Industrie 4.0
 - Besteht aus Workshops zur Ideenfindung für innovative Produkte und verbesserte Produktumgebungen

Hinweis:

- Implementierung nicht nur durch Hilfe der Bundesregierung möglich
 - Benötigt Unterstützung der Unternehmen
- Notwendigkeit der Dringlichkeit einer Veränderung muss von Unternehmen wahrgenommen werden
 - falls nicht berücksichtigt in kommenden Jahren möglicherweise schlechte Wettbewerbsfähigkeit Deutschlands
- Anpassung von Produktionsmitarbeitern ebenfalls notwendig
 - Risiken können besser erörtert werden, da Industrie 4.0 noch am Anfang steht
 - Besser Gegenmaßnahmen einleitbar