Safety 4.0 - von statisch zu dynamisch

Armin Glaser
Vice President Product Management

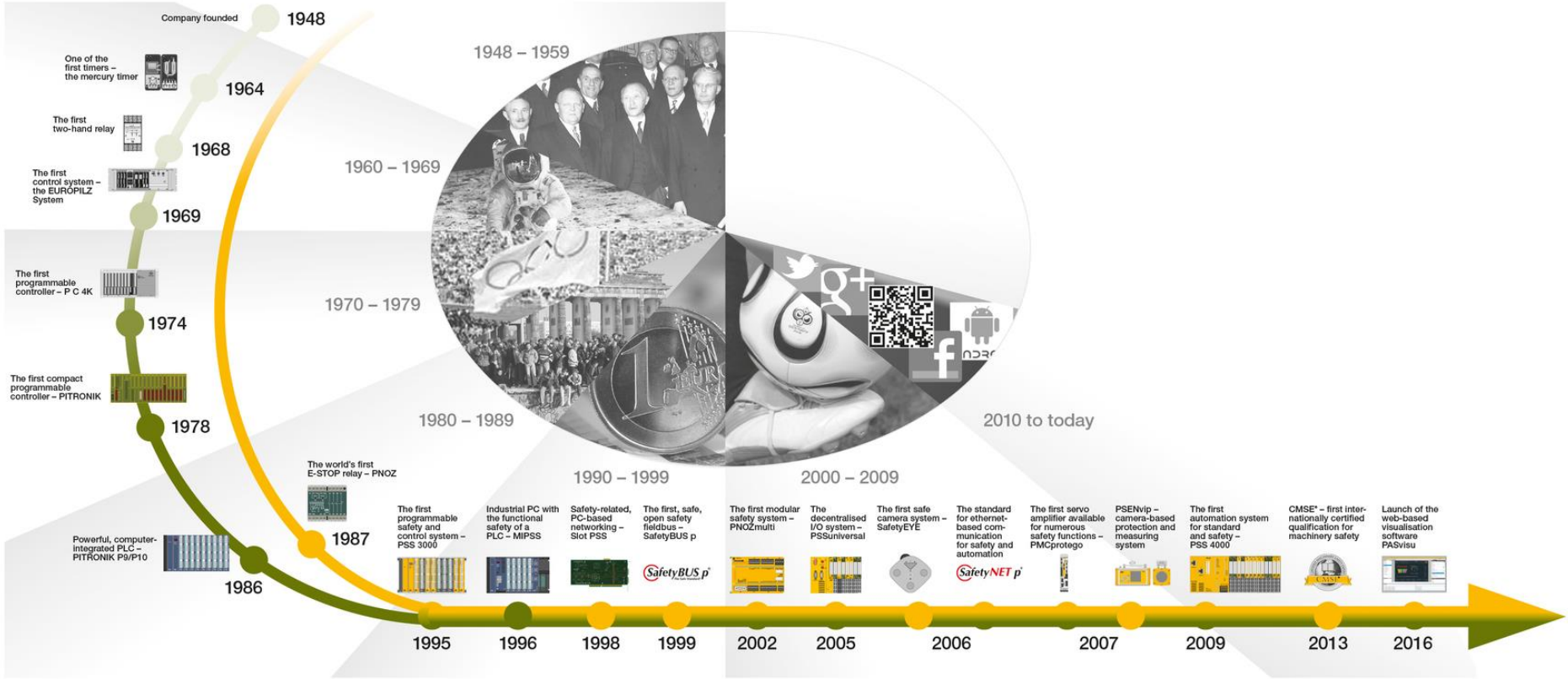
HMI - Forum Industrial Automation
25. April 2017

Agenda

- Digitalisierung und Industrie 4.0
- Von statischer zu dynamischer Sicherheit
- Safety 4.0 – neue Anforderungen
- Zusammenfassung

Sicherheit ist keine Selbstverständlichkeit

Sichere Automatisierung ist eine relativ junge Disziplin



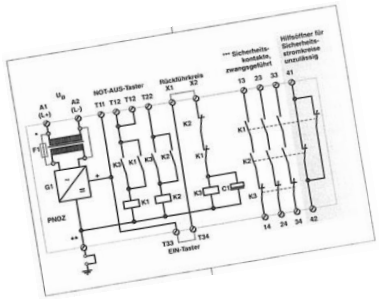
Zeitreise 20 Jahre – 1995
Elektronische Sicherheit? - Digitalisierung?

Für die Not-Aus-Funktion der Stop-Kategorie 0 dürfen nur festverdrahtete, elektromechanische Bauteile verwendet werden. Die Auslösung darf nicht von einer Schaltlogik (Hardware oder Software) oder von der Übertragung von Befehlen über ein Kommunikationsnetzwerk oder eine Datenverbindung abhängen.

Bei der Stop-Kategorie 1 für die Not-Aus-Funktion muß die endgültige Abschaltung der Energieversorgung der Maschinenantriebe sichergestellt sein und muß durch Verwendung von elektromechanischen Bauteilen erfolgen.

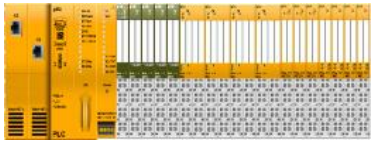
- Sicherheitslösungen, die mit elektronischen Abschaltpfaden arbeiten, wurden vor dem Jahr 1995 z.B. schon von der DIN EN 60204-1 verboten.

.



SafetyNET p®

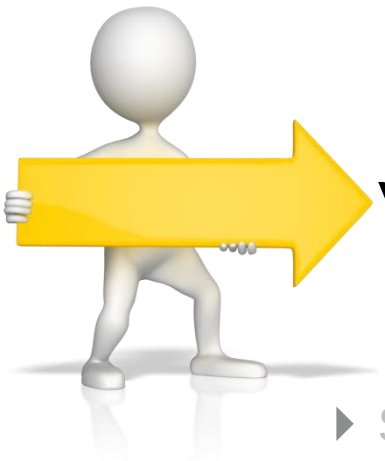
SafetyBUS p® Der sichere Standard!



- Leichtathletik WM 1993 Stuttgart
  - Stuttgarter Zeitung setzte erstmals Digitalkameras ein
  - Datenspeicher von der Kamera getrennt - unhandlich, schwer
  - Datenübertragung an die Redaktion über Telefonkoppler (alternativ: Diskette)
  - Kamera (ohne Objektiv): 17.000 DM – 2 Megapixel
- Nutzen: hohe Geschwindigkeit (Effizienz)

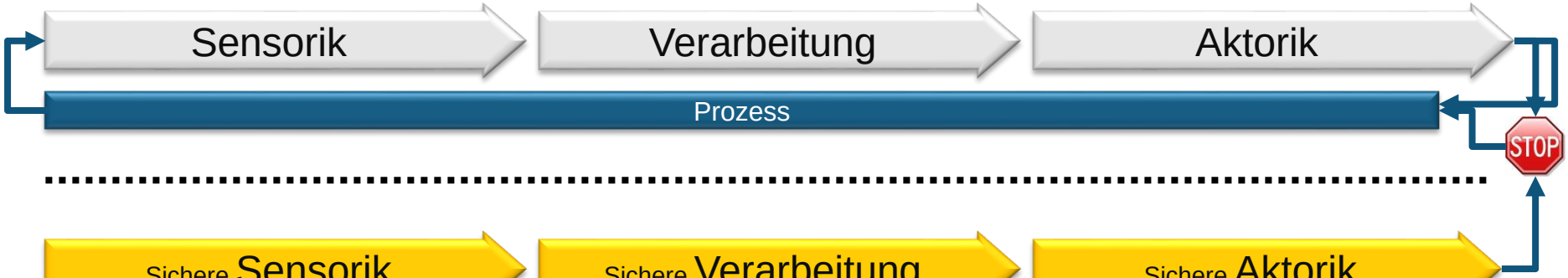
Agenda

- Digitalisierung und Industrie 4.0

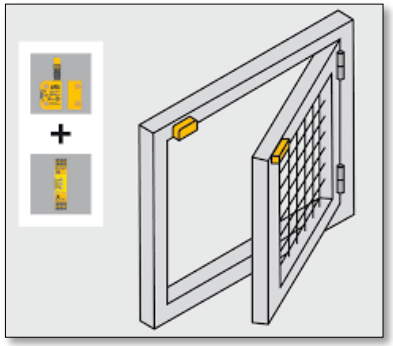


- **Von statischer zu dynamischer Sicherheit**
- Safety 4.0 – neue Anforderungen
- Zusammenfassung

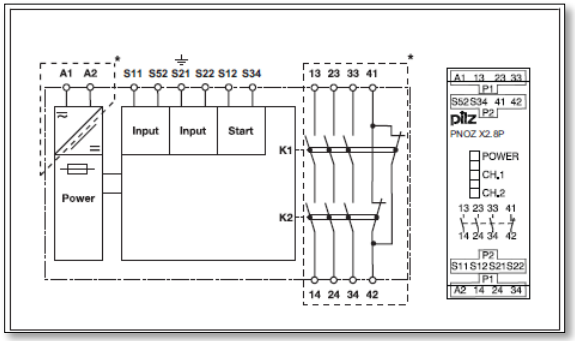
Digitalisierung und Industrie 4.0
Statische Sicherheit vs. dynamische Sicherheit



Sichere Sensorik	Sichere Verarbeitung	Sichere Aktorik
Binäres Schaltverhalten	Starre Kopplung (Verdrahtungslogik) Direkte Wirkrichtung – direkte Reaktion	***Herstellen der Sicherheit durch direktes Abschalten*** der Energie (elektrisch, hydraulisch, pneumatisch)



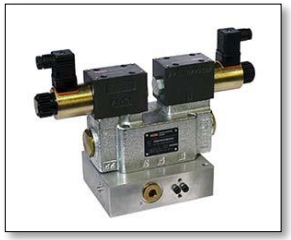
Schutztüre
(Bildquelle Pilz)



Sicherheitsschaltgerät
(Bildquelle Pilz)

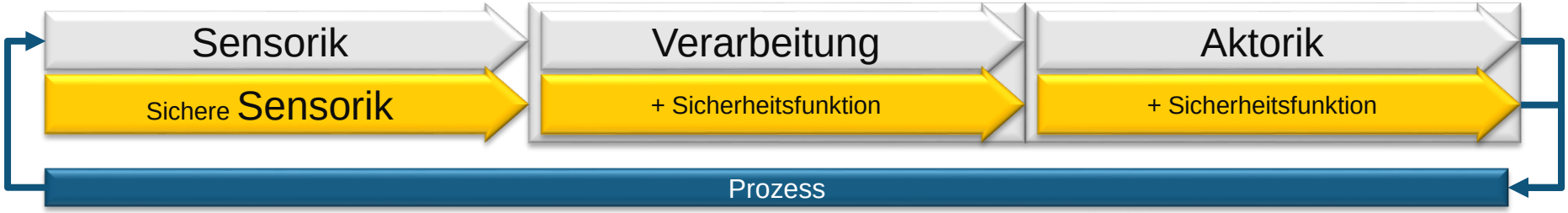
Schütz (Bildquelle Eaton)

Pneumat. Scherheitsventil
(Bildquelle Festo)



Hydr. Pressensicherheitsventil
(Bildquelle Norgren)

Digitalisierung und Industrie 4.0
Statische Sicherheit vs. dynamische Sicherheit



- Sichere Position
- Sichere Geschwindigkeit
- Sichere Identifikation

- Unterscheidung in Warn- und Abschaltbereiche
- mehrdimensionale Überwachung
- sichere Kennfelder
- dynamische Schutzbereiche, auch: der Bewegung nachgeführt

- Einführung eines 3. Sicherheitszustandes
  - 0 (Aus, Fehler…)
  - 1 (Ein)
  - Aktiv/passiv

- Safety & Control & Motion
- flexible Kopplung (Funktionslogik)

- Sichere Betriebsarten

- Kommunikation:
  - Hohe Bandbreite,
  - Echtzeitfähig für Safety und MotionControl
  - Austausch komplexer Daten

- Rückwirkungsfreiheit
  - physikalisch gemischt – aber logisch getrennt

- Stoppkategorien 1,2 , sicherer Halt, sichere Drehrichtung
- sichere Drehzahl/sicherer Stillstand
- sichere Position
- sicheres Drehmoment (Begrenzung)
- sichere kooperierende Achsen

- ***Herstellen der Sicherheit durch eine sicher kontrollierte Prozessführung***
- ***Sichere Prozesskette***
- ***Abschalten nur noch als Notmaßnahme***
- ***= Steigerung der Produktivität***







Digitalisierung und Industrie 4.0
Von statischer zu dynamischer Sicherheit

PILZ
THE SPIRIT OF SAFETY

Statisch:

- Reines Monitoring, Begrenzung der Produktivität, Verlängerte Stillstandzeiten
- Beschränkung im Bedien- und Wartungs-konzept der Maschine
- Sicherheit wird oft nachträglich „aufgesetzt“
- Akzeptanzfragen: Sicherheit wird als ein „produktionsbegrenzender Faktor“ angesehen
- Grund für Manipulation
- **Fokus: Trennung von Mensch und Maschine**

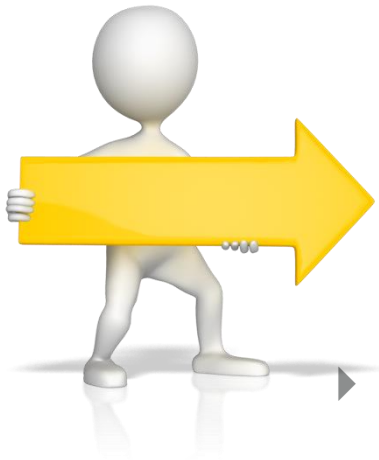
Dynamisch:

- Sichere Prozessführung (Steuerung, Regelung, Monitoring…)
- Keine Prozessunterbrechung
- Funktionale Sicherheit von Anfang an gemeinsam betrachtet

- **Fokus: Zusammenspiel, Hand-in-Hand arbeiten**

Agenda

- Digitalisierung und Industrie 4.0
- Von statischer zu dynamischer Sicherheit



Safety 4.0 – neue Anforderungen

- Zusammenfassung

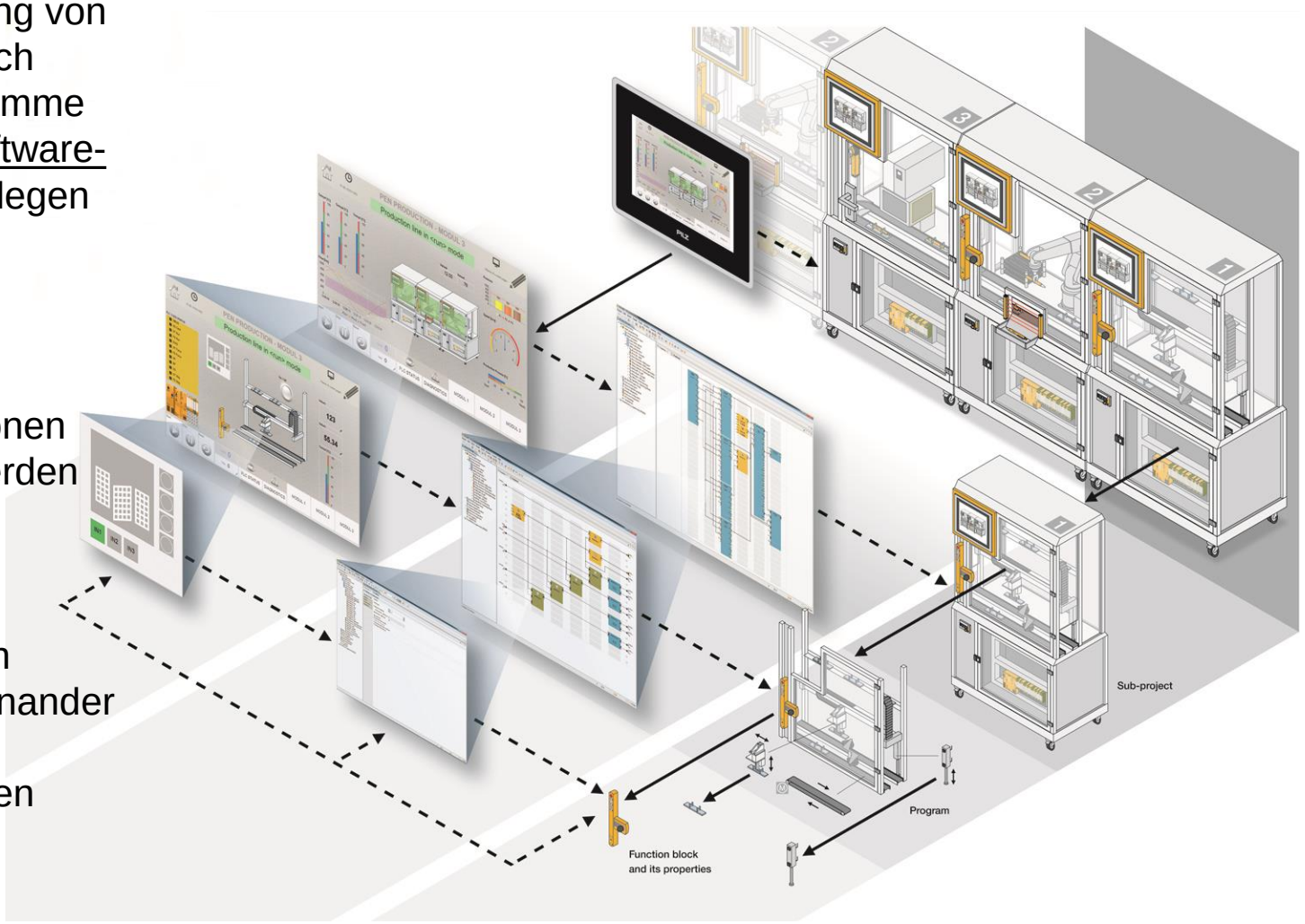
Safety 4.0
Anforderungen

- Maschinen-Module lassen sich re-kombinieren und austauschen
- Steuerungskonzepte werden dezentraler und modular
  - Höhere Flexibilität und gleichzeitig
  - Höherer Grad der Standardisierung durch moderne Methoden (Vererbung, Instanzierung, gleiche Teilungsgrenzen aller Funktionen PLC, Visu, MC, Safety…)
  - Einheitliches Engineering – hoher Grad der Wiederverwendung
  - Sicherheits-Validierung muss mit Flexibilisierung umgehen können
- Höhere Anforderungen an Safety und Security → Schutz vor IT-Angriff
- Höhere Anforderungen an die Rechte und Fähigkeiten der Mitarbeiter

➔ Ein starres Sicherheitskonzept nicht mehr zeitgemäß

Safety 4.0 Lösungsansätze
Modulare Maschinenkonzepte

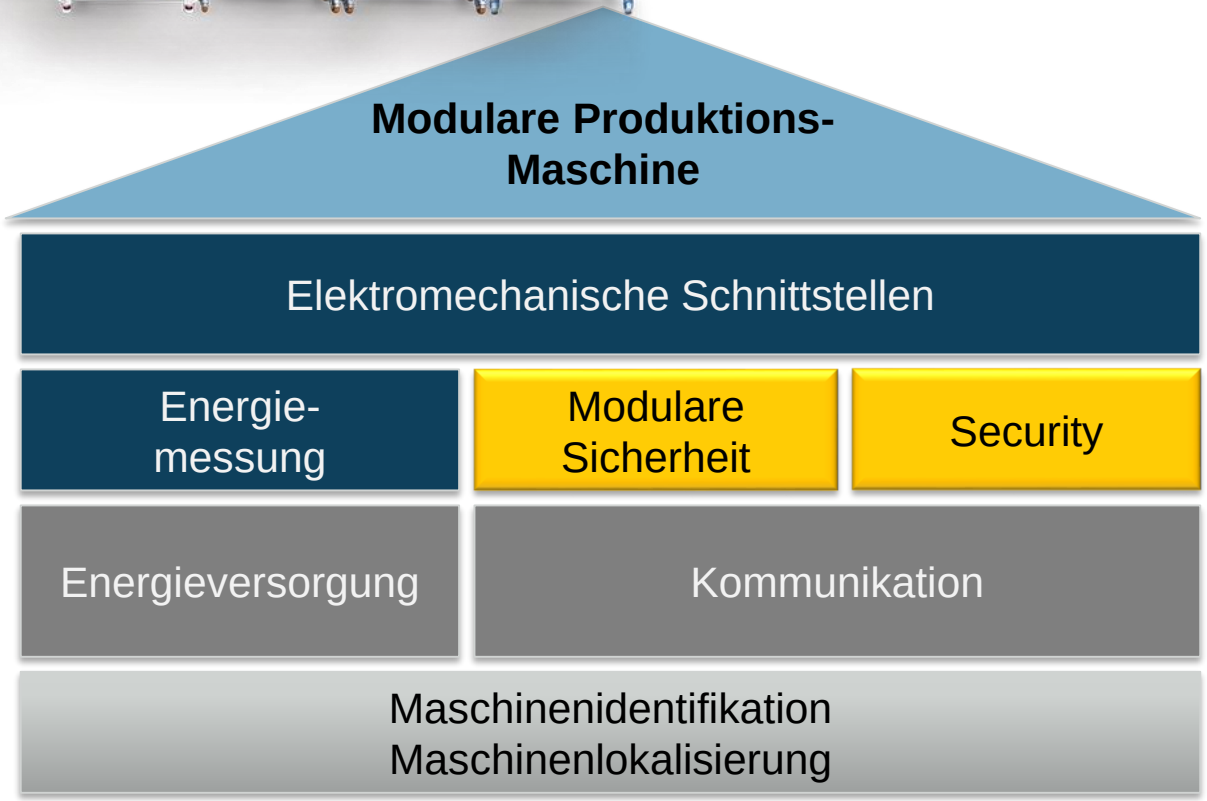
- Zur Modularisierung von Anlagen lassen sich Steuerungsprogramme konsequent in Software-Komponenten zerlegen
- intelligente Steuerungsfunktionen können verteilt werden
- Anlagen werden in unabhängig voneinander funktionierende Maschineneinheiten aufgeteilt



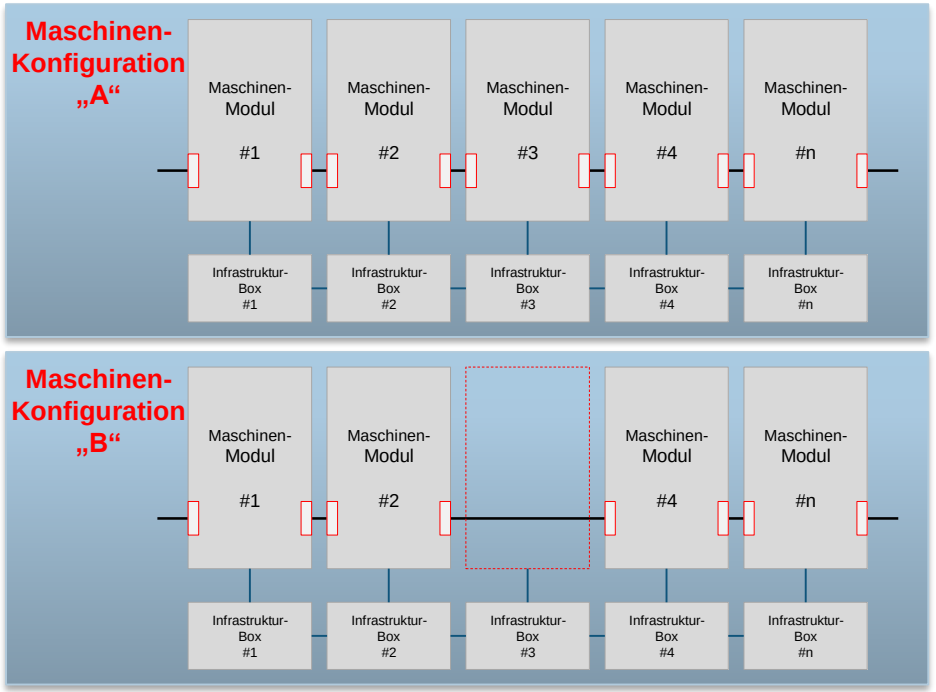
SmartFactory– die intelligente Fabrik

smartFactory KL®

- Funktionale Standardisierungen



SmartFactory– die intelligente Fabrik



- CE Konformitätserklärung
  - CE für unvollständige Maschine A
  - \+ CE für unvollständige Maschine B
  - ≠ CE für Maschine A+B

- Wichtig:
  - flexible Steuerungsarchitekturen benötigen ein flexibles Sicherheitskonzept (CE Erklärung “unvollständige Maschine“)
  - Differenzierung: Anwendungsfälle “beabsichtigte Kombination” – “unbeabsichtigte Kombination” – alle beabsichtigten Kombinationen müssen ein Sicherheitskonzept besitzen (z.B. Kombi…
  - Erst die flexiblen Safety-Konzepte ermög…

Die Maschine ist sicher, wenn ihre einzelnen Module sicher sind und ihre Kombination sicherheitstechnisch bewertet wurde!

Safety 4.0 Lösungsansätze
Not-Halt nach Maß für die Smart Factory

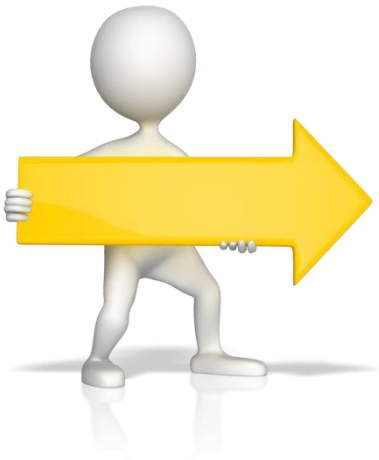
- Sicherheit nach dem Ruhestromprinzip:
  - An/High: Ein, Start, Signal
  - Aus/Low: Stop, Fehler, sicherer Zustand
- Neu:
  - Dritter Zustand: Aktiv/passiv

- Sicherheit nach ISO 13850, IEC 60204:
  - aktiver Not-Halt und inaktiver Not-Halt durch Beleuchtung klar unterscheidbar

- Maschinenteile können komplett abgeschaltet werden, da kein Not-Halt Kreis aufrecht gehalten werden muss.
- Maschinenmodule können flexibel aktiviert werden, da jetzt auch der Not-Halt Taster je nach Maschinenstatus aktiviert werden kann

Agenda

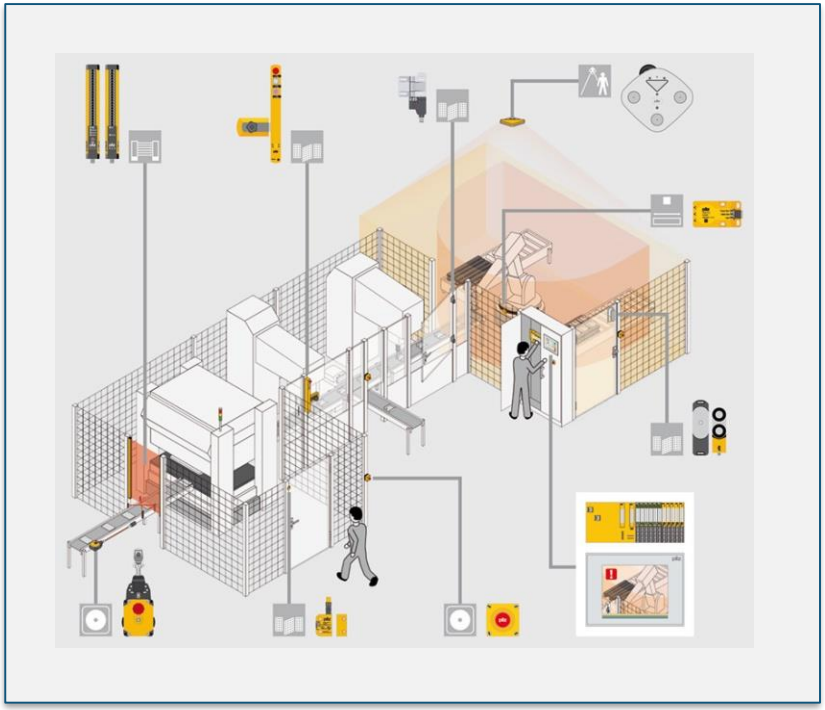
- Digitalisierung und Industrie 4.0
- Von statischer zu dynamischer Sicherheit



- Safety 4.0 – Definition & Anforderungen
  - Safety 4.0 - Modulare Maschinenkonzepte - Modulare Zertifizierung?
  - Safety 4.0: Safety und Security
- Zusammenfassung

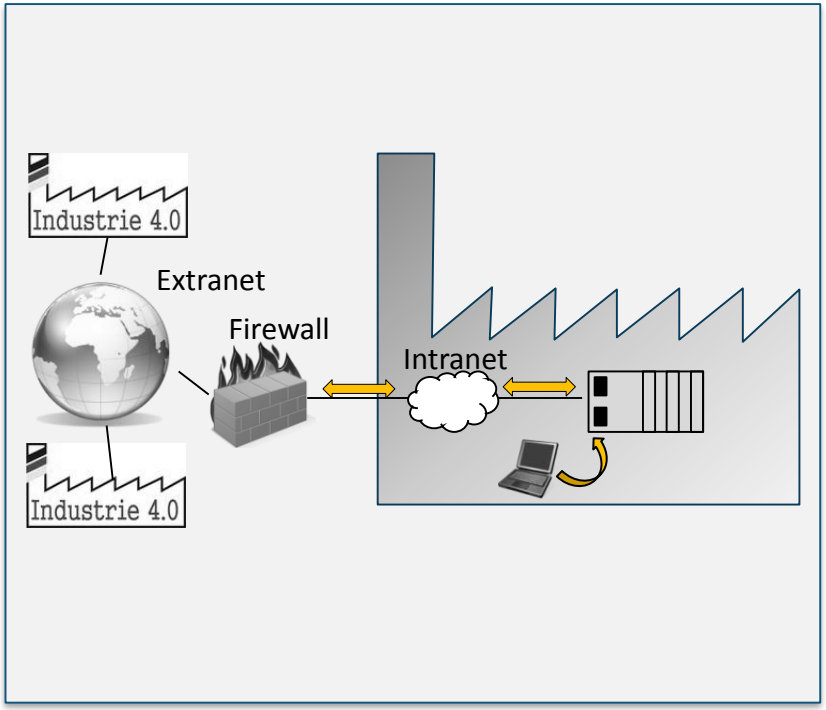
Was bedeutet Sicherheit in der Automation

Safety



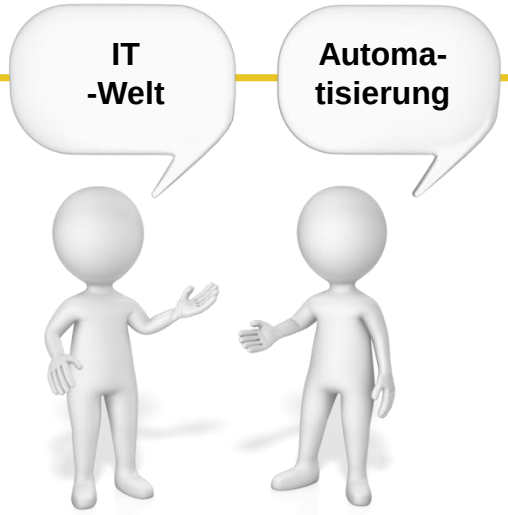
- Schutz des Menschen und der Umwelt vor Gefahren von oder an Maschinen
- ISOLATION der Gefahr

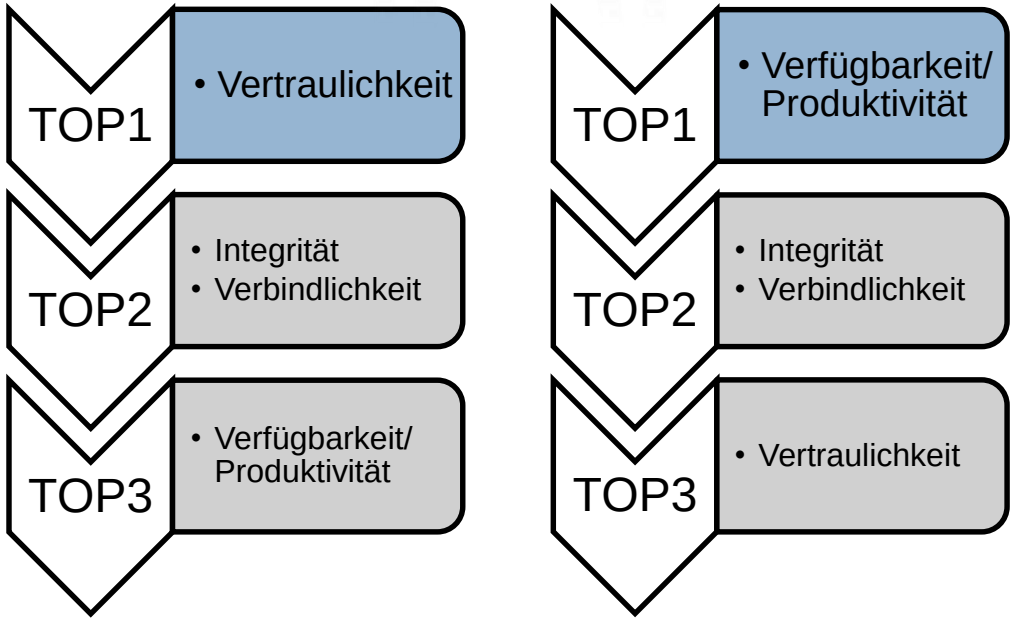
Security



- Schutz von Know-how, Produktivität und Daten vor Menschen
- IMMUNITÄT der Maschine/Anlage

Zielsetzungen und Prioritäten bezüglich Security





Vertraulichkeit
Daten sind nur für Berechtigte zugänglich

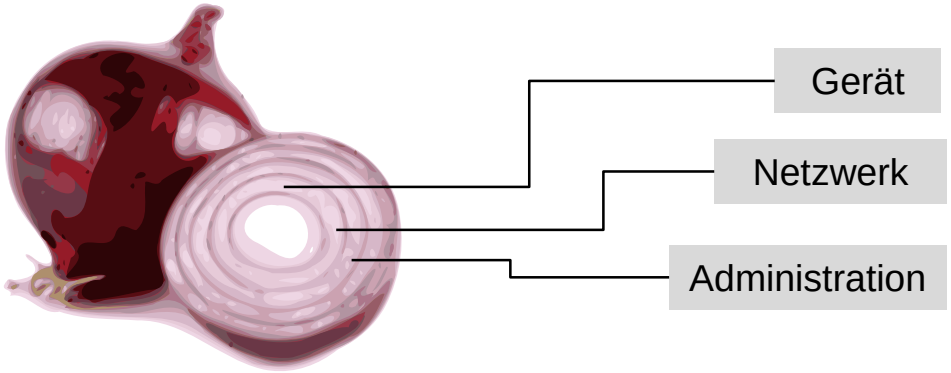
Verfügbarkeit
Zugriffe auf Systeme sind jederzeit möglich

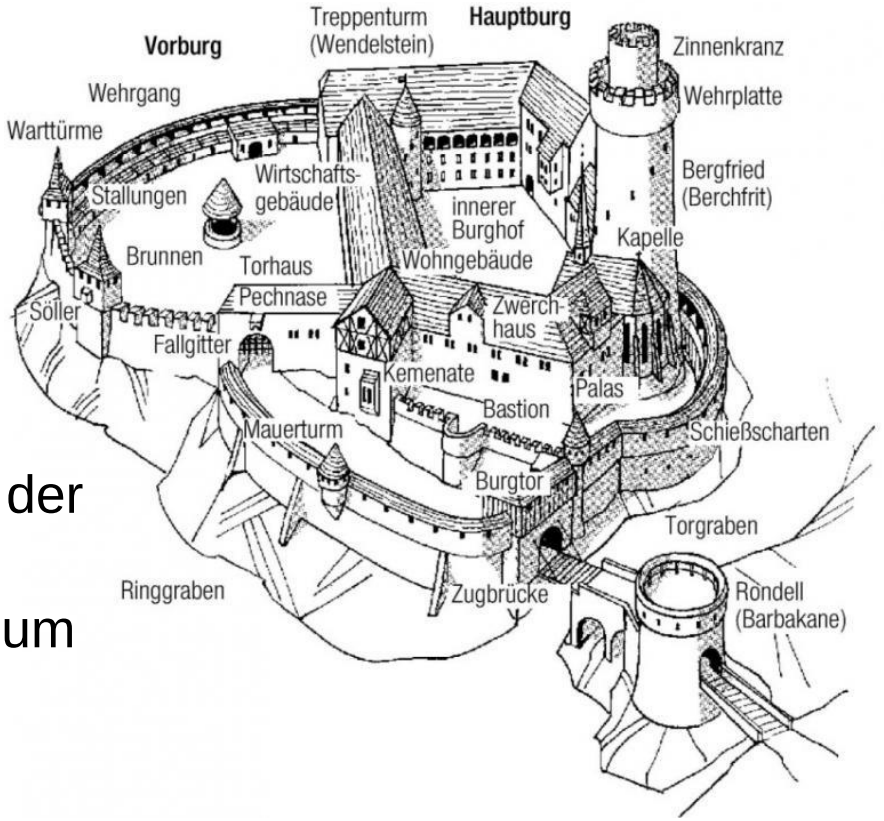
Integrität
Daten sind konsistent, korrekt sowie vollständig und Änderungen sind nachvollziehbar

Verbindlichkeit
Durchgeführte Transaktionen lassen sich eindeutig zuordnen

Um Zielkonflikte zu lösen sind neue Standards erforderlich

Handlungsfelder Security





- Erhöhen der Netzwerksicherheit:
  - Nie auf eine Maßnahme alleine verlassen
  - Alle Schutzmechanismen einsetzen
  - Schutzmaßnahmen sond ofnt nur in der Kombination wirksam
- Ergänzen des Entwicklungsprozesses um Anforderungen aus der IEC 62443-4-1
- Dezidiertes Benutzermanagement
  - Benutzergruppenverwaltung

Safety 4.0 Lösungsansätze
Safety und Security

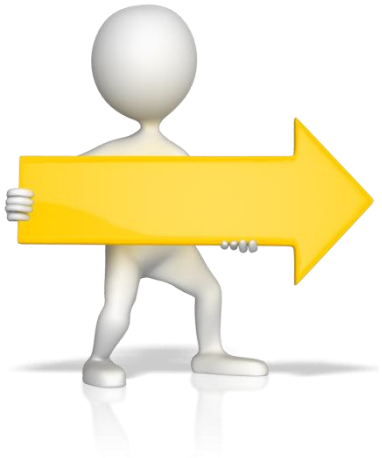
- Normative Anforderungen (Security)
  - **IEC 61508-1**: … wenn die Gefährdungsanalyse feststellt, dass eine böswillige oder nicht autorisierte Handlung, die eine Bedrohung der IT-Sicherheit darstellt, als vernünftigerweise vorhersehbar gilt, sollte eine Bedrohungsanalyse zur IT-Sicherheit durchgeführt werden.
  - **DIN EN 415-10**: Ist die Maschine mit Funktionen für die Ferndiagnose oder -steuerung (Teleservice) ausgestattet, muss der Hersteller technische Mittel und detaillierte Angaben bereitstellen, um das Risiko zu vermindern, dass während der Betriebsart Teleservice Gefährdungen verursacht werden. …
  - **IEC 62443**: Teilt Anlagen in Zellen auf, die über definierte Kanäle (Conduits) kommunizieren, FS-Steuerungen sind immer in einer eigenen Zelle

- Neue Norm *geplant*: IEC 63074
  - Ziel: eine Norm im Umfeld der Funktionalen Sicherheit (Maschinensicherheit), die dem Maschinenbauer bei Anwendung der ISO 13849-1 oder IEC 62061 helfen soll, „Security-Aspekte“ zu berücksichtigen

  - Teilnahme Pilz beim IEC/Technical Committee 44, WG 15

Agenda

- Digitalisierung und Industrie 4.0
- Von statischer zu dynamischer Sicherheit
- Safety 4.0 – Definition & Anforderungen
- Zusammenfassung



Zusammenfassung

- Bild der Sicherheit wandelt sich
- Industrie 4.0: definiert Sicherheit als erfolgskritischer Faktor
- Die Rolle des Menschen wird in der Smart Factory neu definiert: Kollaboration Mensch und Maschine
- Sicherheit als Unternehmenswert
- Standards nähern sich an, werden geprägt durch internationale Firmen (Anbieter wie Anwender):
  - Sicherheitskultur: Lernen aus Fehlerfällen (Offenheit)
  - Abwesenheit von Sicherheit wird wahrgenommen – deren Anwesenheit wird vorausgesetzt !
  - Weg von der statischen zur dynamischen Sicherheit – erzeugen produktivere Lösungen
  - Voraussetzung ist die von Vornherein gemeinsame Betrachtung von Sicherheit und Automation (Verschmelzen)

The 4-fold safety of automation

COMPONENTS
SYSTEMS
SERVICES

Technical Ecological
Personal Economical

Armin Glaser

Pilz GmbH & Co. KG
Felix-Wankel-Straße 2
73760 Ostfildern, Germany
Tel.: +49 711 3409-678
Fax: +49 711 3409-9678
a.glaser@pilz.de

Keep up-to-date on Pilz
www.pilz.com

PILZ
THE SPIRIT OF SAFETY