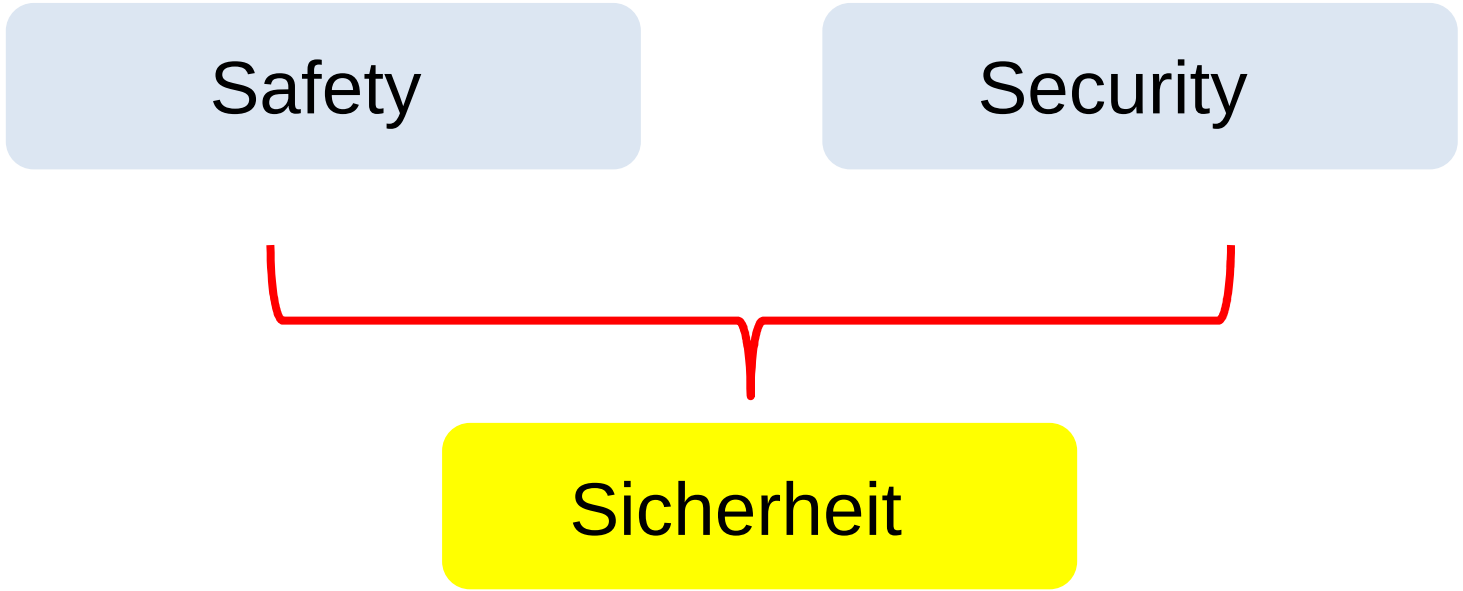
Safety vs. Security

Fachveranstaltung Maschinen
-Sicherheit in Konstruktion und Betrieb-

Erlangen 27. Juni 2014

Dipl.-Ing. Berthold Heinke
FB HM / SG MAF



Sicherheit von ***lat.*** *sēcūritās* zurückgehend auf *sēcūrus* „sorglos“…..

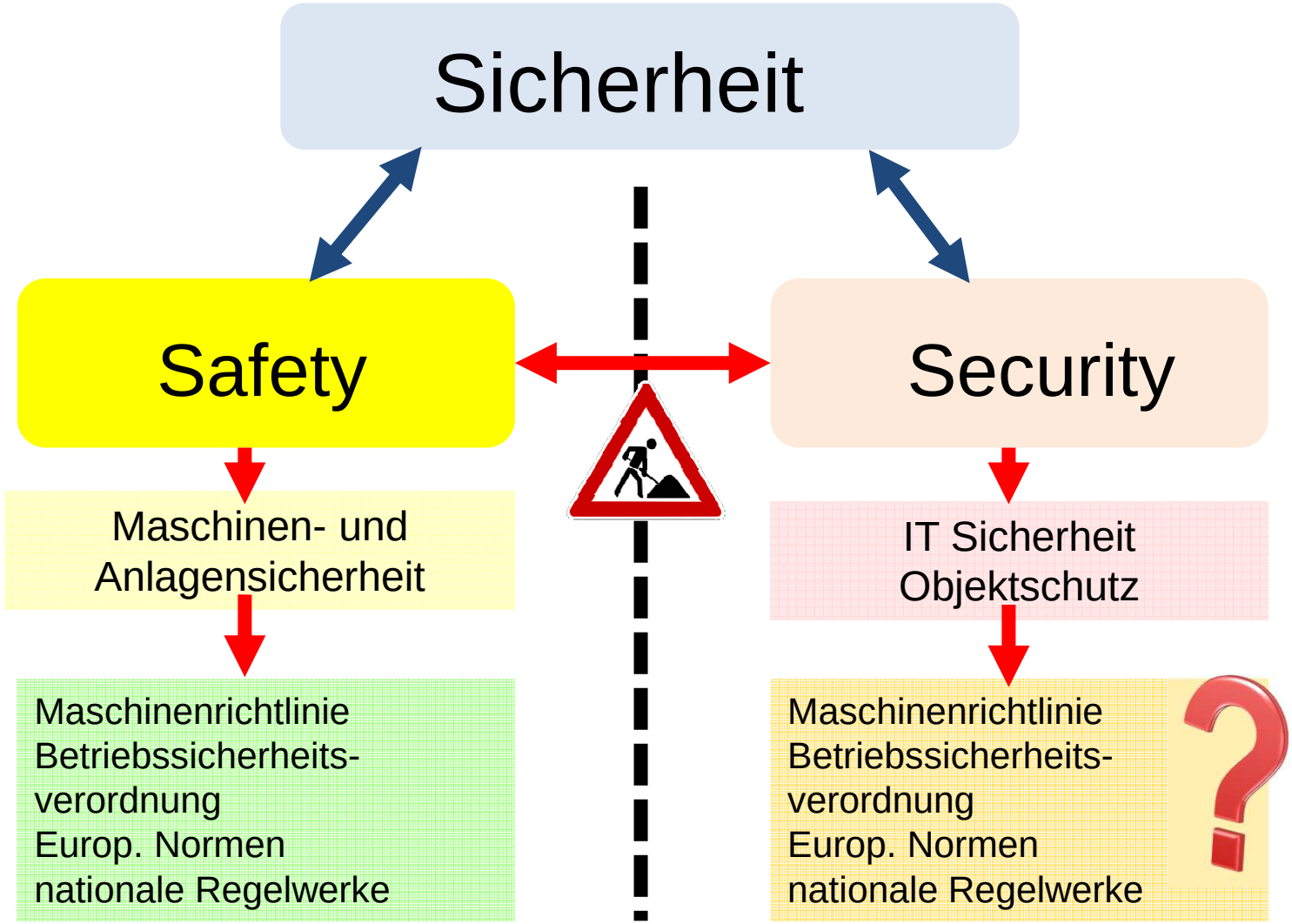
Zustand, der frei von unvertretbaren Risiken der Beeinträchtigung ist oder als gefahrenfrei angesehen wird. …..

Quelle: Wikipedia

„Sicherheit“

- **Safety = Betriebssicherheit (technische Sicherheit)**,
  d.h. Schutz der Umgebung vor einem Objekt.
  - z. B. durch Fehler in der Logik, Defekte in der Hardware

- **Security = Angriffssicherheit (IT Sicherheit)**,
  d.h. Schutz des Objektes vor einer Umgebung.
  - z. B. durch Änderung ihrer Funktionalität (etwa durch einen Hacker, Virus, Wurm)


Sicherheit
Safety
Security
Maschinen- und Anlagensicherheit
IT Sicherheit Objektschutz
Maschinenrichtlinie Betriebssicherheits-verordnung Europ. Normen nationale Regelwerke
Maschinenrichtlinie Betriebssicherheits-verordnung Europ. Normen nationale Regelwerke

Problemlage

2008 Hacker bringen in Polen einen Zug zum Entgleisen

2009 Angreifer übernehmen Verkehrsleitsystem in Los Angeles

2010 Stuxnet kann in die Steuerung von Frequenzumrichtern der Fa. Vacon und Fararo Paya eingreifen

2012 zehn Rechner eines Stromversorgers sind infiziert worden, die zur **Steuerung von Kraftwerksturbinen** dienen. Ursache: Fremdfirma benutzte einen USB-Stick, um Software-Aktualisierungen aufzuspielen. USB Stick war infiziert.
Wiederinbetriebnahme der Anlage um etwa drei Wochen verzögert.

u.v.m.

Problemlage

Versuch der Fa. Tend Micro GmbH im Zeitraum März bis Juni 2013
(Honeypot-Netzwerk)

- 33 466 automatisierte Angriffe auf ein simuliertes Industrienetztwerk
  - 11 Angriffe kritisch
  - 60 % Angriffe aus Russland
  - 10 % Angriffe aus China
  - 7% Angriffe aus Deutschland

Kritsche Angriffe auf:

- simuliertes SCADA System (Supervisory Control and Data Acquisition)
  - gefälschte Befehle, Schadsoftware
  - Benutzerschnittstelle um Login Daten zu erlangen

Quelle: VDI Nachrichten, 2014, Nr.5

Problemlage

3 % Pishing Mails („Passwort fishing“) reichen im Schnitt, um einem Hacker eine fünfzig zu fünfzig Chance zu geben.
Mit 18 Mails bekommt er fast mit Sicherheit seinen Klick

14 % der allgemeinen Angriffe erfolgen durch Firmeninsider

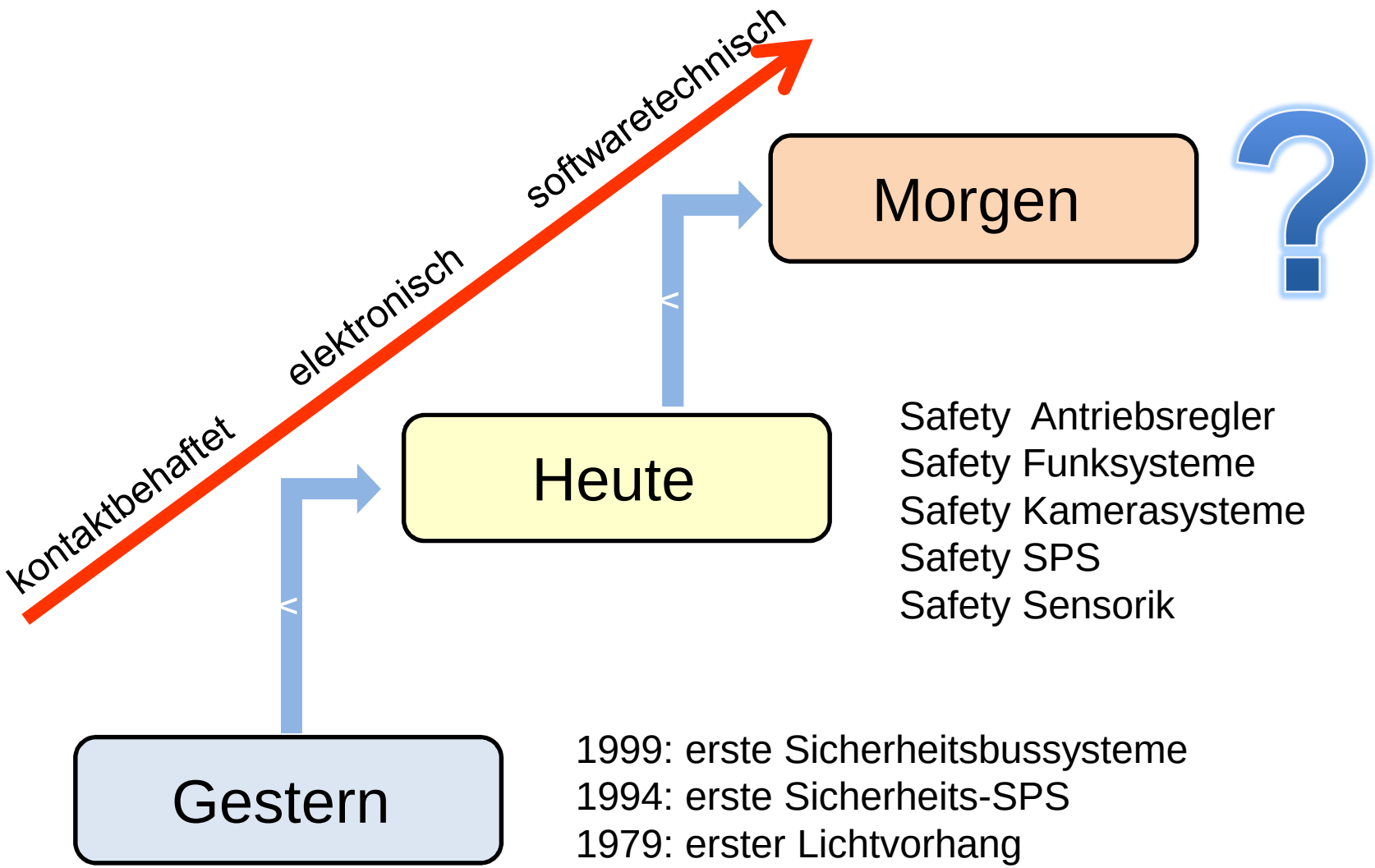
19% aller Attacken dienten der Spionage, Schwerpunkt aus Ostasien

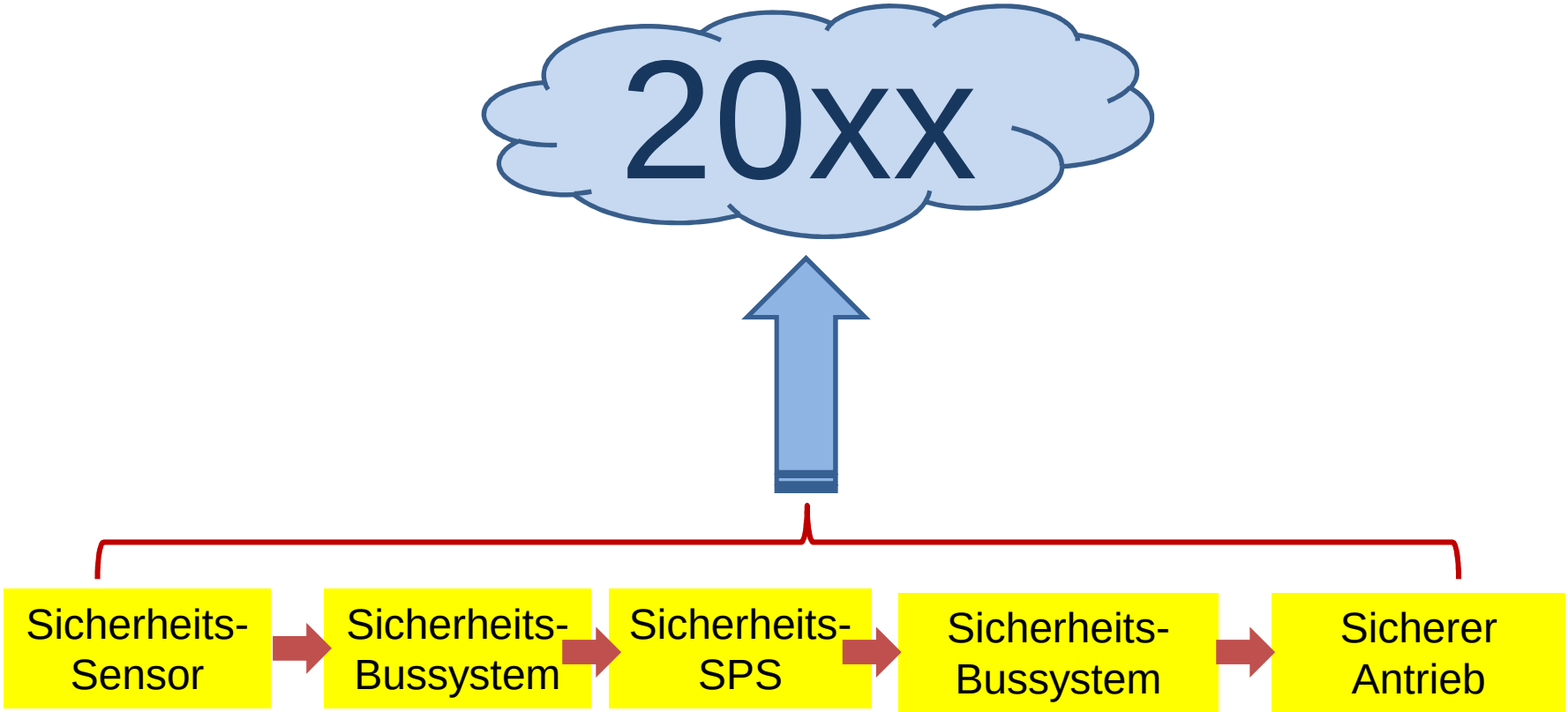
29% der Angriffe geschehen über soziale Taktiken, Infos über Zielpersonen per Telefon, Email, soziale Netzwerke. Ziel: Fälschung von Mails oder Webseiten

78 % aller Angriffe werden als technisch einfach eigestuft, nur 1% als hoch anspruchsvoll
Die alten Tricks funktionieren immer noch

Quelle: Verizon DBI Reports, 2013

Entwicklung der „Safety-Technik“





Sicherheitsrelevante Steuerung im Jahr 2014

Zukunft ???

Hypothese 1

Die Unterscheidung zwischen Standard- und Sicherheits-Komponenten ist bedeutungslos.

- Es gibt nur noch sichere Bauteile. Alle Komponenten entsprechen konstruktiv den Anforderungen des höchsten Sicherheitsniveaus.
- Eine getrennte Bewertung für die Eignung in sicherheitsrelevanten Applikationen entfällt.
- Berechnung von Zuverlässigkeitswerten sowie Begriffe wie PL, SIL oder andere werden überflüssig.

Bereits heute:

- verarbeiten SPS-Systeme sog. Standard- und Safety-Komponenten im Mischbetrieb.
- werden Standard- und Sicherheitssoftware mit gemeinsamen Werkzeugen erstellt.
- werden sicherheitsrelevante Signale und nicht sicherheits-gerichtete Signale über ein Bussystem ausgetauscht.
- enthält beinahe jeder Antriebsregler eine Reihe unterschiedlicher Sicherheitsfunktionen.
- enthalten viel Antriebsregler auch SPS-Funktionen.

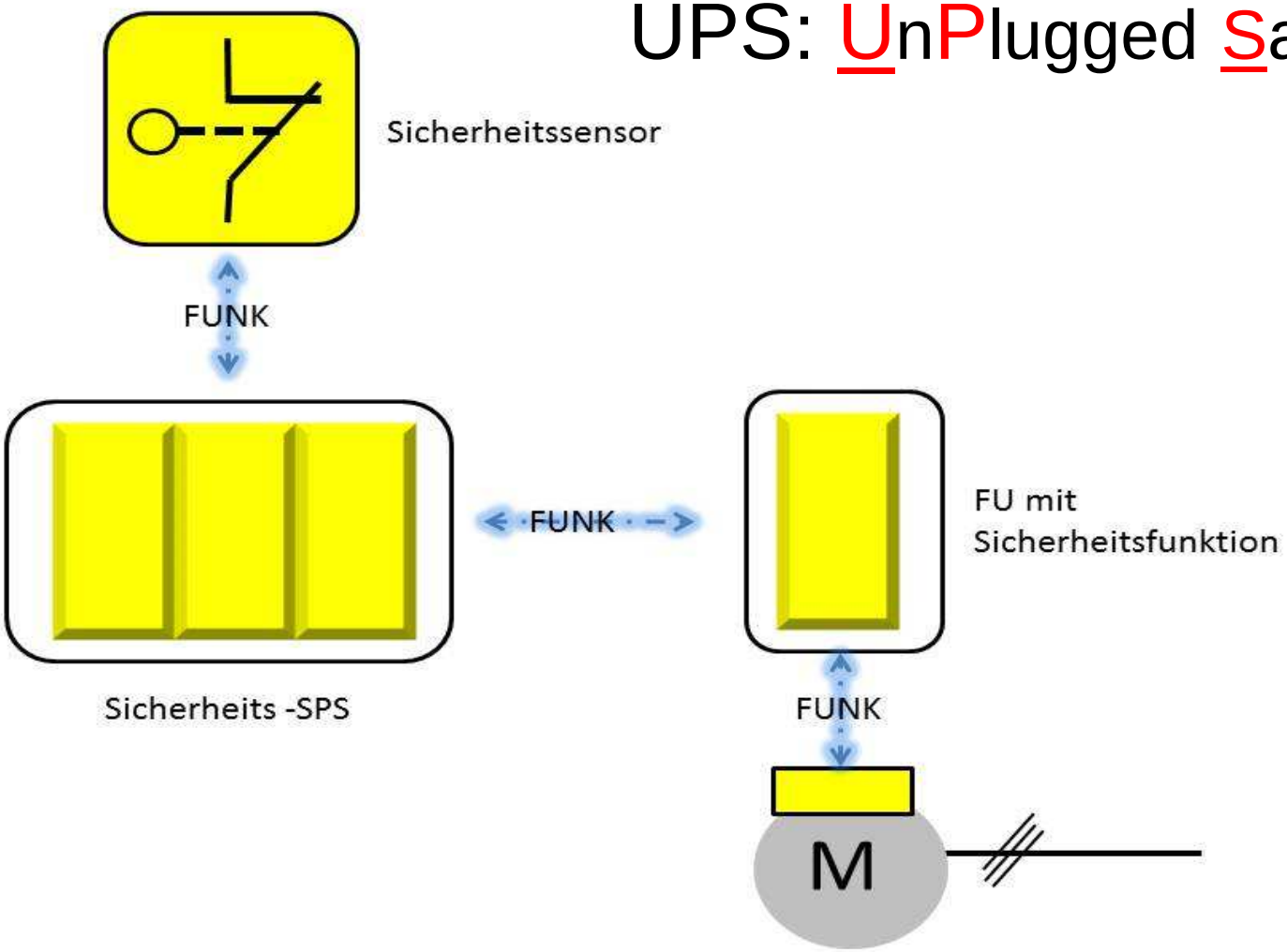
BGHM

Hypothese 2

Die „Verdrahtung“ von sicherheitsrelevanten Bauteilen entfällt.

- Alle Bauteile kommunizieren über sichere drahtlose Verbindungstechniken (Funksysteme)
- Jedes Bauteil hat eine eindeutige Kennung (ähnlich der heutigen MAC-Adresse)
- Bussysteme sind nicht mehr „kabelgebunden“
- Die Energieversorgung erfolgt kontaktlos

UPS: UnPlugged Safety

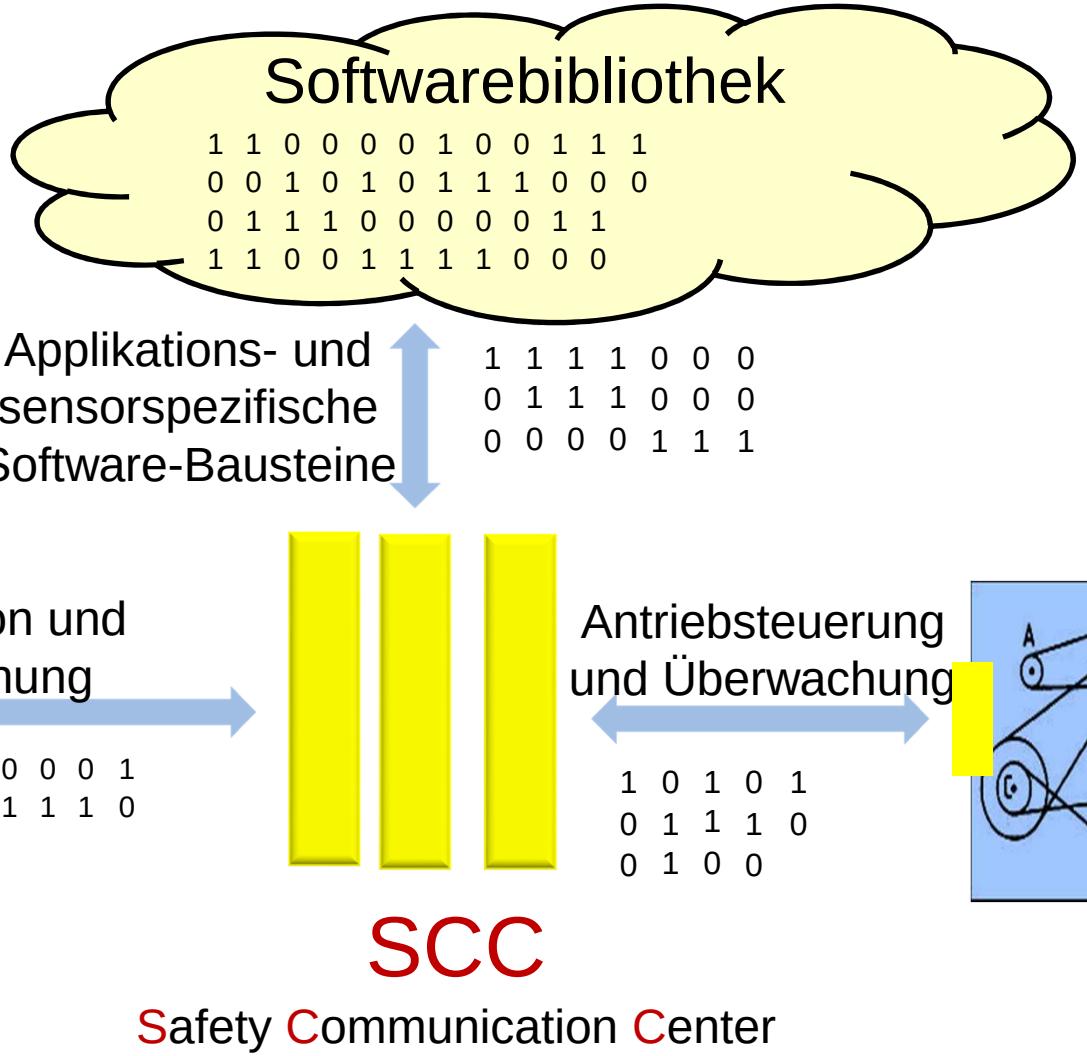


Hypothese 3

Sicherheitsrelevante Bauteile werden automatisch, eindeutig und richtig parametriert.

- Nach Aufbau der Kommunikation wird die in dem Bauteil vorhandene richtige Kennung und der notwendige Softwarebaustein per „Download“ übermittelt.
- Aufgrund der „Software-On-Demand“ Funktionen der Komponenten erfolgt lediglich die Verknüpfung.
- Softwarebaustein / -katalog wird „on-Demand“ immer sicherheits-technisch richtig mitgesendet.
- Lediglich Zuordnung (Parametrierung) zu den jeweiligen Anlagenteilen bzw. -Bausteinen ist erforderlich.

SAS:
Safety Application Server



SCC
Safety Communication Center

Zunahme von Intelligenz in der Sensorik, Logik und Aktorik ermöglicht Einfluss auf Anlagensteuerungen

- gewollt (Anpassungen an Fertigungsprozess, Fehlerbeseitigung usw.)
- ungewollt (Angriffe durch Hacker, Viren, Trojaner usw.)

Maschinensicherheit

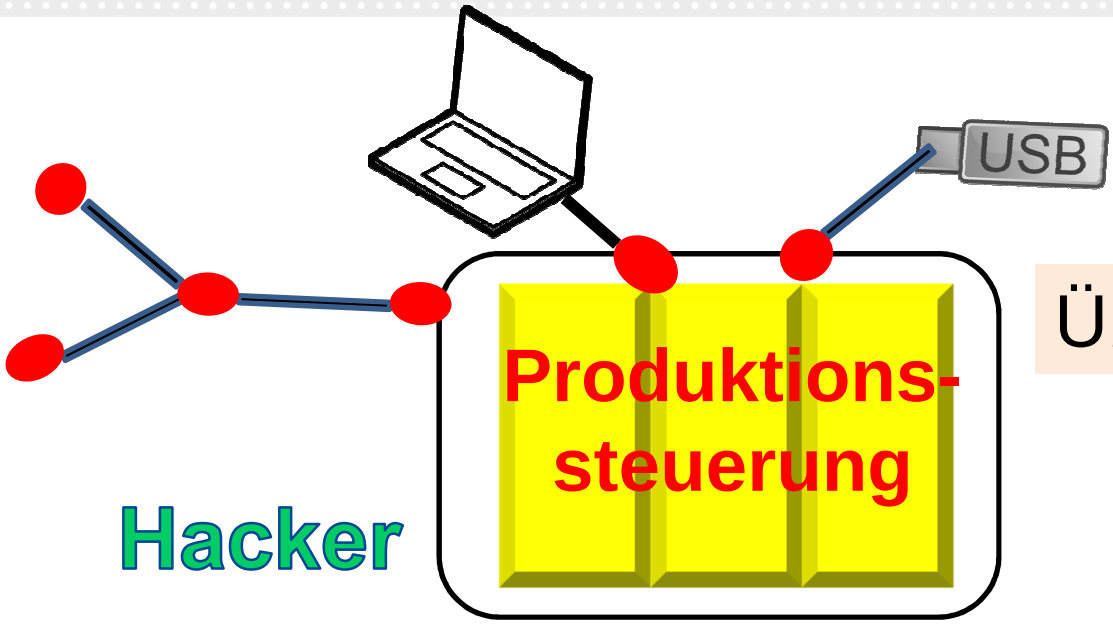
Konsequenz

Anforderungen an die Sicherheit (Safety) werden bis zu einer endgültigen Verschmelzung von Funktion und Sicherheit steigen.

Anforderungen zum Schutz gegen Angriffe (Hacker, Viren usw.) im Sinne von Security müssen ebenfalls mit entwickelt werden

Ganzheitliche Betrachtung unabdingbar

Safety-Security „Schon HEUTE“!?



Übertragungswege

Auswirkungen

Virus

Backdoor
Hintertür

Trojaner

Malware

Rootkit
Zugriffsrechte Administratoren

Wurm

Key-Logger
Eingabe Daten aufzeichen

Stuxnet

TOP 10 Bedrohungen

gem. BSI (Bundesamt für Sicherheit in der Informationstechnik)

	Bedrohung	Erklärung
1	Infektion mit Schadsoftware über Internet und Intranet	Office Programme sind stark mit dem Internet verbunden. Angreifer nutzen Verbindungen von Office ins ICS Netz IT-Komponenten werden auch häufig im ICS -Netz verwendet. z.B. Server, Betriebssysteme. Angreifer nutzen Schwachstellen aus
2	Einschleusen von Schadsoftware über Wechseldatenträger und externe Hardware	Verwendung in Office Welt und Industrieumgebung, Fremdpersonal hat eigene Wechseldatenträger Meist steht Safety im Vordergrund, Bewusstsein für Security fehlt
3	Sozial Engineering	Missbrauch von Vertrauen, Hilfsbereitschaft als Ablenkungsstrategie, z.B. gewinnspiele

***ICS**: Industrial Control System

Quelle: BSI-CS 005 Vers. 1.10 vom 26.3.2014

TOP 10 Bedrohungen gem. BSI

	Bedrohung	Erklärung
4	Menschliches Fehlverhalten / Sabotage	Vorsätzliche Handlung, Fahrlässigkeit, Sicherheit kann nicht allein durchtechnische Maßnahmen erreicht werden, sondern erfordert auch organisatorische Regelungen
5	Unberechtigte Nutzung von Fernwartungs-zugängen	Bewusste Öffnung des ICS* Systems nach außen Verwendung für Downloads, Diagnosen, Wartung, Dienstleister, Hersteller
6	Internet verbundene Steuerungskomponenten	Verbindung von ICS mit Internet, IT-Sicherheit fehlt z.B. im SPS Bereich
7	Technisches Fehlverhalten und höhere Gewalt	Technische Defekte, Umwelteinflüsse, Softwareeinflüsse,

Quelle: BSI-CS 005 Vers. 1.10 vom 26.3.2014

TOP 10 Bedrohungen gem. BSI

	Bedrohung	Erklärung
8	Smartphones im Umfeld	Anzeige von Betriebsdaten, Produktionsparameter auf Tablet oder Smartphone, Ähnlich wie Fernwartungszugang
9	Kompromittierung von Extranet und Cloud Komponenten	Extern betriebene Softwarekomponenten, komplexe Berechnungen von Maschinen, Datenerfassung, Datenverarbeitung
10	(D)DoS Angriffe	Distributed Denial of Service, Beeinträchtigung von Resourcen im ICS Netzt, Systemabstürze; Blockierung von Übertragungswegen für Mess- und Steuerdaten

Quelle: BSI-CS 005 Vers. 1.10 vom 26.3.2014

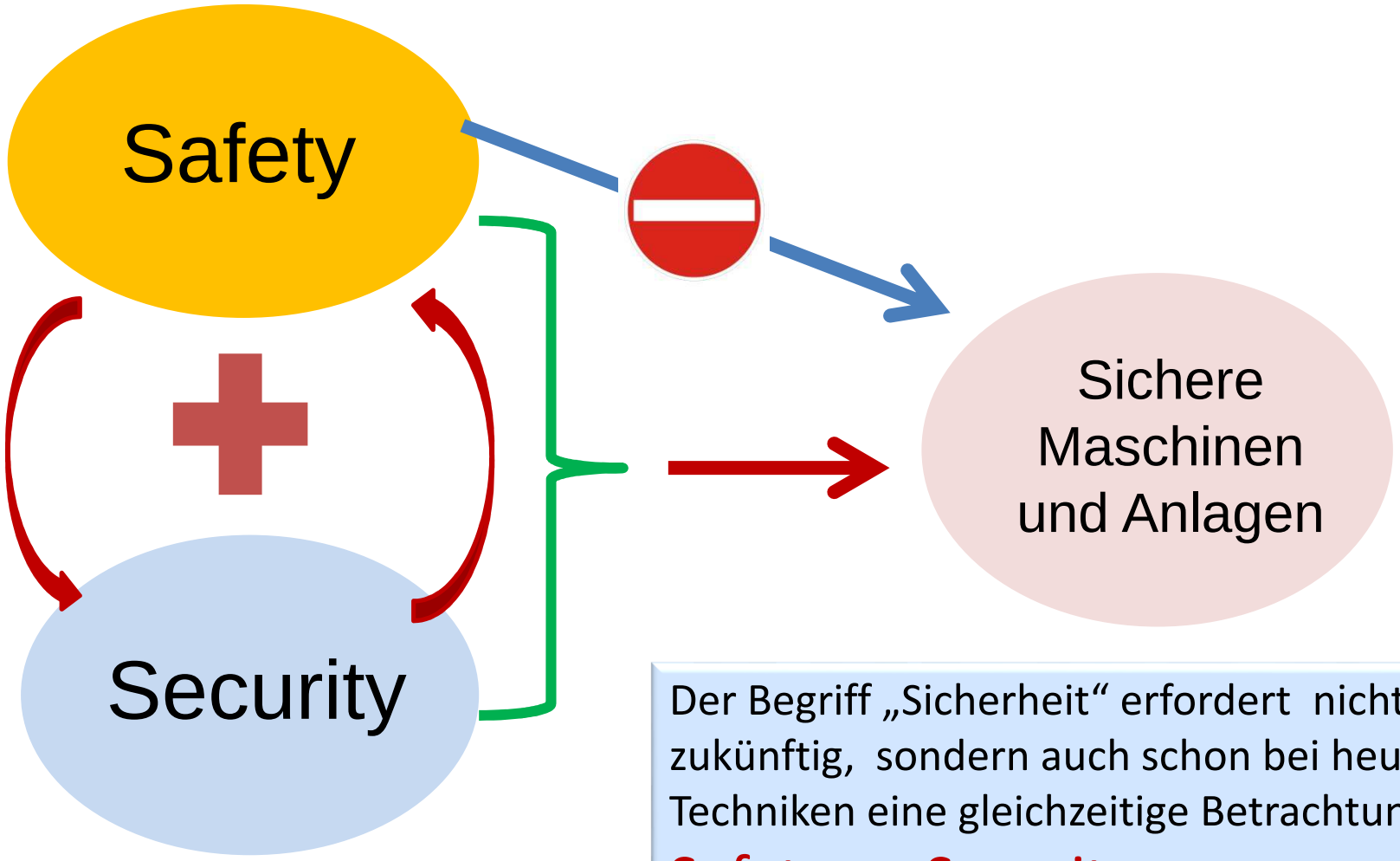
Mögliche Auswirkungen

- Produktionsausfall einer Maschine oder einer kompletten Fertigungsstraße
- Zerstörung von Maschinen
- Manipulation der Netzwerkkommunikation
- Veränderung von Produktionsdaten -> Qualitätsmängel
- Diebstahl von Produktionsdaten (Qualitäts- oder Prozessdaten)
- Veränderung von Maschinenparametern auch von sicherheitsrelevanten Informationen
- Passivierung von Sicherheitseinrichtungen
- Aktivierung von Safety Prozeduren

Ursachen und Konsequenz

- Unerfahrenheit der Maschinen- und Anlagenbauer bzgl. IT-Sicherheit
- (Alt-)Anlagen ohne jeglichen Schutz
- Anti-Virus-Software für Automatisierungstechnik ?
- Maschinen unterschiedlicher Hersteller mit Komponenten unterschiedlicher Hersteller werden kombiniert
- Heterogene Automatisierungshardware
- Unterscheidung in Office Security und Produktions-IT
- IT-Security Maßnahmen ungeeignet / nicht vorhanden für Automatisierungstechnik

Gemeinsames Security Management für Office- und Automatisierungsanwendungen



Der Begriff „Sicherheit“ erfordert nicht nur zukünftig, sondern auch schon bei heutigen Techniken eine gleichzeitige Betrachtung von

Safety und Security.

Hilfreiche Literatur und Checklisten

Bundesamt für Sicherheit in der Informationstechnik (BSI)
www.bsi.bund.de:

- ICS Security : Top 10 Self-Check
- ICS Security : Top 10 Bedrohungen und Gegenmaßnahme

VDMA Studie „Status Quo der Security in Produktion und Automation“ 2013/2014
www.vdma.org

Danke
für Ihre
Aufmerksamkeit