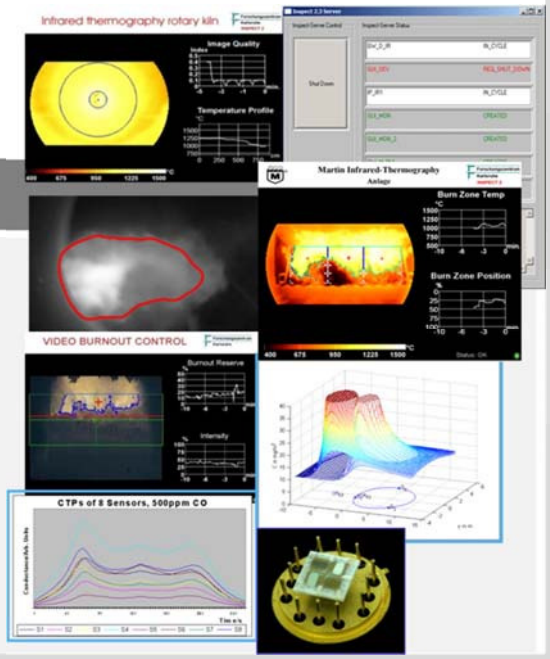
Karlsruher Institut für Technologie

IT-Sicherheit in ihrer Doppelrolle

Vortrags- und Diskussionsabend –
Qualitätsmerkmal Technische Sicherheit
Ein Denkansatz und Leitfaden aus dem VDI
für die Gesellschaft



Institut für Angewandte Informatik IAI

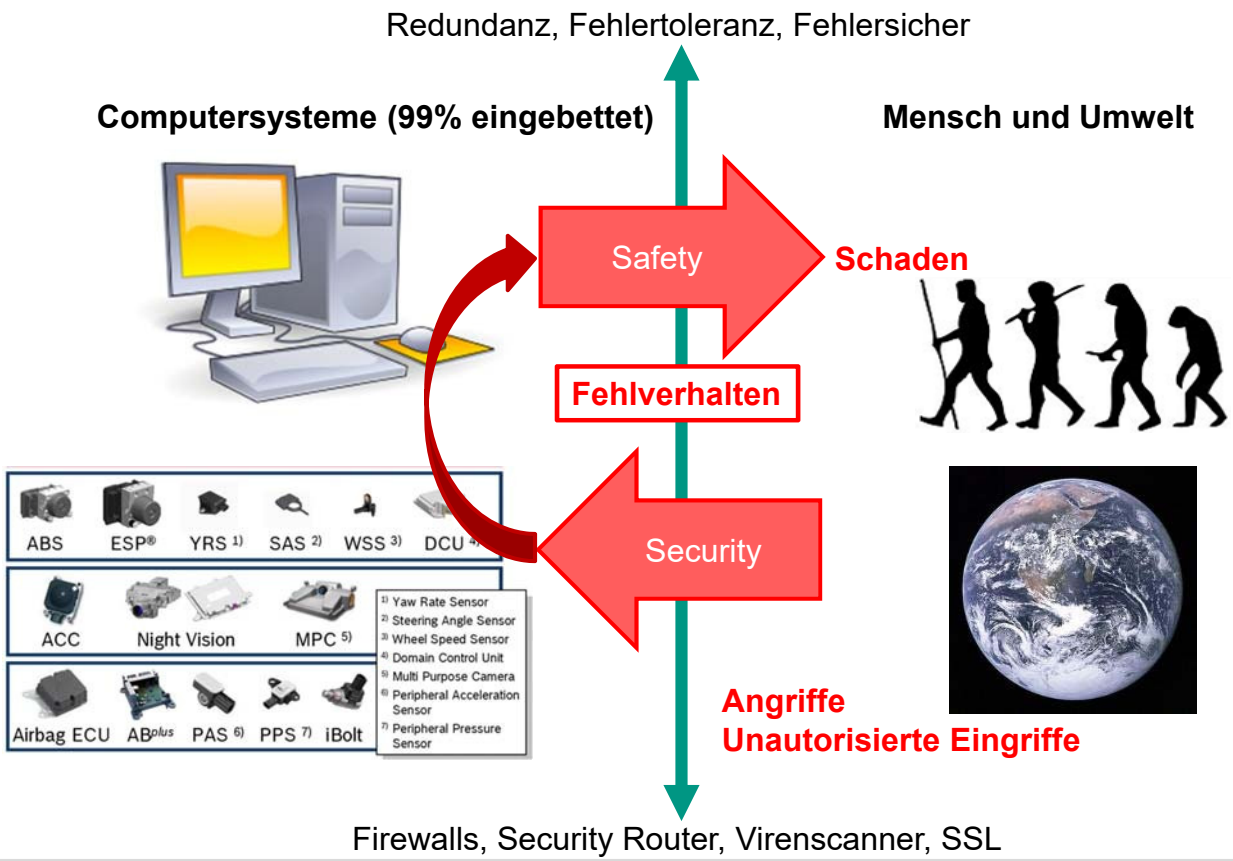
Hubert B. Keller, Oliver Schneider
AG ProSys - Prozessoptimierung,
intelligente Sensorsysteme und sichere Software

VDI/VDE-Arbeitskreises Sicherheit (AKSi) in Kooperation mit dem „Forum Technologie und Gesellschaft“ im FORUM46 – Interdisziplinäres Forum für Europa e.V., und dem Cluster PROMPT im VDI Bezirksverein Berlin-Brandenburg e.V.

Karlsruher Institut für Technologie

Motivation

Zweiseitige Sicherheit



Motivation

Wie sicher sind unsere derzeitigen automatisierten Infrastrukturen (Computersysteme) mit Firewalls, virtuellen Maschinen, Virenscanner, sicherem Transport etc.?

→ US-CERT Cyber Security Bulletin

- [National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) in the past week. The NVD is sponsored by the Department of Homeland Security (DHS) National Cybersecurity and Communications Integration Center (NCCIC) / United States Computer Emergency Readiness Team (US-CERT)]

- Common Vulnerability Scoring System (CVSS): High Vulnerabilities will be labeled High severity if they have a CVSS base score of 7.0 - 10.0
- **Beispiele:**
  VMware has released security updates to address a vulnerability in VMware ESXi, Fusion, Player, and Workstation. Exploitation of this vulnerability may allow **escalation of privileges**. January 08, 2016
  Symantec has released Symantec Endpoint Encryption 11.1.0 to address a vulnerability that may allow an attacker to **take control of an affected system**. December 15, 2015

US CERT etc. Januar 2016

Und so weiter
und **grundsätzlich**
so weiter …
da auch Vulnerabilities in der Automatisierung
(Tool CoDeSys) vorhanden sind:
Affected vendors:
Arbiter, Catapult Software, Codesys, Ecava IntegraXor,
Festo, Innominate, KEP (Kessler-Ellis Products),
Meinberg, Microsys, spol. s r.o., Nordex Energy GmbH,
Pepperl+Fuchs GmbH, Progea, Red Lion,
Roche Diagnostics GmbH, SELINC, Sielcosistemi, Siemens,
Sierra Wireless, SUBNET, Trihedral Engineering Limited,
and Wind River Systems.

Cisco

2015: TOP 5 Most Vulnerable Vendors

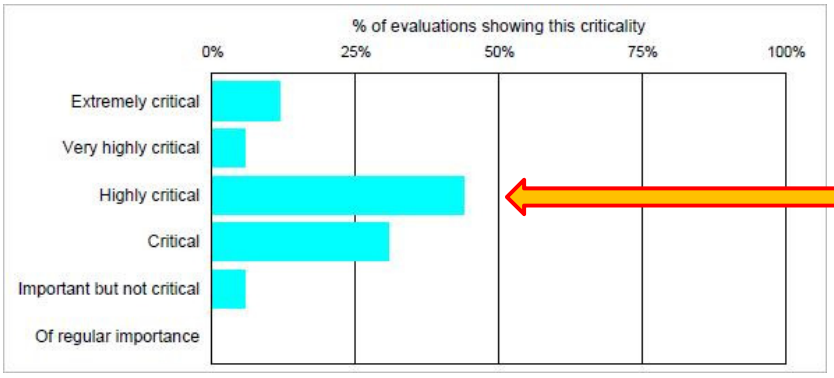
	2015 Place	2015 CVE Count	2014 Place	2014 CVE Count
Apple	1	654	5	288
Microsoft	2	571	3	376
Cisco	3	480	4	368
Oracle	4	479	2	433
Adobe	5	440	8	138

Router, Security Equipment, …

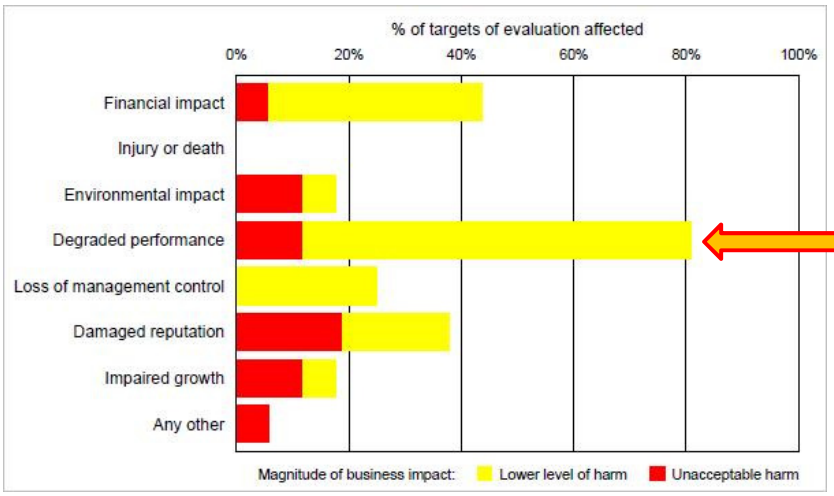
The most vulnerable software vendors of 2015
13/01/2016, By Chris Goettl

http://www.itproportal.com/2016/01/13/the-most-vulnerable-software-vendors-of-2015/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+itproportal%2Frss+%28Latest+ITProPortal+News%29

Risiko Studie für SCADA und ICS

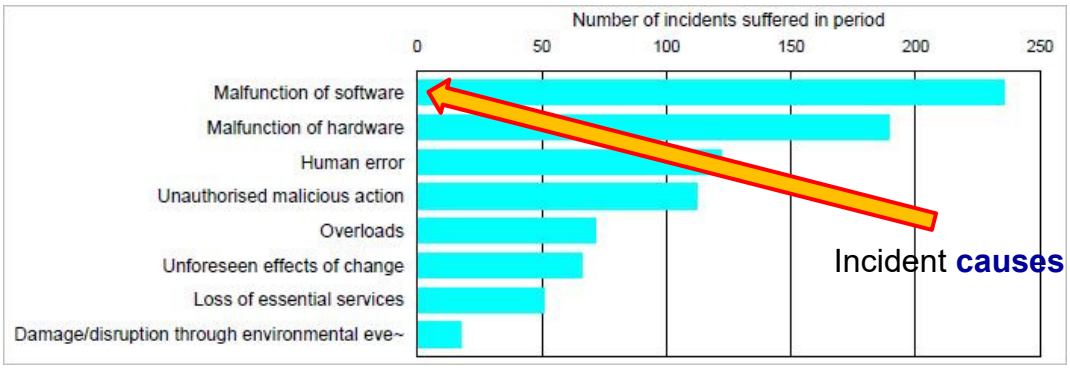


Business **criticality** of the target industrial control systems

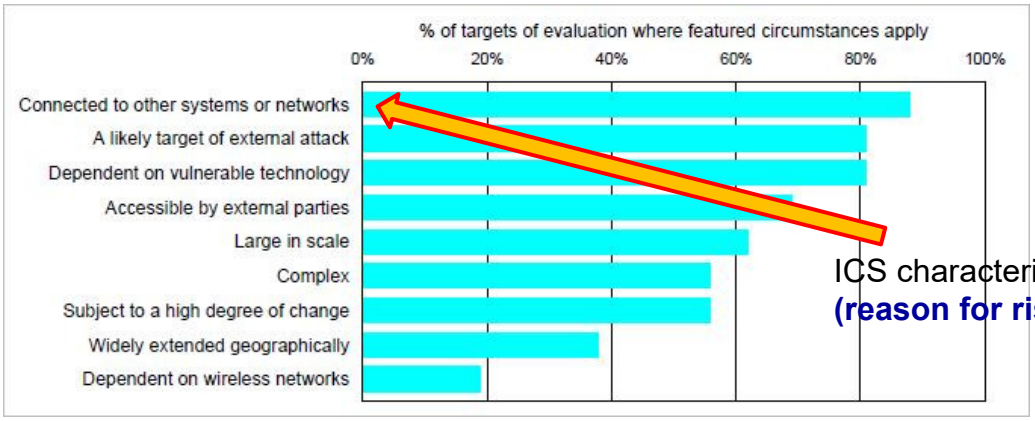


Risk metrics for industrial control systems
(SCADA and related systems that automate industrial processes)
Feb 24, 2016
Simon Oxley, Managing Director
Citicus Limited, Garden Studios
71-75 Shelton Street, Covent Garden
London WC2H 9JQ, England

Business **impact** of incidents



Incident **causes** and reported **volume**



ICS characteristics that drive risk up **(reason for risk)**

Zuverlässigkeit von Software als Grundprinzip

Zuverlässigkeit als durchgehende Erbringung der Funktion über einen definierten Zeitraum.

„Funktion“ der Mathematik

x→f→y

x ∈ D, y ∈ W
Bildmenge D
Wertemenge W

D ⊂ G, W ⊂ Z
G, Z = ℜ

Funktion f ist **auf D definiert** und **bildet** Bildmenge D **in Wertemenge W** ab

„Funktion“ der Informatik

x→f→y
x ∈ D, y ∈ W

x‘→f→error
D‘ = G \ D, W‘ = Z \ W = error

D ⊂ G, W ⊂ Z
D‘ = G \ D, W‘ = Z \ W = error
G, Z = ℜ

Algorithmus f berechnet für jede **Eingabe aus D** die **Ausgabe aus W**.
Für jeden **Wert außerhalb von D** erfolgt **Fehlermeldung !!!**

Unzuverlässigkeit der Implementierung

„Funktion“ als Ergebnis der Programmierung

x→f→y
x ∈ D, y ∈ W
D ⊂ G, W ⊂ Z

x‘→f→ „undefined behaviour“
D‘ = G \ D
W‘ = Z \ W
G, Z = ℜ

x‘→f→ „undefined behaviour“

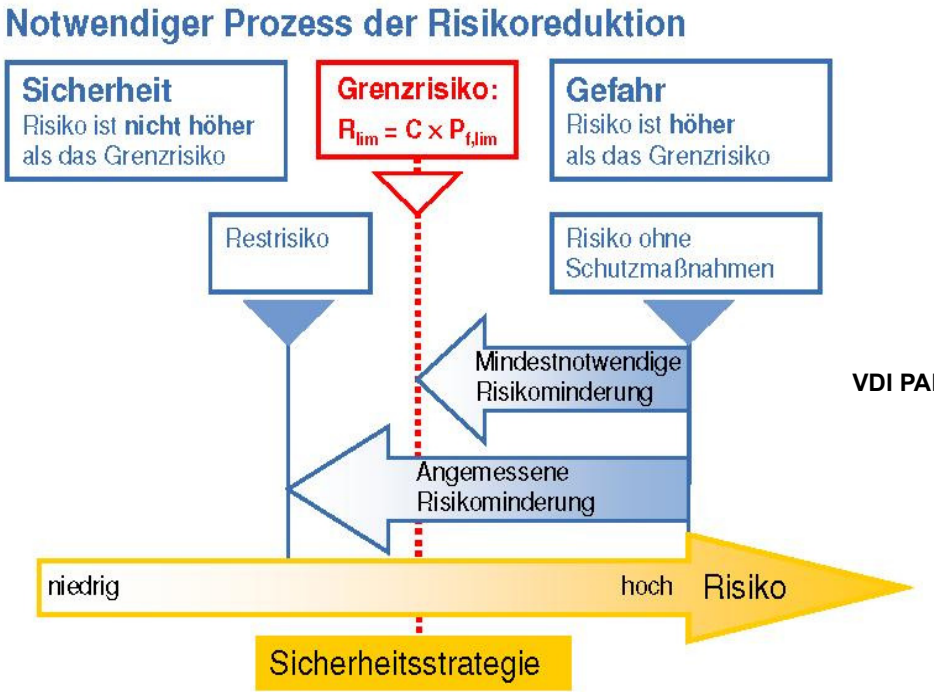
D‘ = G \ D = „handcrafted“
W‘ = Z \ W = „gain administrator privileges“

Programm liefert für jede Eingabe aus D korrekte Werte.
Für jeden Wert außerhalb von D erfolgt Stack/Buffer Overflow,
Rücksprungadresse wird überschrieben,
Unbekannter Code ausgeführt und
Der Angreifer erhält Administratorrechte.

Vulnerability :=
Schwachstelle in Programmen, die es einem Angreifer erlauben, durch spezielle Bitmuster die Ausführung von nicht vorgesehenem Code initiieren. Ursache ist die nicht typstrenge Prüfung von Kommandos und Daten und nachfolgend Programmmanipulation.

(siehe: ISO/IEC TR 24772: Guidance to Avoiding Vulnerabilities in Programming Languages through Language Selection and Use)

Risikobetrachtung – Safety und Security

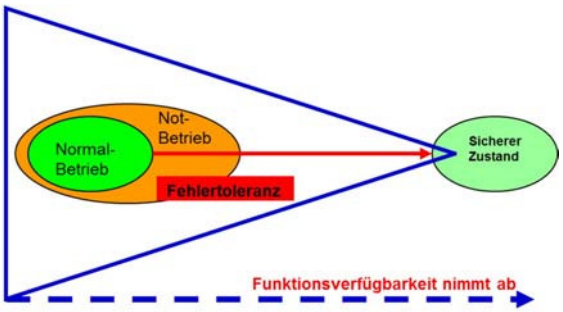


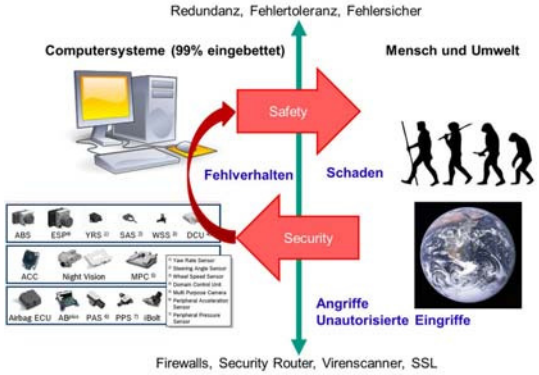
Normen:
→ Kompetenz der Angreifer [0..1] bei Security!!??

VDI PAK Technische Sicherheit

Risiko – Safety und Security

- Toleriertes Risiko, das von jemandem getragen wird (Restrisiko):
  - Versicherung [Flugbetrieb pauschal]
  - Gesellschaft [200 Tote]
  - Individuum [Absturz]
- Absolut sichere Systeme gibt es nicht, aber sichere Zustände, und die Zeit, diese mittels präventiver Maßnahmen auch zu erreichen:
  - Redundanz
  - Degradierung
- Dies muss unter integrativer Betrachtung von Safety und Security erfolgen!





Relevanz Zuverlässigkeit, Security und Safety in der Zukunft unserer technisierten Welt

Beispiel Energiesystem der Zukunft

- Software ist zentrale Basis für hoch vernetzte Infrastrukturen.
- Automatisierung basiert auf softwaretechnischen Funktionen.
- Münchner Kreis:
  - … **intelligente, dezentrale Steuerung** auf der Basis von Informations- und Kommunikationstechnologien (IKT)
  - … dezentral gestaltetes IKT-Steuerungssystem … wird … bezüglich seiner **Komplexität über alle** bisher bekannten IKT Systeme hinausgehen.
  - Die IT-Infrastruktur muss **Sicherheit und Zuverlässigkeit** gewährleisten.
  - … besonders relevant: …… die Gestaltung von **System-Software-Architekturen** …, … Entwicklung von **gesamtsystemischer Resilienz**… die Entwicklung von Evolutions- und **Migrationsstrategien** für Legacyinfrastrukturen und -systeme …
  - …neue **Verschlüsselungsmethodiken für ressourcenbeschränkte** Sensoren benötig.

50 Empfehlungen für eine erfolgreiche Energiewende. MÜNCHNER KREIS, Übernationale Vereinigung für Kommunikationsforschung e.V., Tal 16, 80331 München. www.muenchner-kreis.de, Stand Juli 2015

Cyber Attacken werden Standard

- Beginning in 2009, a series of attacks were launched against the **global energy**, **oil**, and **petrochemical** sectors.
- In a 2010 survey on critical infrastructure security by McAfee and the Center for Strategic and International Studies (CSIS), nearly **half of the respondents from the energy sector** said they had **found Stuxnet** on their systems.
- More recently, an apparent descendant of Stuxnet called Duqu has been reported in energy facilities **in at least eight countries**.
- Another source of vulnerability is the **age of much of the infrastructure**. An estimated 70 percent of the existing energy grid is more than 30 years old.
- The Brains of the Smart Grid: The third and perhaps **most alarming cause of vulnerability** is the proliferation and increasing **interconnection of embedded software and devices directing the flow of energy**.

(Smarter protection for the smart grid, Report of McAfee, an Intel Company, 2012)

Cyber Sicherheit

- Die überwiegende Anzahl der Security **Schwachstellen** können laut (/You2003/) auf **Implementierungsschwachstellen** zurück geführt werden.
- Die genannten Schwachstellen betreffen nicht nur **Anwendungssysteme**, sondern auch **Betriebssysteme** und gerade auch **Security-Infrastruktursysteme** wie **Security-Router**, **virtuelle Maschinen** etc.
- **Cisco** - Auszug (**294 Schwachstellen** gefunden innerhalb 1 Jahr) → ... durch Bitmuster Code ausgeführt und nachfolgend Privilegien erreicht werden. Damit ist es möglich, die Kontrolle über das System zu übernehmen.
- **Vmware** (virtuelle Maschine) - Auszug (**85 Schwachstellen** gefunden innerhalb 1 Jahr)
- **Juniper Virtual Private Network** (VPN) - Auszug (**45 Schwachstellen** gefunden innerhalb 1 Jahr) → „to gain privileges via unspecified combinations of CLI commands and arguments“
- 3S Smart Software Solutions **CoDeSys** (Tool für Automatisierungssysteme) - Auszug (**12 Schwachstellen** gefunden innerhalb 1 Jahr)
- **Siemens** Simatic - Auszug (**60 Schwachstellen** gefunden innerhalb 1 Jahr)
- **Windturbinensysteme** - Auszug (**6 Schwachstellen** gefunden innerhalb 1 Jahr) → … Steuerungs-Software der Windturbinen kann die Kontrolle übernommen werden, damit ist das System nicht mehr kontrollierbar.

Zielsetzungen für technische Sicherheit

Zielthemen für effektive technische Sicherheit

- Ursachen von **Schwachstellen** (Vulnerabilities) analysieren und beseitigen
- **Angriffstolerante** bzw. -**sichere** Systeme bauen (Analyse/Entwurf/Implementierung)
  - Architekturen
  - Komponenten
  - Kommunikation

Neu denken und neu realisieren!

- Beherrschung der **Wechselwirkung von Safety – Security – Safety**
- **Privacy** Aspekte im Sinne **explizite** Erlaubnis für Zugriff auf Informationen basierend auf Prozesskonzept

- **Anwendungen**,
- **Betriebssysteme und Laufzeitsystem** (Prozesskonzept/Mikro-Kernel),
- **Programmiersprachen** (Semantik und Syntax) sowie
- **sichere Infrastruktur** (Ziel-Quelle-IDs, Verschlüsselung ohne Schwachstellen)

Besonderes Zielthema in der Zukunft für komplexe Systeme

Beherrschbarkeit (controlability):=
der Benutzer eines Systems ist mental in der Lage die intendierte Zielfunktion zu realisieren.

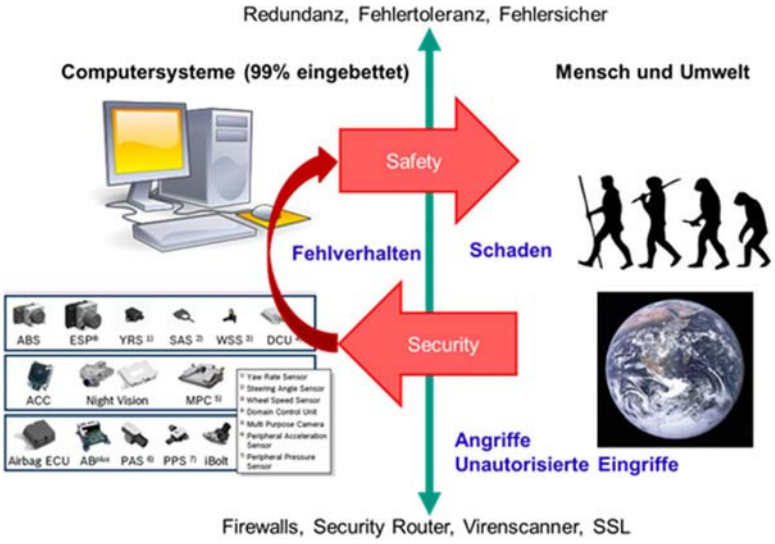
Bei fehlerhaftem Verhalten des Systems besteht eine graduelle Beherrschbarkeit (mental) im degradierten Zustand.

(siehe: Dietrich Dörner, Psychologe/em. Prof. Otto-Friedrich-Universität Bamberg: Lohhausen. Vom Umgang mit Unbestimmtheit und Komplexität;
Die Logik des Misslingens: strategisches Denken in komplexen Situationen)

Beispiel:
Landung eines Airbus auf dem Hudson River (US-Airways-Flug 1549)
Inlandslinienflug vom Flughafen LaGuardia (New York City) nach Seattle/Tacoma, Washington)
15. Januar 2009, Probleme mit den Triebwerken nach Vogelschlag,
Notwasserung auf dem Hudson River (Airbus A320-214 setzte um 15:32 Uhr Ortszeit auf dem Hudson auf.

Publikationen

- Namurempfehlung NE 153 Automation Security 2020 - Design, Implementierung und Betrieb industrieller Automatisierungssysteme / Automation Security 2020 - Design, Implementation and Operation of Industrial Automation Systems, NAMUR – Interessengemeinschaft Automatisierungstechnik der Prozessindustrie e.V., NAMUR-Geschäftsstelle, c/o Bayer Technology Services GmbH, Geb. K 9, 51368 Leverkusen, Deutschland
- Keller, H.B.: Gesellschaftliche Relevanz der Informatik als Strukturtechnologie. Chancen und Risiken der Wagnisgesellschaft : Schriftlicher Beitrag zur Dokumentation der Veranstaltung am 15.Oktober 2014 in der Bundesanstalt für Materialforschung und -prüfung (BAM), Berlin, Berlin : FORUM46 - Interdisziplinäres Forum für Europa e.V., 2014 S.16-39, gedruckt
- Felix Freiling, Rüdiger Grimm, Karl-Erwin Großpietsch, Hubert B. Keller, Jürgen Mottok, Isabel Münch, Kai Rannenberg, Francesca Saglietti: Technische Sicherheit und Informationssicherheit, Unterschiede und Gemeinsamkeiten. Informatik Spektrum 1 (37) 2014. Pg. 14ff
- Leitfaden „Technische Sicherheit“ (2016), Leitfaden „Zuverlässige Software“ (2016/17) u.w.



Technische Sicherheit ist eine notwendig grundlegende Eigenschaft.
In technisierten Gesellschaften ist Security ebenfalls eine notwendig grundlegende Eigenschaft.
Der VDI als Ingenieursgesellschaft muss grundlegend hierzu beitragen.