Kritische Infrastrukturen erfordern kritisches Denken

Konflikte zwischen Safety und Security

Know-how to go Wissensfrühstück 22.05.2023

Manuel Atug

Manuel Atug
Head of Business Development

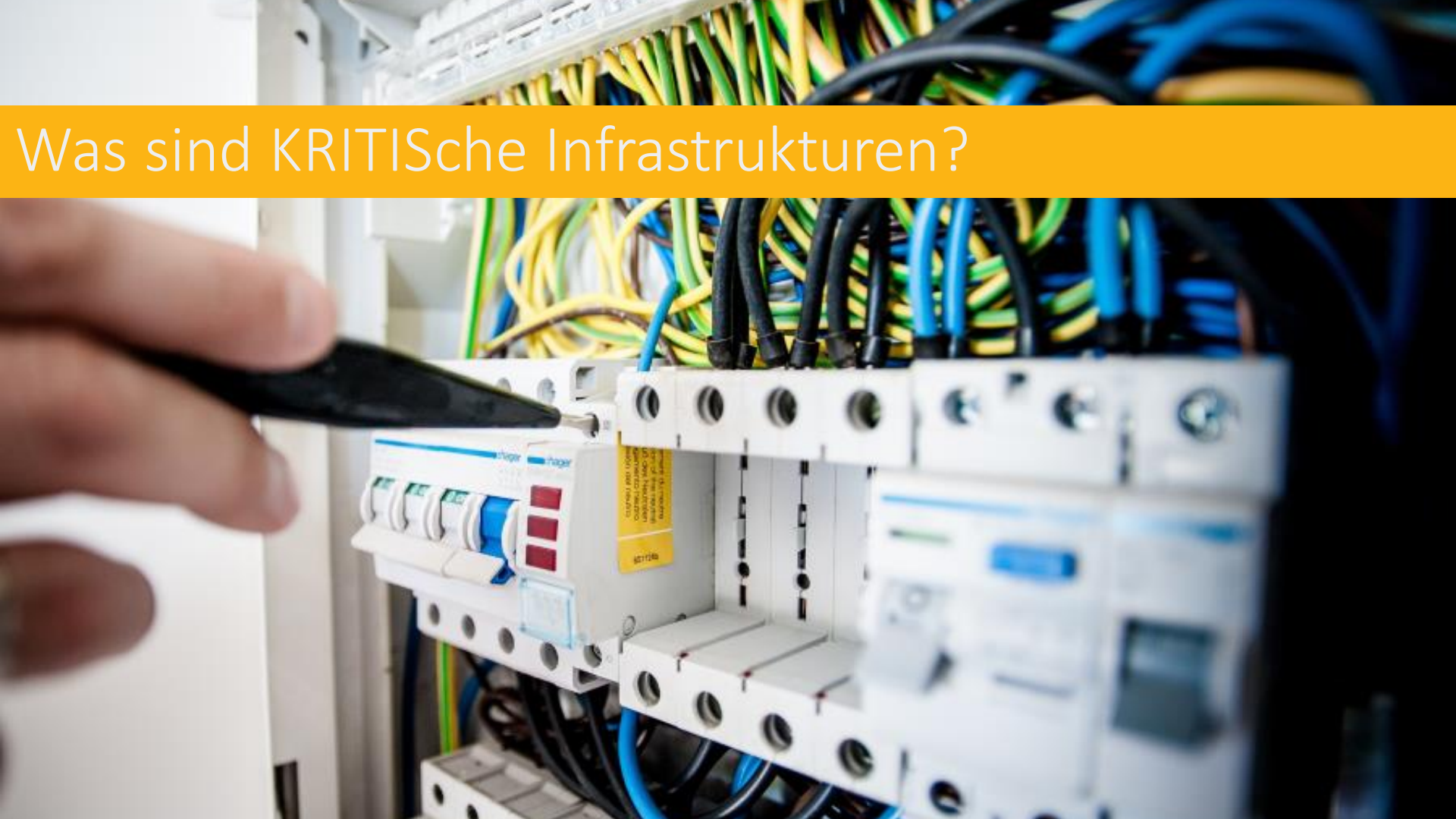
Schwerpunkte und Qualifikationen:

- Diplom-Informatiker, Master of Science in Applied IT Security, Ingenieur
- Weit über 23 Jahre in der Informationssicherheit tätig
- langjährige Erfahrung im Bereich technische IT-Sicherheit und Auditierungen
- Themen: KRITIS, ISMS, BCM
- prägender Berater des BSI für § 8a BSIG

@HonkHase

© HiSolutions 2023

Was sind KRITISche Infrastrukturen?



§ 2 (10) BSI-Gesetz

Begriffsbestimmungen

Kritische Infrastrukturen im Sinne dieses Gesetzes sind Einrichtungen, Anlagen oder Teile davon, die

1. den Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen, sowie Siedlungsabfallentsorgung angehören und
2. von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden.

Die Kritischen Infrastrukturen im Sinne dieses Gesetzes werden durch die Rechtsverordnung nach § 10 Absatz 1 näher bestimmt.

© HiSolutions 2023

Die 10 Kritische-Infrastrukturen-Sektoren in Deutschland

Quelle https://www.bbk.bund.de/DE/Themen/Kritische-Infrastrukturen/Sektoren-Branchen/sektoren-branchen_node.html

© HiSolutions 2023

Wenn das Licht ausgeht…

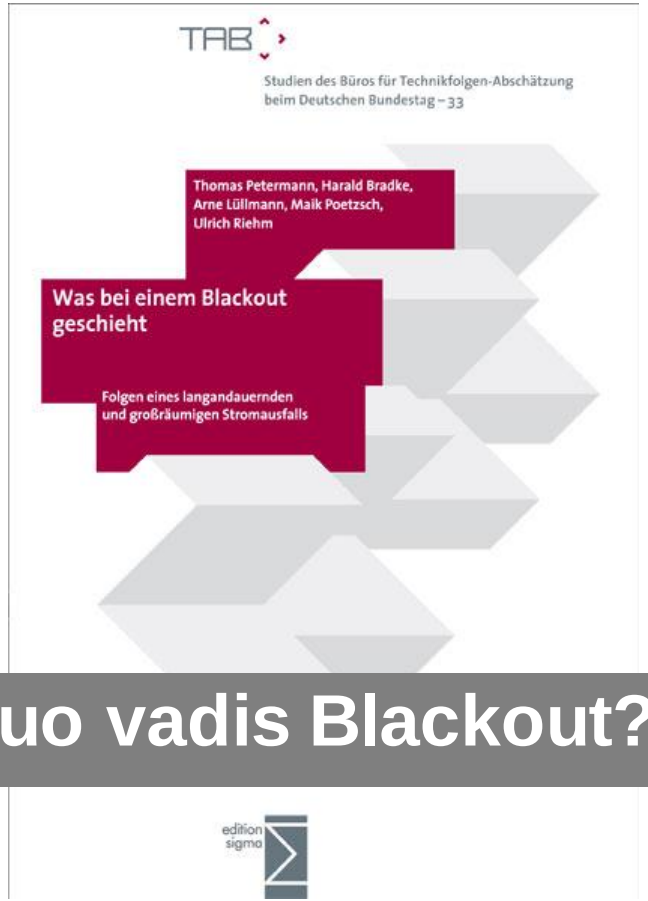
© HiSolutions 2023

Blackout

TAB: „Was bei einem Blackout geschieht“

Folgen eines langandauernden und großflächigen Stromausfalls

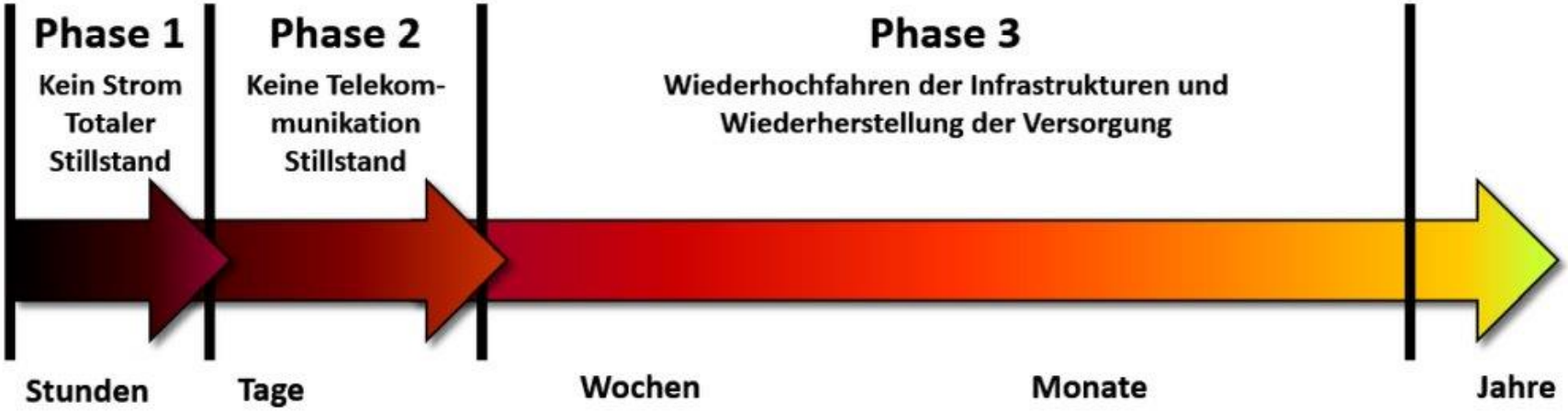
Blackout != Stromausfall



https://www.tab-beim-bundestag.de/news-2011-07-05-was-bei-einem-blackout-geschieht.php

© HiSolutions 2023

Die drei Phasen eines Blackouts



© HiSolutions 2023

Auswirkungen auf alle kritischen Infrastrukturen

- Gefängnisse, Katastrophenmanagement und Bevölkerungsschutz, Rettungsdienste
- Transport und Verkehr: Straße, Schiene, Wasserwege und Aviation
- Internet und Telekommunikationsdienste, Rechenzentren, Öffentliche Sicherheit, Digitaler Rundfunk, Radio und Medien/Presse
- Gesundheitswesen, Ernährung, Wasser und Abwasser
- Staat und Verwaltung
- Finanz- und Versicherungswesen

© HiSolutions 2023

Konsequenzen eines Blackouts

- Die flächendeckende Versorgung der Bevölkerung mit (lebens-)notwendigen Gütern und Dienstleistungen ist nach wenigen Tagen nicht mehr möglich
- Die öffentliche Sicherheit ist ernsthaft gefährdet, da der Staat Leben und Gesundheit seiner Bürger nicht mehr schützen kann
- Der Staat verliert das Vertrauen seiner Bürger
- Nach einigen Tagen ohne Strom sind bürgerkriegsähnliche Zustände zu erwarten

© HiSolutions 2023

Schwarzstart

© HiSolutions 2023

Schwarzstart-fähige Kraftwerke

Die Schlüsselrolle beim Wiederaufbau haben Kraftwerke mit sogenannten Schwarzstart-Eigenschaften

Anlagen, die

- aus eigener Kraft und
- ohne externe Stromversorgung

in Betrieb genommen werden können

Sie sind der Ausgangspunkt, von dem aus im Ernstfall die Versorgung wieder aufgebaut wird

© HiSolutions 2023

Herausforderungen beim Schwarzstart

1. Dezentraler Netzwiederaufbau dauert Zeit!

2. Kommt es beim Zusammenschluss der Inseln zu einer Fehlschaltung, fällt das gesamte System wieder aus!

3. Europaweit noch nie geübt oder real erlebt worden!

© HiSolutions 2023

Cybersecurity – Problem oder Lösung?

© HiSolutions 2023

Verknüpfung physischer und digitaler Systeme

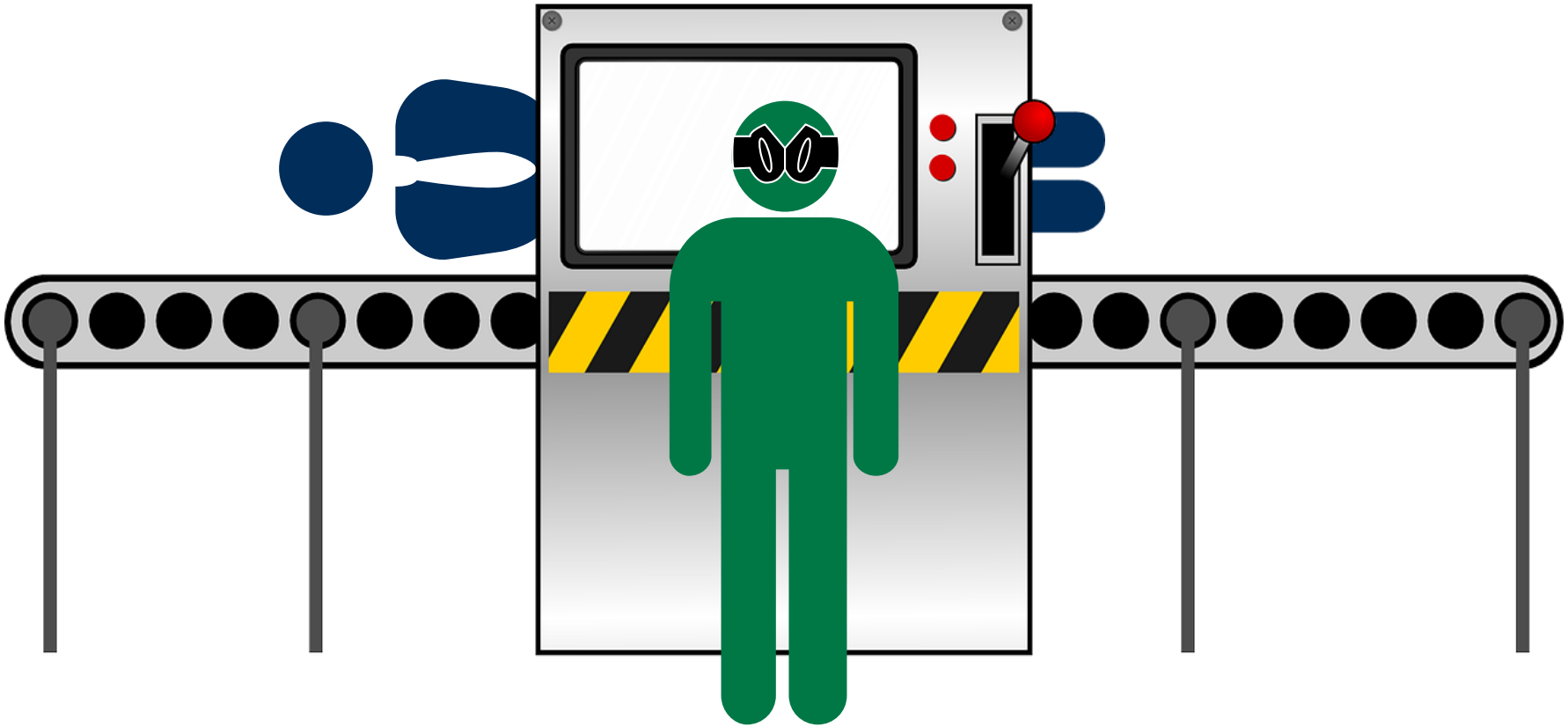
© HiSolutions 2023

> Safety schützt Menschen (und Umwelt) vor Maschinen,
> Security schützt Maschinen vor Menschen

Fluchs, S. 2020

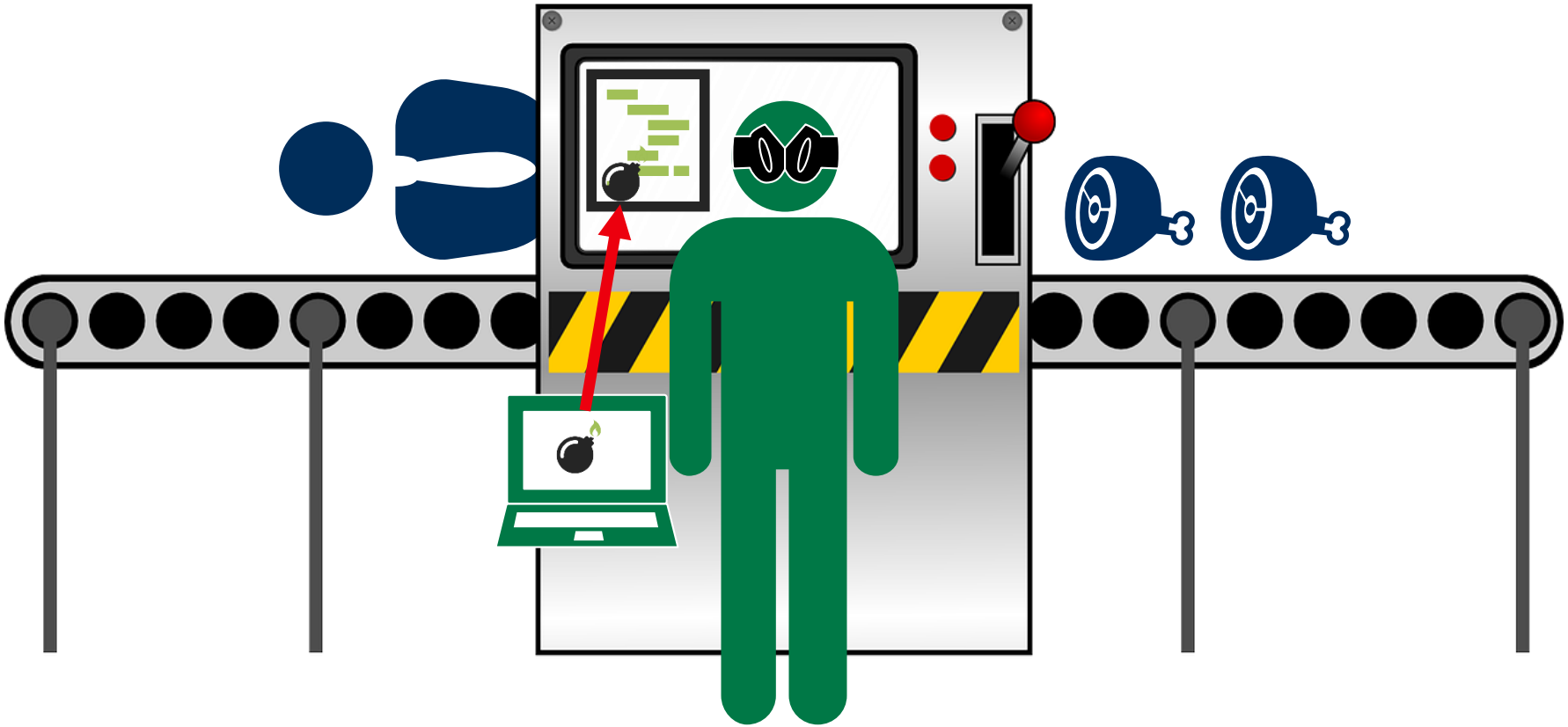
© HiSolutions 2023

Safety vs. Security – aus Sicht der Safety



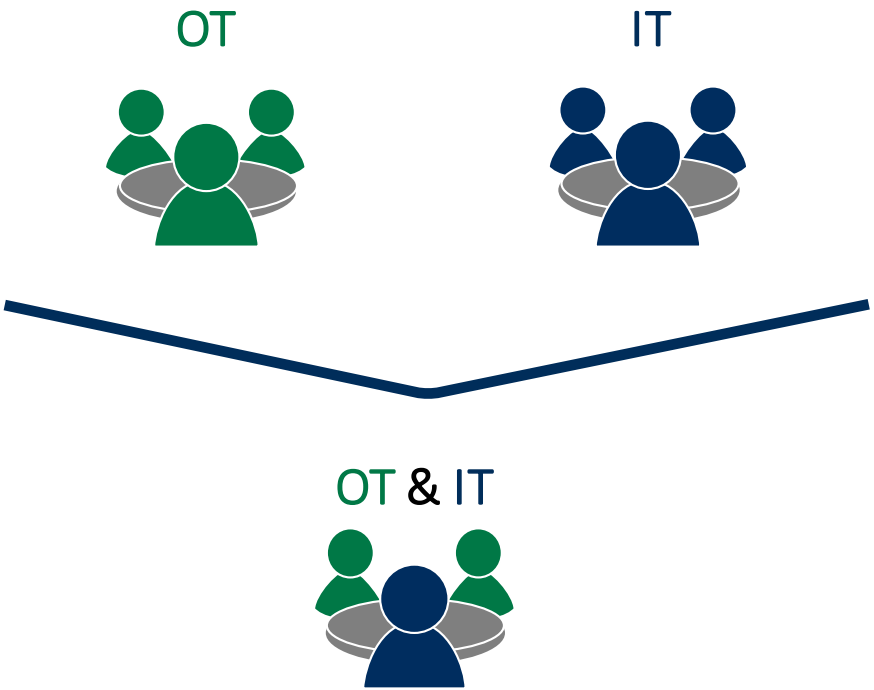
© HiSolutions 2023

Safety vs. Security – aus Sicht der Safety

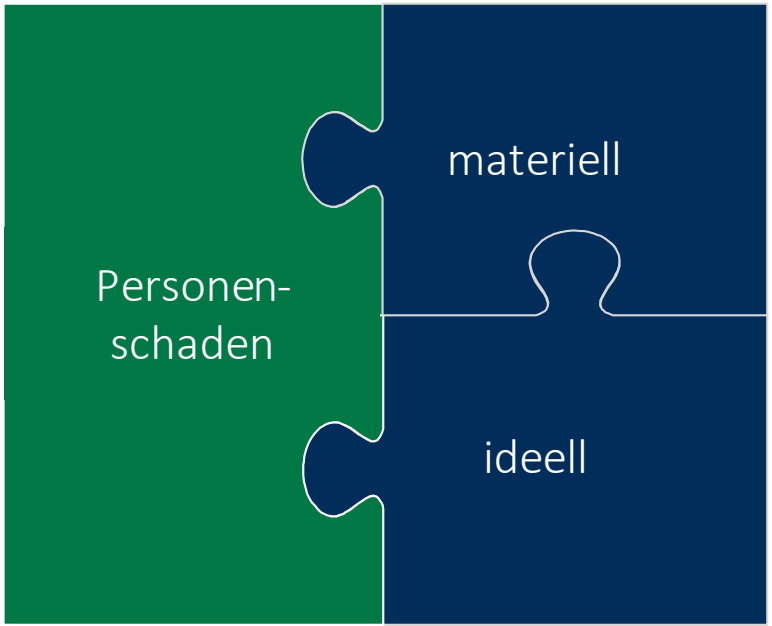


© HiSolutions 2023

Mix Safety & Security



Schutzziele



© HiSolutions 2023

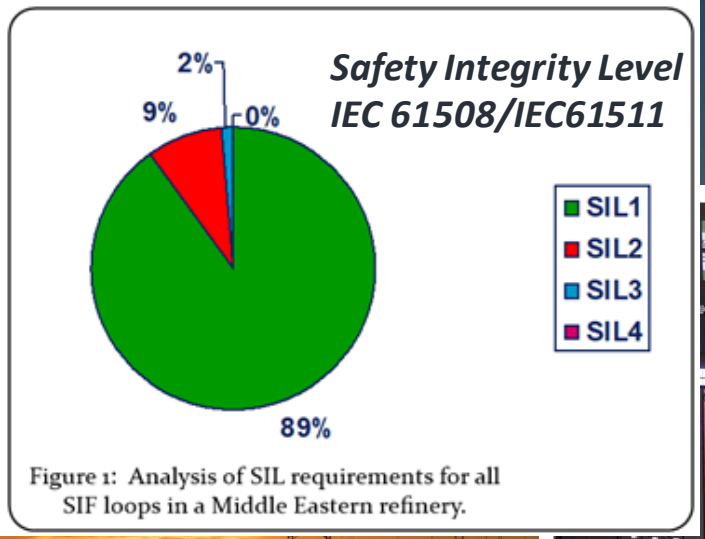


Figure 1: Analysis of SIL requirements for all SIF loops in a Middle Eastern refinery.


Triconex Tricon

Attacke auf Saudi-Arabisches Petrochemiewerk

- TRITON: passiver Implant mit Remote-Access-Funktion
- Folge wäre gewesen: Explosionen und die Freisetzung von Schwefelwasserstoffgas

Safety-PLC gemäß Safety Instrumented System (SIL3)
Firmware wurde im RAM gezielt manipuliert

© HiSolutions 2023

Cyberresilienz ➔ Widerstandsfähigkeit gegen Ereignisse

Die Ursache für eine Katastrophe ist derzeit für den Katastrophenschutz nicht relevant

→ ABER: Präventive und reaktive Maßnahmen aus einer spezifischen Fachrichtung (OT oder IT) können im anderen Bereich Schwachstellen bewirken

Kritische Frage:

→ Wurde bei der Digitalisierung nachhaltiges **Security by Design** & **Privacy by Design** berücksichtigt?

→Nur damit können wir die Cyberresilienz kritischer Infrastrukturen erhöhen!

© HiSolutions 2023

Gibt es Bedrohungen für KRITIS?

- Digitalisierung?
  …schreitet bei KRITIS (langsam & schlecht) voran
- Ransomware wird mehr!
- Fachkräftemangel wird mehr!
- Naturereignisse werden mehr!

- „Cyberwar-“, Geheimdienste- & Hackback-Szenarien bringen zukünftig mögliche Kollateralschäden

© HiSolutions 2023

Cyber-Verteidigung

(it‘s all about Cyber…)

Wie? Das ist doch quasi Magie… wie KI oder Blockchain…

Cyberresilienz! Zur Erhöhung der Widerstandsfähigkeit von KRITIS

** Fähigkeit eines Systems, Ereignissen zu widerstehen bzw. sich daran anzupassen und dabei seine Funktionsfähigkeit zu erhalten oder möglichst schnell wieder zu erlangen*

Warum? Angriffe verpuffen wirkungslos durch Basis-Maßnahmen

** Hallo, BSI Grundschutz*

© HiSolutions 2023

Make it so!

All-Gefahren-Ansatz

Berücksichtigung aller Gefahrenarten (z. B. Naturgefahren, technologische Gefahren, etc.) im Rahmen des Risiko- und Krisenmanagements.

Quelle: BBK

360°-Risikosicht erforderlich

Angriffe können von allen Seiten kommen

- Bei KRITIS verwendet man den All-Gefahren-Ansatz

Root-cause ermitteln

- Chain of small Problems → Epic Fail

Risiko im Vertrag auslagerbar, klar

- Verantwortung und Imageschaden aber nicht

Was bleibt übrig?

- Absichern & Handeln statt Abwarten & Hoffen

➢ **Security by Design & Privacy by Design für nachhaltige Digitalisierung**

© HiSolutions 2023

>> All-Gefahren-Ansatz <<

„Berücksichtigung aller Gefahrenarten (z. B. Naturgefahren, technologische Gefahren, etc.) im Rahmen des Risiko- und Krisenmanagements“

** Hallo BBK*

© HiSolutions 2023

Vielen Dank für Ihre Aufmerksamkeit!

Haben Sie noch offene Fragen zum Thema Blackout?

HISOLUTIONS

Schloßstraße 1 | 12163 Berlin

info@hisolutions.com | +49 30 533 289 0

www.hisolutions.com