

A black and white photograph of an industrial facility, likely a refinery or chemical plant. The image shows a complex network of large pipes, metal structures, and scaffolding. In the foreground, a large, dark, curved pipe dominates the left side. In the background, there are tall distillation columns and various smaller vessels. The overall scene is industrial and technical.

# DGKM & DGSMTech Digitale Woche

Manuel „HonkHase“ Atug

© HonkHaseSecurity 2022 | © HonkHase



# KRITIS und Digitalisierung

Manuel „HonkHase“ Atug

© IfT BlaBlaSecurity 2022 | © HonkHase

# Manuel (HonkHase) Atug

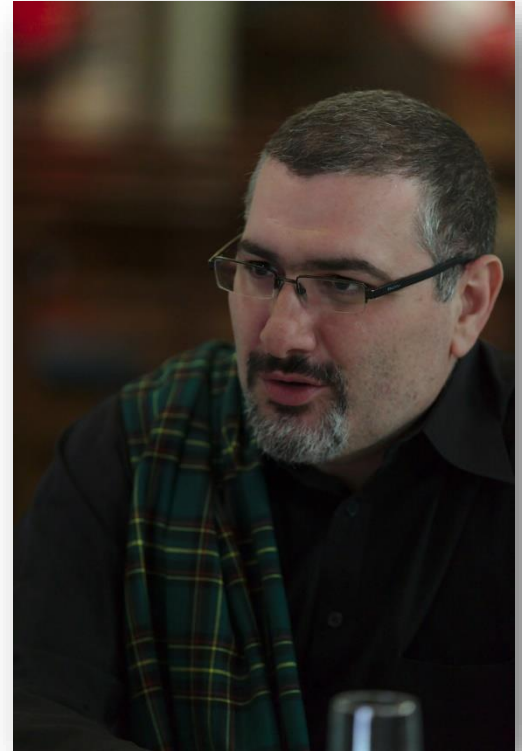
Head of Business Development bei der HiSolutions AG

- Diplom-Informatiker, Master of Science in Applied IT Security, Ingenieur
- Weit über 23 Jahren in der Informationssicherheit tätig
- Sachverständiger für das IT-SiG 2.0 im Bundestag
- Themen: KRITIS, Hackback, Ethik, Hybrid Warfare, Cyberresilienz, Bevölkerungs- und Katastrophenschutz
- Mitgründer der AG KRITIS: [ag.kritis.info](https://ag.kritis.info)
- Mitgründer der AGND: [www.agnd.eu](https://www.agnd.eu)

 [@HonkHase](https://twitter.com/HonkHase)  [@HonkHase@chaos.social](https://mastodon.social/@HonkHase)



Ich habe #KRITIS im Endstadium



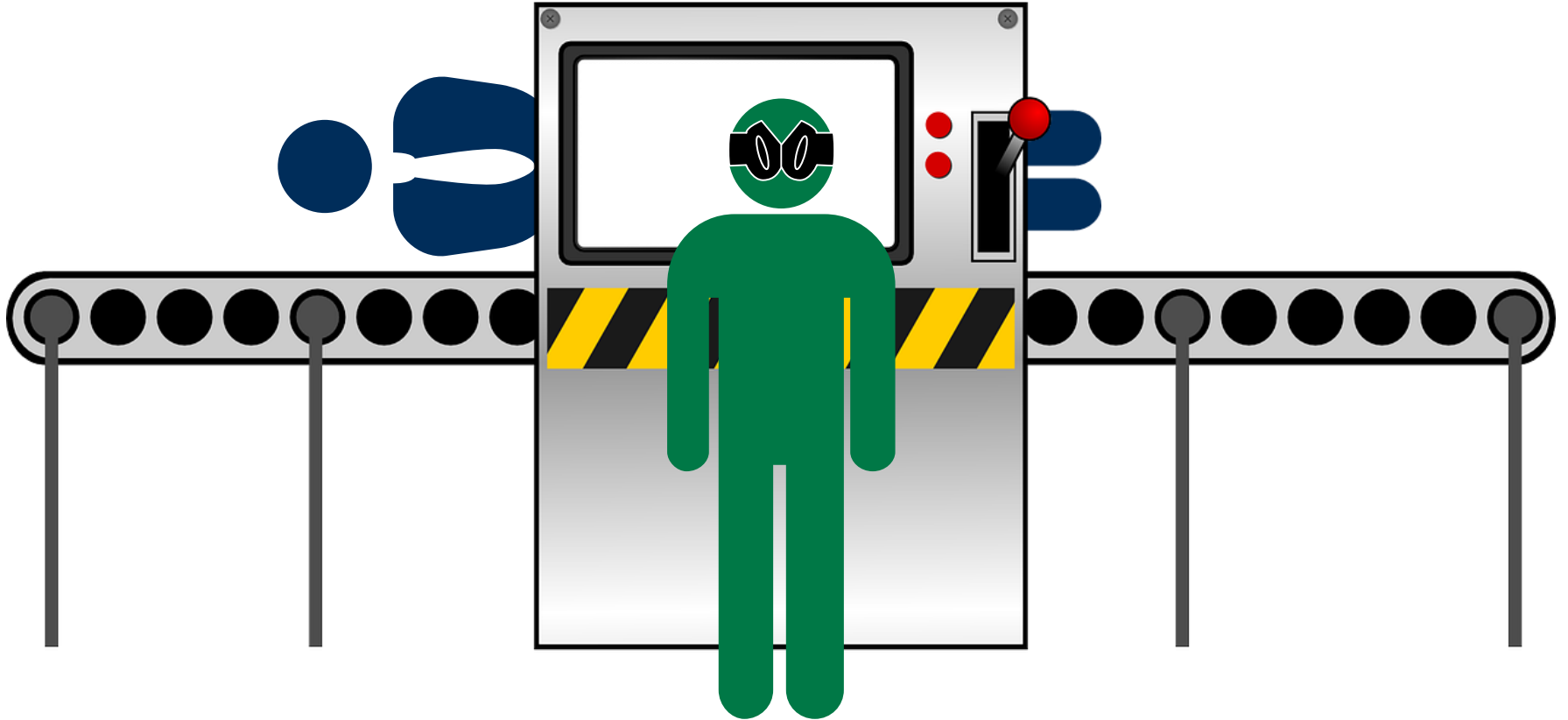
# Verknüpfung physischer und digitaler Systeme



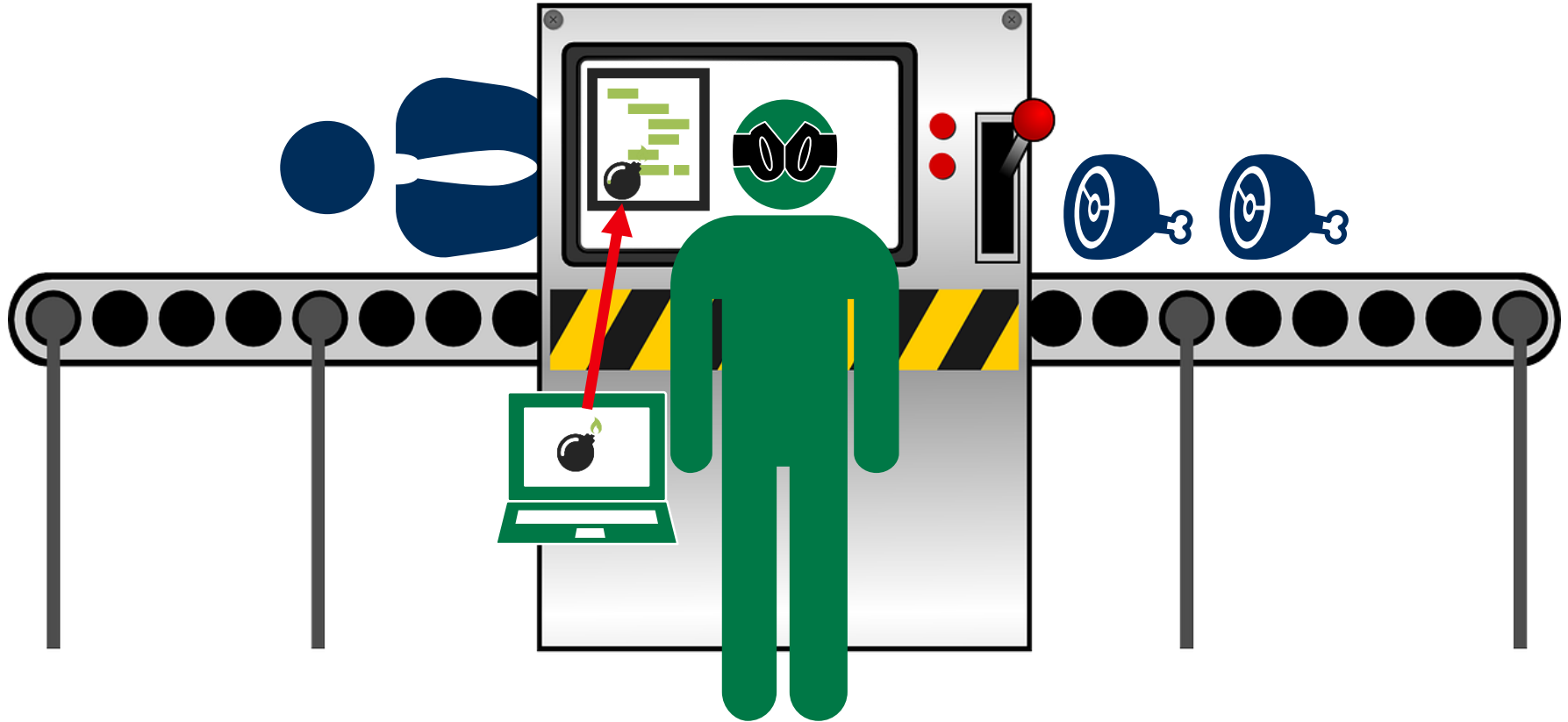
” Safety schützt Menschen (und Umwelt) vor Maschinen,  
Security schützt Maschinen vor Menschen

Fluchs, S. 2020

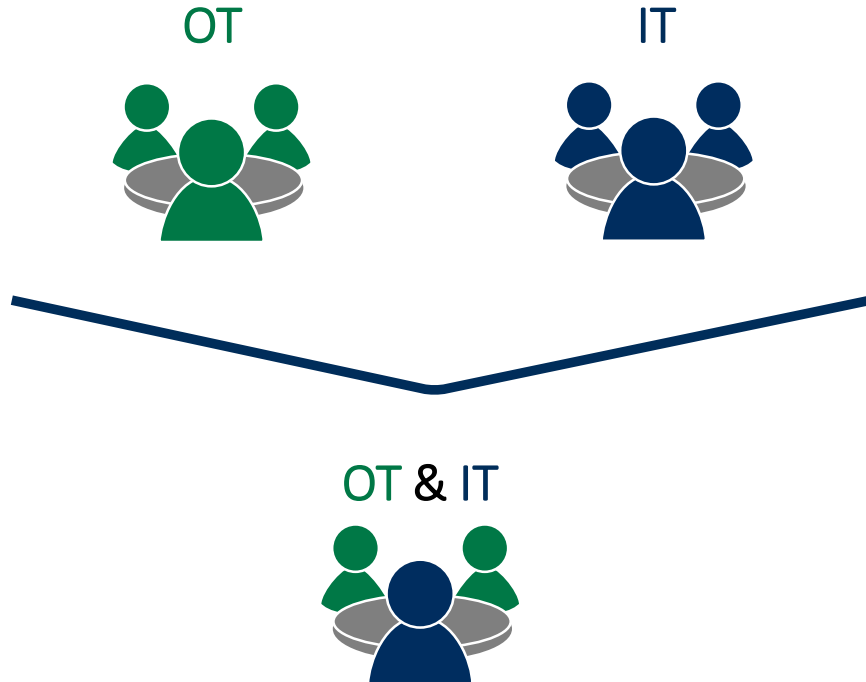
## Safety vs Security - aus Sicht der Safety



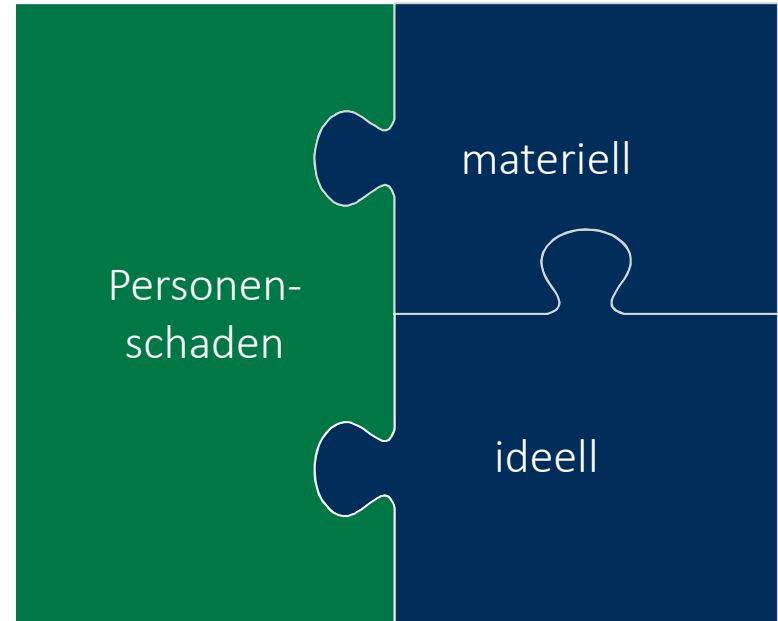
# Safety vs Security - aus Sicht der Security



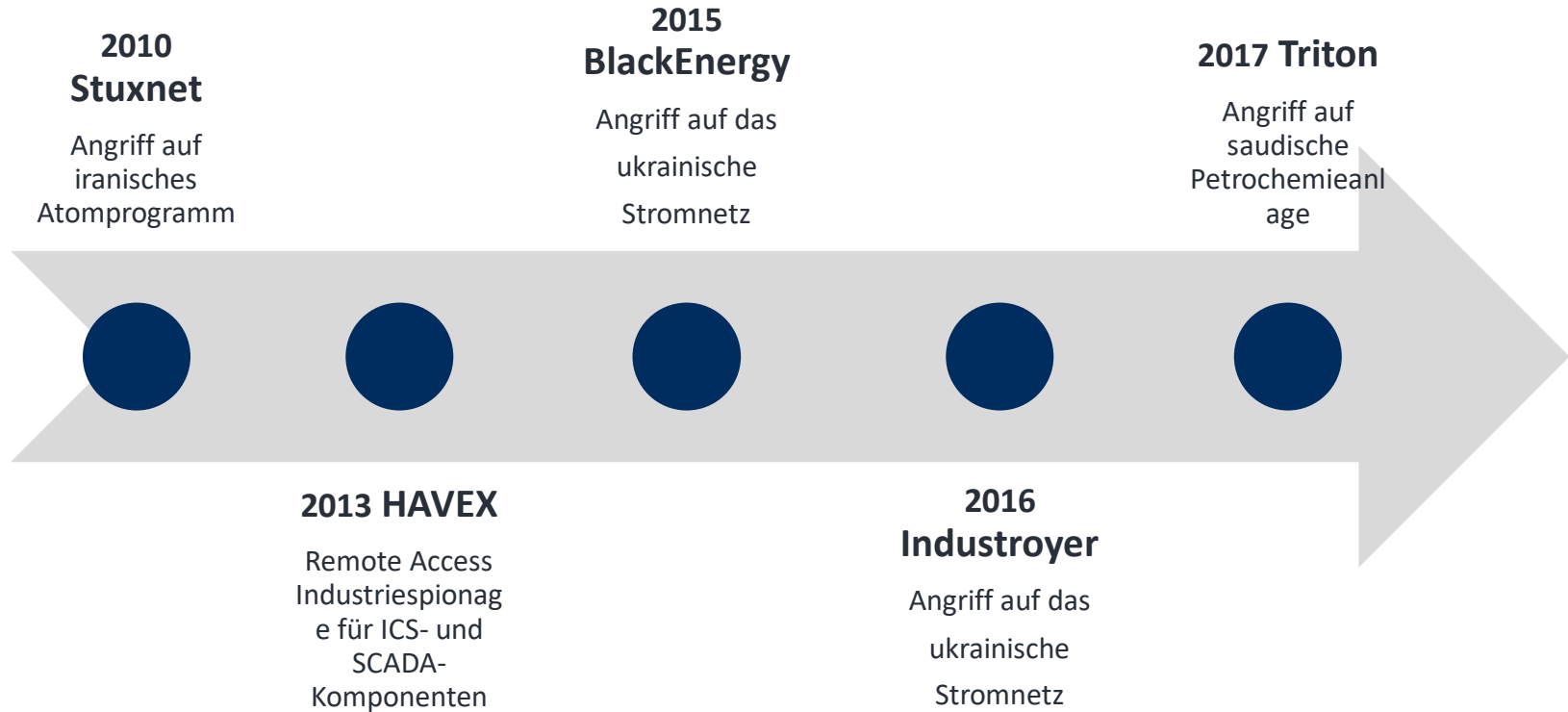
## Mix Safety & Security



## Schutzziele



# Timeline der wesentlichen ICS Angriffe



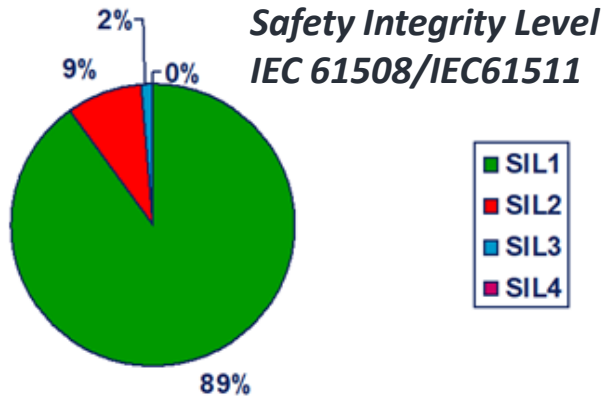


Figure 1: Analysis of SIL requirements for all SIF loops in a Middle Eastern refinery.



Triconex Tricon

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

## Attacke auf Saudi Arabisches Petrochemiewerk

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

# Wie sehen denn Cyber-typische Vorfälle aus?

- i.d.R. eher nicht langanhaltend, sondern temporär
- Wirtschaftliches Interesse (zB Ransomware)
- Spionage und Aufklärung
- Fake News und Propaganda
- Umfassende Kollateralschäden möglich, aber in der Risikoanalyse nicht kalkulierbar



# Mehr Bedrohungen für Produktionsumgebungen?

- Digitalisierung schreitet bei Produktionsautomatisierung (langsam & schlecht) voran
- Ransomware wird mehr!
- Fachkräftemangel wird mehr!
- Naturkatastrophen werden mehr!
- Cyberwar-, Geheimdienste- & Hackback Szenarien bringen zukünftig mögliche Kollateralschäden



# Cyberresilienz → Widerstandsfähigkeit gegen Ereignisse

- Ursache für Katastrophe oder Cybervorfall ist für die Bevölkerung nicht relevant
- Aber: eine Krise (Pandemie) in der Krise (Putins Angriffskrieg) in der Krise (Ransomware) in der Krise (Gasmangellage) in der **<beliebige Krise hier einfügen>** braucht keiner!
- Kritische Fragen:
  - Ist Digitalisierung immer erforderlich?
  - Können wir damit die Cyberresilienz im KRITIS Sektor Staat und Verwaltung erhöhen?
  - Was ist eine gute Digitalisierung?

# Nachhaltigkeit in der Digitalisierung

- Bei der **digitalen Transformationen** verantwortungsvolle Maßnahmen einzuleiten und gewissenhaft durchzuführen, also zu operationalisieren, ist daher gleichsam eine **technische** wie **ethische Aufgabe!**
- Vermeidet daher **technische Schulden** an **kommende Generationen**
- Hinter jedem **Datensatz** steht ein **Mensch**
- **Security by Design** und **Privacy by Design** ist **Menschenschutz**

## >> All-Gefahren-Ansatz <<

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

*\* Hallo BBK*

Und was mache ich, wenn alles nichts hilft?



# Irgendwas mit Holz?

# Kokosnusspflücker!

[www.kokosnusspfluecker.de](http://www.kokosnusspfluecker.de)

