InfraTech 2022

Manuel ‚HonkHase' Atug

Auswirkungen der Digitalisierung auf Produktionsumgebungen

Manuel ‚HonkHase' Atug

© Soft BlaBlaSecurity 2022 | @HonkHase

Manuel (HonkHase) Atug

Ich habe #KRITIS im Endstadium

Head of Business Development bei der HiSolutions AG

- Diplom-Informatiker, Master of Science in Applied IT Security, Ingenieur
- > 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

AG KRITIS

- Mitgründer der AGND: www.agnd.eu

AGND

@HonkHase

©left BlaBlaSecurity 2022 | @HonkHase

Verknüpfung physischer und digitaler Systeme

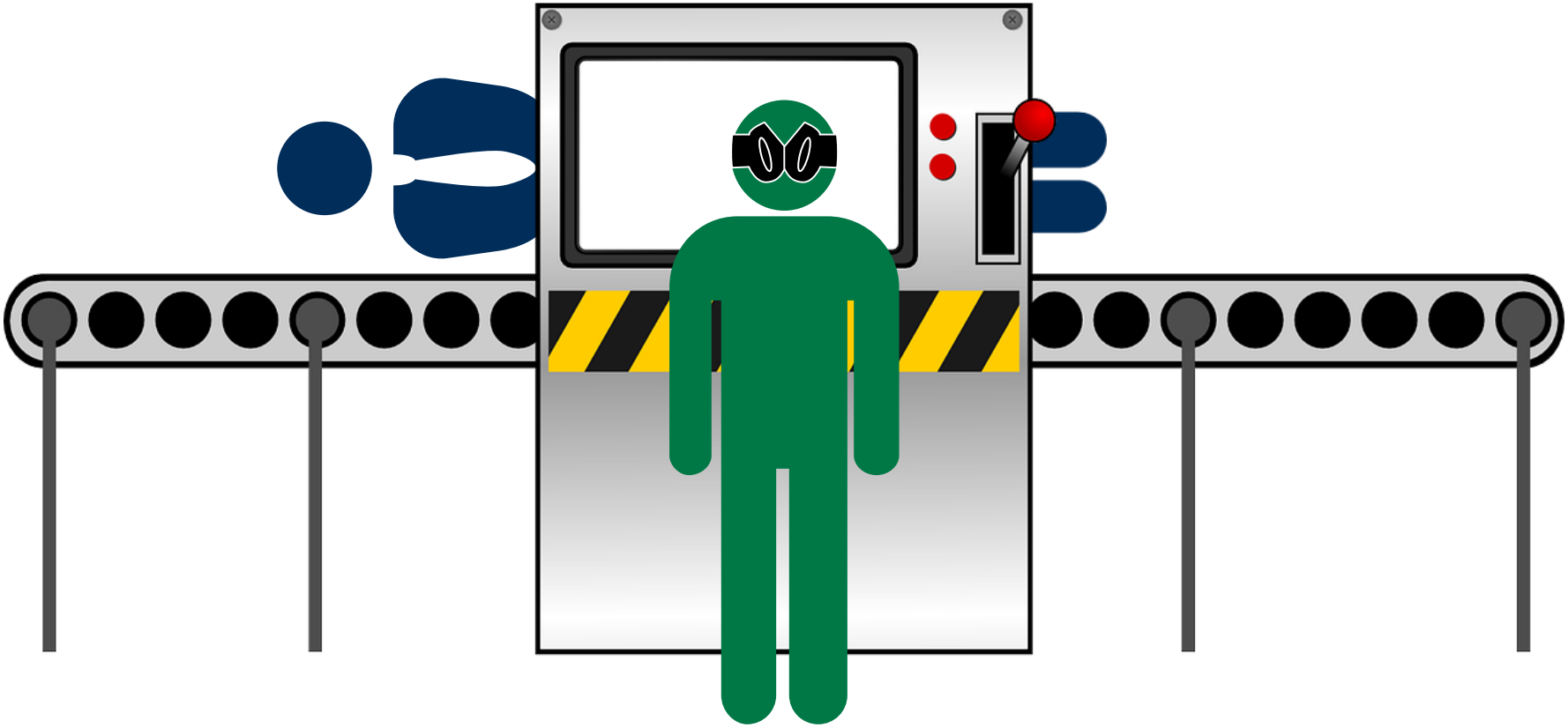
©left BlaBlaSecurity 2022 | @HonkHase

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

Fluchs, S. 2020

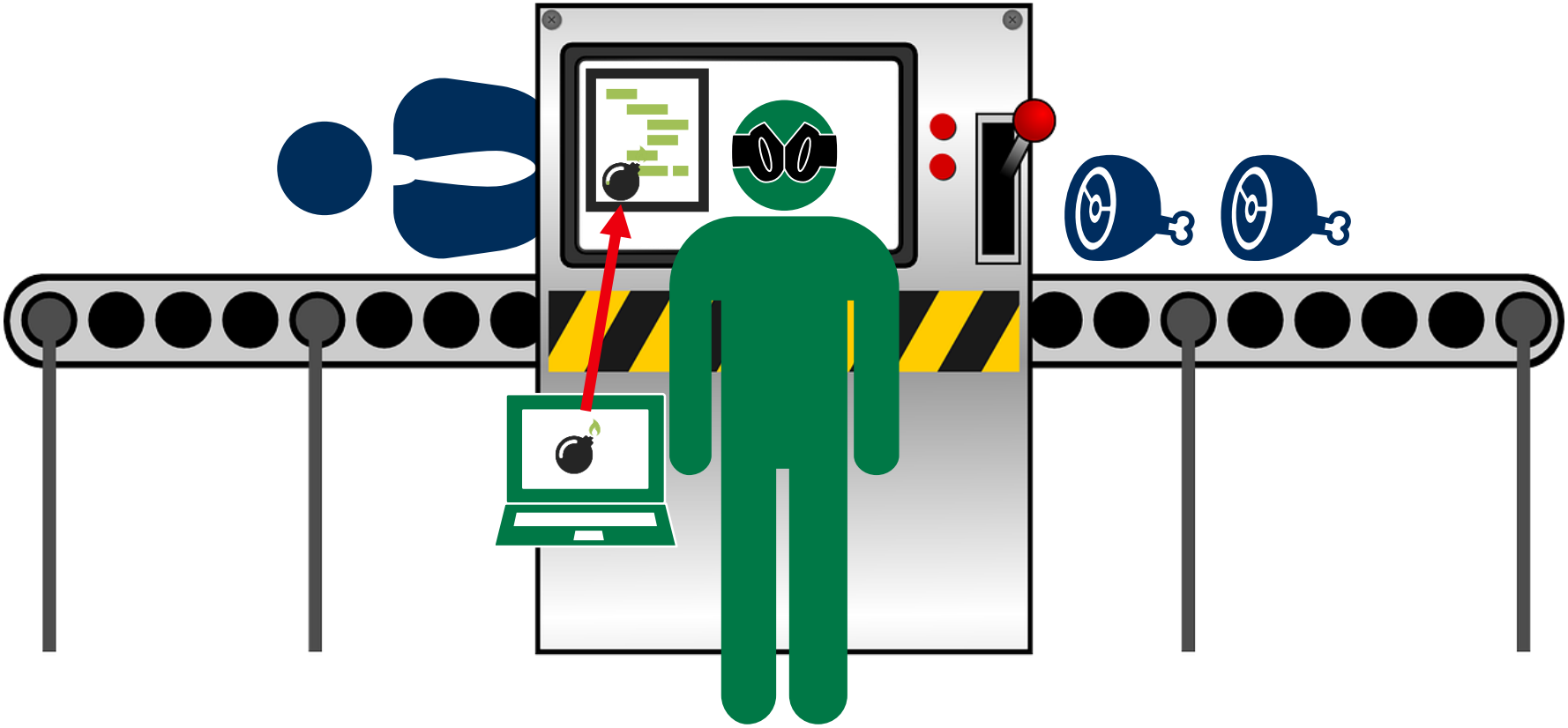
©left BlaBlaSecurity 2022 | @HonkHase

Safety vs Security - aus Sicht der Safety



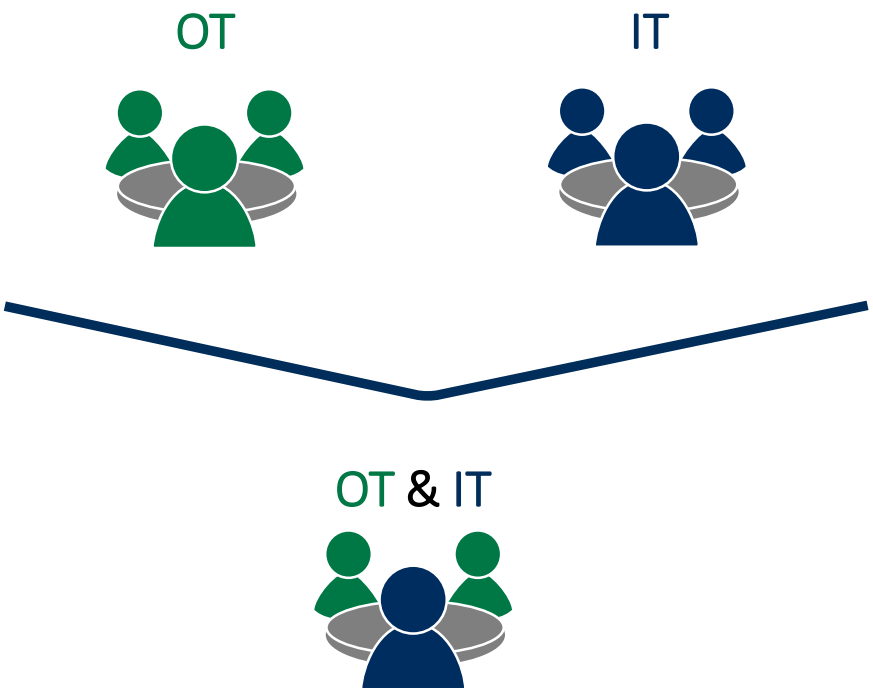
©left BlaBlaSecurity 2022 | @HonkHase

Safety vs Security - aus Sicht der Security

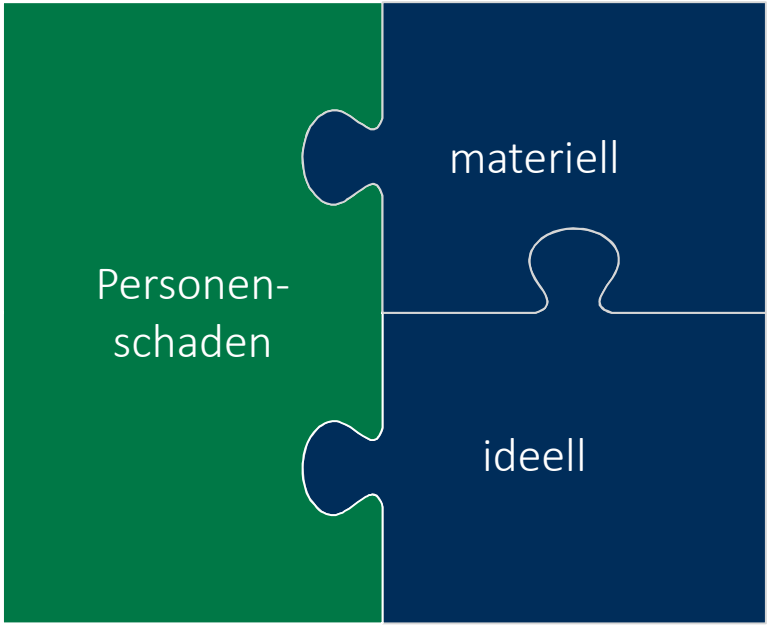


©left BlaBlaSecurity 2022 | @HonkHase

Mix Safety & Security



Schutzziele



©left BlaBlaSecurity 2022 | @HonkHase

Timeline der wesentlichen ICS Angriffe

2010
Stuxnet

Angriff auf iranisches Atomprogramm

2013 HAVEX

Remote Access Industriespionage für ICS- und SCADA-Komponenten

2015
BlackEnergy

Angriff auf das ukrainische Stromnetz

2016
Industroyer

Angriff auf das ukrainische Stromnetz

2017 Triton

Angriff auf saudische Petrochemieanlage

©left BlaBlaSecurity 2022 | @HonkHase

Attacke auf Saudi Arabisches Petrochemiewerk

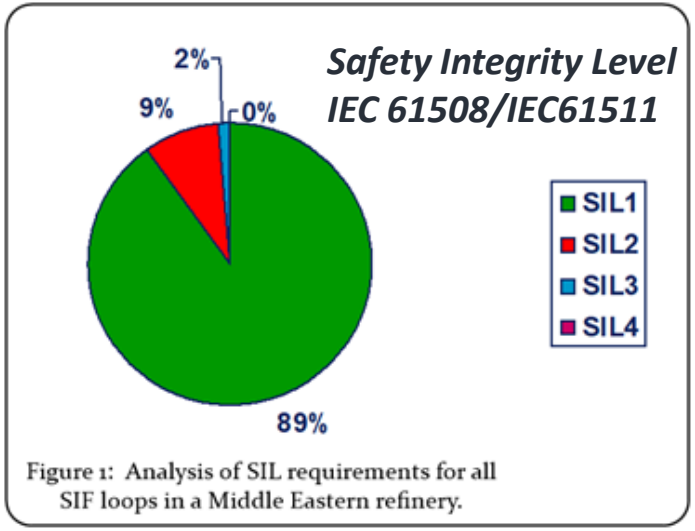


Figure 1: Analysis of SIL requirements for all SIF loops in a Middle Eastern refinery.

Triconex Tricon

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

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

©left BlaBlaSecurity 2022 | @HonkHase

Wie sehen denn Cyber-typische Vorfälle aus?

- i.d.R. eher nicht langanhaltend, sondern temporär
- Wirtschaftliches Interesse
- Spionage und Aufklärung
- Fake News und Propaganda

- Umfassende Kollateralschäden möglich, aber in der Risikoanalyse nicht kalkulierbar

©left BlaBlaSecurity 2022 | @HonkHase

Mehr Bedrohungen für Produktionsumgebungen?

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

©left BlaBlaSecurity 2022 | @HonkHase

Cyberresilienz & Ausblick

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

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

- Kritische Frage:

  → Ist Digitalisierung in solchen Bereichen immer erforderlich?

  → Können wir damit die Cyberresilienz von Produktionsumgebungen (zB in kritischen Infrastrukturen) erhöhen?

©left BlaBlaSecurity 2022 | @HonkHase

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!

- Vermeiden sie daher technische Schulden an kommende Generationen

- Security by Design und Privacy by Design ist Menschenschutz

©left BlaBlaSecurity 2022 | @HonkHase

Und was mache ich, wenn alles nichts hilft?

©left BlaBlaSecurity 2022 | @HonkHase

Irgendwas mit Holz?

Kokosnusspflücker!

www.kokosnusspflücker.de

©left BlaBlaSecurity 2022 | @HonkHase