www.AVQ.cc

AVQ GmbH

Safety und Security

Trennendes und Verbindendes

Vortrag Safety & Security 2019

02.07.2019

Safetyberatung

ISO 26262, IEC 61508, Maschinenrichtlinien, 93/42/EWG

MIL STD 882E
Luftfahrt
Raumfahrt
Marine

Sicherheitshandbuch
Sicherheitslebenszyklus
Unterstützende Prozesse

Arbeitssicherheit
SOTIF, Automatisierung

©Copyright 2015, Alle Rechte vorbehalten.

Definitionen

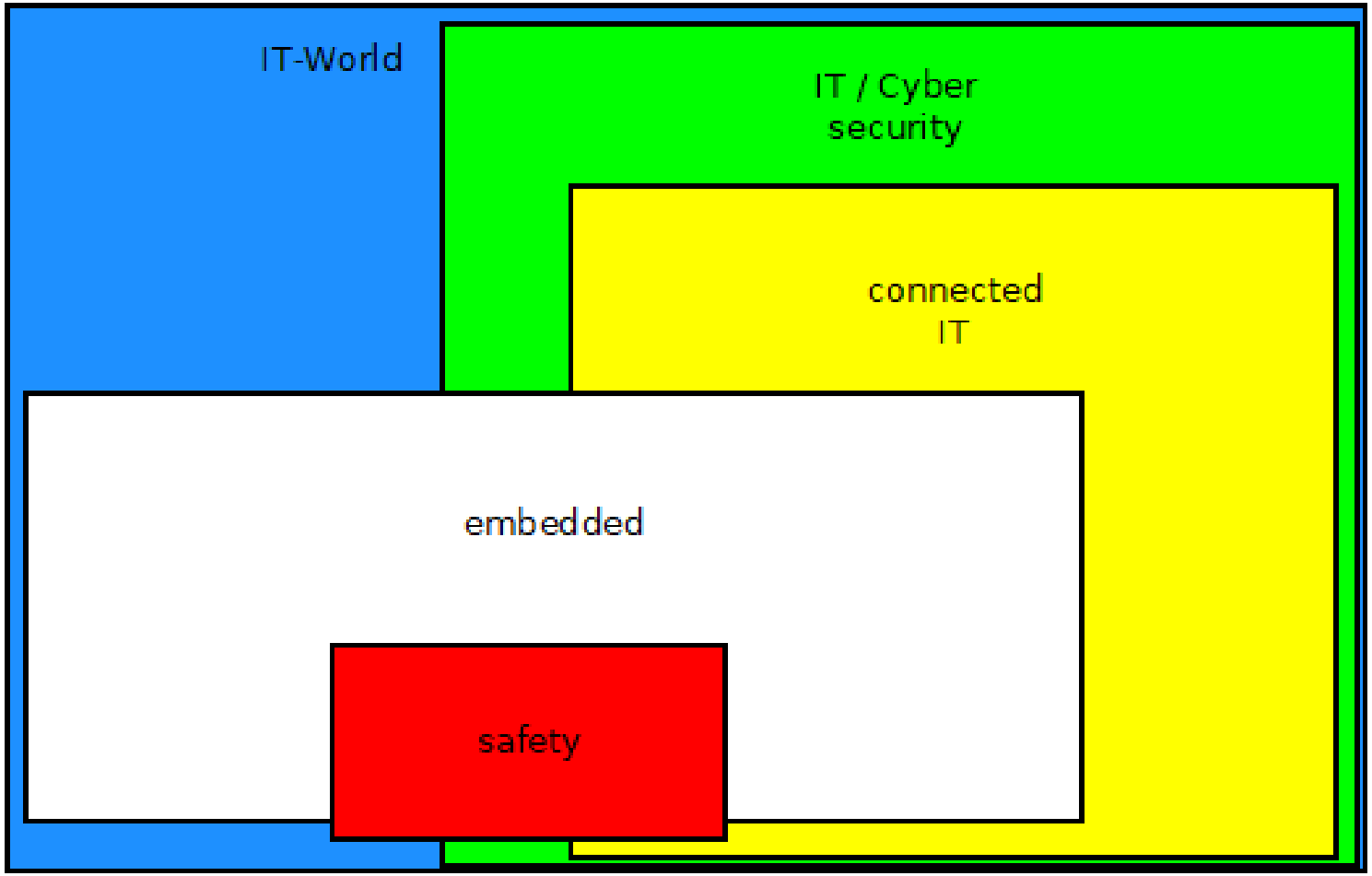
Safety (IEC 61508)
freedom from unacceptable risk
risk
combination of the probability of occurrence of harm and the severity of that harm
harm
physical injury or damage to the health of people or damage to property or the environment

Security (ISO 17799)
information security
preservation of confidentiality, integrity and availability of information; in addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved
risk
combination of the probability of an event and its consequence (ISO/IEC Guide 73:2002])

Security is freedom from, or resilience against, potential harm (or other unwanted coercive change) caused by others. (Wikipedia)

©Copyright 2015, Alle Rechte vorbehalten.

Anwendungsrahmen



©Copyright 2015, Alle Rechte vorbehalten.

Severity / Definition of harm

Safety

physische Verletzungen / Tod von Menschen

(keine psychischen Verletzungen)

Security

unerlaubte

- Dateneinsicht / Veröffentlichung
- Datenveränderung / Vandalismus
- Datenklau / Änderung der Zugriffsrechte /Erpressung
- Herstellung von verändertem Verhalten von Systemen

durch Dritte

©Copyright 2015, Alle Rechte vorbehalten.

Risikoklassen – keine 100%ige Sicherheit

Safety

Risikoklassen durch SIL 1-4 (IEC61508) definiert
“Average frequency of a dangerous failure of the safety function 1E-9 1/h“
Akzeptiertes Grenzrisiko definiert durch Minimale Endogene Mortalität.
MEM ist ein Maß für das akzeptierte (unvermeidliche) Risiko, durch die betreffende Technologie zu Tode zu kommen.
Der SIL ist zugeordnet einer Funktionsabsicherung

Security

Risiko wird bestimmt durch:
Organisation
Target of Evaluation
Attackvektor

Kein quantitatives Maß an Security.

©Copyright 2015, Alle Rechte vorbehalten.

Aufwandsbegrenzung – keine 100%ige Sicherheit

Safety

Der Stand der Technik zum Zeitpunkt des Inverkehrbringens (Anforderungen der Norm) muss erreicht sein.

Mehr ist freiwillig.

ALARP:

„As low as reasonable practical“

Security

Der mögliche Gegner und seine Fähigkeiten werden selten modelliert: Scriptkiddi, erfahrener Hacker oder NSA?
Motivation + Zeit + Ressourcen bilden den Rahmen der äußeren Bedrohung.

Übliche Regel:
„Gelegenheit macht Diebe“
Keine Gelegenheiten zulassen!

(Bild Torwalds)

©Copyright 2015, Alle Rechte vorbehalten.

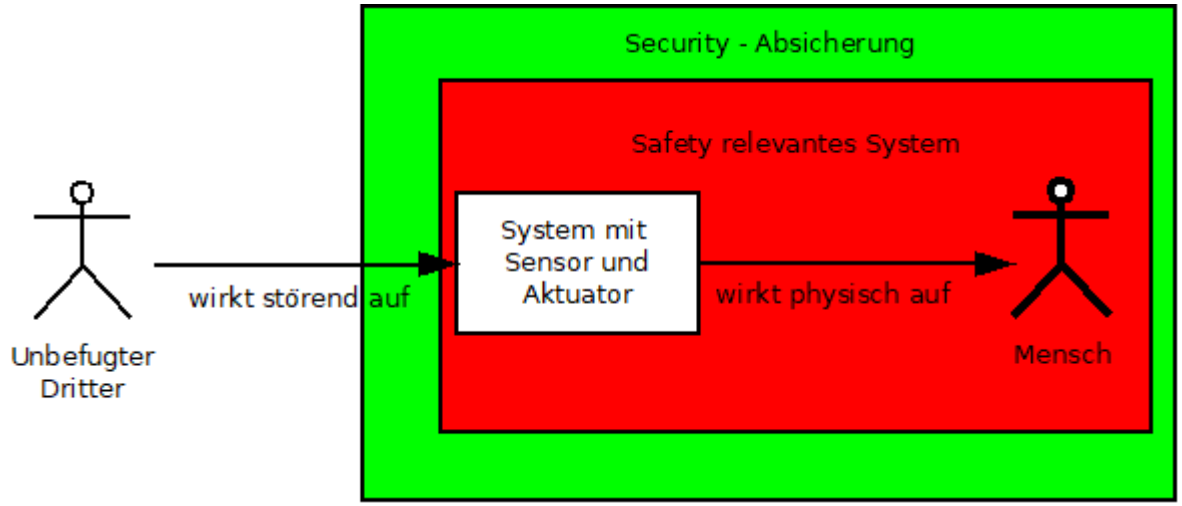
Architektur (sofern vorhanden)

Safety

befasst sich mit den „inneren Werten“ des Systems.
Der gefährdete Mensch ist Bestandteil der Analysen.

Security

befasst sich mit den äußeren Schnittstellen des Systems.
Der Gefährder ist außerhalb des Betrachtungsrahmen des Systems.



©Copyright 2015, Alle Rechte vorbehalten.

Massnahmen zur Mitigation

Safety

Variabilität **einschränkend**.

Nichts Unnötiges, da es Gefahren bringen kann.
Klarheit schaffen, um systematische Fehler zu vermeiden.
Anteil von Safety-Funktionen ca. 5% vom Code.

Security

Variabilität (teilw.) **vergrößernd**.
z.B. Lange Passwörter, 2 Faktor Anmeldung
Viele Möglichkeiten definieren, um Wahrscheinlichkeit für frühen Einstieg zu verringern.
Aber auch:
Reduktion der Variabilität, um Übersicht über Einfalltore zu schaffen.

©Copyright 2015, Alle Rechte vorbehalten.

Wenn es schiefgeht?

Safety
Safety Incidence, zu melden.
Staatsanwalt ermittelt oder Hersteller des Produkts prüft selbst Vorfall auf Designschwäche.
Produkt bekommt Sperre, Rückruf und ggf. Überarbeitung.

Täter:
Bei nachgewiesener grober Fahrlässigkeit droht dem Hersteller Gefängnis.

Security
Schadensentdeckung ggf. zunächst nötig.
Umfangreiche IT-Aufräumaktionen folgen. Patching.

Täter:
Urheber (ungefugter Dritter) meistens nicht greifbar.
System-Hersteller bzw. Dienstleister werden ggf. mit Haftung konfrontiert.

©Copyright 2015, Alle Rechte vorbehalten.

Verbindung in Assessments

Wenn „Security Incident“ passiert ist…
Ist das Prodikt immer noch safe, wenn nachweisbar nicht mehr secure?

Automotive:
ISO 26262 Edition 2 fordert im Safety Case ein Statement zur Cybersecurity.

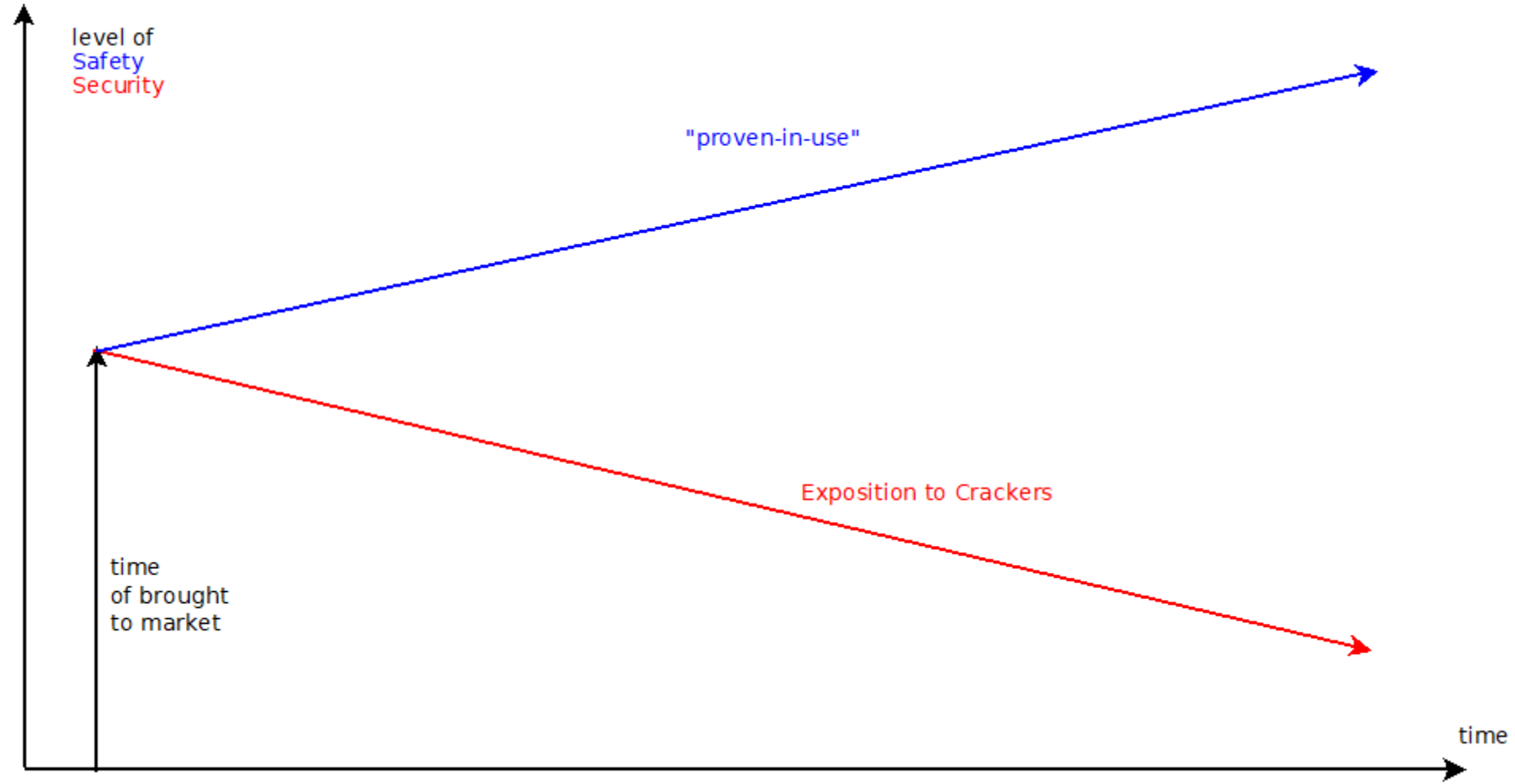
Luftfahrt:
FAA, EASA etc. entscheiden. Bislang gibt es keine verbindliche Regelungen.

Andere Branchen…?
Rechtslage?
Bislang unklar.

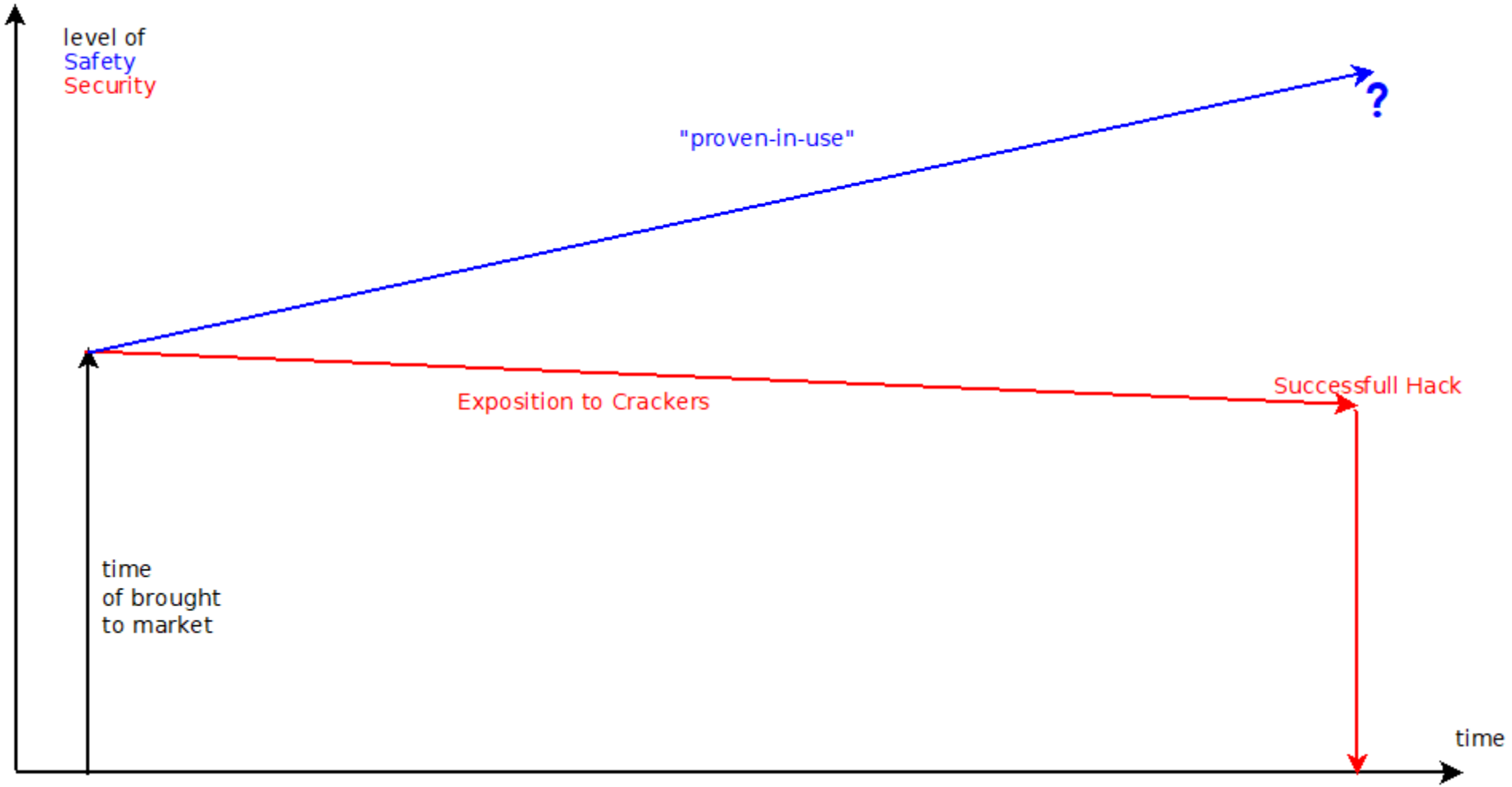
©Copyright 2015, Alle Rechte vorbehalten.

Safety & Security
Trennendes und Verbindendes

A … Assurance
V … Veritas
Q … Quality



©Copyright 2015, Alle Rechte vorbehalten.



©Copyright 2015, Alle Rechte vorbehalten.

Empfehlungen

Soweit wie möglich trennen.

Keine verbindenden Assessments,
keine abhängigen Anforderungen.

Trennung im Produkt durch Architektur

- Security außen,
- Safety innen,
- Getrennt durch kontrollierten Airgap.

Vielleicht hilfreich:
https://www.nist.gov/publications/considerations-managing-internet-things-iot-cybersecurity-and-privacy-risks

©Copyright 2015, Alle Rechte vorbehalten.

Danke für Ihre Aufmerksamkeit!

Bahnhofstrasse 37
D 82152 Planegg bei München
Tel +49 89 203570 62
Fax +49 89 203570 63
E-Mail: info@AVQ.cc
Web: www.AVQ.cc

©Copyright 2015, Alle Rechte vorbehalten.