

Keine Safety ohne Security:

Funktionale Sicherheit und Cybersicherheit in softwareintensiven Systemen

Alexander Much

Über mich

Zeitschiene:

- 1995-2004: Mathematik & Informatik in Erlangen und Cambridge (UK)
- 2000-2003: SuSE Linux
- 2003-2025: Elektrobit Automotive GmbH
Director, Head of quality, functional safety, cybersecurity and software compliance
- 2025: Safionyx GmbH & Co KG, Founder

Qualifizierungen:

- Principal Automotive SPICE assessor
- ECQA certified automotive quality manager
- ECQA certified functional safety manager
- EuroSPI certified cybersecurity manager
- OpenChain (ISO/IEC 5230)



Aktuelle Gremien:

- VDA Automotive SYS conference
- EuroSPI conference
- Intacs working group cybersecurity
- Soqrates working group
- Intacs working group AI

Wer war diese Frau?



Bridget Driscoll (1851 – 17 August 1896)

Bridget Driscoll wurde bekannt als sie den Bordstein am 17. August 1896 verließ und in die Geschichtsbücher eintrat.

Eine 44 jährige Hausfrau, die von Old Town, Croydon auf eine Volkstanzschau im Crystal Palace ging war die **erste Fußgängerin in UK, die von einem Auto getötet wurde.**

Sie wurde von einem Vorfühswagen erfaßt, der mit ca. 6 km/h unterwegs war. Sie war nach wenigen Minuten tot.

Der Rechtsmediziner meinte damals er hoffe, "dass eine solche Sache nie mehr passieren würde". **Er war der erste, der das Wort "accident" für durch Geschwindigkeit verursachte Gewalt benutzt.**

Im Deutschen? **Unfall!** Quasi etwas das nicht vorkommt.

Zeugen meinten, dass der Fahrer Arthur Edsel mit einer **"waghalsigen Geschwindigkeit"** unterwegs war, so "wie eine Feuerwehr".

Zur Verteidigung meinte Mr. Edsel, dass er seine Hupe betätigt hätte.

Der Jury haben damals 6 Stunden gereicht um zum Ergebnis zu kommen sie wäre eines **"accidental death"** gestorben.

https://en.wikipedia.org/wiki/Death_of_Bridget_Driscoll

Wo kommt die funktionale Sicherheit her?

Vorher: Brandschutz, berufliche Bestimmungen z.B. in Gilden, Lagerungsvorschriften (Schießpulver!), usw.

Dann: sich (schnell) bewegende Dinge, aktivere Dinge, gar explosive Sachen

USA: Waggonkopplungsunfälle Eisenbahn¹

- Zwischen 1888 und 1894 (6 Jahre!!): ca. **16.000 tote Arbeiter** und ca. **170.000 verkrüppelt**.
- Die Manager meinten: "Dies sind Fehler der Arbeiter und ihrer Sorglosigkeit".
"Wir können nichts machen als ihnen zu raten sorgsamer zu sein".
- 1893: Safety Appliance Act (US Congress).
- Juni 1896 (nach 3 Jahren!!): automatisches Koppeln, noch nicht komplett ausgerollt.
-> **Todesrate bereits um 35% reduziert**.

Deutschland²:

- Dampfmaschinen
- Explodierende oder zerknallende Dampfkessel
- Januar 1865: Explosion in der Mannheimer Aktienbrauerei -> Ruf nach regelmäßiger Kontrolle.
- 6. Januar 1866: 20 **badische** Kesselbesitzer gründen in Mannheim die "*Gesellschaft zur Ueberwachung und Versicherung von Dampfkesseln*". Der erst dieser Art in Deutschland.
- Vorläufer des heutigen "TÜV".

¹ Hammer, Willie. 1980. Product Safety Management and Engineering. Englewood Cliffs, NJ: Prentice-Hall.

² <https://de.wikipedia.org/wiki/T%C3%9CV>

Was ist “funktionale Sicherheit”?

O tempora o mores!

„Das Ziel der funktionalen Sicherheit ist die Freiheit von **unvertretbaren Risiken** einer physischen Verletzung oder einer Schädigung der Gesundheit von Menschen, entweder direkt oder indirekt (durch Schädigung von Sachwerten oder der Umwelt).“¹

Schon die Definition ist umstritten, je nach Standard und Branche unterschiedlich und ändert sich im Verlauf der Zeit.

Die Frage der Sicherheit ist eine Frage des gesellschaftlichen Konsenses in der jeweiligen Zeit.

¹https://de.wikipedia.org/wiki/Funktionale_Sicherheit

Normen, Normen, Normen:

- Es gibt allgemeine Normen, solche für Luftfahrt, Medizin, Bahn, Automobil, etc.
- Normen gibt es deren viele (... und ich muss die kennen)

Urteile, Urteile, Urteile:

- Z.B. [BGH](#), Urteil vom 16.06.2009 - VI ZR 107/08, “BMW Airbag Urteil”².
- Toyota versus Bookout

Regularien, Gesetze, usw.

Stichwort: “Stand der Technik und Wissenschaft”.

²<https://openjur.de/u/72232.html>

Funktionale Sicherheit versus Cybersicherheit



Funktionale Sicherheit:

Schütze den Menschen vor der Maschine.



Cybersicherheit:

Schütze die Maschine vor den Menschen.

Warum steht Wasser in der Toilette?

Problem: Faulgase in Rohren / Räumen.

Ergebnis: Brände in Häusern.



Rauchmelder

Pflicht!

Deutschland:

- Schleswig-Holstein, Hamburg, Mecklen-Vorpommern ab Mitte der 2000er
- Nachzügler: NRW, Bayern, Berlin und Baden-Württemberg: zwischen 2013 und 2020
- Sachsen: letzter Termin 31.12.2023

Eigentlich unglaublich!

Vergleich: England, USA, Japan. Jahrzehnte früher!



Mikrowelle

Hand aufs Herz:

Wer schaltet schon seine Mikrowelle vor dem Öffnen der Tür aus?

... wenn man die Tür einfach so aufmachen kann!

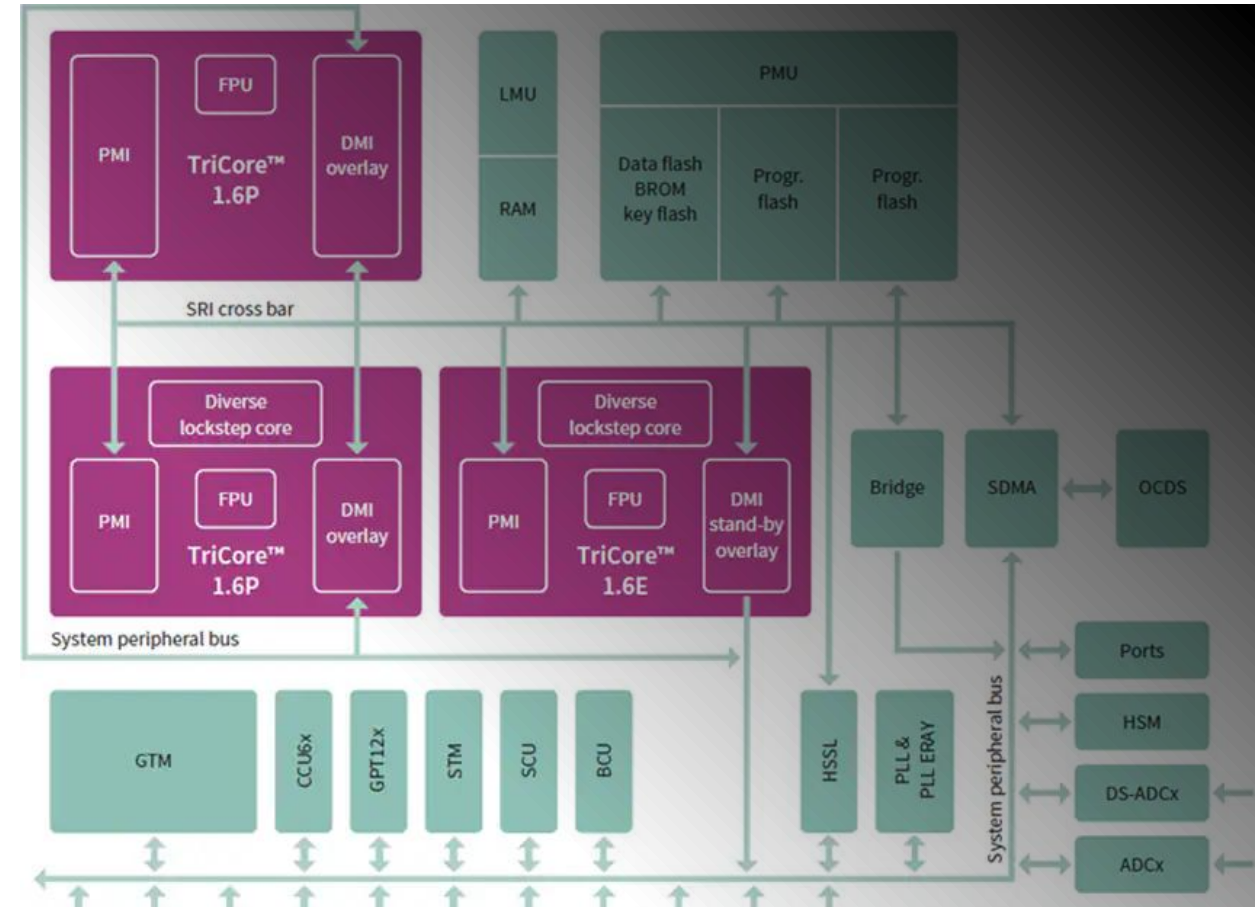


Mikrokontroller

Beispiel: Infineon Technologies Aurix TriCore-32-Bit Mikrokontroller



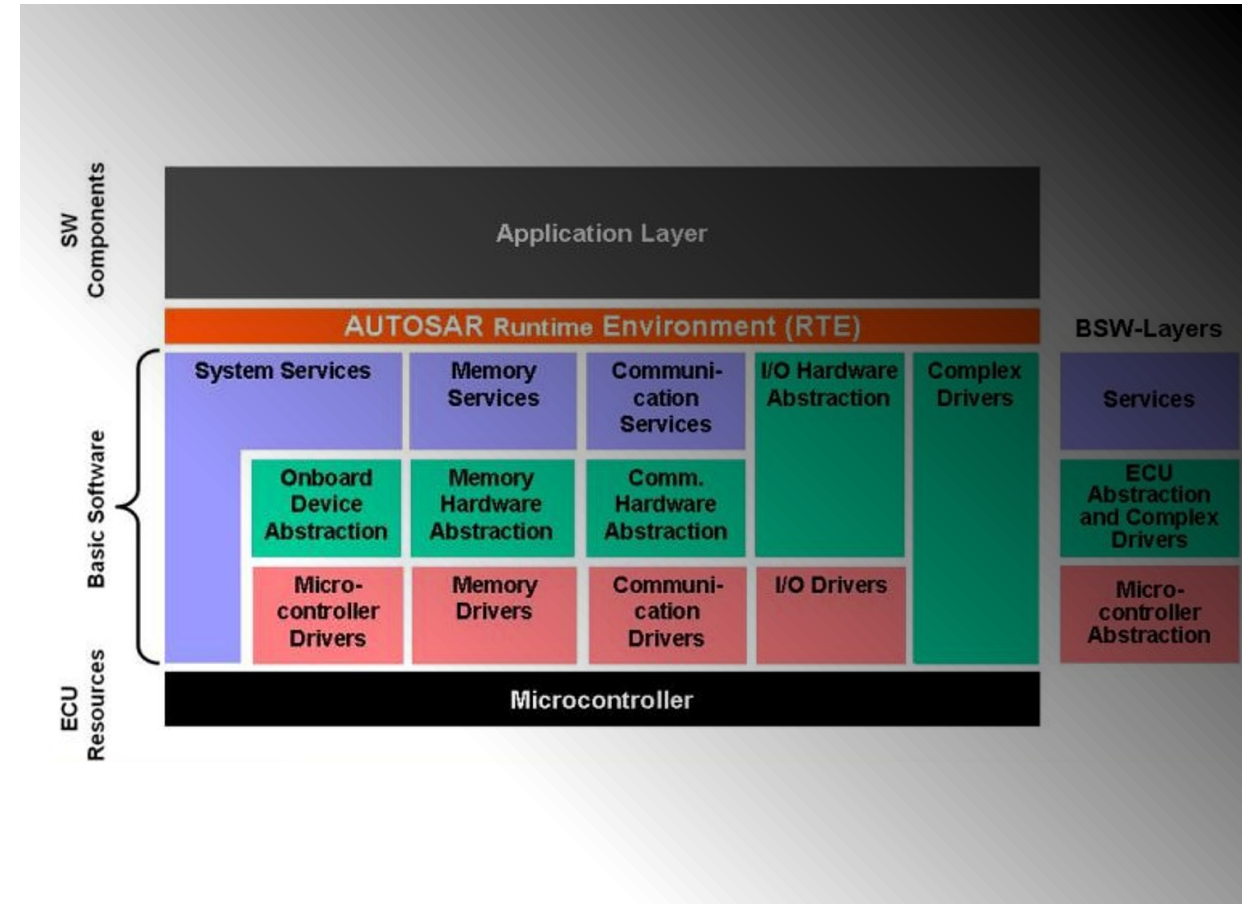
- Mikrowelle braucht einen Mikrokontroller
- Spaßfrage: Wie viele Mikrokontroller kommen auf einen Bürger? (wohl > 50, > 100?)
- **Keine Entscheidung dann mehr in Hardware!**
- **Bis auf die Integrität ist jede Entscheidung Software!**
- Auf einmal ist funktionale Sicherheit ein Softwarethema
- **Und damit kommt die Cybersicherheit ins Spiel!**



https://www.mouser.de/images/marketingid/2018/microsites/146796284/AURIX_BD.png

Beispiel: AUTOSAR Software-Architektur (Automobile)

- Wenige Hersteller schreiben heute ihr Betriebssystem, ihre Treiber oder die mittleren Schichten selbst.
- Der Hersteller konfiguriert die Software, schreibt die Anwendung und wird zum Systemintegrator.
- Aber: wie stellt man sicher, dass das auch richtig funktioniert?
- Funktionale Sicherheit basiert heute auf sehr viel Software.
- Und auf Zulieferketten, Audits, Zertifizierungen, Schulungen, effektive Organisationen, usw.



Beispiel: Systeme im Automobil

Anmerkung: (ASIL-)A == “etwas Safety nötig”, (ASIL-)D == “sehr viel Safety nötig”

- Automatic Distance Control – ADC [B/C]
- Electronic Stability Program – ESP [D]
- Adaptive Front Steering – AFS [D]
- Back wheel Steering [B]
- Electric Power Steering – EPS [D]
- Damper Control, Air Spring [B/C]
- Automatic Gearbox [C]
- (Horizontal) Torque Control [C/D]
- Clutch Control for 4WD [A/B]
- Combustion Engine Control [B/C]
- Electric Parking Brake – EPB [C]
- Automatic Light, „Automatisches Fahrlicht“ [B]
- Lane Departure Warning [A]
- Automatic Parking [B]
- Airbag [C/D]
- Anti Blocking System [C]
- Brake Assistant [B]
- Electronic Gas Pedal [C]
- Hybrid Drive, Electric Motor Drive [C/D]
- Night Vision [B/C]
- Headup Display [B/C]
- Dashboard (Speed, Gear, Warnings) [B/C]
- Rear Drive Camera [B]
- Window Lifter, Sunroof [A/B]
- Gateway [QM..D]
- Steering lock [D]

ASIL Level sind hier nur beispielhaft, kann in der Realität abweichen!



Gedankenspiel: Rolltreppe

Was kann schon schiefgehen?

Typische Szenarien:

- Einklemmen (beim Ein- oder Ausstieg, zwischen den Stufen, usw)?
Geringere Safety (eine Person, Notknopf)
- Sehr steile Rolltreppe in U-Bahn randvoll mit Menschen stoppt sehr abrupt?
Sehr viel Safety!!

Cybersicherheit und was wir machen

From Code to Compliance

Und wie kommt nun die Cybersecurity hinein?

- Funktionale Sicherheit ist im Wesentlichen physikalische Alterung und systematische Fehler
- Security: echte Akteure. Menschen sind kreativ!
- Andere Motivationen:
 - Geld (Bereicherung)
 - Rufschädigung
 - Diebstahl geistigen Eigentums
 - Kriegsführung
 - Etc.

Cybersicherheit >> Funktionale Sicherheit

Ohne Cybersicherheit keine funktionale Sicherheit!

Wie kommen wir als Safionyx ins Spiel?

- Audits (Principal Automotive SPICE Assessor)
- Qualitätsmanagement
- Management und Engineering von
 - Funktionaler Sicherheit (ISO 26262, IEC 61508)
 - Cybersicherheit (CRA, ISO 21434, ISO/PAS 5112)
- CSMS (Cybersicherheits-Managementsysteme)
- Open-source handling und Cybersecurity
- Aufbau effektiver Organisationen
- Trainings
- usw.

Erfahrung zählt! Mag die KI dazu sagen was sie will!

Vielen Dank!

Alexander Much – alexander.much@safionyx.com
+49 151 6843 2342
Safionyx GmbH & Co KG – <https://www.safionyx.com>
Hagsfelder Allee 19a
76131 Karlsruhe
Germany

