



## Sicherheit<sup>2</sup>

Das Zusammenspiel von Safety & Security im Fokus der Kryptoagilität

Karolin Varner & Wanja Zaeske  
<https://rosenpass.eu>

# Der Plan



1. **Wir stellen uns vor**
2. **Safety & Security: Kulturelle Aspekte**
3. **Kryptografie und Avionik im Dialog**
4. **Kryptoagilität als Prozess**



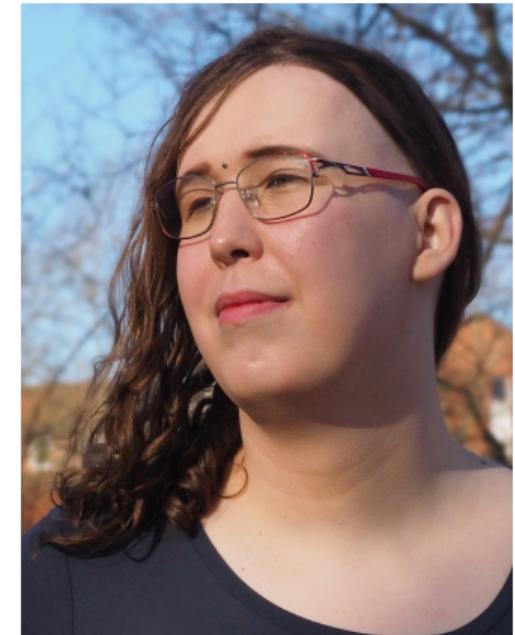
Zum mitschauen:

[github.com/rosenpass/slides/blob/main/ 2025-05-15-cast/slides.pdf](https://github.com/rosenpass/slides/blob/main/2025-05-15-cast/slides.pdf)

# Karolin Varner



- Softwareentwicklerin & Kryptografin
- 11 Jahre in der Industrie bei Startups und Konzernen
- Seit 2024 am Max Planck Institut für Sicherheit und Privatsphäre
- Initiatorin & Leiterin des Rosenpass Projekts
- Arbeit an weiteren Projekten wie zum Beispiel der X-Wing KEM



# Wanja Zaeske



# Rosenpass e.V.



- 2023 gegründet zur Betreuung des gleichnamigen Projekts
- Institution für Transaktionsforschung in der Kryptografie
- Schnittstelle zwischen Forschung, Industrie und Gesellschaft schaffen

[rosenpass.eu](http://rosenpass.eu)



# Safety & Security

---

Kulturelle Aspekte



# Safety & Security: Unterschiede

## Safety

- Zufällige Fehler
- Systemausfall kann tödlich sein
- Stabile Zieldefinition: Physik bleibt gleich
- TODO
- TODO

## Security

- Intelligente Angreifer
- Im Fehlerfall, lieber das System stoppen
- Zieldefinition ist in Bewegung: Angreifer lernen auch dazu
- TODO
- TODO

# Safety & Security: Gemeinsamkeiten

- Hohes Zuverlässigkeit nötig
- Analyse von Softwaresystemen in reeller Hardware
- Rigorose Validierungsprozesse
- TODO
- TODO

## Methodiken

- Sicherheit kann durch bewährte Praxis argumentiert werden, oft gilt „alt==Gold“
- Sicherheit kann nicht so argumentiert werden, der goldene Weg ist die formale Verifizierung
- => niemand behauptet, dass 3DES aufgrund seines Alters gut ist
- => aber auch neuartigen Algorithmen wird weniger vertraut...
- Sicherheit geht (oft) von zufälligem Versagen aus
- Sicherheit geht von gezielten Angriffen aus
- Sicherheit, die gegen entschlossene Angreifer gilt, gilt auch gegen zufälliges Versagen
- Redundanz funktioniert in beiden Bereichen

# Kryptografie und Avionik im Dialog

## Die Vier Domänen der Sicherheit sind...



**Luftfahrt**

**Automobile**

**Medizintechnik**

**Automatisierung**

Zum erschrecken aller...



...wird in der Luftfahrt heutzutage keine sichere Kryptografie eingesetzt.

## Zum erschrecken aller...



...wird in der Luftfahrt heutzutage keine sichere Kryptografie eingesetzt.

Der eine Ernstzunehmende Vorschlag den wir gefunden hatten – ein System zum kryptografischen absichern von LDACS – setzte auf post-quanten chiffren (SIKE), gegen die ein Jahr später Angriffe gefunden wurden.

TODO: Insert REFERENCE

## Ansätze für Verbesserung in beiden Bereichen



Verifikationstechniken

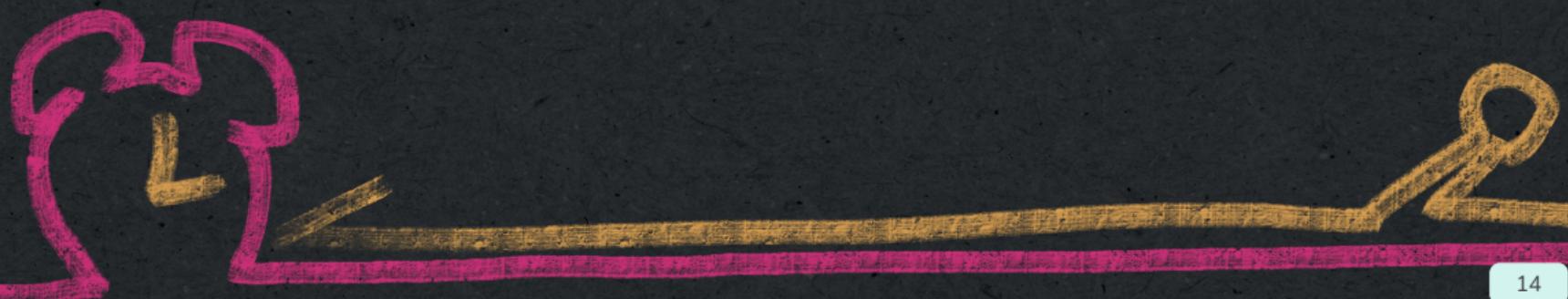
Zertifizierung <-> Sicherheitsbeweise

Kompartimentalisierung

Partitionierung <-> Brokerarchitekturen

=> Kryptoagilität

# Kryptoagilität als Prozess



# Modulare Systemdesigns

## Möglichkeiten:

- Rapider Komponentenaustausch
- Vereinfachtes Systemdesign
- Validierung einzelner Komponenten

## Herausforderungen:

- Abstraktionen sind häufig unvollständig
- Gute Modulgrenzen finden braucht Erfahrung
- Viele funktionelle & nicht-funktionelle Anforderungen
- Schlecht gewählte module bringen eine Illusion von Sicherheit
- Cargo Culting

## Ein agiler Lebenszyklus für Module

- Laufende, agile Modulentwicklung
- Enge Zusammenarbeit zwischen Modul- und Systemdesignern
- Einsatz besonders Erfahrener Ingenieure
- Breite, industrieübergreifende Zusammenarbeit hilfreich

# Korrekt von Anfang an

## Reaktiv vs Proaktiv

- Externe Validierung essenziell (Sicherheitsbeweise, Zertifizierung)
- Ansätze können kombiniert werden
- Proaktive Methoden sind in Safety und Security weit verbreitet

## Proaktives Vorgehen ist besonders schwer

- Avionik: Zertifizierung ist schwer
- Kryptografie: Formelle Beweise sind schwer
- Die Bürde der Verifikation erdrückt Innovation

## Schritte für den Anfang

- Investition in Lehrmaterialien, Handbücher, Nutzerfreundliche Verifikationssysteme
- Benutzbare Beweistools, Menschenfreundliche Zertifizierungsbehörden
- Innovation für bessere, effektivere Verifikation müssen gefördert werden
- Kontinuierliche Verifikation in Aktiver Zusammenarbeit zwischen allen Akteuren

## Konsequenzen & Chancen



- Sicherheit: Hochgradig formalisierte Prozesse
- Krypto: Strenge ethische, weniger formalisierte Prozesse
- => Shannons Prinzip
- => Verantwortungsvolle Offenlegung
- => Staatlich vorgeschriebene Berichterstattung über Schwachstellen
- => Es geht darum, eine Umgebung zu schaffen, in der man aus Fehlern lernen kann



# Kryptoagilität

---

Eine Definition



Fortschritt benötigt fortschrittliche Prozesse:

- Abkehr von der technokratischen Perspektive auf Agilität: Es geht um Prozessgestaltung und soziale Realitäten
- Kontinuierliche Bereitstellung: Sie sind nicht fertig, nur weil das Produkt geliefert wurde
- Fehler akzeptieren – Ein Argument für Bescheidenheit
- Planen Sie für Fehlerszenarien, um auf Fehlerszenarien einfach und professionell reagieren zu können
- Keine Schuldzuweisungen für bestmögliche Reaktionen auf Vorfälle
- Scham und Bestrafung für absichtliches Verschweigen von Problemen
- Aufbau einer Infrastruktur zur Unterstützung von Einsatzkräften – Serviceorientierung statt Schuldzuweisungen