



CAST-Workshop

2025-05-15



RosenPass

Sicherheit²

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**



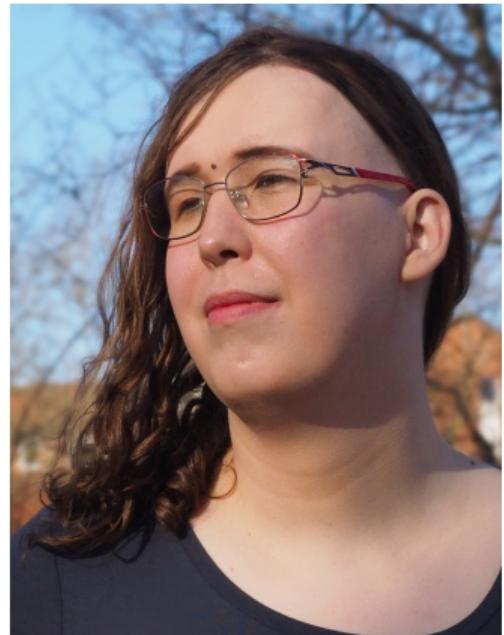
Zum Mitschauen:

[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



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



Wanja Zaeske



- Researcher & Software-Entwickler
- 4 Jahre Forschung im Deutsches Zentrum für Luft- und Raumfahrt (DLR)
- Schwerpunkte: Moderne Softwaretechnologien in die Avionik bringen
- Mitgründer von RoRosenpass

Rosenpass e.V.



- 2023 gegründet zur Betreuung des gleichnamigen Projekts
- Absicherung von WireGuard gegen Attacken durch Quantencomputer mittels Protokol-Level Hybridisierung
- Institution für Translationsforschung in der Kryptografie
- Schnittstelle zwischen Forschung, Industrie und Gesellschaft

rosenpass.eu



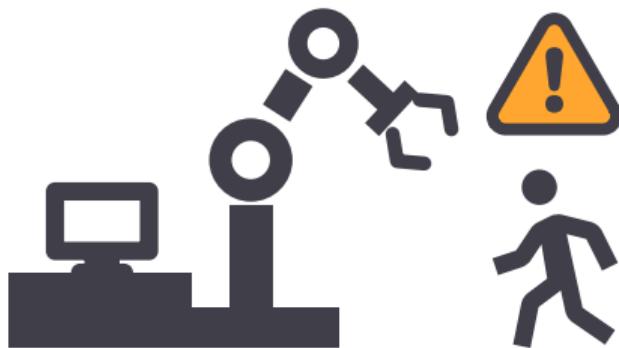
Safety & Security

Kulturelle Aspekte



Safety & Security in Computersystemen

Mensch in Gefahr



Safety

Daten in Gefahr



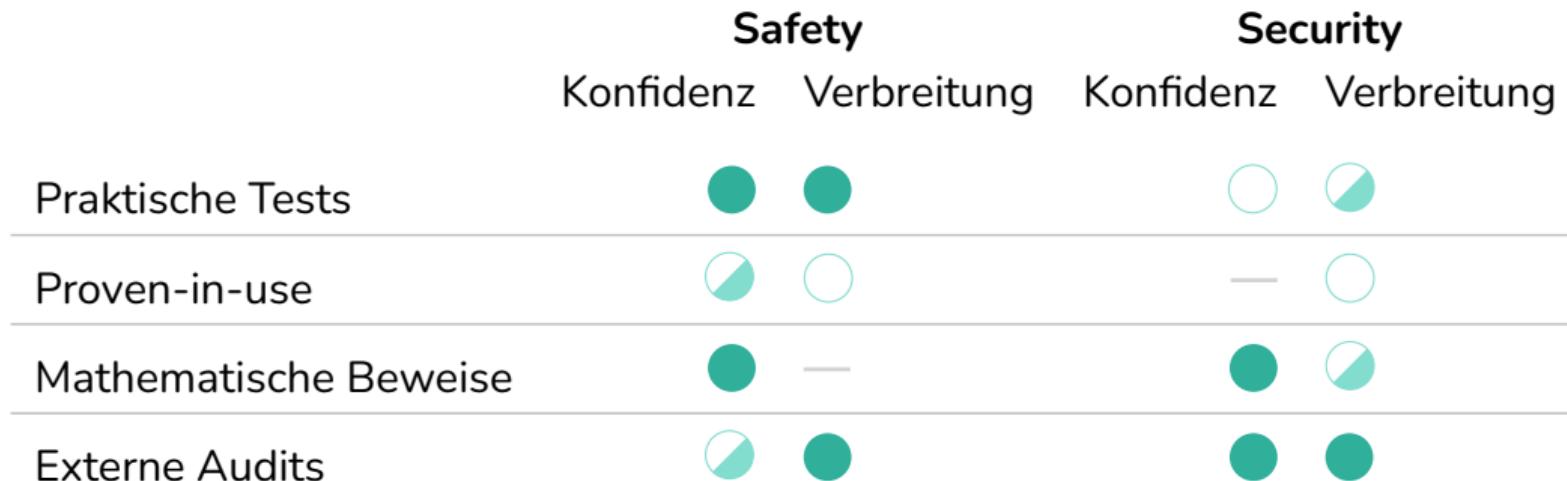
Security



Problemstellungen & Rahmenbedingungen

	Safety	Security
Fehlerauftreten	Zufällig	Gezielt (durch Angreifer)
Fehlerbehandlung	Weiterbetrieb notwendig	System stoppen
Zieldefinition	Stabil (Physik bleibt gleich)	In Bewegung (Angreifer lernen)
Abgehängene Software	Stabil!	Unsicher?
Validierungsprozess	Normiert	Dynamisch

Vertrauen schaffen: Akzeptanzkriterien



Verbreitung Häufigkeit als tragendes Argument im Assurance-Case
Konfidenz Vertrauen in das Kriterium



Ingenieurskulturen

Safety \Rightarrow Konservativ

- Menschen Sterben bei Versagen
- Probleme sind Verstanden und Stabil

Security \Rightarrow Progressive

- Versagen erzeugt eher finanziellen Schaden
- Problemtypen sind dynamisch und ändern sich dauernd

Security + Safety \Leftrightarrow Konservativ $\not\Leftarrow$ Progressiv

- Menschen sterben bei Versagen
- Probleme sind dynamisch, Zielsetzung in Bewegung

SAFETY + SECURITY: CHECKLISTE

- | | |
|---|-------------------------------------|
| 5. HOHE ZUVERLÄSSIGKEIT | <input checked="" type="checkbox"/> |
| 6. KLARHEIT ÜBER SYSTEMZIELE | <input checked="" type="checkbox"/> |
| 7. UMFASSENDE VALIDIERUNG..... | <input checked="" type="checkbox"/> |
| 8. UNABHÄNGIGES REVIEW | <input checked="" type="checkbox"/> |
| 9. ANALYSE VON SOFTWARESYSTEMEN IN REELLER HARDWARE | <input checked="" type="checkbox"/> |
| 10. REDUNDANTE SYSTEME | <input checked="" type="checkbox"/> |
| 11. KRYPTOAGILITÄT | <input type="checkbox"/> |

Die vier Domänen der Sicherheit sind...



Luftfahrt



Automotive



Medizintechnik



Automatisierung

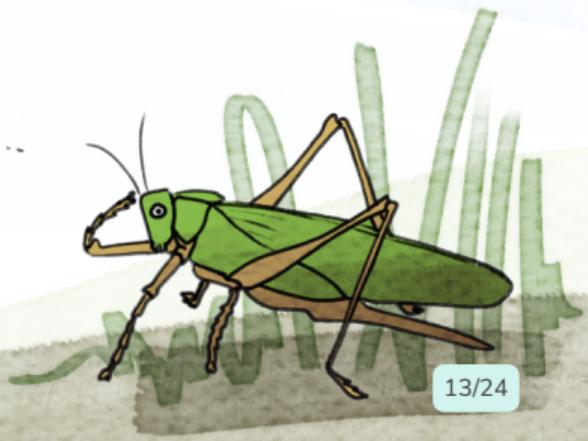
Kryptografie in der Avionik

Sichere Kryptografie in der Avionik

zirp

zirp

zirp



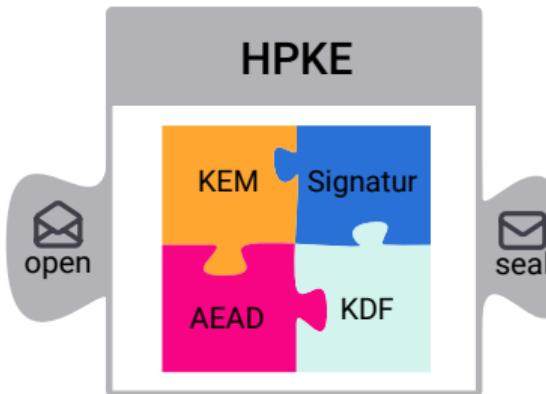
Zum Erschrecken aller...

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



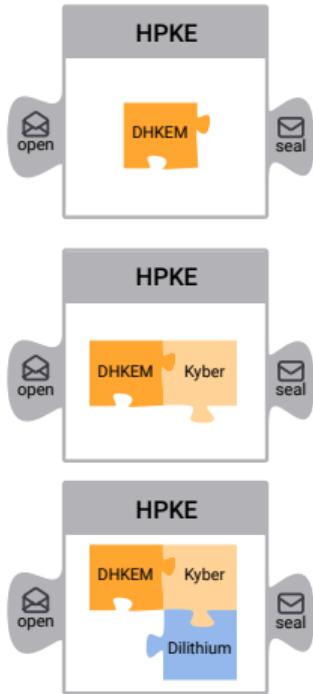
Kryptographie in der Avionik: Unser Ansatz

- Kryptographischer Standard:
Hybridge Public Key Encryption (HPKE)
- Schnittstelle aus HPKE
 - Seal: Nachricht verschlüsseln (und signieren)
 - Open: Nachricht entschlüsseln (und prüfen)



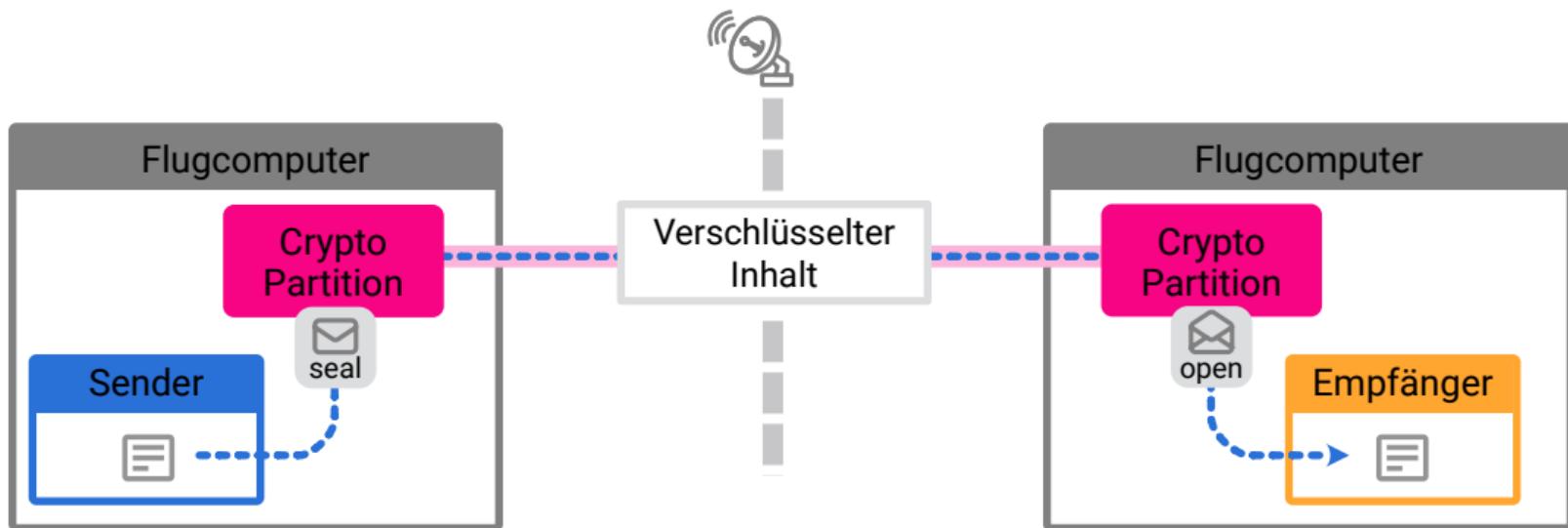


Flexible Einsatzszenarien, gleiche Schnittstelle



- Pre oder post-Quantum?
- Mehr oder weniger Speicherbedarf?
- Schnell oder langsam?
- Post-quantum Authentisierung?

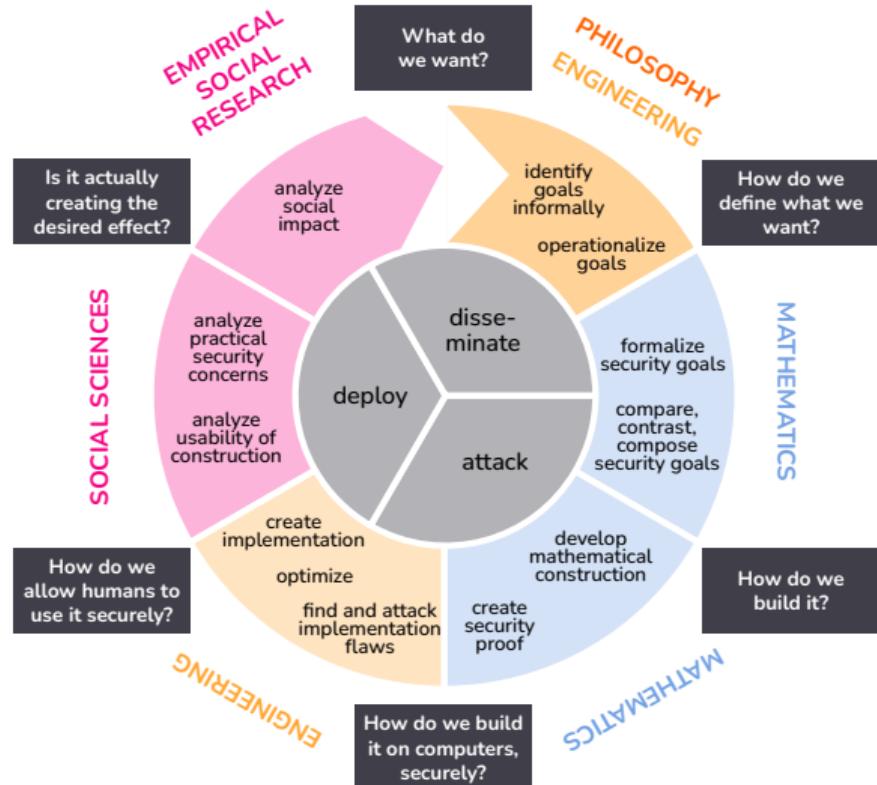
Partitionen zur Integration in die Avionik



Erkenntnisse

Kryptoagilität als Prozess





Technik: Empfehlungen für die Umsetzung

- Klare Zielsetzung
 - Modularisierung reduziert Scope, ermöglicht Fokus
 - Tiefgreifendes Problemverständnis, Schutz wie und wogegen?
- Spielraum
 - Infrastruktur für Continuous Delivery
 - Freiheit, technische Neuerungen zu integrieren



Prozess: Empfehlungen für die Planung

- Knowledge-Management
 - Dokumentation von Anforderungen und Entscheidungen
- Change-Management
 - Incident Response
 - Neue mit alten Anforderungen zusammenführen
- Continuous ...
 - ...Development
 - ...Delivery
 - ...Deployment





Kultur: nachhaltig kryptoagil

Kooperation



Kultur



Kontrolle

Staatliche Förderung
Methodenforschung
Offene Werkzeuge
Freundlicher Wettbewerb
Kollegiale Unterstützung
Förderung von Austausch

Weitsicht
Gründlichkeit
Transparenz
Innovation
Reaktionsfähigkeit
Ehrlichkeit
Zusammenarbeit

Staatliche Kontrolle
Zertifizierung
Unabhängige Reviews



Kryptoagilität

Leitmotiv



AVIATE

Was müssen wir konkret tun?

Modularisierung,
Continuous Delivery

NAVIGATE

Was müssen wir für die Zukunft planen?

robust, aber mit Blick auf die Zukunft

COMMUNICATE

Wie arbeiten wir zusammen?

interdisziplinäre Zusammenarbeit,
Fördern und Fordern

