

## **T.I.S.P. Community Meeting 2014**

**Berlin, 03. - 04.11.2014**

# **Wie können wir sichere Systeme entwickeln?**

**Dr. Yun Ding**  
Secorvo Security Consulting



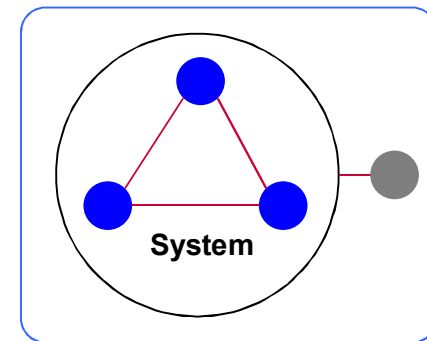
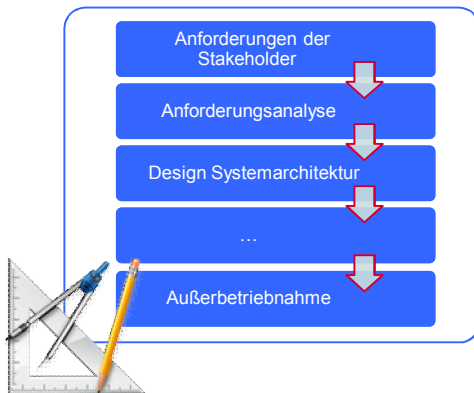
# Ingenieurs-Ansatz für Sicherheit

# Was Ingenieurskunst hat:

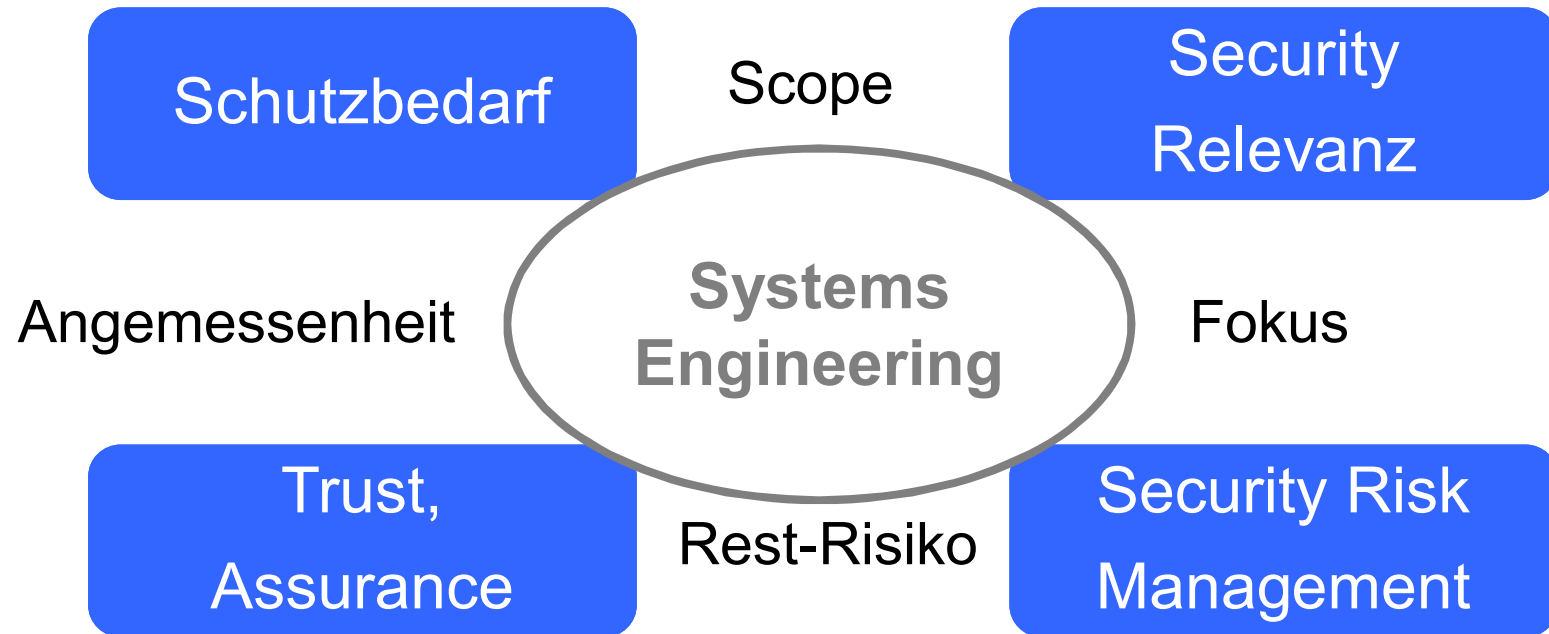
- Erfahrungen aus Jahrtausenden
  - Erkenntnisse sind in Normen und Vorschriften eingeflossen
- „Safety“ ist von Beginn an integraler Bestandteil
  - Nur das Bauwerk, welches der Natur widersteht, nützt
- Hohe Testkultur: Keine Freigabe ohne Abnahme
- Kontinuierliche und regelmäßige Kontrollen im Betrieb
  - Z. B. TÜV
- Eindeutige Haftungsverhältnisse

# Was ist Systems Security Engineering?

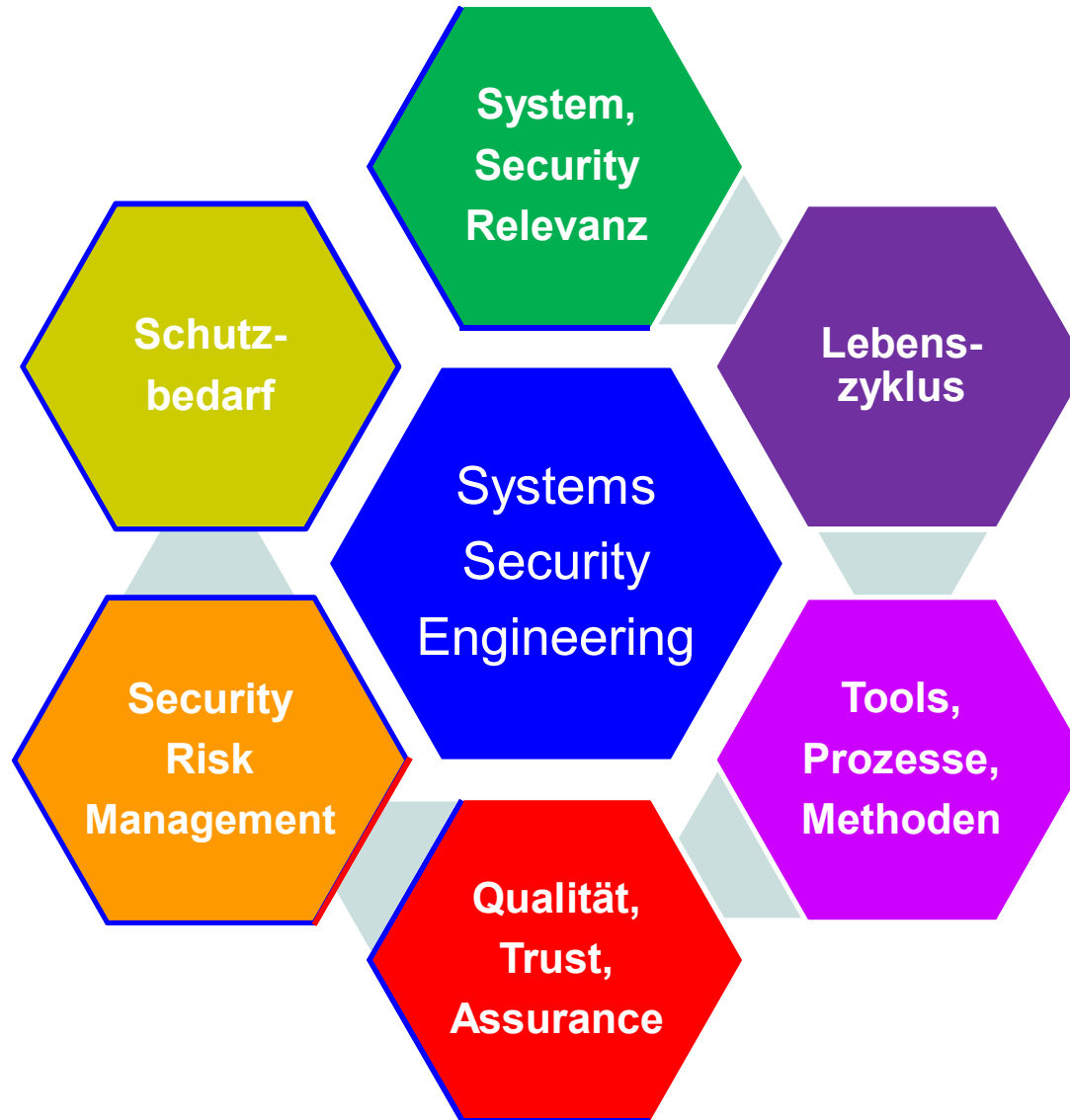
- ...*ingenieurwissenschaftlicher Ansatz* für Sicherheit
- ... verwendet bewährte *Security Prinzipien, Konzepte* und *Best Practices* im gesamten *Systemlebenszyklus*
- ... produziert *zuverlässige Systeme*, die trotz anhaltenden *Bedrohungen und Störungen* dem *Schutzbedarf* der Stakeholder gerecht werden



## .... Systems Engineering mit Fokus auf Security



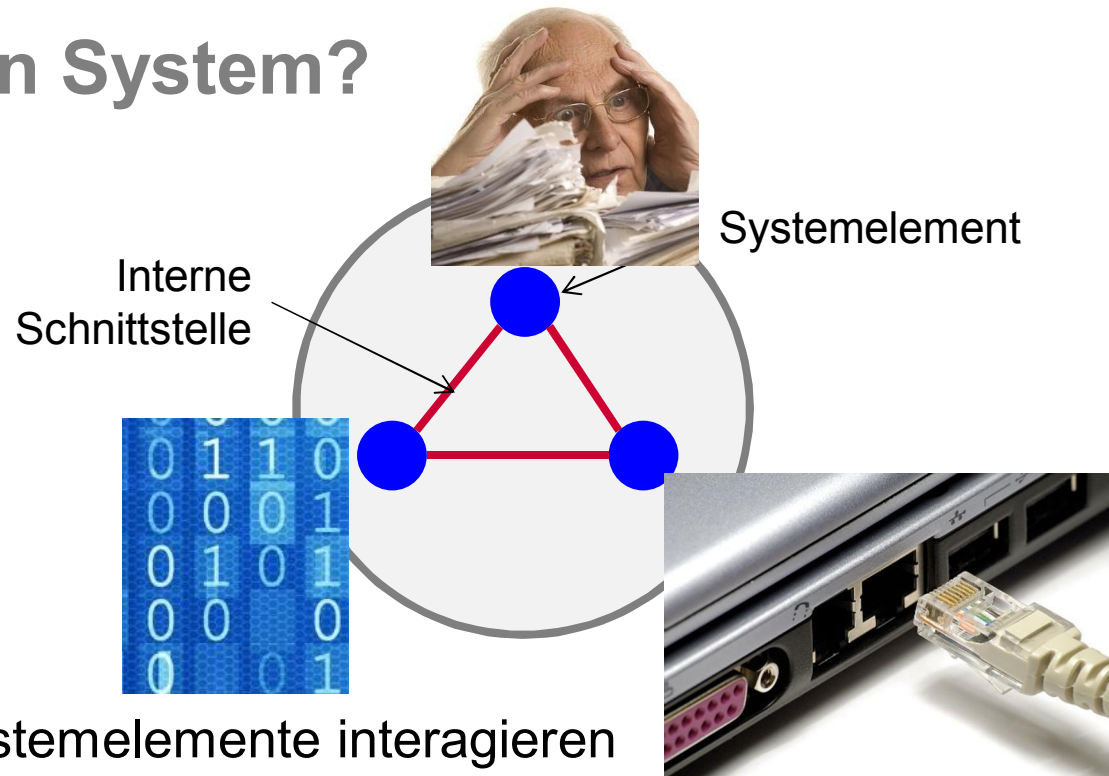
# Konzepte des Systems Security Engineerings





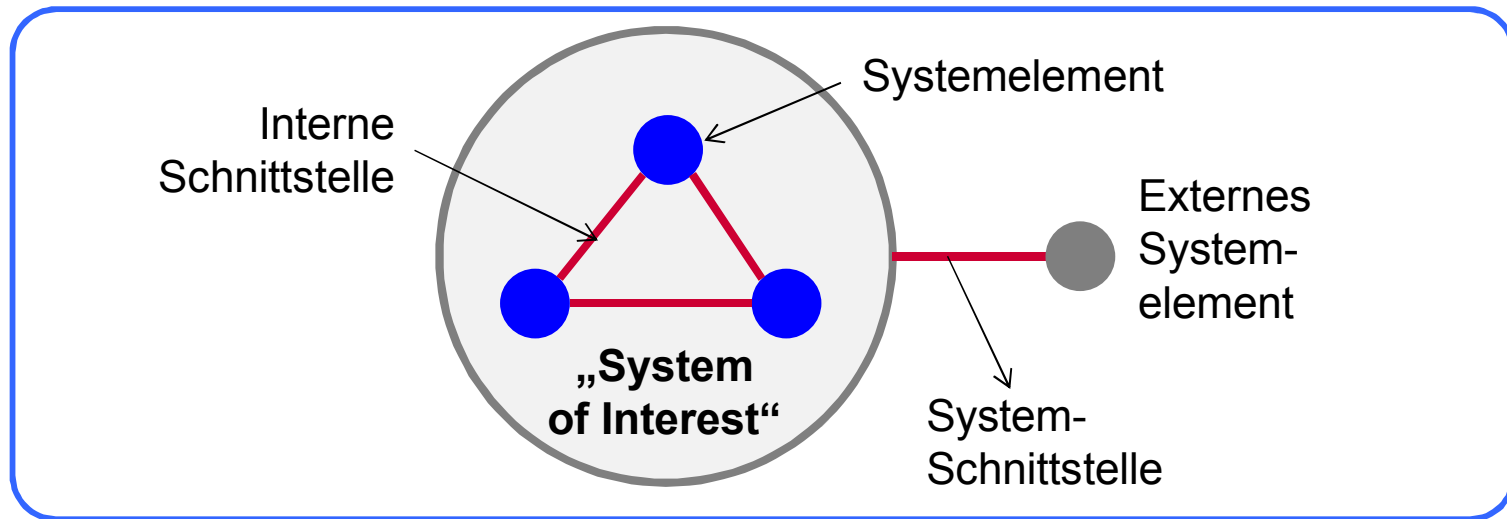
Das System ist so sicher wie das  
schwächste Glied

# Was ist ein System?



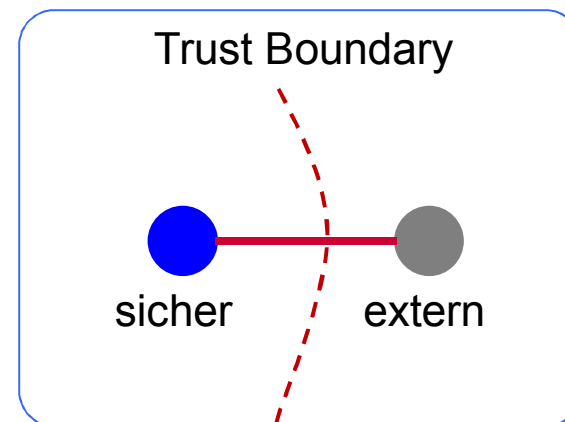
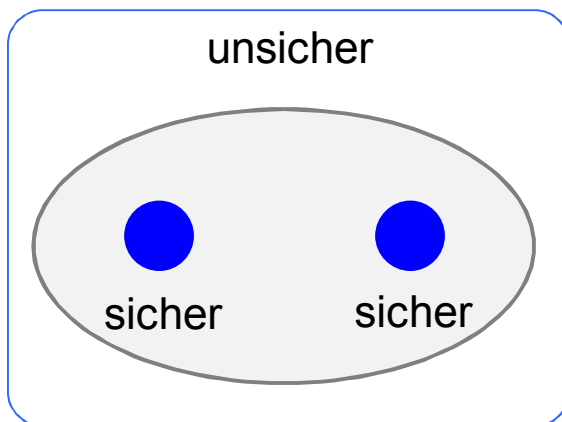
- Systemelemente interagieren
- Systemelemente sind interdisziplinär

# Was ist ein System?



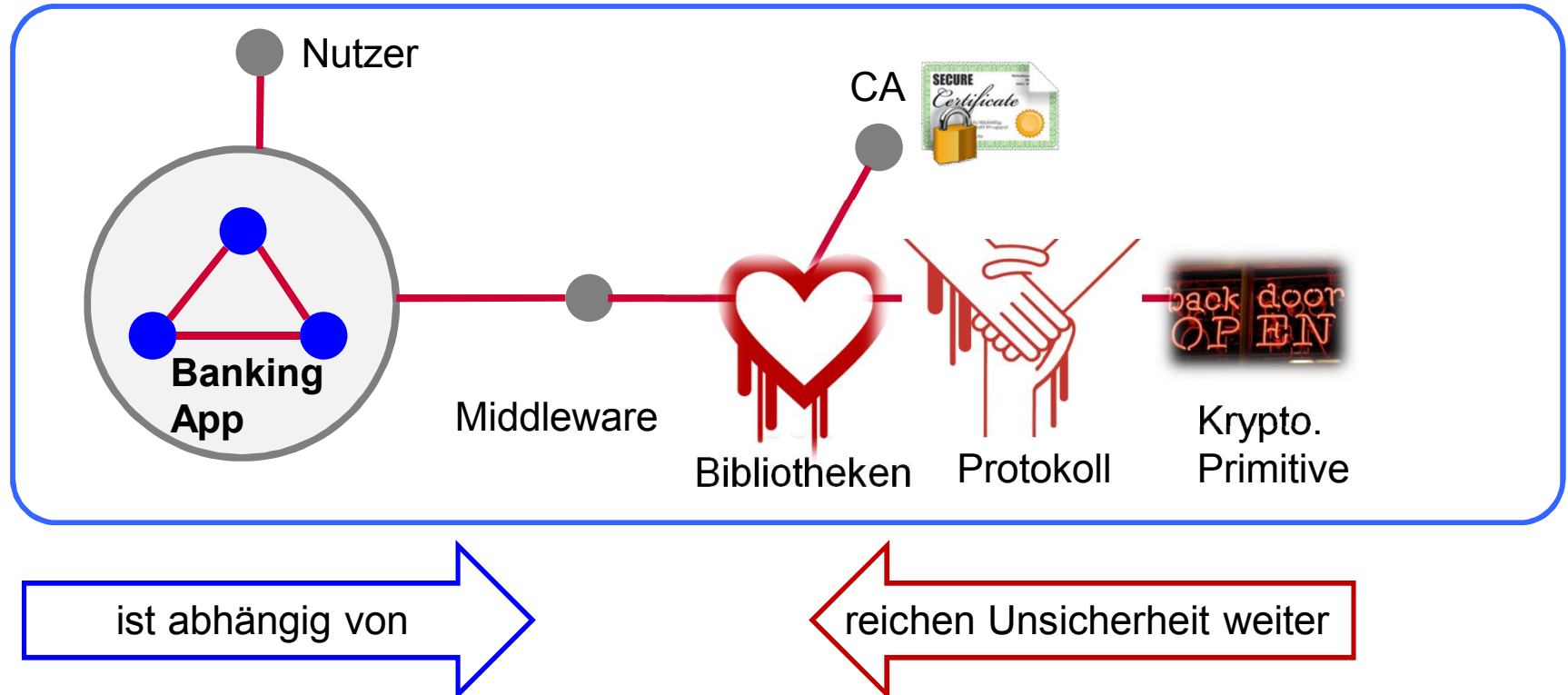
- Systemelemente interagieren
- Systemelemente sind interdisziplinär
- System-of-Interest: Fokus des Engineerings erweitern
- Externe Systemelemente stehen in Wechselwirkung
- Ganzheitliche Systemsicht

- ... so sicher wie das unsicherste Systemelement
- ... mehr als Sicherheit einzelner Komponenten
- Erfahrungen nutzen: Was ging schief?
  - Abhängigkeiten und Annahmen
  - Komposition: sicher + sicher = unsicher!
  - Interaktion



# Beispiel: das SSL-System

System,  
Security  
Relevanz



# SSL Handshake-Protokolle

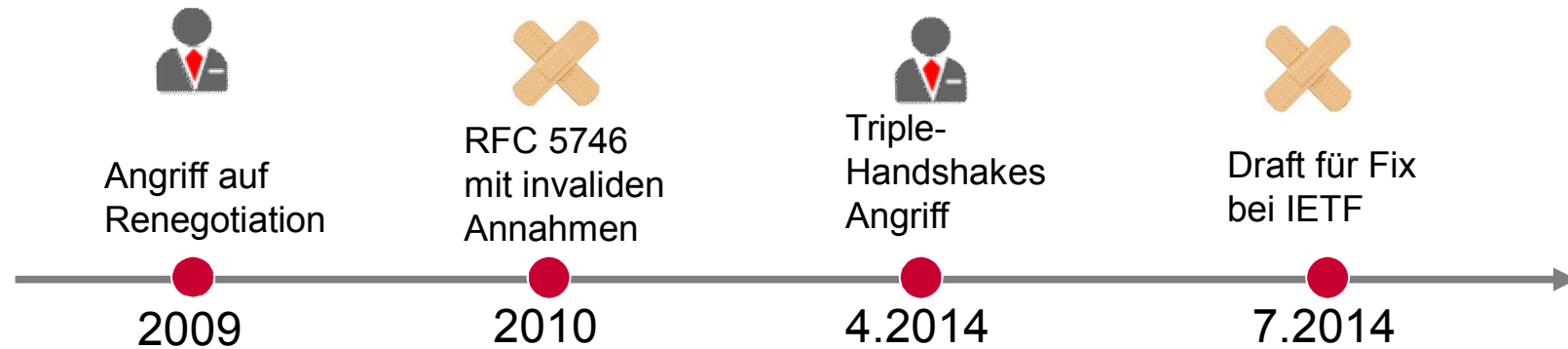
System,  
Security  
Relevanz

| Standard Handshake      | Resumption Handshake                                                                                                                                                                                       |
|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Renegotiation Handshake | <ul style="list-style-type: none"><li>♦ Jedes einzelne Handshake-Protokoll ist sicher.</li><li>♦ „Triple-Handshakes“ nutzt die <i>ungewollte Interaktion</i> zwischen den Handshake-Protokollen.</li></ul> |

# Flickschusterei bei SSL



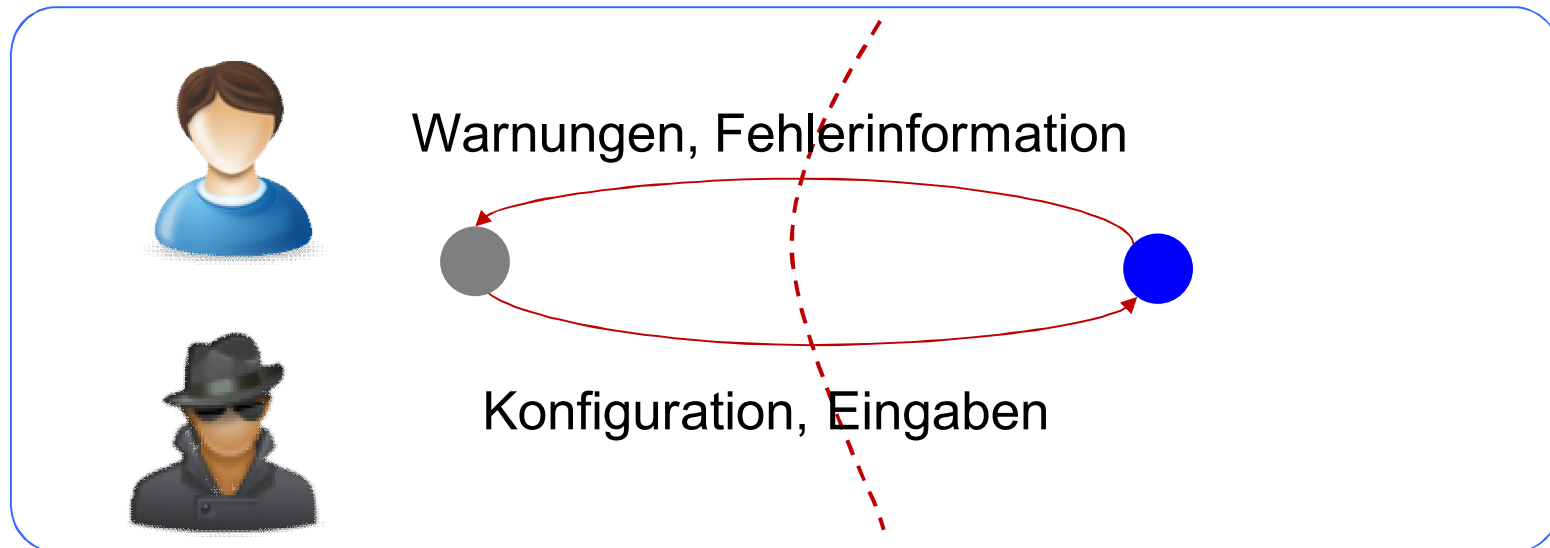
System,  
Security  
Relevanz



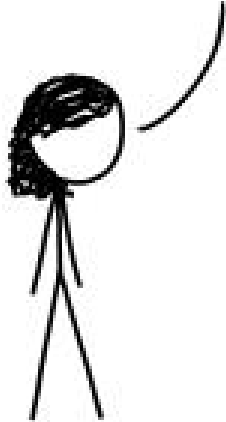
# Interaktion mit Menschen

System,  
Security  
Relevanz

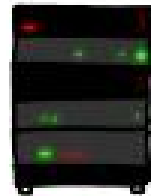
- Benutzer treffen falsche Entscheidungen: SSL Warnungen
- Benutzer verwenden (unwissend) unsichere Konfiguration
- Angreifer wird das System für seine Zwecke missbrauchen



SERVER, ARE YOU STILL THERE?  
IF SO, REPLY "HAT" (500 LETTERS).



a connection. Jake requested pictures of deer.  
User Meg wants these 500 letters: HAT. Lucas  
requests the "missed connections" page. Eve  
(administrator) wants to set server's master  
key to "14835038534". Isabel wants pages about  
snakes but not too long". User Karen wants to  
change account password to "CoHoBaSt". User



HAT. Lucas requests the "missed connections" page. Eve (administrator) wants to set server's master key to "14835038534". Isabel wants pages about "snakes but not too long". User Karen wants to change account password to "CoHoBaSt". User

a connection. Jake requested pictures of deer.  
User Meg wants these 500 letters: HAT. Lucas  
requests the "missed connections" page. Eve  
(administrator) wants to set server's master  
key to "14835038534". Isabel wants pages about  
snakes but not too long". User Karen wants to  
change account password to "CoHoBaSt". User



# Interaktion mit externen Systemen



Tamper-Resistant

Security API

Scanning...



Schutzbedarf und Security Relevanz

# Schutzbedarf

Schutz-  
bedarf

## Stakeholder-Perspektive

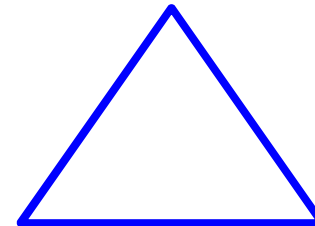
- Business, Mission
- Assets und ihre Werte
- Gesetze, Richtlinien, Regulierungen
- ...

## System-Perspektive

- Konzepte aus der Betriebsphase
- System-Selbstschutz
- ...

## Schutzbedarf

Integrität



Vertraulichkeit    Verfügbarkeit

Aktualität    Gerätebindung

Schutz-  
bedarf

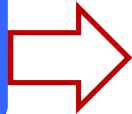
Schutzbedarf

Sicherheitsrichtlinien

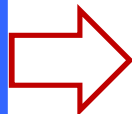
Sicherheitsanforderungen

# Security Risk Management

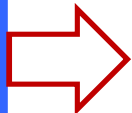
Threat  
Assessment



Vulnerability  
Assessment

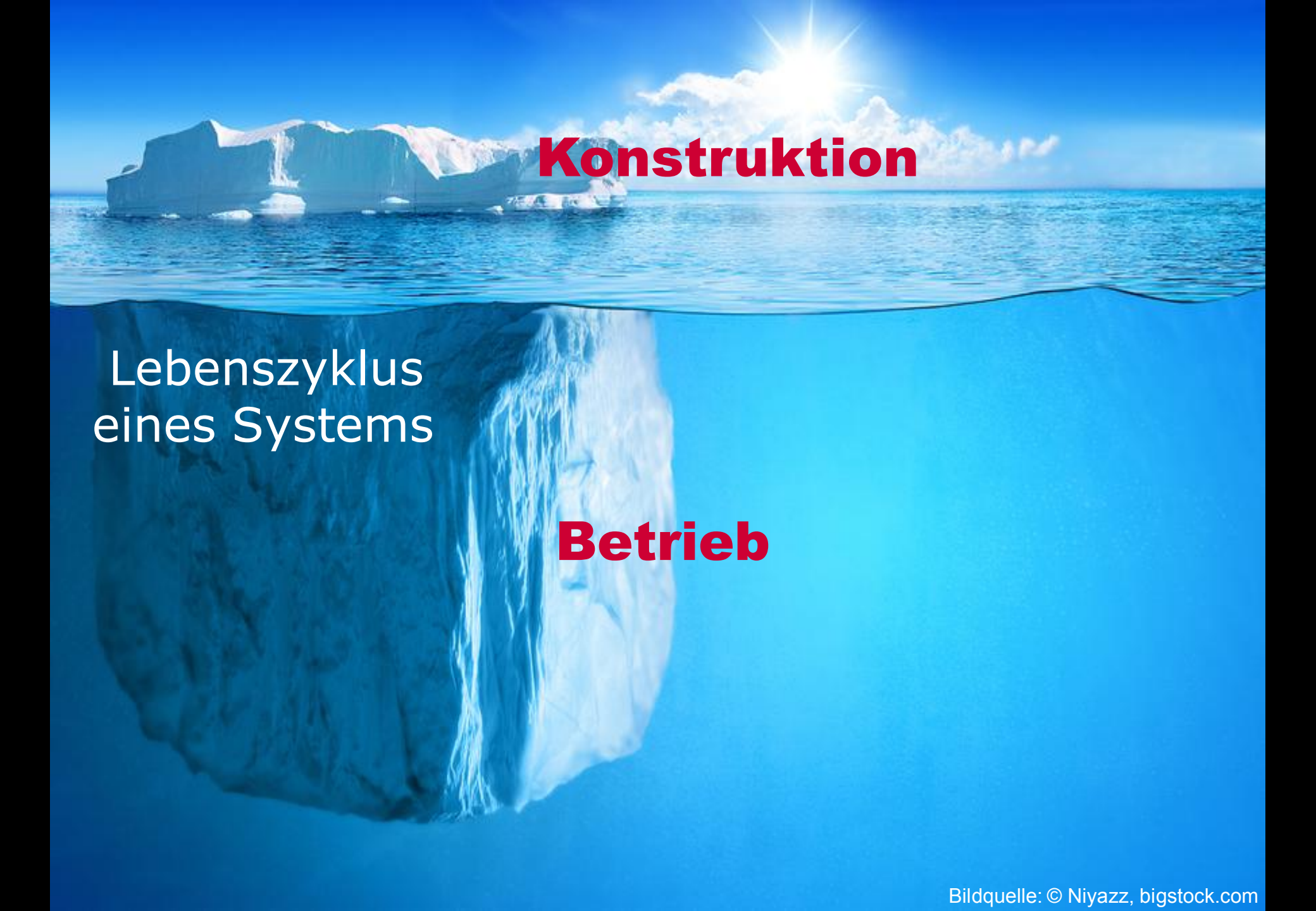


Analyse  
Schutzbedarf



## Security Risk Management



An iceberg floating in a blue ocean under a bright sun. The visible tip of the iceberg is labeled 'Konstruktion' (Construction) in red. The much larger, submerged part of the iceberg is labeled 'Betrieb' (Operation) in red. The text 'Lebenszyklus eines Systems' (Lifecycle of a system) is written in white on the submerged part of the iceberg.

**Konstruktion**

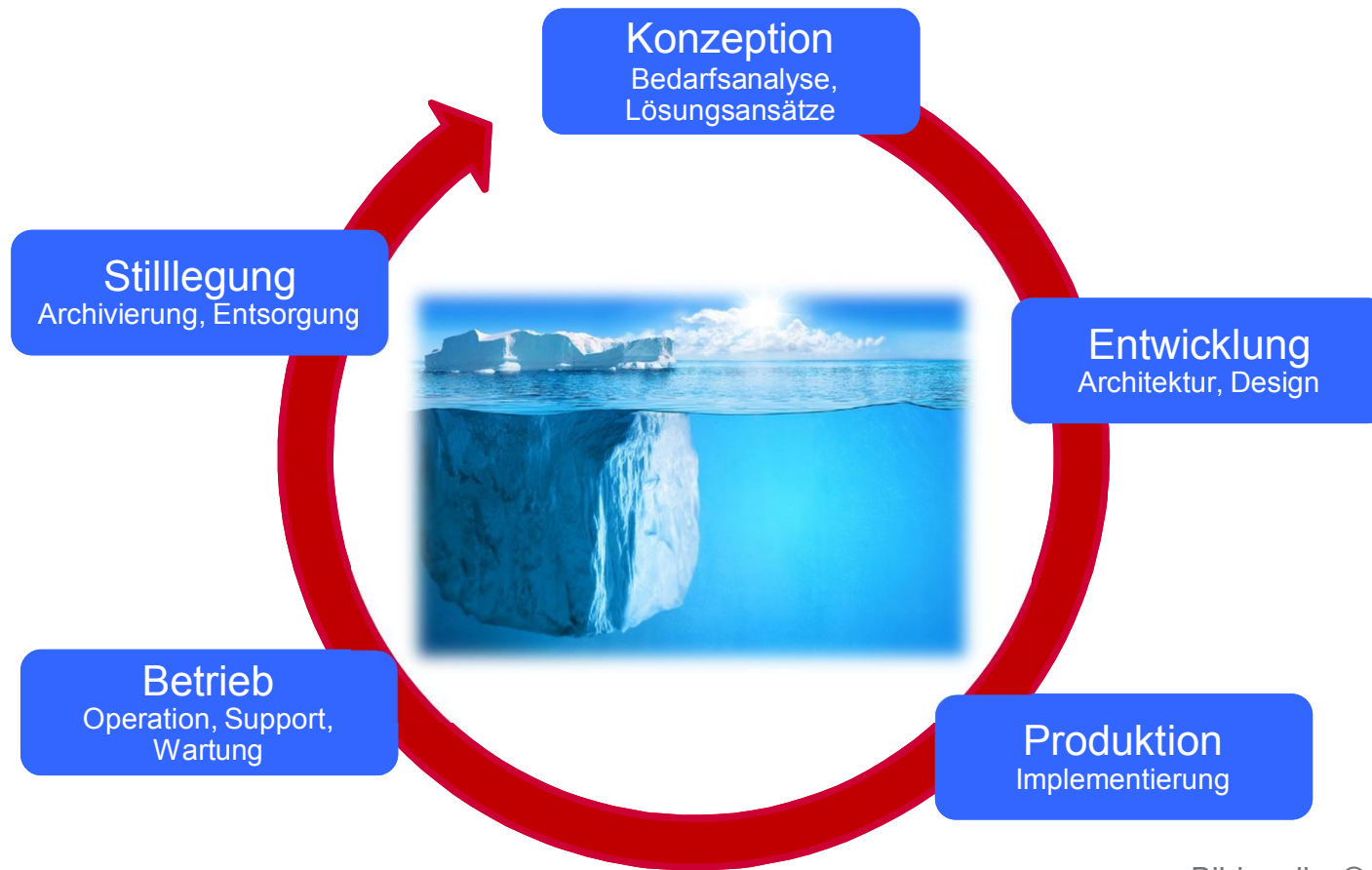
Lebenszyklus  
eines Systems

**Betrieb**

# Lebenszyklus eines Systems

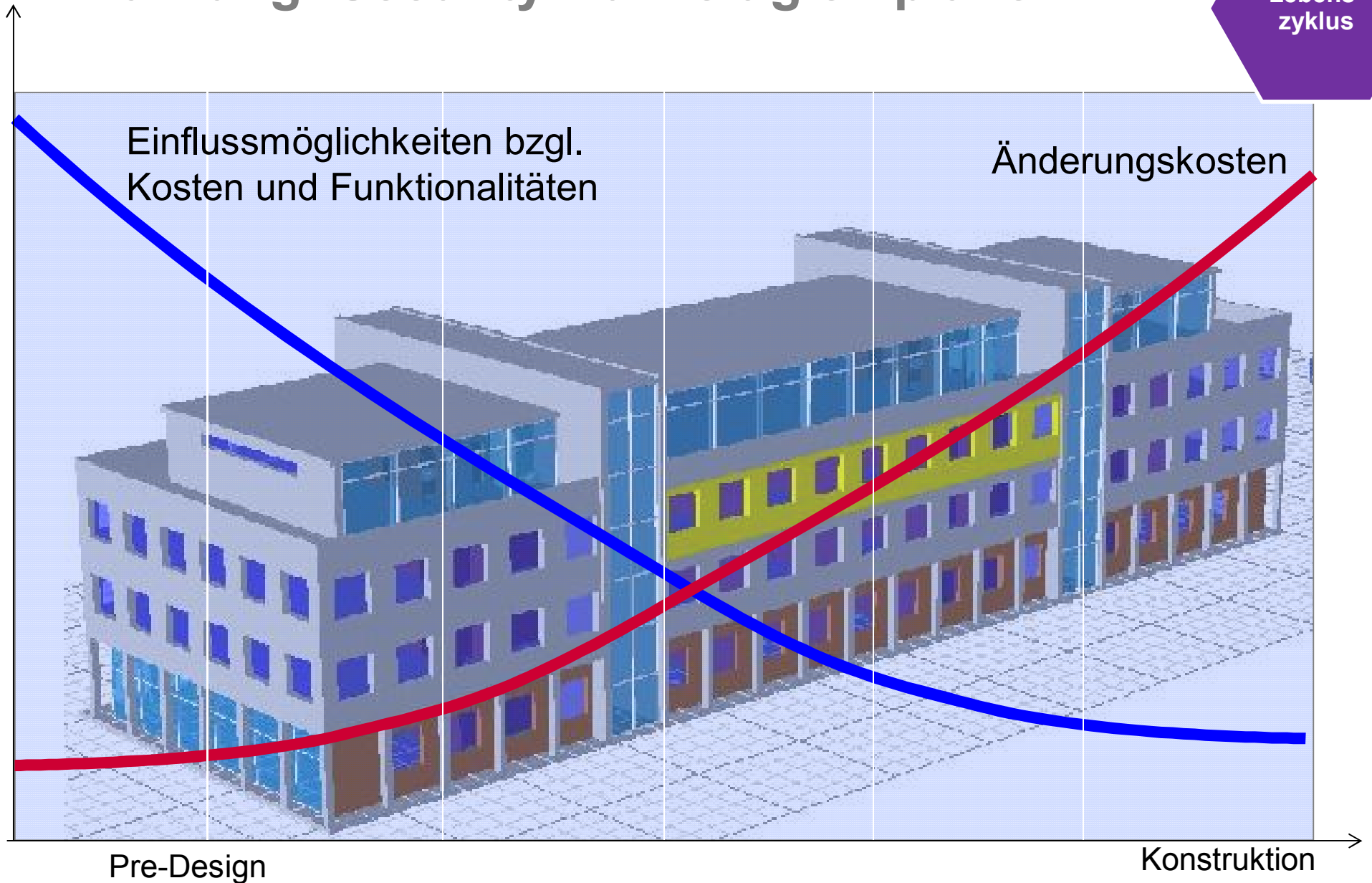
Lebens-  
zyklus

- Sicherheit als integrierter Bestandteil **des gesamten Lebenszyklus**.
- Konzepte des Betriebs beeinflussen die Sicherheitsanforderungen.



# Erfahrung: Security frühzeitig einplanen

Lebens-  
zyklus





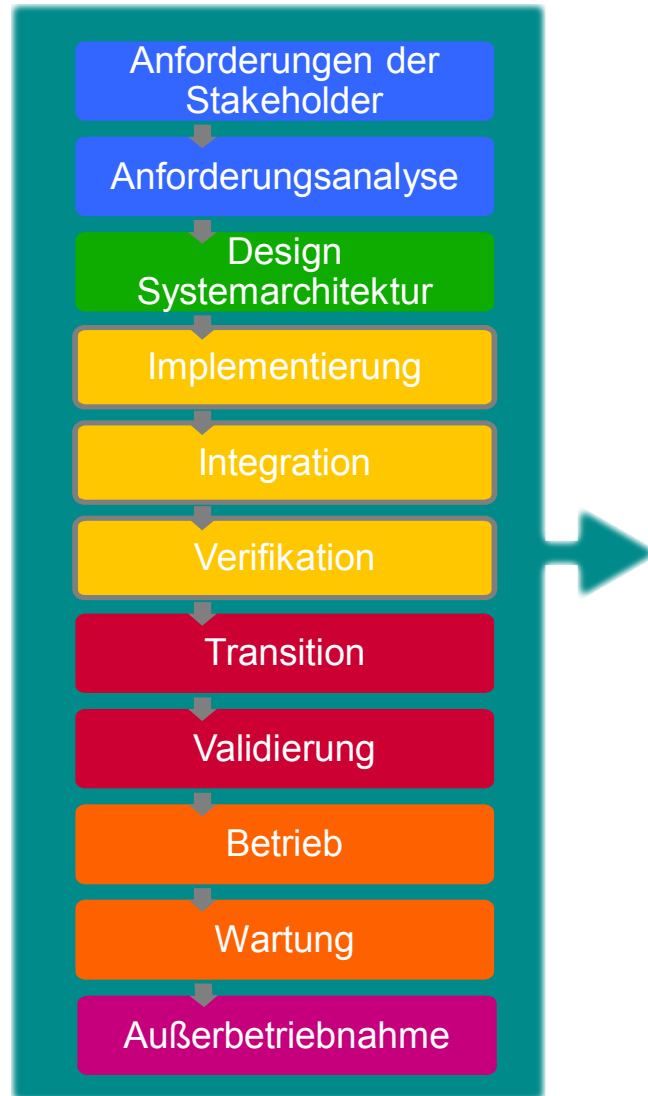
# Prozesse im Systemlebenszyklus



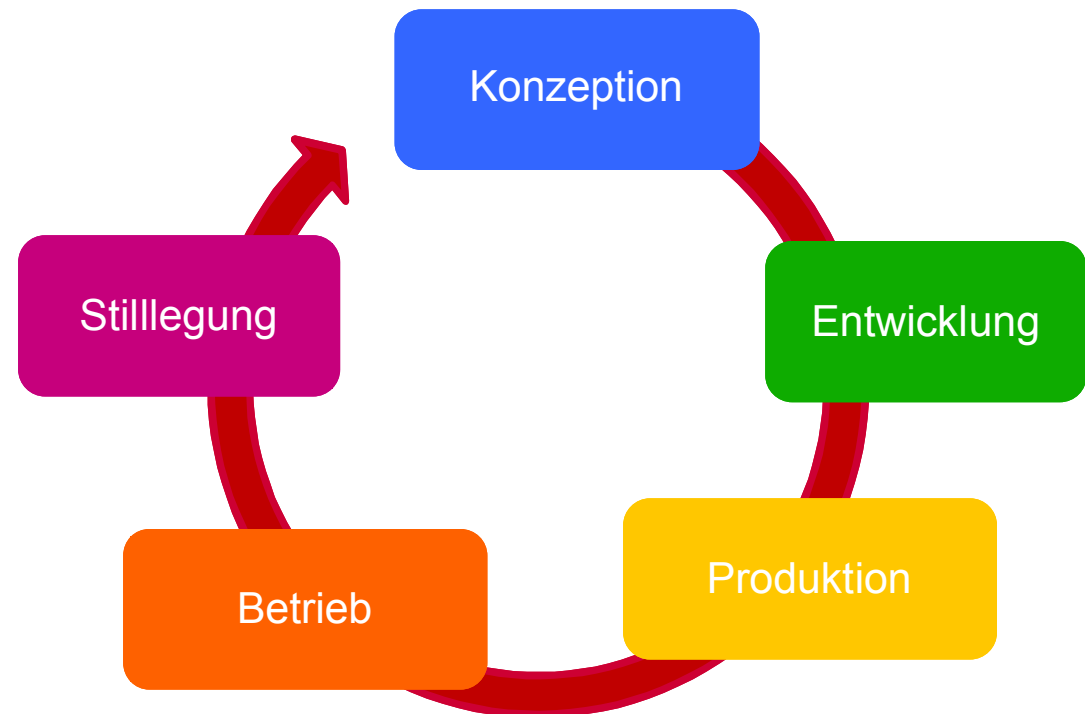
Bildquelle:  
© GoodMood Photo,  
bigstock.com

# Prozesse des Security Engineerings

Tools,  
Prozesse,  
Methoden



- ISO/IEC 15288
- NIST SP 800-160





Trust & Assurance

- Security Engineering produziert *zuverlässige Systeme* mit *messbarem Schutz*, die trotz anhaltenden *Bedrohungen* und *Störungen* dem *Schutzbedarf* der Stakeholder gerecht werden.
- Wann haben wir Vertrauen in Produkte?
  - Die verwendeten Materialien wurden getestet.
  - Der Hersteller ist ISO 9001 zertifiziert.
  - Produkte wurden von unabhängigen Prüfstellen geprüft und haben einen Siegel bekommen.
  - Das Produkt wird während der Lebensdauer regelmäßig geprüft.
  - Es gibt die Produkthaftung ...

# Assurance

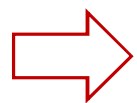


- Überzeugende Sicherheitsnachweise erzeugen Vertrauen
- Design Assurance:
  - Wer hat das Produkt entwickelt?
  - Wie wurde das Produkt entwickelt?
- Objektiver Nachweise: Testing
- Evaluierung durch eine akkreditierte Organisation

➡ Assurance:  
„Das System hat die vereinbarte Funktionalität korrekt implementiert“

# Was nützt uns Security Engineering?

- Sie ermöglicht Systeme ganzheitlich zu denken
- Sie integriert Sicherheit im gesamten System-Lebenszyklus
- Sie unterstützt Design-Assurance durch die Integration von Sicherheit in die Prozesse des Lebenszyklus
- Treibt über den Schutzbedarf die Sicherheit voran
- Fördert Security Risk Management mit strukturiertem Threat & Vulnerability Assessment



Schafft Vertrauen in Systeme  
trotz Bedrohungen und Störungen!



Dr. Yun Ding  
yun.ding@secorvo.de

