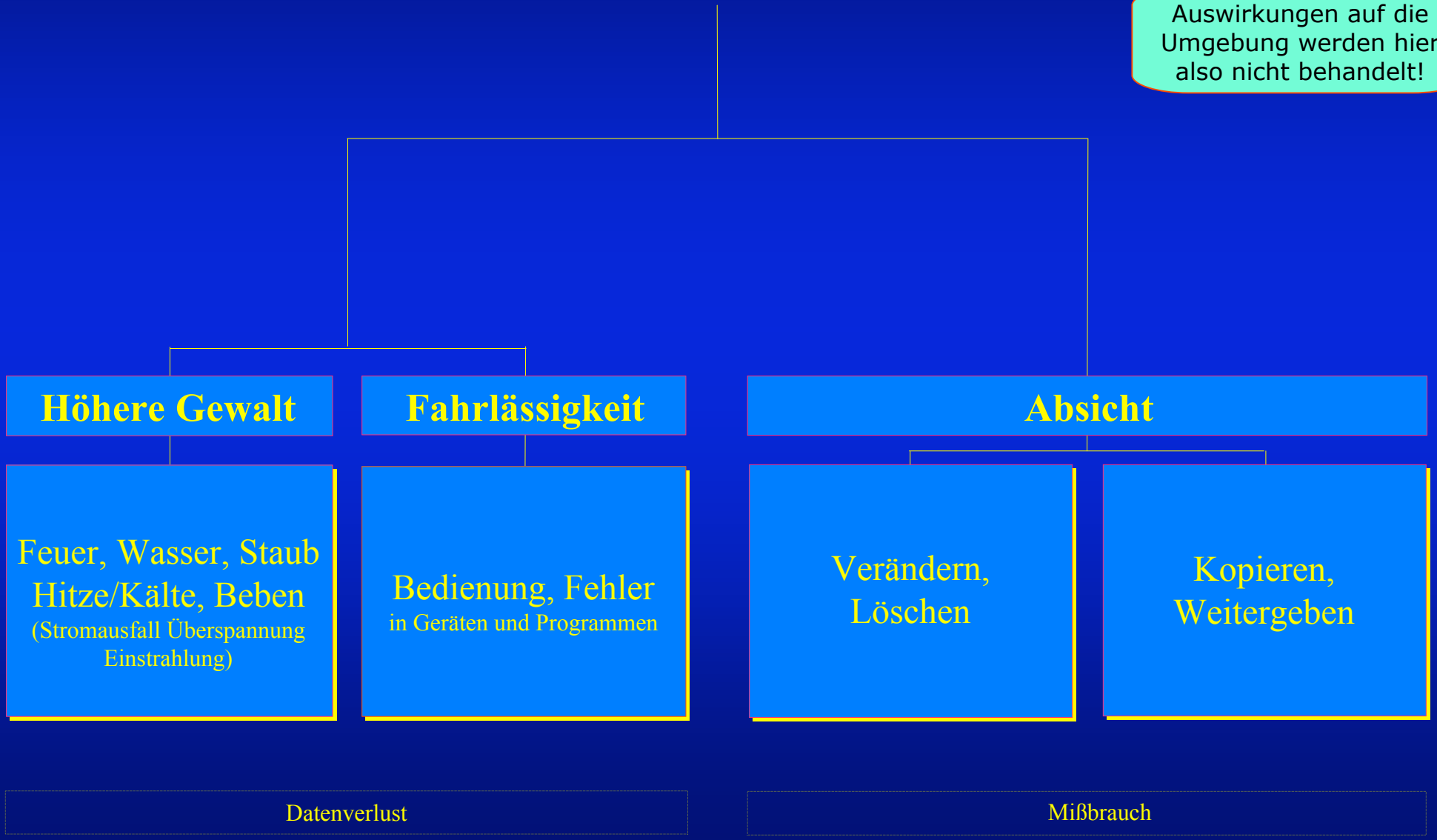
# Taxonomie und Modellbildung
## in der Begriffswelt Safety und Security
am Beispiel ausgewählter internationaler Normen

Hartmut Pohl

# Inhaltsverzeichnis

# Sicherheitsprobleme der Informationsverarbeitung

Auswirkungen auf die Umgebung werden hier also nicht behandelt!



# IT-System (Rechensystem)

Funktionseinheit zur Verarbeitung von Daten
nämlich zur Durchführung mathematischer, umformender, übertragender und speichernder Operationen.

DIN 44 300

# IV-System

Das IT-System zusammen mit der

- technischen Infrastruktur (Stromversorgung, Klimatisierung etc.), den unterstützenden
- Personen (Bedienung, Programmierung etc.) sowie den zugehörigen
- organisatorischen Regelungen.

# Inhaltsverzeichnis

# Safety

Zustand eines **Systems**
frei von unvertretbaren schadenverursachenden Risiken zu sein.

Der Schaden kann an dem System oder außerhalb enstehen.

– – –

Frei von Gefahren, die vom Betrieb der Hardware oder Software ausgehen
und die der Umwelt drohen – gekennzeichnet durch Begriffe wie Betriebssicherheit, Arbeitssicherheit.

DIN EN 61508-4, TR 13335-1, RFC 2828

# Security

Zustand eines **IT-**Systems, in dem Maßnahmen zum Schutz des Systems wirksam sind.

RFC 2828

Zustand eines IT-Systems, in dem folgende **Sachziele** angestrebt werden:

Vertraulichkeit: Informationen sind nur für Berechtigte zugreifbar.
Integrität: Genauigkeit und Vollständigkeit von Informationen und Verfahren sind sichergestellt.
Verfügbarkeit: Berechtigte erhalten bei Bedarf Zugriff.

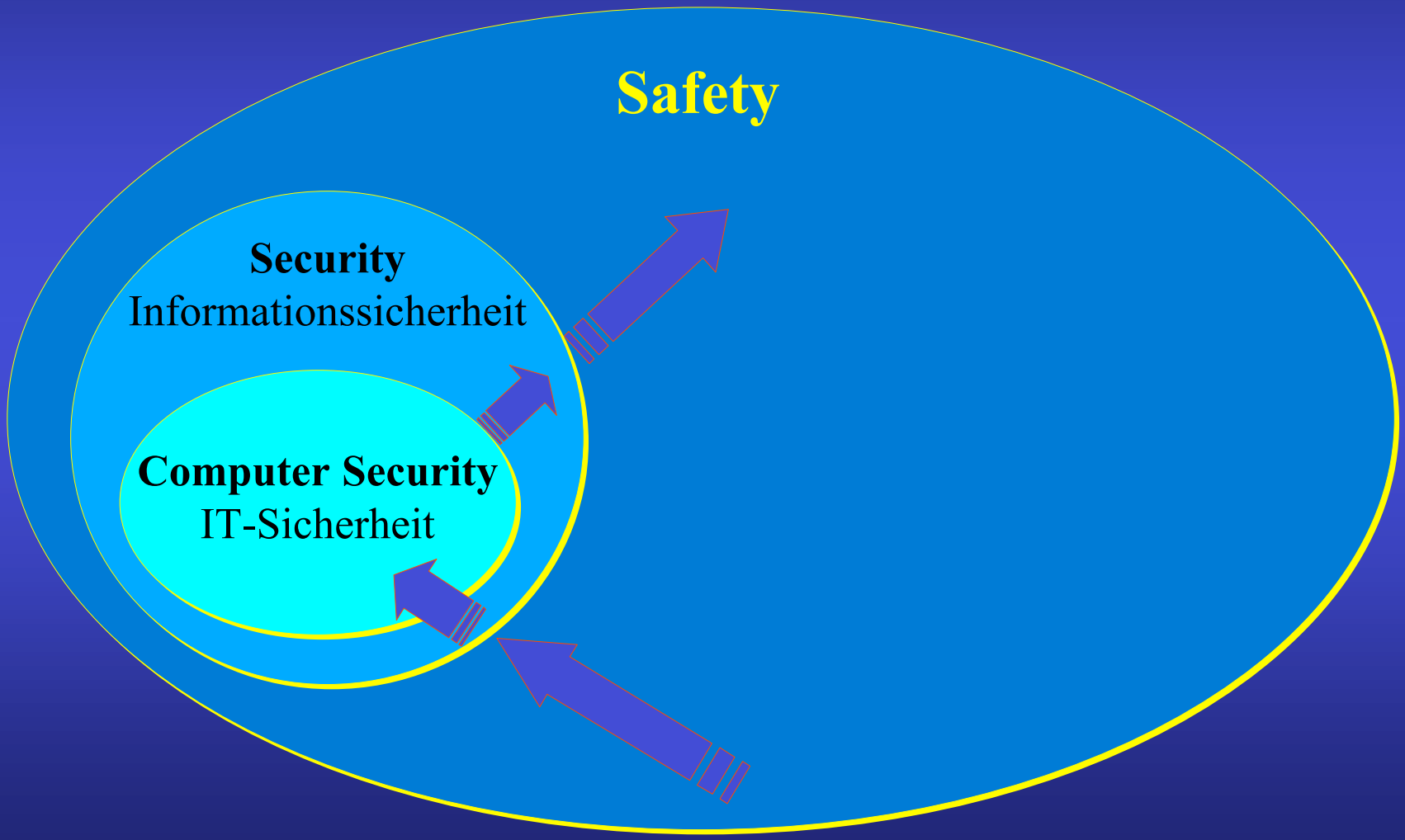
ISO/IEC 17799

# Safety – Security

- **Safety**
  Schutz der Umgebung vor 'inkorrektem Verhalten' des Rechners.

- **Security**
  Schutz des Rechners vor 'inkorrektem Verhalten' der Rechnerumgebung.

# Safety, Security, Computer Security



# Inhalte der Informationssicherheit

# Information Security (INFOSEC) – Informationssicherheit

Zustand eines IV-Systems, in dem die folgenden Sachziele angestrebt werden.

- Vertraulichkeit: Informationen sind nur für Berechtigte zugreibar.
- Integrität: Genauigkeit und Vollständigkeit von Informationen und Verarbeitungsmethoden schützen.
- Verfügbarkeit: Berechtigte haben erforderlichenfalls Zugriff auf Informationen und verknüpfte Elemente.

ISO/IEC 17799

Zustand eines IT-Systems, in dem
1. die berechtigte Nutzung unterstützt wird,
2. die unberechtigte Nutzung kenntlich gemacht oder mindestens erschwert wird und

und das verbleibende **Restrisiko** als tragbar bewertet wird.

ISO/IEC DIS 14980

# Wichtige Sachziele der Informationssicherheit

- **Vertraulichkeit** – **confidentiality**
  Eigenschaft eines Systems, nur berechtigten Subjekten den Zugriff
  auf bestimmte Objekte zu gestatten und unberechtigten Subjekten
  den Zugriff auf alle Objekte zu verwehren. [Auch: Kennzeichnung des Schutzniveaus.]

- **Integrität** – **integrity**
  Eigenschaft eines Systems, die Korrektheit der Objekte sicherzustellen:
  Die Daten sind auf dem aktuellen Stand. Das System ist (korrekt) verfügbar.
  Objekte sind gg. unberechtigte Modifikation (und/oder Zerstörung) geschützt.

- **Verfügbarkeit** – **availability**
  Wahrscheinlichkeit, ein System zu einem vorgegebenen Zeitpunkt,
  in einem funktionsfähigen Zustand anzutreffen.

- **Verbindlichkeit** – **liability**
  Eigenschaft eines Systems, authentische, rechtsverbindliche Kommunikation zu unterstützen.
  Geschützt gegen Täuschung, Abstreiten (non-repudiation).

# Vertraulichkeit – confidentiality

Eigenschaft eines Systems,

berechtigten Subjekten den Zugriff auf bestimmte Objekte zu gestatten

und unberechtigten Subjekten den Zugriff auf alle Objekte zu verwehren.

Auch: Kennzeichnung des Schutzniveaus.

ISO/IEC 2382, ISO/IEC 7498, RFC 2828

# Integrität – integrity

Eigenschaft eines Systems,
die Validität der Objekte sicherzustellen.

Eigenschaft eines Systems,
dass Daten nicht verändert, zerstört oder verloren wurden.

(Objekte sind gegen unberechtigte Modifikation (und/oder Zerstörung) geschützt.)

ISO 7498-2, ISO 8732, ISO/IEC 2382, ISO/IEC 9797 2nd ed., TR 13335-1, RFC 2828

# Validität – validity

**Übereinstimmung** (Konsistenz – consistency) eines Werts hinsichtlich
**Genauigkeit** (Accuracy),
**Korrektheit** (correctness) und
**Vollständigkeit** (completeness)
mit dem tatsächlichen Sachverhalt.

Die Daten sind richtig/fehlerfrei, regelgemäß (z.B. formatiert), auf dem aktuellen Stand.

CSE 1993, ISO 7498-2, ISO 8732, ISO/IEC 9797 2nd ed., TR 13335-1

# Korrektheit – correctness

Grad der Übereinstimmung zwischen dem tatsächlichen Wert
eines Objekts (einer Variablen) und dem verarbeiteten Wert.



ISO 7498-2, ISO 8732, ISO/IEC 9797 2nd ed., TR 13335-1

# Vollständigkeit – completeness

Geschlossenheit, Ganzheit.



ISO 7498-2, ISO 8732, ISO/IEC 9797 2nd ed., TR 13335-1

# Verfügbarkeit – availability

Eigenschaft eines Systems,
für Berechtigte zugreifbar und nutzbar zu sein
– entsprechend der spezifizierten Performanz.

Das beinhaltet u.a. zeitlich kritische Prozesse.

Wahrscheinlichkeit,
ein System zu einem vorgegebenen Zeitpunkt,
in einem funktionsfähigen Zustand anzutreffen.

DIN 40042, ISO/IEC 2382-08, ISO/IEC 7498, RFC 2828

# Verbindlichkeit – liability

Eigenschaft eines Systems,
zurechenbare, rechtsverbindliche Kommunikation zu unterstützen –
geschützt gegen Täuschung (Sender) sowie gegen Abstreiten (non-repudiation)
durch Sender und Empfänger.

Eigenschaft eines IV-Systems,
versuchte und erfolgte Aktivitäten (wie Zugriffe) von Subjekten auf Objekte nachvollziehen
zu können indem diese Aktivitäten den Subjekten zugeordnet werden.

Ermöglicht die Erkennung und Untersuchung von Angriffen.

Ukonline, ISO/IEC 2382-08, ISO 7498-2, TR 13335-1, RFC 2828

# Weitere mögliche Sachziele

| Sachziel | Schutz gegen | Fachbegriff |
|---|---|---|
| Anonymität | Identifizierung | anonymity |
| Pseudonymität | Namentliche Identifizierung | pseudonymity |
| Unbeobachtbarkeit | Protokollierung | untraceability |
| Nicht-Vermehrbarkeit | "Viren"-Aktivitäten | non-propagation |
| Netz-Verfügbarkeit | Angriffe auf das Netzwerk | net availability |
| Transparenz | Fehlende Nachvollziehbarkeit | transparency |
| ... | | |

# Wichtige Sachziele der Informationssicherheit




Laprie 1992

# Vertrauenswürdigkeit, Verlässlichkeit
# dependability, assurance

Oberbegriff für die Sachziele der Informationssicherheit
wie Vertraulichkeit, Integrität, Verfügbarkeit und Verbindlichkeit

| | |
|---|---|
| Assurance: | Grounds for confidence that an entity meets its security objectives. |
| Vertrauenswürdigkeit: | Gründe für das Vertrauen, daß eine Entität die Sicherheitsziele erreicht. |

ISO/IEC 15408

# IT-Sicherheit – computer security

Zustand eines IT-Systems,
in dem Sicherheitsdienste zur Erreichung der Sachziele*
implementiert sind und garantiert werden.

Ein vertrauenswürdiges = verlässliches = zuverlässiges System.

* Vertraulichkeit, Integrität, Verfügbarkeit, Verbindlichkeit/Zurechenbarkeit sowie Authentizität und Zuverlässigkeit. ISO/IEC 1996

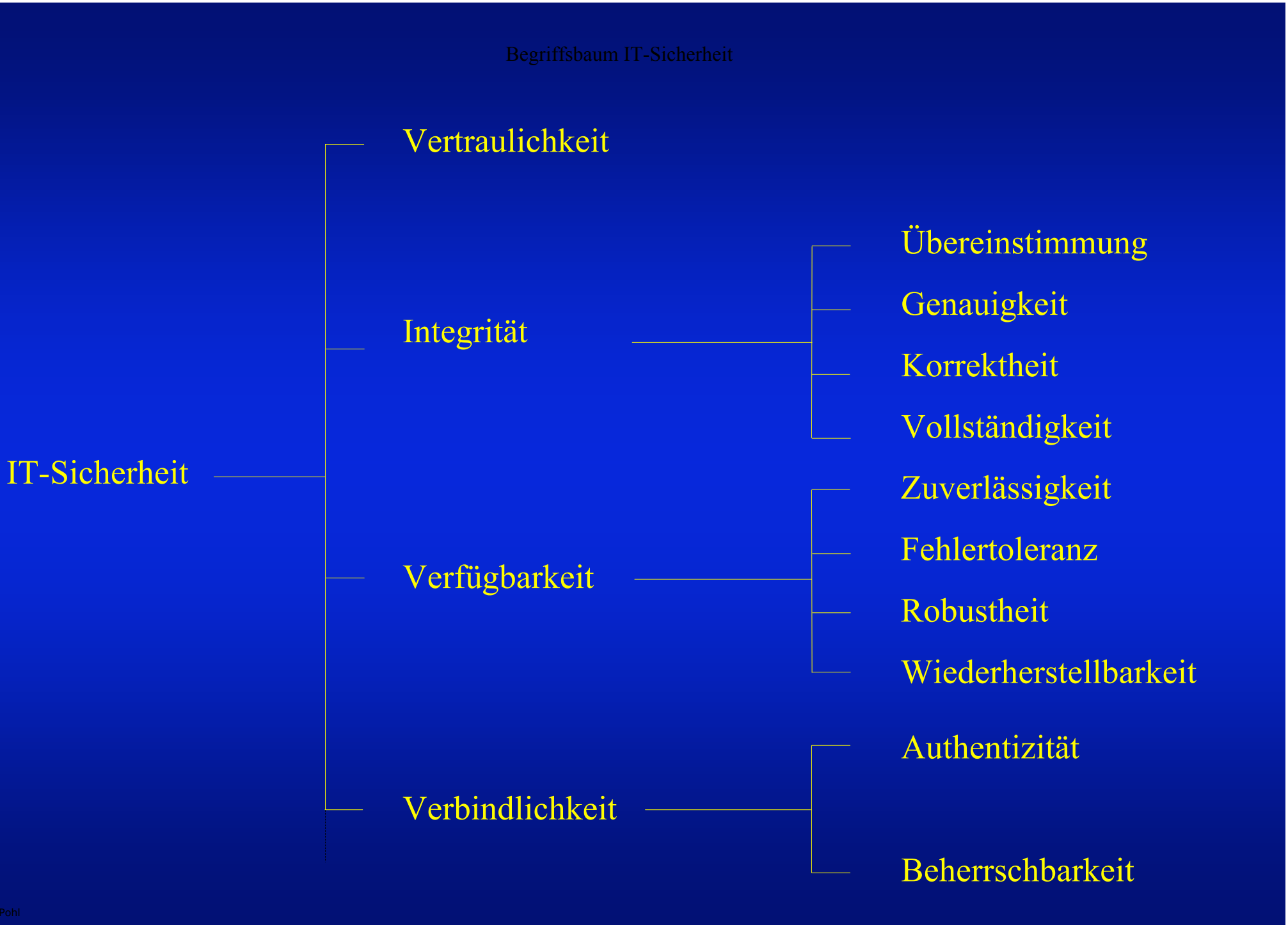
Laprie 1992, RFC 2828

# Organisatorische Sicherheit – administrative security

Organisatorische Verfahren und Regelungen zur Verhinderung unberechtigter Zugriffe.

RFC 2828

Begriffsbaum IT-Sicherheit



# Zuverlässigkeit – reliability

Funktionsfähigkeit

Zustand eines IT-Systems
vorgegebenen Anforderungen innerhalb vorgegebener Grenzen zu genügen
– das Leistungsniveau unter festgelegten Bedingungen über einen festgelegten Zeitraum zu bewahren.

**Mechanismen**:

- **Reife**: Eigenschaft geringer Versagenshäufigkeit durch Fehlerzustände.
- **Wiederherstellbarkeit**: Eigenschaft bei Versagen das Leistungsniveau wiederherzustellen und die direkt betroffenen Daten wiederzugewinnen.



NTG 3004, DIN 40 041, ISO/IEC 9126, RFC 2828

# Fehlertoleranz – fault tolerance

Eigenschaft eines IT-Systems mit einer begrenzten Zahl fehlerhafter Subsysteme seine spezifische Funktion zu erfüllen.



Laprie 1992

# Robustheit – robustness

Eigenschaft eines Systems,
eine bestimmte Mindestmenge an Funktionen der Gesamtfunktionalität abzuwickeln.

# Wiederherstellbarkeit – recovery

Eigenschaft eines Systems,
von fehlerhafter zu korrekter Leistungserbringung zu gelangen
und die betroffenen Daten wiederzugewinnen.



Laprie 1992

# Authentizität – authenticity

Integres Objekt.

Eigenschaft eines Systems echt, unverfälscht und verifizierbar zu sein.

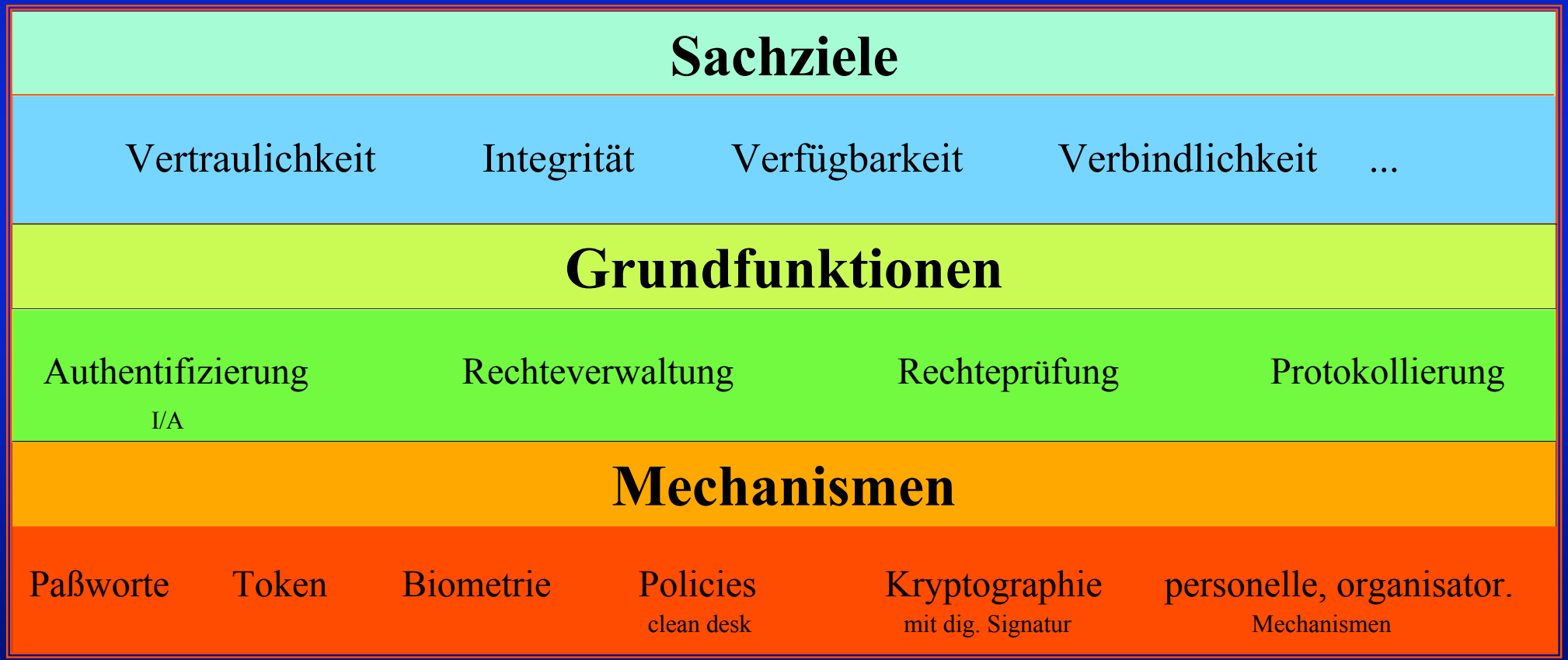
ISO/IEC 2382-08, HL7, GPKA, ISO/IEC 10181-2

# Beherrschbarkeit – governance

- Steuerbarkeit (controllability).
- **Handlungsfolgen** (eindeutig) identifizierbar.
- Zurechenbarkeit (accountability) der ergriffenen Aktionen.

# Inhaltsverzeichnis

# 3-Schichtenmodell der Informationssicherheit



# Grundfunktionen sicherer Systeme

Zur Erreichung von Sachzielen notwendige Funktionen

- Identifizierung und Authentifizierung
- Rechteverwaltung
- Rechteprüfung
- Beweissicherung/Protokollierung

---

- Überdeckungsfreiheit [Zusatzforderung der Wirtschaftlichkeit]

# Authentifizierung – authentication

**Überprüfung und Bestätigung einer behaupteten Integrität eines Objekts**.

Das Objekt kann ein Benutzer, eine Nachricht, ein Dokument sein.

Authentifizieren: Die behauptete Integrität eines Objekts überprüfen und bestätigen.

ISO/IEC 2382-08

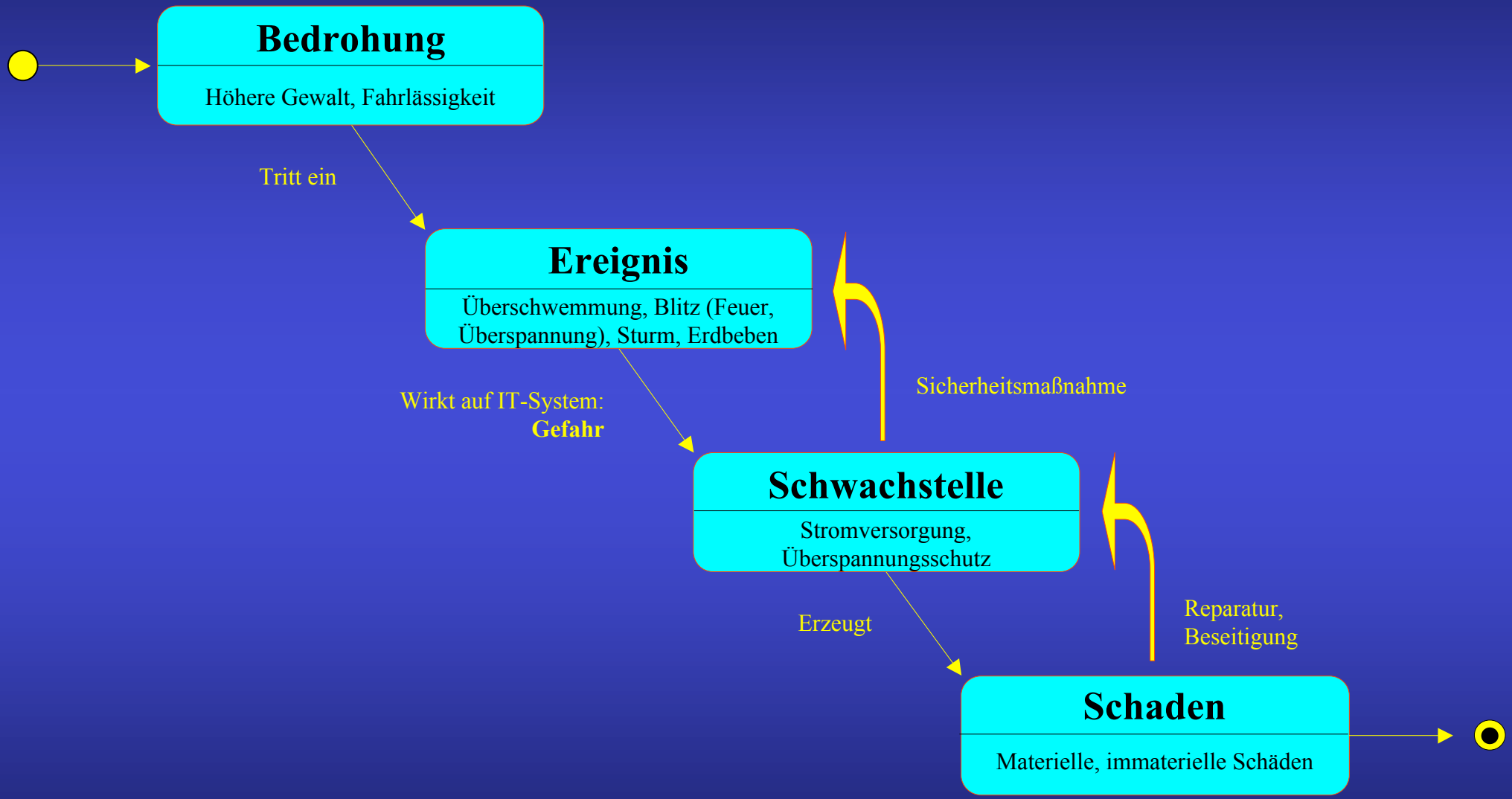
# Sicherheitsmechanismen

Zur Erreichung der Grundfunktionen

- Paßworte
- Token
- Biometrie
- Policies
- Kryptographie
- Digitale Signatur
- Personelle: Kontrollen, Überprüfung, ...
- Organisatorische: Clean desk, ...

# Inhaltsverzeichnis

# Höhere Gewalt/Schadenmodell



# Bedrohung – threat

Mögliche unberechtigte Aktivitäten und Ereignisse,
die ein IT-System negativ beeinflussen können.

ISSO 1996, ISO/IEC 2382-08, HL7, ISO 7498-2, TR 13335-1, RFC 2828

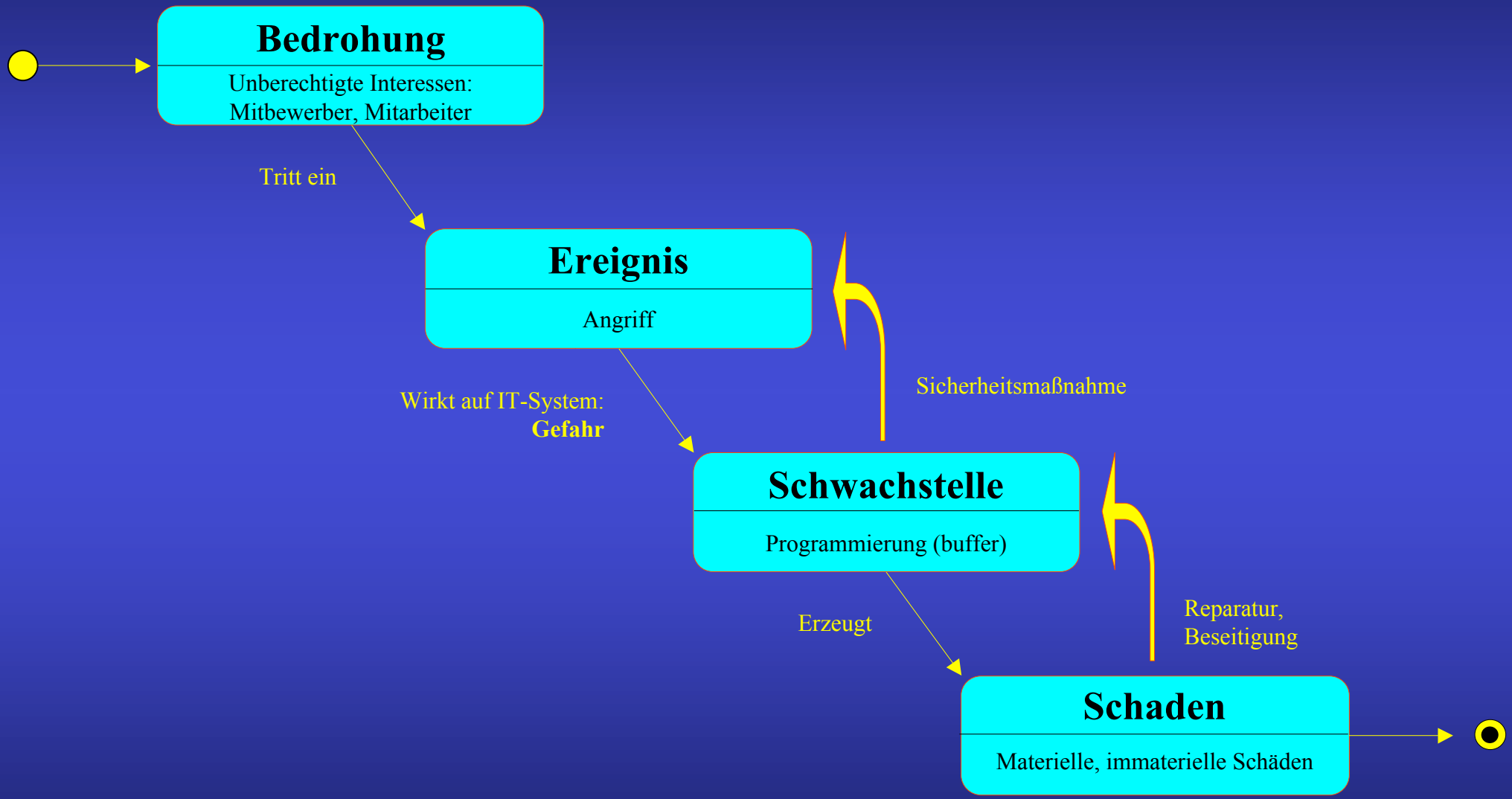
Ursache für ein unerwünschtes Ereignis.

ISO/IEC 1996

# Gefahr – danger

Eintritt eines – sich gegen eine mögliche Schwachstelle richtendes – Ereigniss.

# Angriffs-/Schadenmodell

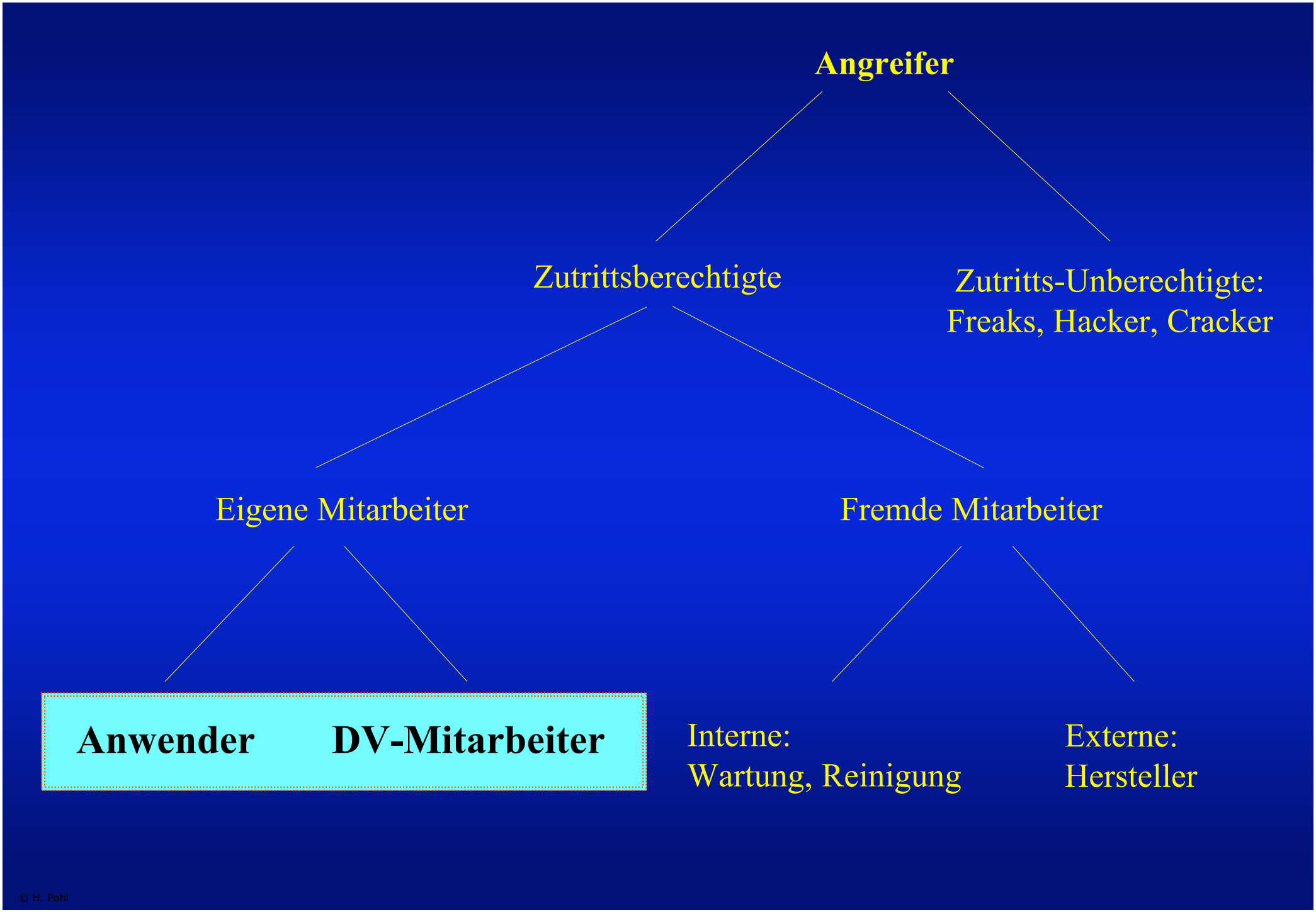


# Angriff – attack

Versuchte oder gelungene Verletzung der Sicherheit.

Der Erfolg eines Angriffs hängt dabei ab von der Angriffsstärke,
der Qualität der Verwundbarkeit und der Wirksamkeit von Gegenmaßnahmen.

ISO/IEC 2382-08

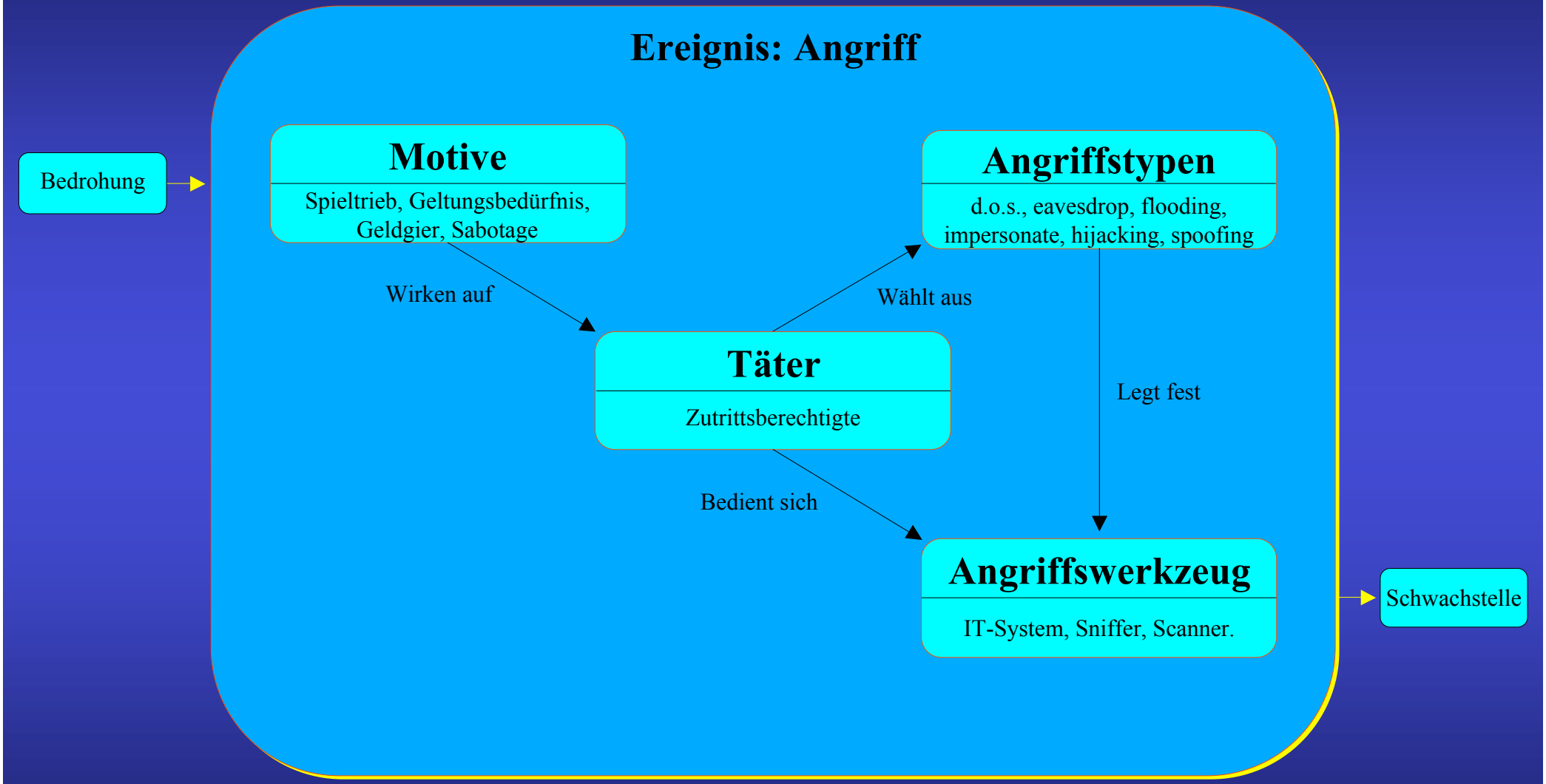

Angreifer
Zutrittsberechtigte
Zutritts-Unberechtigte:
Freaks, Hacker, Cracker
Eigene Mitarbeiter
Fremde Mitarbeiter
Anwender
DV-Mitarbeiter
Interne:
Wartung, Reinigung
Externe:
Hersteller

# Schwachstelle, Verwundbarkeit – vulnerability, weakness

Sicherheitsrelevanter Fehler eines IT-Systems – speziell eines Mechanismus.

RFC 2828

# Angriffsmodell

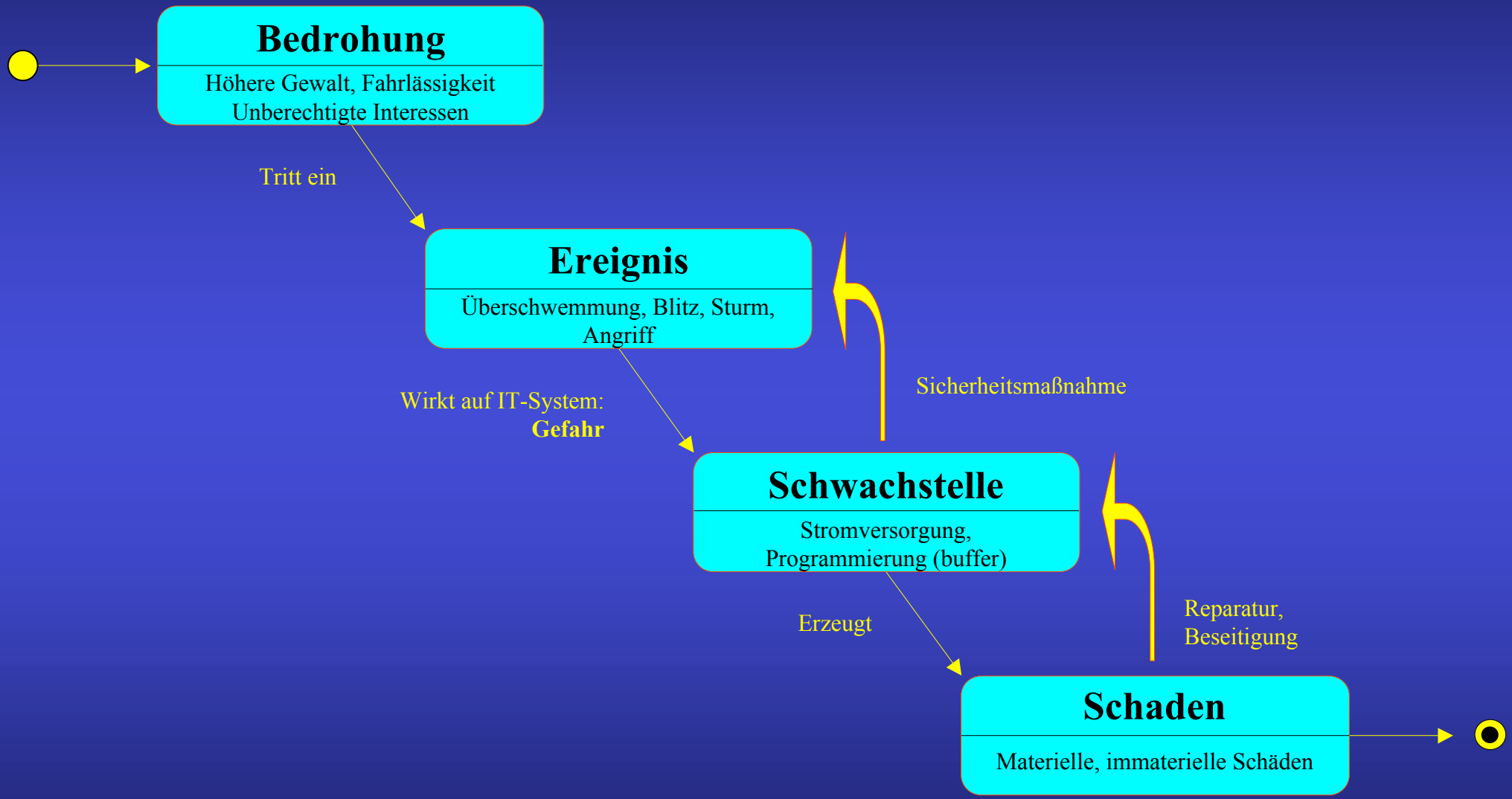


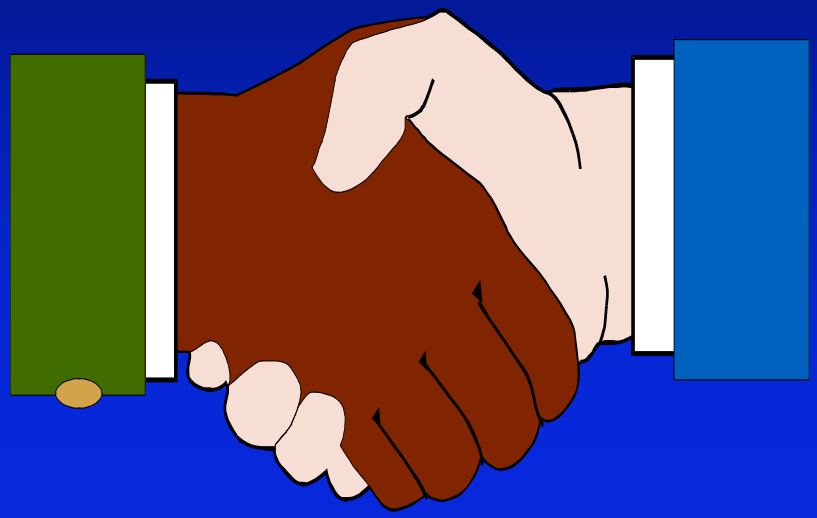
# Angriffswerkzeug – attack tool

Methoden und Werkzeuge zur Ausnutzung einer Schwachstelle eines Systems.

ISSO 1996, ISO/IEC 15408

# Generisches Bedrohungs-/Schadenmodell





# Gemeinsame Weiterarbeit

beim Aufbau einer (deutschen) Safety/Security Taxonomie?