Technische Universität
Kaiserslautern

0101seda010100

software engineering dependability

# Integrierte Sicherheitsanalyse komplexer Syteme

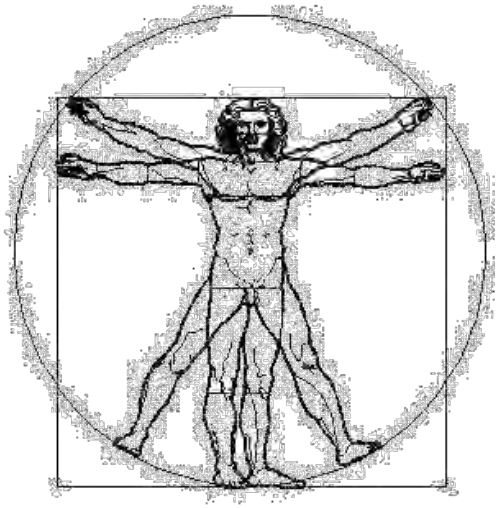
**Michael Roth, Max Steiner, Peter Liggesmeyer**

**TU Kaiserslautern**

# Agenda

- Motivation/Problem
- Standardisierte Safety und Security Analyse
- Integrierte Safety und Security Analyse
  - Systemmodellierung
  - Angreifermodellierung
  - Qualitative Analyse
  - Quantitative Analyse
- Evaluation
- Ausblick

# Motivation



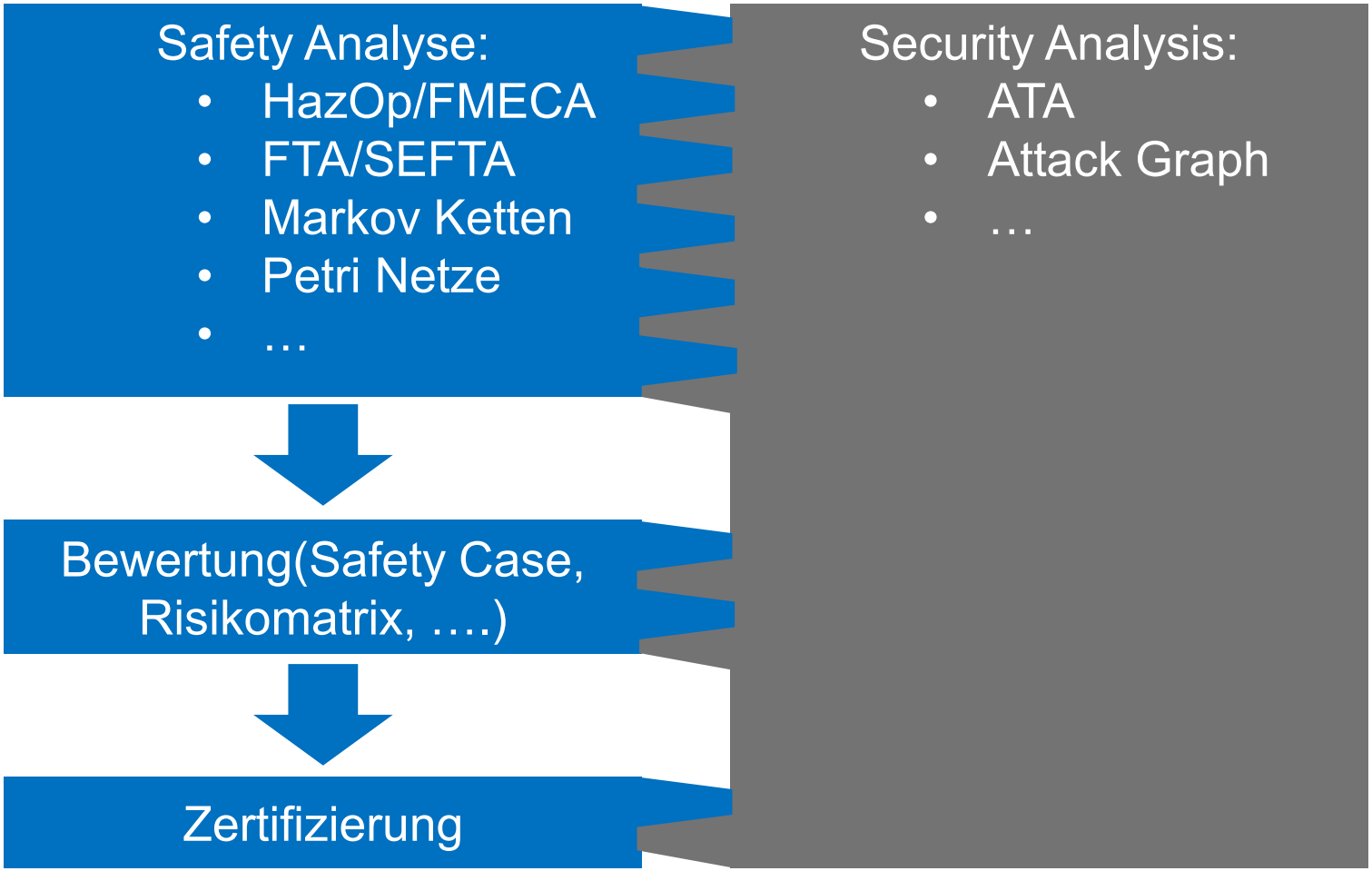
failures

Embedded System

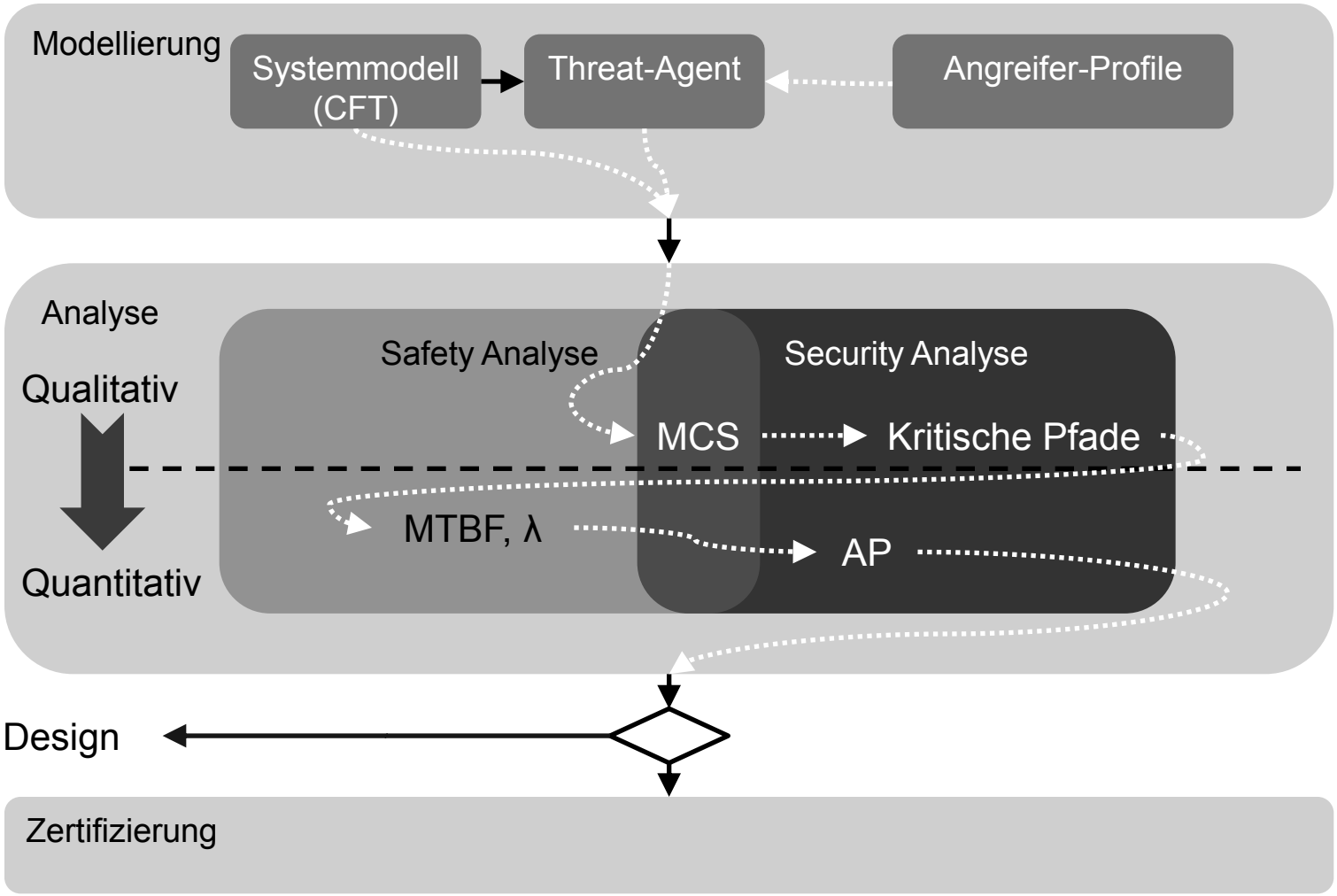
attacks

Network

# Standardisierte Safety und Security Analyse

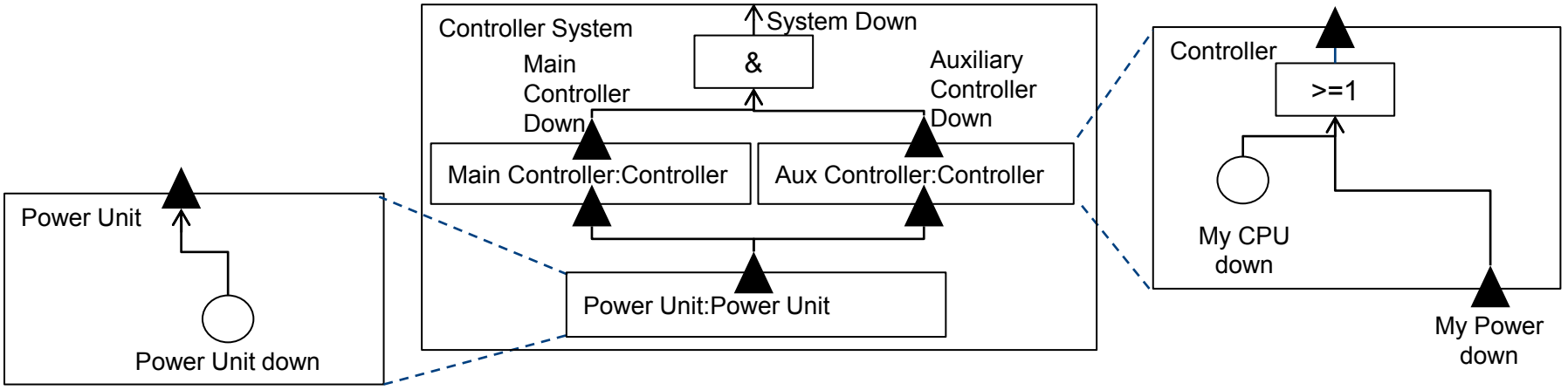


# Integrierte Safety- und Security Analyse



# Modellierung – System

- Qualitatives Modell in Baumstruktur (ähnlich Fault-Trees)
  - Komponentenkonzept (CFTs) (*






* Kaiser, Liggesmeyer, Mäckel: A new component concept for Fault Trees, 2003

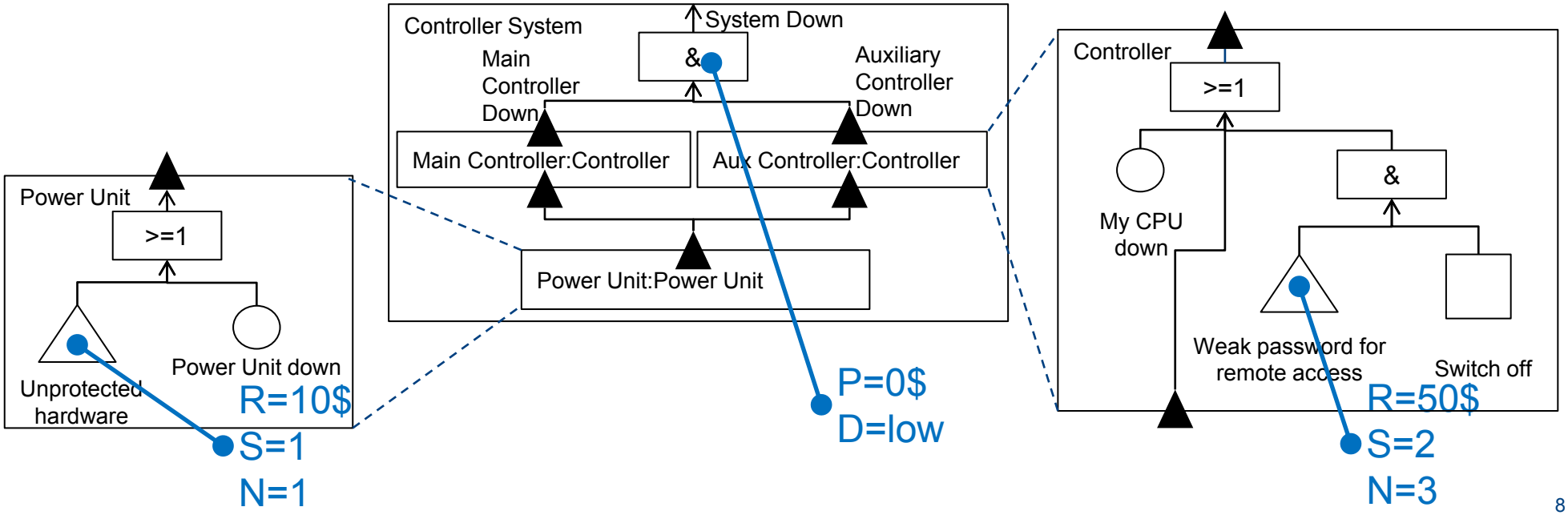
# Modellierung – System

- Qualitatives Modell in Baumstruktur (ähnlich Fault-Trees)
  - Komponentenkonzept (CFTs)
  - Unterscheidung der Basis-Ereignisse

| | Darstellung Basis-Ereignisse | MCS Darstellung |
|---|---|---|
| Ausfall |  | (…) |
| Schwachstelle (im Sinne von Security) |  | /…\ |
| Angriff |  | <…> |
| Annahme |  | […] |

# Modellierung – System

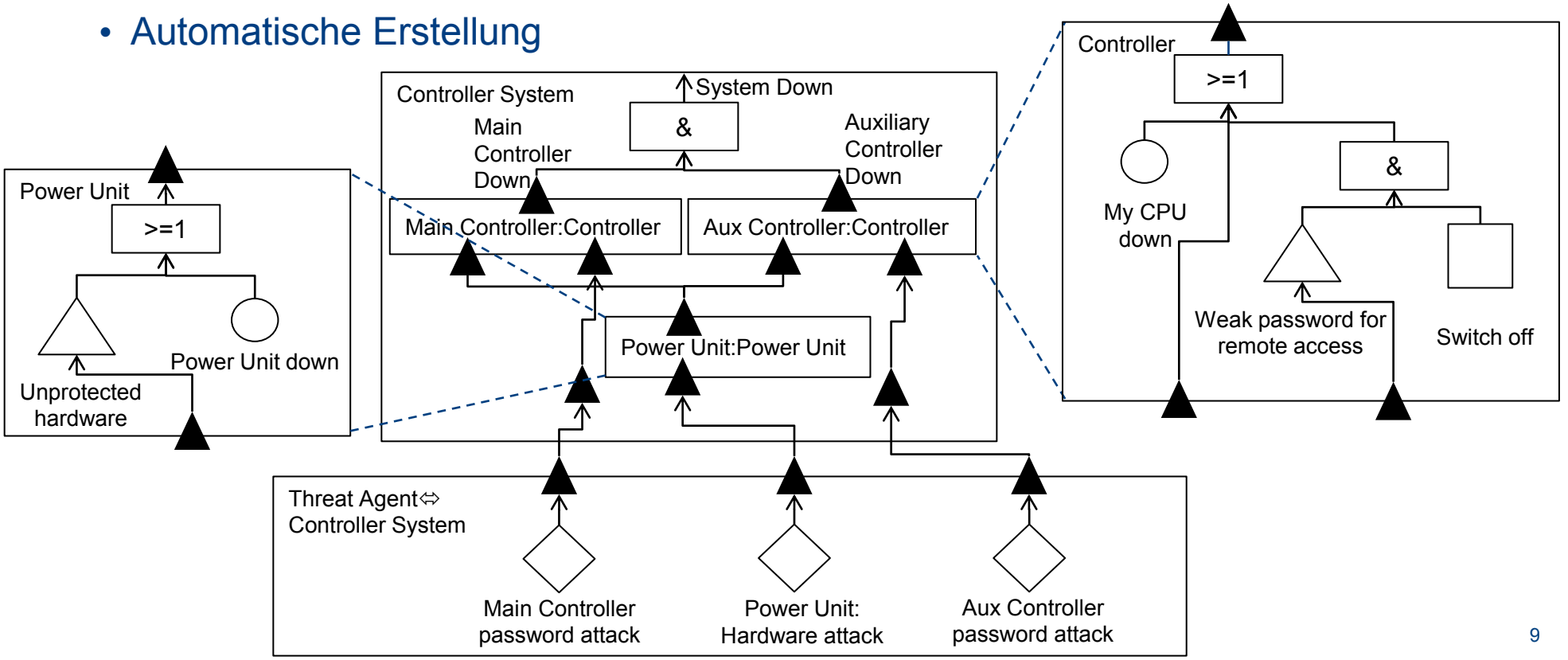
- Qualitatives Modell in Baumstruktur (ähnlich Fault-Trees)
  - Komponentenkonzept (CFTs)
  - Unterscheidung der Basis-Ereignisse
  - Ausgehend vom Safety-Modell werden Schwachstellen modelliert
  - Erweiterung des System-Modells um zusätzliche Kontextinformationen



# Modellierung – Angreifer-Komponente (Threat-Agent)

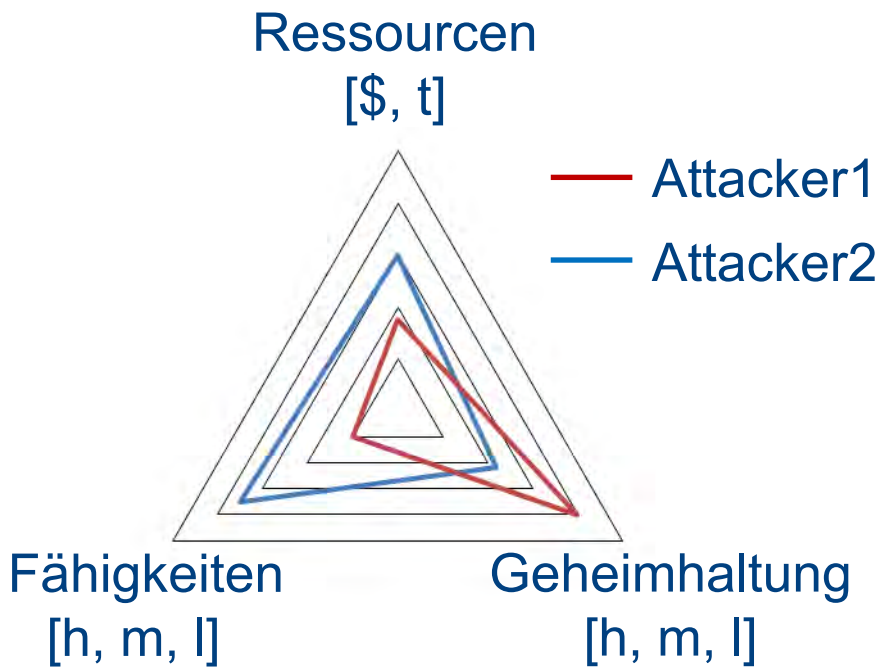
- Enthält die Angriffe, die auf das System durchgeführt werden können
  - Angreifer-Komponente befindet sich auf gleicher Hierarchieebene wie das betrachtete System

  → **Angriffe können nur von außen auf ein System einwirken**
- Fügt sich harmonisch in Komponenten-Fehlerbaum ein
- Automatische Erstellung



# Modellierung – Angreifer-Profil

- Spiegelt Eigenschaften eines Angreifers wieder
- $\mathcal{A}$*(Resource, Skills, Non-Noticeability, Relations)*



# Modellierung – Angreifer-Profil

- Spiegelt Eigenschaften eines Angreifers wieder
- $\mathcal{A}$*(Resource, Skills, Non-Noticeability, Relations)*
- Relationen: $\mathcal{R}$*(Resources, Profit, Non-Noticeability)*

Korrelationsmatrix ($C$) → Präferenz verschiedener Eigenschaften

Angreifer= Hacker (R = low; S = medium; N = ??)
Korrelationen könnten wie folgt aussehen:

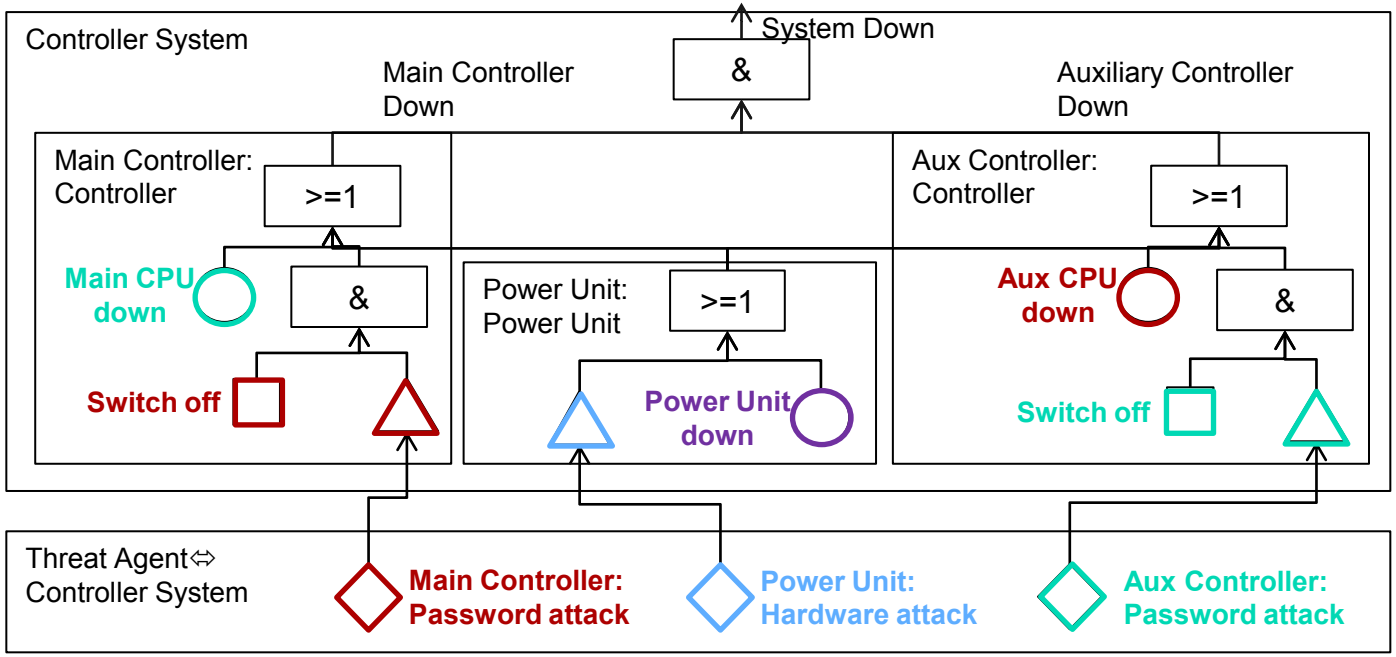
- Save resources is less important than make profit
- Non-Noticeability is much more important than save resources
- Non-Noticeability is less important than make profit

$$C_H = \begin{array}{c} \\ R \\ P \\ N \end{array} \begin{array}{c} \begin{array}{ccc} R & P & N \end{array} \\ \begin{bmatrix} 1 & 1/3 & 1/7 \\ 3 & 1 & 3 \\ 7 & 1/3 & 1 \end{bmatrix} \end{array}$$

- Kontextinformation + $\mathcal{A}$ () → Spezialisierung der Angreifer-Komponente

# Qualitative Analyse – MCS

- Domänenübergreifende Safety und Security Analyse
  - Minimal Cut Set Analyse




<AuxController:Password attack>
[AuxController:Switch off]
(MainContoller:CPU down)

<MainController:Password attack>
[MainController:Switch off]
(AuxController:CPU down)

<PowerUnit:Hardware attack>

(PowerUnit:Power Unit down)

<MainController:Password attack>
[MainController:Switch off]
<AuxController:Password attack>
[AuxController:Switch off]

(Main CPU down)
(Aux CPU down)

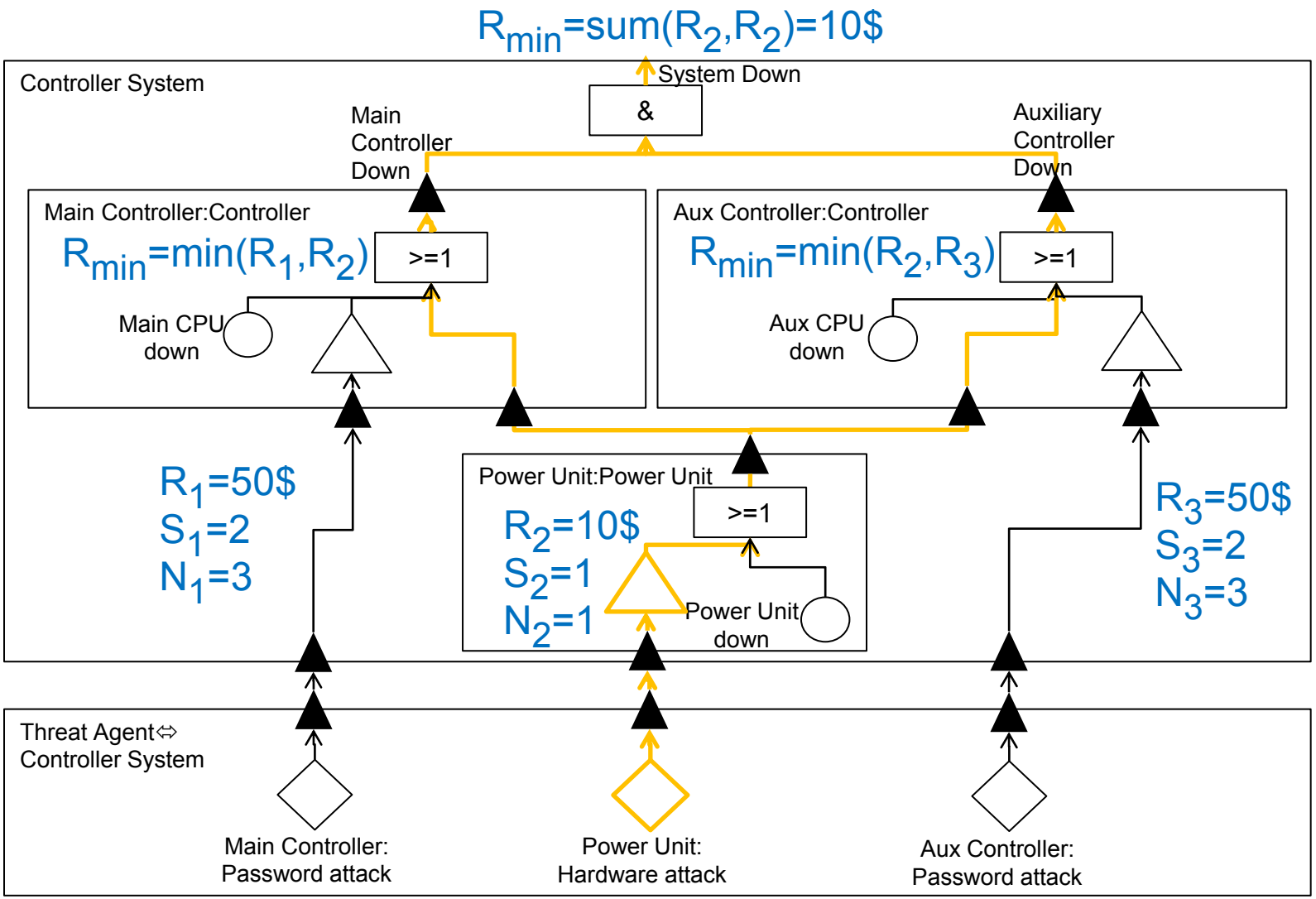
→ Zusammenhänge von Ausfällen und Angriffen können auf einen Blick wahrgenommen werden

# Qualitative Analyse – Security

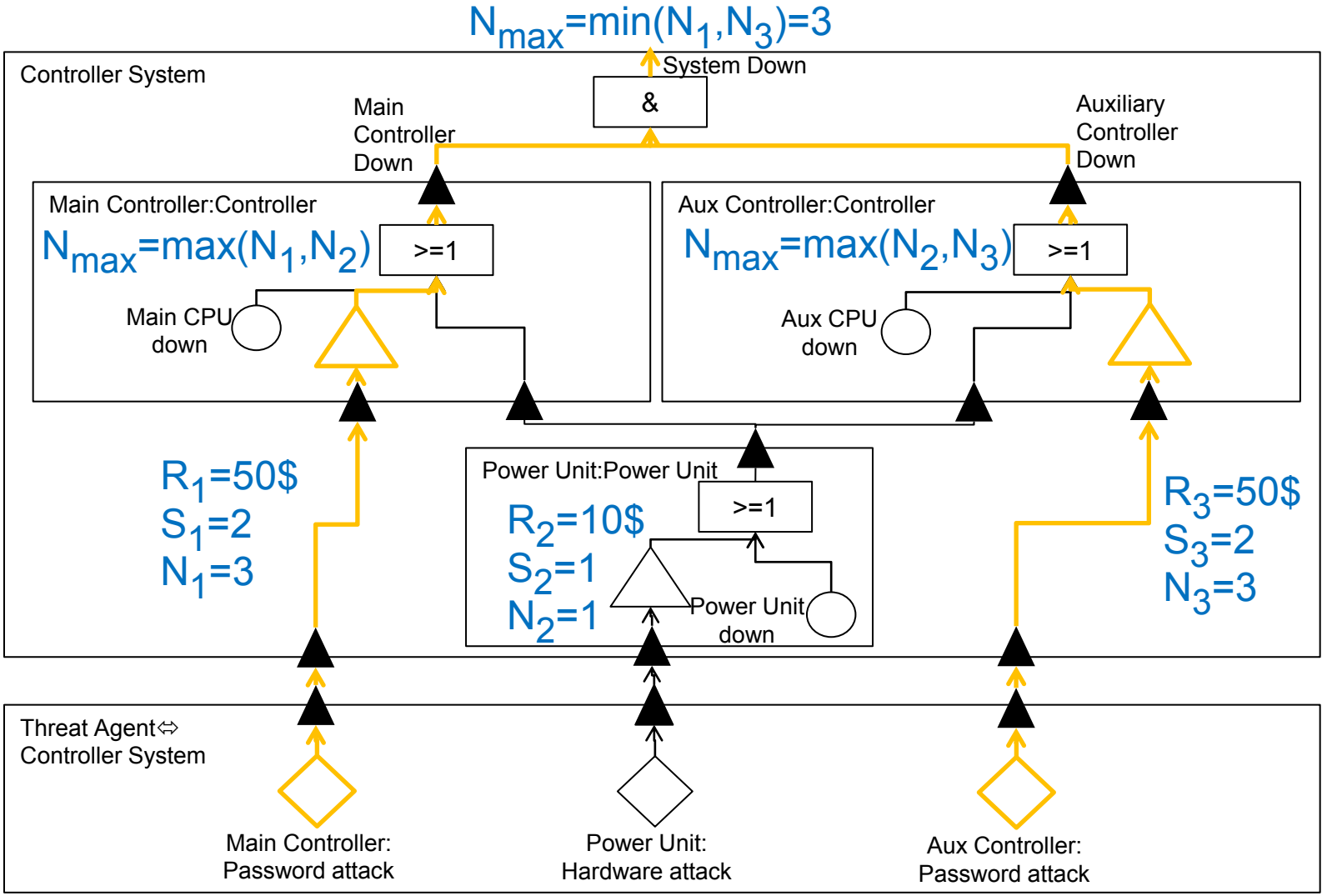
- Qualitative Security Analyse aus System Sicht
- Analyse der kritischen Pfade (minimale Kosten für Angriffe, minimale Fähigkeiten des Angreifers, …)

| | UND | ODER |
|---|---|---|
| **Minimale Ressourcen ($R_{min}$)** | $R_{min}=add(R_1,\ldots,R_n)$ | $R_{min}=min(R_1,\ldots,R_n)$ |
| **Minimale Fähigkeiten ($S_{min}$)** | $S_{min}=max(S_1,\ldots,S_n)$ | $S_{min}=min(S_1,\ldots,S_n)$ |
| **Minimale Wahrnehmbarkeit ($N_{max}$)** | $N_{max}=min(N_1,\ldots,N_n)$ | $N_{max}=max(N_1,\ldots,N_n)$ |

# Qualitative Analyse – Kritischer Pfad R



# Qualitative Analyse – Kritischer Pfad N



# Quantitative Analyse – Ausfallanalyse

- UND-Gatter: $P_{out} = \prod_{i=1}^{n} P_i$
- ODER-Gatter: $P_{out} = 1 - \prod_{i=1}^{n} (1 - P_i)$
- Ausfallanalyse (Wahrscheinlichkeitsbasierend)

→ Standardisiertes Verfahren eingebettet in integrierter Analyse
→ Etablierte Prozesse können unverändert abgearbeitet werden

Bestimmung der Eintrittswahrscheinlichkeit:

- Korrelationsmatrix → Prioritätsvektor
- Priorisierung der Eigenschaften eines Angreifers
  → Hilfe zur genaueren quantitativen Analyse

$$C = \begin{bmatrix} c_{11} & \cdots & c_{13} \\ \vdots & \ddots & \vdots \\ c_{31} & \cdots & c_{33} \end{bmatrix} \qquad p_i = \frac{1}{3} \sum_{j=1}^{3} \frac{c_{ij}}{\sum_{k=1}^{3} c_{kj}}; i = 1,2,3 \qquad \vec{p} = \begin{bmatrix} p_R \\ p_P \\ p_N \end{bmatrix} mit \quad p_r + p_p + p_N = 1$$

Bestimmung der Eintrittswahrscheinlichkeit:

- Korrelationsmatrix → Prioritätsvektor
- Priorisierung der Eigenschaften eines Angreifers
  → Hilfe zur genaueren quantitativen Analyse
- MCS Angriffe kumulieren und normalisieren → Angriffsmatrix

$$r_{MCSi} = add(r_1 \ldots r_k);$$
$$p_{MCSi} = add(p_1 \ldots p_k);$$
$$n_{MCSi} = \min(n_1 \ldots n_k)$$

$$\Rightarrow \quad r_{MCSi} = 1 - \frac{r_{MCSi}}{\sum_{k=1}^{m} r_{MCSk}};$$

$$p_{MCSi} = \frac{p_{MSCi}}{\sum_{k=1}^{m} p_{MCSk}}$$

$$n_{MCSi} = \frac{n_{MCSi}}{\sum_{k=1}^{m} n_{MCSk}}$$

$$\Rightarrow \quad A = \begin{bmatrix} r_{MCS1} & \cdots & r_{MCSm} \\ p_{MCS1} & \cdots & p_{MCSm} \\ n_{MCS1} & \cdots & n_{MCSm} \end{bmatrix} = \begin{bmatrix} \vec{r} \\ \vec{p} \\ \vec{n} \end{bmatrix}$$

- Angriffsmatrix & Prioritätsvektor → Angriffs-Prioritätenvektor

$$\vec{a} = A^T \cdot \vec{p}$$

- MCS1: <AuxController:Password attack>; [AuxController:Switch off]; (MainController:CPU down)
- MCS2: <MainController:Password attack>; [MainController:Switch off]; (AuxController:CPU down)
- MCS3: <PowerUnit:Hardware attack>
- MCS4: …

$$C_H = \begin{bmatrix} 1 & 1/3 & 1/7 \\ 3 & 1 & 3 \\ 7 & 1/3 & 1 \end{bmatrix} \quad \vec{p} = \begin{bmatrix} p_R \\ p_P \\ p_N \end{bmatrix} \quad A = \begin{bmatrix} 50 & 50 & 10 & \dots \\ 0 & 0 & 0 & \dots \\ 3 & 3 & 1 & \dots \end{bmatrix} \quad \vec{a} = \begin{bmatrix} 0{,}21 \\ 0{,}21 \\ 0{,}14 \\ \vdots \end{bmatrix}$$

# Quantitative Analyse – Domänenüberg. Analyse

- MCS Ergebnis Tupel
- $\mathcal{MCS}_i(P_{MSCi}, R_{MCSi})$ mit $i=1, \ldots, n$ (*

$$P_{MCSi} = \prod_{i=1}^{n} P_i$$

$$R_{MCSi} = a(i)$$



* Förster, Schwarz, Steiner: Integration of Modular Safety and Security Models for the Analysis of the Impact of Security on Safety, 2010

# Evaluation – RAVON

# Ausblick

- Verbessern des Verfahrens zur domänenübergreifenden quantiativen Analyse
- Ausarbeiten eines Konzepts zur effizienten Modellierung der Bäume
- Ausarbeiten von Pattern zu schnelleren Erstellung von Bäumen
- Toolsupport zur effizienteren Erstellung und Verwaltung komplexer Angreifer Profile
- Weitere Evaluation anhand Ravon

Technische Universität
Kaiserslautern

0101seda010100

software engineering dependability

# Integrierte Sicherheitsanalyse komplexer Syteme

**Michael Roth, Max Steiner, Peter Liggesmeyer**

**TU Kaiserslautern**