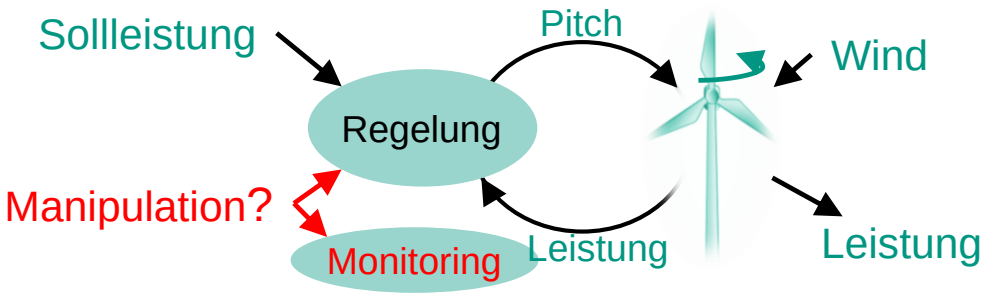
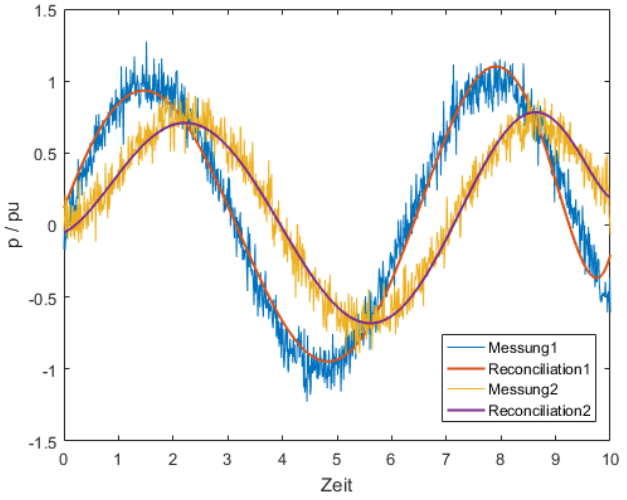
Karlsruher Institut für Technologie

IT-Sicherheit für die vernetzten cyber-physikalischen Komponenten zukünftiger Energiesysteme

Kathrin Reibelt

Institut für Angewandte Informatik (IAI), Gruppe ProSys





Motivation - Energiewende

Wenige große, zentrale Kraftwerke
⇨ Steuerung vor Ort

Viele kleine, verteilte Kraftwerke
⇨ Remotesteuerung

Kontinuierliche Verfügbarkeit
⇨ Statisches Stromnetz

Stark schwankende Verfügbarkeit
⇨ Flexible Netzstruktur mit steuerbaren Elementen wie Transformatoren, Umformer usw.

Sicherheit,
auch für informationstechnische Komponenten,
basierend auf physischen Zugriffsbeschränkungen

Gefährdung
durch Steuerung über unsichere Netzwerke mit zahlreichen Zugriffspunkten
Unabhängiger informations-technischer Schutz erforderlich!

Mögliche Ziele von IT-Manipulationen

Drosselung der Anlage

EEG §9:

(1) Anlagenbetreiber und Betreiber von KWK-Anlagen müssen ihre Anlagen mit einer installierten Leistung von mehr als 100 Kilowatt *(30 KW bei Solaranlagen)* mit technischen Einrichtungen ausstatten, mit denen der Netzbetreiber jederzeit

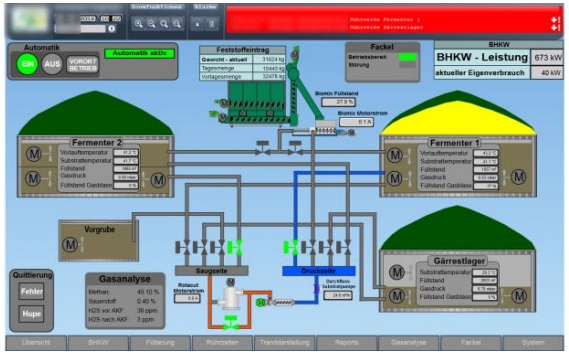
1. die Einspeiseleistung bei Netzüberlastung ferngesteuert reduzieren kann und
2. die Ist-Einspeisung abrufen kann

Thermische Belastungen

Kieler Nachrichten 2017

Neue Presse 2010

Fehlverhalten der internen Regelkreise



Golem.de 2016

Ansprechen der Anlagen-sicherung

U	+10%	-25%	0,1 s
ΔU	+5,5%	-5,5%	0,2 s
I	+10%		0,2 s
I	+900%		0 s
ΔI	+44%	-44%	0,2 s
$W_{Generator}$	+2,5%	-2,5%	5 s

simulink

Mechanische Belastungen

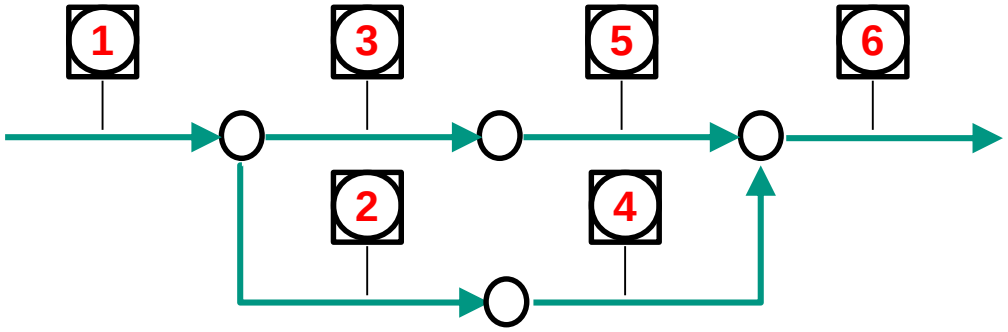
spiegel.de 2017

Sicherheitsmaßnahmen in Anlagen

- Intervalle für sicheren Betrieb — Kraftwerke
  - Vergleich der Messwerte mit vordefinierten Intervallen
- Redundante Messungen — Kernkraftwerke
- Parallele Simulation — Produktionsanlagen
  - Vergleich der Messwerte mit den Ergebnissen der Simulation
  - Vergleich der Abweichungen mit Mustern bekannter Fehler
- Data Reconciliation — Chemieanlagen
  - Reduzierung der statistischen Sensorfehler
  - Berechnung nicht direkt gemessener Größen
  - Detektion von Sensorausfällen
  - → Weiterentwicklung für Energiesysteme

Data Reconciliation: Verbesserung der Daten

- einfaches Beispiel:
  Kühlkreislauf



- Modell aus Zusammenhängen

$$A\vec{y} = \vec{0} \qquad \vec{y} = \begin{bmatrix} F_1 \\ \vdots \\ F_6 \end{bmatrix}$$

$$A = \begin{bmatrix} 1 & -1 & -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 & 1 & -1 \end{bmatrix}$$

- Wert mit der größten Wahrscheinlichkeit:

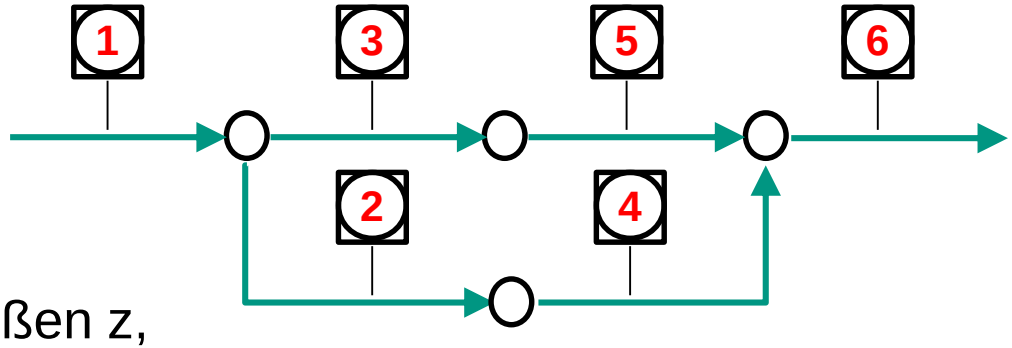
$$\hat{\vec{y}} = \left(\mathbf{1} - \boldsymbol{V}\boldsymbol{A}^T\left(\boldsymbol{A}\boldsymbol{V}\boldsymbol{A}^{\boldsymbol{T}}\right)^{-1}\boldsymbol{A}\right)\vec{y}$$

$$V = \begin{pmatrix} \sigma_1^2 & 0 & 0 \\ 0 & \sigma_2^2 & 0 \\ 0 & 0 & \ddots \end{pmatrix}$$

(Berechnung über Lagrange-Variation)

Data Reconciliation: Berechnung von Größen

- einfaches Beispiel:
  Kühlkreislauf



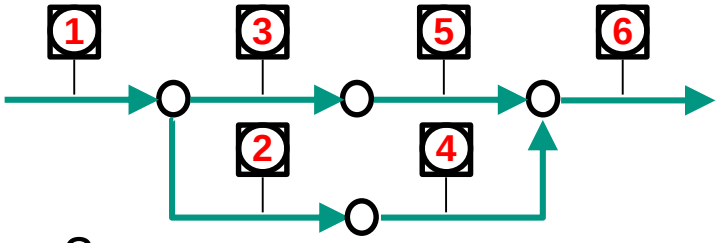
- nicht direkt gemessene Größen z,

$$A_y\vec{y} + A_z\vec{z} = \vec{0} \qquad \vec{z} = P\vec{y}$$

Beispiel 2, 4, 6 ungemessen

$$\boldsymbol{A_y} = \begin{bmatrix} 1 & -1 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{bmatrix} \quad \boldsymbol{A_z} = \begin{bmatrix} -1 & 0 & 0 \\ 1 & -1 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & -1 \end{bmatrix} \Rightarrow \quad \boldsymbol{P} = \begin{bmatrix} 1 & -0.5 & -0.5 \\ 1 & -0.5 & -0.5 \\ 1 & 0 & 0 \end{bmatrix}$$

Modellanalyse: Redundanz



- ist das System vollständig definiert?
- welche Größen sind beobachtbar?
- welche Größen werden redundant gemessen?
- welche Erweiterungen würden Sinn machen?

-1: nicht beobachtbar
0: beobachtbar
>0: redundant gemessen

gemessen: 1, 3, 5

0	0	1	0	1	0

gemessen : 2, 4

-1	1	-1	1	-1	-1

gemessen : 1, 2, 3, 5, 6

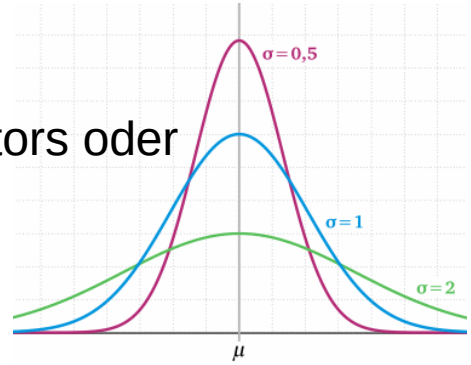
4	4	4	0	4	4

gemessen : 2

-1	0	-1	0	-1	-1

Fehlerdetektion

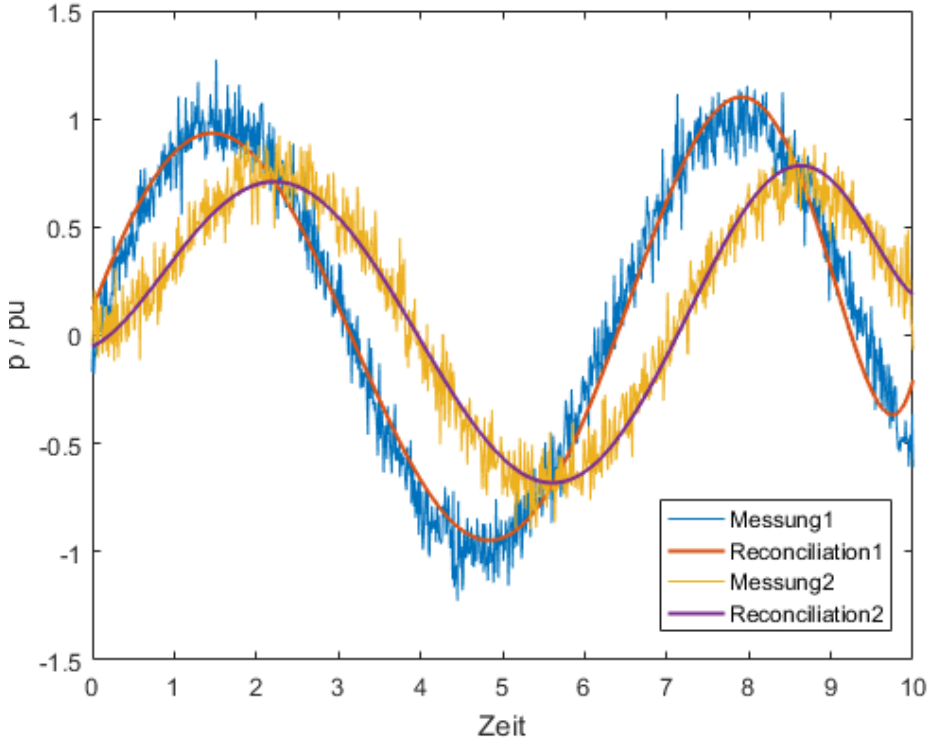
- Analyse der Verteilung der beobachteten Abweichungen
  - Differenz zwischen Messung und reconciliertem Wert geteilt durch die Verteilung des einzelnen Sensors/Aktors oder
  - Differenz geteilt durch Varianz (einzelne Größen oder Summe) oder
  - Residuen der Terme $A\vec{y} \; ! = \vec{0}$



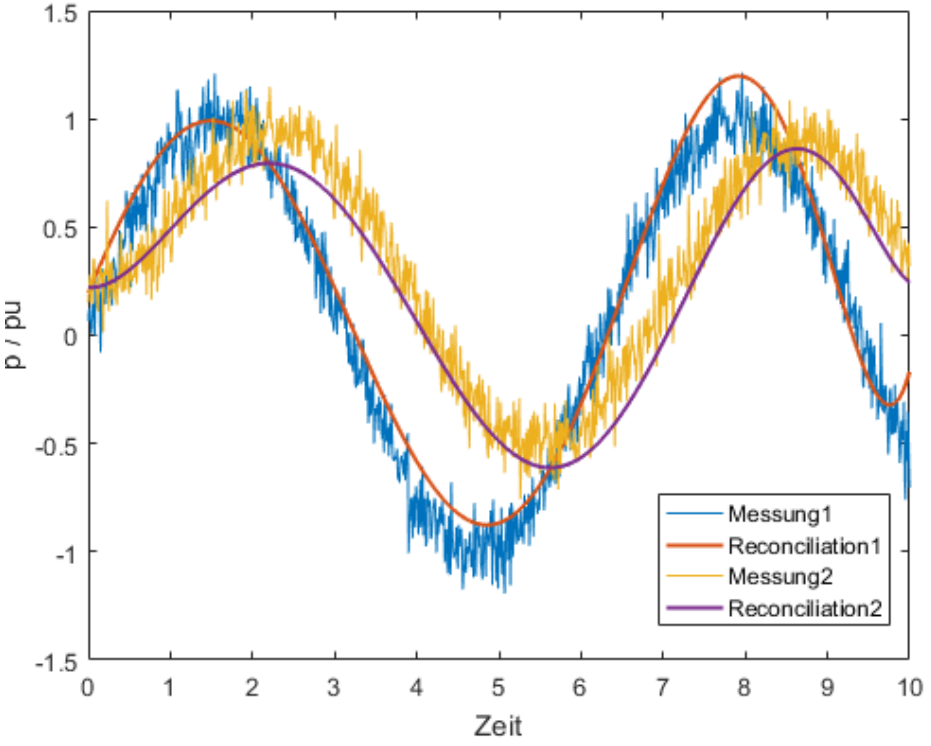
- Hypothesentest
  - kein Fehler $H_0 \colon \langle \vec{r}(t) \rangle = 0$
  - Fehler / Manipulation des Sensors / Aktors i $H_1^i \colon \langle \vec{r}(t) \rangle = b\vec{f_i}$

Beispiel Data Reconciliation

- Ohne Fehler



- Offset in Messung 2
  Verschiebung auch bei 1



Mehrfachfehlerdetektion

- Hypothesentests für Fehlerkombinationen
  - $H_1^{i1,i2,\ldots,ik}: \langle \vec{r}(t) \rangle = b_1 \overrightarrow{f_{i1}} + b_2 \overrightarrow{f_{i2}} + \cdots + b_k \overrightarrow{f_{ik}} = F_k \vec{b}$

- Sequentielle Methoden

  Die einfache Fehlerdetektion wird mehrfach angewendet

  - verdächtige Messung wird eliminiert (nicht berücksichtigt)
  - wahrscheinlichster Wert für die Abweichung wird berechnet und der Messwert angepasst

Erweiterung der Fehlerdetektionsmethoden für die Detektion von IT-basierten Manipulationen

- Zusatzinformationen zu den Parametern
  - Exposition (Zugänglichkeit für Manipulationen)
  - Gemeinsamkeiten / Diversität
  - Kritikalität
  - Bedeutung
- Anwendung
  - Analyse der Sicherheit und Resilienz des Systems
  - Schnelle Manipulationsdetektion durch sinnvolle Vorhersagen
  - Identifikation der korrumpierten Bestandteile / des Angriffswegs
  - Bewertung der Zuverlässigkeit der Kenntnis des Systemzustands
  - Auswahl sicherer Gegenmaßnahmen

Zusammenfassung

- Standardmaßnahmen der IT-Security sind nicht ausreichend
- Idee: Verwendung zusätzlicher Information über die physikalischen Vorgänge zur Manipulationsdetektion → Modellbasierte Ansätze
- Data Reconciliation und Fehlerdetektion
- Erweiterung für die Detektion von IT-Manipulationen

Ausblick

- Anwendung auf reale Energiesystemkomponenten
- Identifikation und Integration sinnvoller Zusatzinformationen