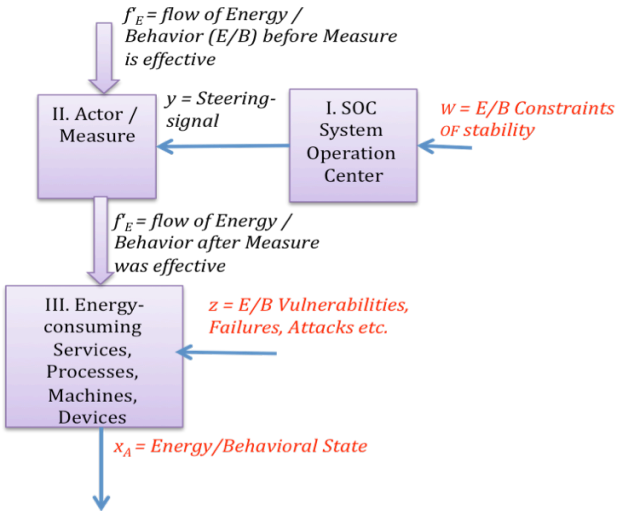
smartspacelab.eu
the Scientific Technology Enterprise

BEST Position Statement Nr.03, 12.12.2014
R2GS Germany c/o
ssl.eu GmbH, Berner Str. 21B,
12205 Berlin: demeer@smartspacelab.de

IT Energie & Sicherheit → Smart Community Modell - Steuerungs- und Kontroll-Maßnahmen von flächendeckenden Infrastrukturen in Unternehmen und Organisationen



Zusammenfassung: Wie in [BEST PS01] bereits beschrieben, wird *IT-Intelligenz* benötigt, um die Energie-Versorgung von Verbrauchern, wie z.B. viele kleine Haushalte, Geräte, Maschinen oder große Dienstleistungszentren etc., zu gewährleisten. Mit der Zunahme der Nutzung erneuerbarer (grüner) Energiequellen, nimmt aber auch die Instabilität der Energieversorgung zu, weil Wetter, Jahres-, Tag-und-Nacht-Zeiten, einflußnehmen auf die Energieerzeugung. Zur Stabilisierung der Energieversorgung benötigt man Informationen, die kontinuierlich, verläßliche Messwerte und Daten über den Zustand der Infrastrukturen, liefern. Diese sog. *ISI* Messwerte (*Information Security Indicator)* müssen zeitnah von einer leistungsfähigen *IT* aufgenommen und verarbeitet werden; indem sie die Zustände von Energie-Erzeugern, –Verbrauchern und –Übertragungskomponenten messen und sie einer Leitstelle, dem *Security Operation Center (SOC)*, zuleiten. Das SOC entscheidet über ggf. vorzunehmende Maßnahmen.

Der *IT E&S* -Maßnahmenkatalog für Unternehmen und Organisationen [BEST PS04] , fußt einerseits auf dem oben dargestellten Architekturmodell zur Energieflußsteuerung in dynamischen Herstellungs- oder Anwendungs-Prozessen und andererseits auf einer integrierten *smartspace*®[1] Infrastruktur, wie sie z.B. in *Smart City (SC), Smart Grid (SG), Smart Building (SB) etc.* vorkommen. Das Architekturmodell zur Energieflußsteuerung besteht aus folgenden Modell-Komponenten: I) Leitstellen/SOC, II) Maßnahmen-Aktoren/Stellglieder, III) Kritische Infrastruktur/Prozesse.

Leitstellen gibt es aber auch bei großen Verbrauchern, z.B. in Unternehmen, Organisationen oder Betreibern eines *Cloud Computing Zentrums.* Während Infrastruktur-Leitstellen für Stabilität des Energieflusses sorgen, nehmen die Verbraucherleitstellen die Aufgabe zur Effizienz der Energienutzung wahr. Alle Leitststellen sind untereinander, mit allen relevanten Geräten und allen Teilhabern einer flächendeckenden intelligenten IT [BEST PS01] verbunden.

Das zur Anschauung besonders geeignete Modell des Smart Grid (s. ‚Das Smart Grid Experiment DSGE' [10]) besteht aus 3 Komponenten: Der Leitstelle/SOC (I), den Akteuren und Stellgliedern zur Ausführung von Maßnahmen (II) für die Sicherheit und Effizienz und der Kritischen Infrastruktur, samt Hardware[2] und dynamischen Energie-Verteilungsvorgängen (III).

Die integrierte Leitstelle (s. R2GS[3]-Empfehlungen) lenkt das System anhand vorher festgelegter Stabilitätskriterien, mittels geeigneter Maßnahmen, um z.B. einen stabilen Stromfluß zwischen volatilen, nicht zur Gänze einschätzbaren Erzeugern und berechenbaren Verbrauchern [s. typisches Lastprofil nach Agüero et al] zu gewährleisten. Dabei hat die integrierte Leitstelle mit Störungen, z.B. aus der Volatilität grüner Energiequellen herrührend oder mit unerwünschten Ausgleichsvorgängen bei der Stromverteilung, zu rechnen.

Während im Strom-Netz *Energie-Effizienz* mittels Kontrolle der Stabilität des Energieverteilungsprozesses erreicht wird, wird in einem großen Verbraucher, z.B. Cloud Datenzentrum, Energie-Effizienz über die Minimierung des Verbrauchs bei gleichzeitiger Optimierung des grünen Energieanteils definiert. *Energie-Effizienz* hat also zusammen mit den grundsätzlichen IT-Sicherheitsanforderungen, folgende zusätzlichen 4 Bedeutungen:

Schutz gegen Informationsverfälschungen[4] *+ Versorgungsstabilität + minimaler Verbrauch + hoher grüner Energieanteil.*

---

[1] Eingetragene Marke DPMA Nr. 306 57 410

[2] Z.B. benötigt man für ein Energie-Verteilungsnetz verlustarme HGÜ-Trassen, sog. Hochspannungs-Gleichstrom-Übertragungsleitungen, die z.B. in Deutschland den erzeugungsstarken Norden mit dem verbrauchsintensiven Süden verbinden; Wechselstromleitung sind über lange Distanzen, nicht so leistungsfähig wie HGÜs.

[3] R2GS **'Recherche et Réflexion en Gestion opérationnelle de la Sécurité'**, s. http://www.school-of-technology.de/7.html

[4] Schutz gegen Informationsverfälschungen umfassen folgende Maßnahmen: *Confidentiality – Integrity – Authenticity* (Geheimhaltung – Unverfälschbarkeit – Authentizität)