WELCHES SMART GRID?

DASS COMPUTER FÜR DEN HOCHDYNAMISCHEN ERNEUERBAREN ENERGIEMIX DER ZUKUNFT WICHTIG SEIN WERDEN, IST UNUMSTRITTEN. DOCH WELCHE RAHMENBEDINGUNGEN SOLLTEN DAS „SMART GRID“ FORMEN?

Über die wirklich wichtigen Dinge will man meistens gar nicht reden, weil sie entweder zu kompliziert oder zu deprimierend sind. Wer will sich schon über Mangel, Probleme, Gefahren oder zukünftige Krisen Gedanken machen. Jeder Umweltschutzverband lernt schnell, dass man mit negativen Themen – egal wie wichtig diese sind – nur wenige Leute motivieren kann. Die Risiken eines auf bedingungslosen Wachstum fokusierten Wirtschafts- und Finanzsystems sind schon seit mindestens 100 Jahren bekannt. Der Zusammenbruch der Erdölproduktion wurde in seiner Struktur vor über 50 Jahren beschrieben und auch die Megakrisen „Klimawandel“ oder „Atommüll“ sind keine Neuentdeckungen dieses Jahrtausends. Leider alles zu deprimierend für eine ernsthafte Debatte. „Uns wird schon etwas einfallen, wenn es dann soweit ist“, ist die gängige Denkweise.

Was lernt man aus Fukushima?

Wenn es dann jedoch so weit ist, stellt man in der Regel fest, dass einem meist nichts einfällt oder man schlichtweg handlungsunfähig geworden ist.

Das Reaktorunglück von Fukushima hat zwar als Rechtfertigung für eine nicht sonderlich ernst gemeinte Energiewende gute Dienste geleistet, aber eine wirkliche Diskussion über die Ereignisse in Fukushima will man eher nicht führen. Die beiden großen Katastrophen „Flutwelle“ und „Kernschmelze“ haben es immerhin geschafft, ein bisschen Aufmerksamkeit auf sich zu ziehen. Doch auch die vielen kleinen Folgekatastrophen sollten wir ernsthaft analysieren und studieren.

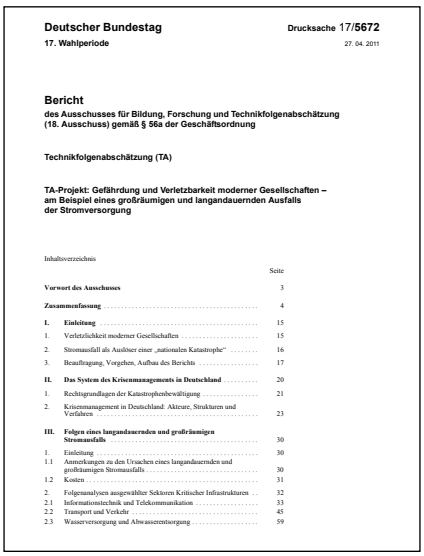
Kleine, aber wichtige Sensoren im AKW sind ausgefallen, weil sie von einer zentralen Stromversorgung abhängig waren. Notstromgeneratoren konnten den Zielort nicht erreichen, weil die Strassen hoffnungslos überlastet und damit faktisch auch ohne echte Zerstörung unbrauchbar waren. Vor allem der Zusammenbruch des Stromnetzes hatte viele fatale Folgen. Die Hightech-Kommunikation ist kollabiert und nur durch dezentrale Uralt-Lowtech-Lösungen wie Mittelwelle-Radiosender konnten Informationen an die Bevölkerung übermittelt werden. Tankstellen konnten kein Benzin mehr hochpumpen und Menschen konnten kein Essen mehr auf ihren Elektroherden zubereiten, um nur einige der Folgeprobleme zu nennen.

Krisenfestigkeit

Resilienz beschreibt die Toleranz eines Systems gegenüber Störungen. Wie gut kommt beispielsweise eine Gesellschaft mit einem unerwarteten Stromausfall klar. Eine hohe Krisenfestigkeit ist von Vorteil, vor allem wenn es kritische Infrastruktur betrifft. Hierzu zählen in unserer Welt neben der Wasser- und Nahrungsmittelversorgung auch Aspekte wie das Finanzsystem, die Telekommunikation und natürlich das Stromnetz.

Dass große Stromnetzausfälle passieren können, ist nicht nur Theorie. In unserer Region gibt es da z.B. das „ Münsterländer Schneechaos“ von 2005, bei dem durch Eis und Schnee eine große Zahl an Strommasten in einer Region zerstört wurden. Bis zu 250.000 Menschen waren tagelang ohne elektrische Energie.

Zu welcher fatalen Verkettung von Problemen es bei einem längerfristigen Stromausfall kommen kann, wurde unter anderem Ende 2010 vom Büro für Tech-

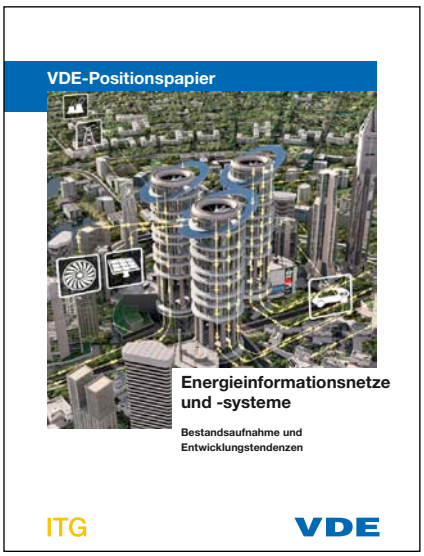

Deutscher Bundestag — Drucksache 17/5672
17. Wahlperiode — 27. 04. 2011

Bericht
des Ausschusses für Bildung, Forschung und Technikfolgenabschätzung (18. Ausschuss) gemäß § 56a der Geschäftsordnung

Technikfolgenabschätzung (TA)

TA-Projekt: Gefährdung und Verletzbarkeit moderner Gesellschaften – am Beispiel eines großräumigen und langandauernden Ausfalls der Stromversorgung

Inhaltsverzeichnis



Bisher werden in der Normungsroadmap der DKE (Stand 2010) die Problemfelder „Cyberwar“ und „Schutz kritischer Infrastruktur“ eher als Randthemen behandelt. Doch der Bericht des Ausschusses für Bildung, Forschung und Technikfolgenabschätzung im Deutschen Bundestag zeigt eindringlich, welche Risiken ein Stromausfall mit sich bringen würde. Überaus erfreulich ist, dass die Autoren des VDE-Positionspapiers die Themen „Angriffe“, „Totalausfall“ oder „Resilienz“ ernsthaft analysieren.

nikfolgenabschätzung in einem Bericht an den Deutschen Bundestag zusammengefasst. Das Papier liest sich wie das Drehbuch für einen erstklassigen Katastrophenfilm. Im Januar 2012 hat sich sogar das Wissenschaftsmagazin „Quarks & Co“ dem Thema zur besten Sendezeit im Fernsehen angenommen.

Ressourcenmangel

Was bei uns heute im nationalen Notstand enden kann, ist in Ländern wie Kambodscha, Laos, Irak oder sogar Indien kein großes Drama. Regionen, in denen Stromausfälle jeden Tag stattfinden, haben sich darauf zwangsläufig eingestellt. Dort ist die Krise Normalität. Notstromaggregate gibt es dort praktisch nicht, denn diese sind dort meist die „Hauptstromaggregate“. Das Stromnetz ist dort bei weitem nicht so wichtig wie bei uns.

In vielen Ländern ist Ressourcenmangel kein Zukunftsszenario, sondern Normalität. Wenn wir klug wären, würden wir diese Länder genau studieren. Als Export-Nation sollten wir uns mit den Problemen dieser Zielmärkte befassen und Lösungen für deren Probleme anbieten, denn dies ist ein gigantischer Markt

Wer wird schon eine Smart Grid-Technologie kaufen, die nur dann funktioniert, wenn gleichzeitig ein immer verfügbares Internet mit hoher Bandbreite und Übertragungsgeschwindigkeit betriebsbereit ist. Wer will schon ein Elektroauto kaufen, dass nicht in der Lage ist, an einem kleinen Notstromgenerator aufgeladen zu werden?

Und wenn wir ehrlich zu uns wären, würden wir uns eingestehen, dass auch bei uns Ressourcenmangel eine reale Zukunftsoption ist. Erst vor kurzem hat der Bundesverband der Deutschen Industrie (BDI) eine „Allianz zur Rohstoffsicherung“ ins Leben gerufen. Auch wir werden früher oder später nicht mehr unseren Überfluss verwalten, sondern uns mit globalem Mangel arrangieren müssen. Denn unsere, durchaus erfolgreiche, Strategie sich mit Gewalt von anderen alles zu nehmen, was man gerne haben will, gerät ins Stocken. In diesem Jahrhundert werden auch andere Kontinente sich ihren Teil vom Kuchen abholen.

Das Leben nach Stuxnet

Dass Mangel Konflikte fördert, ist keine besonders originelle Erkenntnis. Allein die Kriege um Öl oder der Kampf um die Vorherrschaft im Bereich der Atomtechnologie füllen unzählige Bücher und liefern täglich neue Schlagzeilen.

Neu ist aber die Rolle der Computer in diesen Konflikten. Sie dienen nicht mehr nur zur Herstellung oder Kontrolle von Waffen. Im Cyberwar sind Computerprogramme die eigentliche Waffe. Früher hat man seinen Feinden mit Bomben gedroht. Heute reichen oft schon kleine Computerviren.

Im Jahr 2010 wurde ein als „Stuxnet“ bezeichneter Computerwurm entdeckt. Er öffnete vielen IT-Experten die Augen. Computerviren oder Würmer sind grundsätzlich nichts Neues. Das Erstaunliche an Stuxnet war auch nicht, dass er gleichzeitig drei bis dahin unbekannte Schwachstellen ausgenutzt hat, sondern vor allem, dass dieses Programm offensichtlich in Umlauf gebracht wurde, um ganz bestimmte Industrieanlagen zu sabotieren. Eine Analyse des Programmcodes hat gezeigt, dass man gezielt die Kommunikation zwischen Komponenten einer Industrieanlage manipuliert hat, um diese in einen kritischen Zustand zu bringen, der die Anlagen beschädigen oder zerstören sollte. Das primäre Ziel waren offenbar die iranischen Atomanlagen, in denen es auch 2009 zu entsprechenden Unfällen gekommen ist. Als Urheber werden in der Fachwelt die Geheimdienste Israels und der USA angenommen.

Der Vorteil der „Waffe“ namens Schadsoftware ist, dass der Angreifer in der Regel nie eindeutig festgestellt werden kann und der Angreifer zudem nur sehr geringe Risiken eingeht. Doch wie im echten Krieg wird auch hier auf jeden Schlag ein Gegenschlag folgen. Das von Schadsoftware ausgehende Risiko ist auf jeden Fall ernst zu nehmen. Die USA haben vor kurzem ganz ausdrücklich Cyberwar-Angriffe auf ihr Land mit anderen Kriegshandlungen gleichgestellt. Die USA haben somit erklärt, dass sie bereit sind, auf einen Computervirus mit Bomben zu antworten.

Gibt es IT-Sicherheit?

IT-Experten wie Bruce Schneier werden nicht müde zu erklären, dass es echte Sicherheit nicht gibt. Es gibt nur das Gefühl von Sicherheit. Wenn jemand ein Sicherheitsschloss an seiner Tür hat, dann kann man immer noch durch ein offenes Fenster in das Haus gelangen (sog. Seitenangriffe), oder man klingelt einfach an der Tür und erklärt, man müsse die Wasseruhr ablesen (sog. „Social Hacking“).

Nur ein Haus ohne Türen und Fenster (ein Bunker?) erscheint vollends sicher, ist dann aber auch zum Wohnen eher unbrauchbar. Doch selbst so ein Haus kann man „öffnen“. Noch sicherer wäre dann nur ein Haus ohne Räume und ohne Inventar. Aber dann ist es letztlich kein Haus mehr, sondern eher ein Betonklotz. Der Spruch „was man gebrauchen kann, kann man auch missbrauchen“ gilt letztlich auch in der virtuellen Computerwelt.

Technische Sicherheitsmaßnahmen verhindern im Ernstfall keine Angriffe, sie machen diese nur etwas komplizierter. Doch nur weil sich heute nicht jeder Bürger seinen Super-Virus selber zusammenklicken kann, heisst das noch lange nicht, dass hochmotivierte Einzelpersonen oder Geheimdienste mit Software keinen Schaden anrichten könnten.

Was soll uns dieser Exkurs sagen?

Es gibt kein sicheres Smart Grid!

Interessante Cyberattacken der letzten Jahre

Vorfall	Beschreibung
Stuxnet-Virus (2008 bis 2010)	Die Schadsoftware hatte das Ziel, ausgewählte Industrieanlagen zu sabotieren, indem es gezielt die Kommunikation von Siemens „Simatic S7“ Steuerungen manipulierte. Als Urheber gelten der israelische und amerikanische Geheimdienst. Das Angriffsziel waren offenbar die iranischen Atomanlagen, in denen es 2009 auch zu Unfällen gekommen ist.
Root-CA Hacks (2009 bis 2011)	Sichere Computer-Kommunikation basiert heute vor allem auf dem SSL-Protokoll (Secure Socket Layer). Hier spielen Zertifikate (kryptografische Schlüssel) eine zentrale Rolle. Unbefugte waren bei den Zertifizierungsstellen GlobalSign, DigiNotar, Comodo und einigen anderen eingedrungen und haben mit deren Stammzertifikaten eigene „offizielle Zertifikate“ erschaffen. Vermutlich wurden diese Schlüssel im Rahmen von „Man-in-the-Middle“ Attacken genutzt. Bei DigiNotar waren angeblich iranische Hacker am Werk, doch auch die Attacken richteten sich gegen den Iran.
Keylogger gegen US-Drohnen (Sept. 2011)	Die Steuercomputer auf der US-Luftwaffenbasis in Creech (Nevada) sind permanent von Keyloggern-Viren befallen. Diese Form der Schadsoftware zeichnet jede Tastatureingabe der Piloten auf. Angreifer könnten auf diesem Weg auch die Kontrolle über die Kampf-Roboterflugzeuge gewinnen oder zumindest Wissen über die Kommandobefehle erlangen.
GPS-Hack gegen US-Drohnen (Dez. 2011)	Der Iran erbeutet eine bis dahin geheime US-Tarnkappendrohne, die offensichtlich im Auftrag der CIA die iranischen Atomanlagen ausspionieren sollte. Die vorherrschende Meinung der Fachwelt ist, dass hierbei eine Manipulation des GPS-Positionssignals zum Einsatz gekommen ist, mit der die automatische Navigation der Drohne manipuliert wurde.

Smart Grid – Catch 22?

Auch wenn es schwer ist, zwei Leute zu finden, die die gleiche Definition des Begriffes „Smart Grid“ verwenden, so kann man sich vermutlich zumindest darauf einigen, dass es darum geht, mehr Computertechnik in den Betrieb der Stromnetze zu integrieren. Das fatale an diesem Ansatz ist, dass Computer Strom brauchen um zu arbeiten. Wenn nun das Stromnetz wiederum die Computer braucht um korrekt zu funktionieren, so hat man einen Ringschluss erzeugt. Wo ist der Anfang von diesem Kreis? Wie fährt man so ein System hoch?

Bereits heute haben wir das Problem, dass fast alle Kraftwerke ein funktionierendes Stromnetz brauchen, um selber starten zu können. Leider sind auch Solarstrom- und Windkraftanlagen in der Regel nicht inselnetz- bzw. schwarzstartfähig, obwohl sich gerade diese Energiequellen dafür perfekt anbieten. In einem Land wie Deutschland ist diese Fähigkeit bisher nicht notwendig, weil das europäische Stromnetz ja so gut wie nie ausfällt.

In dem Smart Grid, das den meisten Akteuren der Energiewirtschaft heute so vorschwebt, wird alles noch komplizierter. Dann kommt zur Abhängigkeit vom Stromnetz noch die Abhängigkeit von Kommunikationsnetzen, Leitwarten und anderen externen Systemen. Vor allem die Kommunikationsnetze sind hier ein echtes Problem, denn diese sind weder zuverlässig, noch sicher oder wirklich kostengünstig im Betrieb.

Zu den Hauptproblemen bei der Einführung von digitalen Stromzählern („Smart Metern“) zählen die für den Kunden nicht ersichtlichen Vorteile und der durch die zusätzlich benötigte Internet-Anbindung verursachte Mehraufwand (die Mehrkosten). Dadurch werden die sowieso schon geringen Potentiale zur Stromkostensenkung in der Regel wieder aufgebraucht.

Das Internet der Energie?

In den Hochglanzprospekten als auch in den oft nichtssagenden Vorträgen zum Thema „Smart Grid“ taucht oft die Floskel vom „Internet der Energie“ auf. Leider hat man den Eindruck, dass die dazugehörenden Urheber weder das Energiesystem noch das Internet verstehen.

In den „Smart Grid“-Dokumenten wird sehr gerne von Use-Cases, Marktrollen, Marktstrukturen, Geschäftsmodellen, Billingsystemen, Leitzentralen, Prosumern, Smart Homes, Smart Generation, Smart Meter, Smart Storage und vielen anderen modischen Dingen gesprochen. Bereits die Sprache zeigt, dass hier vermutlich die gleichen Betriebswirte, Manager und Rechtsanwälte am Werk sind, die auch schon das Finanzsystem ruiniert haben. Das „Smart Grid“ verspricht ihnen die Chance Stromtarife auszuarbeiten, die kein Kunde mehr durchblickt; so wie heute beim Mobiltelefon. Das „Smart Grid“ soll den zentralistischen Überwachungs- und Kontrollfanatikern den Weg bis in jede Wohnung eröffnen; wie bei Google und Facebook. Das „Smart Grid“ wird so viele sinnlose und unnötige Computerprobleme erzeugen und Software-Updates verlangen, dass ein gigantisches und dennoch völlig sinnfreies Wirtschaftswachstum (sprich „Strompreissteigerung“) generiert werden kann; wie bei Microsoft Windows und anderen Softwareprodukten. Das Beste an allem ist jedoch, dass man mühelos alle unnötigen Mehrkosten mit dem Schutz des Klimas und der Energiewende begründen kann.

Still und heimlich träumen viele in der Energiewirtschaft vermutlich davon, der nächste Google oder Facebook zu werden – unersetzbar und „reich wie Scheich“.

Was ist das Internet?

Das Internet wurde jedoch nicht durch die Normungsgremien der Industrie erschaffen, sondern vom US-Militär und einem Haufen, oft langhaariger und ungewaschener Computer-Freaks. Die von ihnen verfassten RFCs (Request for Comment) sind im Gegensatz zu gängigen Normen für jeden Menschen kostenlos verfügbar. Das Internet hat, aus gutem Grund, auch keine zentrale Leitstelle, denn es sollte nach dem Wunsch der Militärs unzerstörbar sein. Die Technik des Internets ist unabhängig von der Größe des Systems. Es funktioniert mit zwei Rechnern genauso wie mit 2 Milliarden.

Im Gegensatz zum längst vergessenen BTX der Deutschen Post ging es bei der Entwicklung des Internets (TCP/IP) nie um Abrechnungssysteme, sondern nur um Datentransfer. Geld stand nie im Zentrum der Überlegungen, denn das Militär hatte reichlich davon und die Studenten hatten meistens sowieso kein Geld.

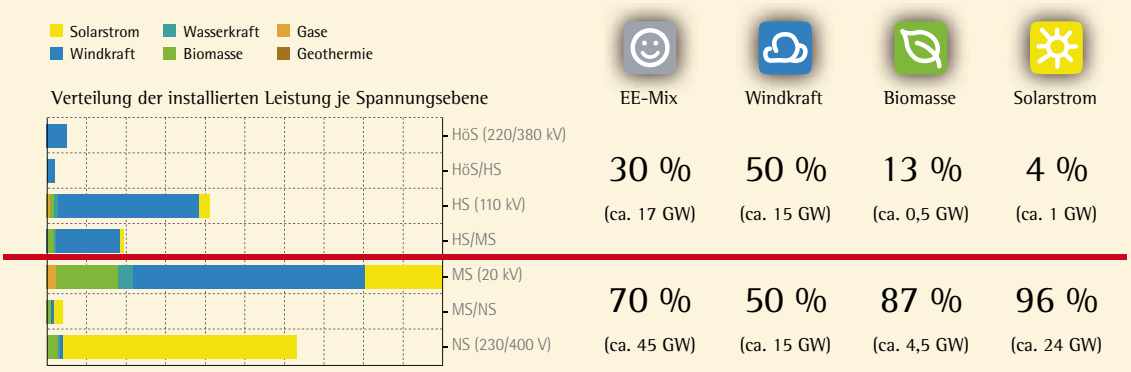
Das Internet ist, trotz Google, Amazon und Co, geprägt von der Idee der Kooperation und der Dezentralität. Die Funktion (Physik) stand immer im Vordergrund und nicht das Geld.

Zentral oder dezentral

Das Smart Grid als „Internet der Energie“ zu bezeichnen, ist eigentlich eine gute Umschreibung. Aber es ist ein anderes „Internet“ als das, wovon Betriebswirte gerne träumen.

Das „Internet der Erneuerbaren Energien“ kann eine extrem krisenfeste Struktur erschaffen. Doch man sollte sich auch

Die dezentrale Struktur der Erneuerbaren Energien



Grafik 1: Obwohl gerne über die dezentrale Natur der Erneuerbaren gesprochen wird, so scheinen die Konsequenzen dieser Eigenschaft nur bedingt ins Bewußtsein durchzudringen. Der deutsche EE-Mix hat bereits im Jahr 2011 rund 45 Gigawatt Erzeugungskapazität im Mittel- und Niederspannungsnetz. Die Zahl der Anlagen liegt bei rund einer Million. Heute sind die Netzbetreiber auf diesen Netzebenen so gut wie blind und daran wird sich auch in den nächsten Jahren nur wenig ändern.

ernsthaft mit diesem Gebilde befassen.

Heute ist das Stromnetz eine zentrale „Top-Down"-Architektur. Das Internet gleicht jedoch eher den Erneuerbaren, denn beide sind eine „Bottom-Up"-Entwicklung. Die Erneuerbare Erzeugungsleistung ist bereits heute zu 70% im Mittel- und Niederspannungsnetz konzentriert (siehe Grafik 1). Dieser Trend wird sich weiter verstärken. Will man Krisenfestigkeit erreichen, so müssen auch die Regelenergiekraftwerke und Stromspeicher auf diesen Ebenen angesiedelt werden. Dies ist einer der Gründe, der gegen den Bau neuer Pumpspeicherkraftwerke spricht. Denn sie werden aufgrund ihrer Baugröße immer eine zentralistische Technik des Hoch- und Höchstspannungsnetzes bleiben. Ein derartiges Stromnetz könnte jedoch nicht problemlos in kleinere Einheiten zerfallen, da die kleinen Zellen ohne Speicher und Regelenergiekraftwerke nicht stabil zu betreiben wären.

Das smartere Smart Grid

Wirklich intelligent wäre ein Smart Grid, wenn es nahezu ohne Märkte und ohne Kommunikation auskommen könnte.

Die Märkte verursachen bereits heute mit ihrem egoistischen Verhalten die meisten Probleme im Stromnetz (siehe Grafik 2 und 3). Je undurchsichtiger die Marktstrukturen werden, desto mehr Betrug kann man erwarten. In Anbetracht der essentiellen Bedeutung des Stromnetzes müssen die Betriebsregeln für die Physik des Stromnetzes so gestaltet werden, dass beim Versagen des Marktes automatisch die verpflichtende, technische Kooperation aller Netzteilnehmer dem Treiben ein Ende setzt. Faktisch sind die netzfrequenzabhängigen Regelenergievorgaben im europäischen Verbundnetz bereits so ein Mechanismus, den man jedoch weiterentwickeln müsste. Wir werden hierzu in einer der kommenden Ausgaben einige Überlegungen vorstellen.

Kommunikation ist per Definition ein Sicherheitsproblem. Deshalb sollte man wirklich kritische Dinge auch ohne Kommunikation erledigen können. Ein banales Beispiel für Kommunikationsrisiken sind zeitvariable Stromtarife. Hier braucht man noch nicht einmal einen bösen Hacker, um Probleme zu verursachen. Strompreise werden an der Leipziger Strombörse von ein paar wenigen Händlern gebildet. Nur weil dort Strom für den Mittag teuer gehandelt wird, heisst das noch lange nicht, dass es in jedem Ast des deutschen Niederspannungsnetzes auch tatsächlich einen Mangel gibt. Was für Brandenburg gilt, muss für ein Dorf in Bayern noch lange nicht gelten. Mutwillige Preismanipulationen könnten sehr einfach dazu verwendet werden, um große Nachfragen in Zeiten mit einem geringem Angebot zu legen. Wenn in solchen Fällen die Physik dem Markt nicht Einhalt gebietet, so ist das Netzchaos vorprogrammiert.

Rahmenbedingungen

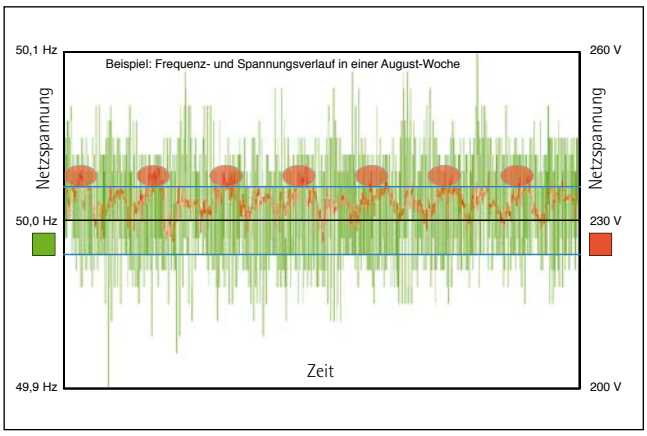
Dass sich im Zuge einer ernsthaften und vollständigen Energiewende die Stromerzeugung von den Hoch- und Höchstspannungsnetzen in die unteren Netzebenen verlagern wird, ist unumgänglich. Will man das Stromnetz, eine der wichtigsten Infrastrukturen unserer heutigen Gesellschaft, wirklich krisenfest gestalten, so müssen auch die Regelenergiekraftwerke und Stromspeicher auf die unteren Netzebenen verlagert werden.

Computer werden in dem hoch dynamischen Erneuerbaren Energiemix ein wichtiges Hilfsmittel sein. IT-Kommunikation sollte jedoch lieber gar nicht oder nur für zeitunkritische bzw. unwichtige Dinge eingesetzt werden. Mit zunehmender Ressourcenunsicherheit werden in Zukunft auch die Konflikte zunehmen. Die Kriegsführung mit Softwarewürmern, Trojanern und anderen Mitteln des Cyberwar ist eine kostengünstige und überaus mächtige Waffe geworden. Kommunikationssysteme wie etwa das Internet oder die exakte Orts- und Zeitbestimmung via GPS sind praktisch, aber es wäre smart, wenn die Funktionsfähigkeit unseres Stromnetzes davon nicht auf Gedeih und Verderb abhängen würde.

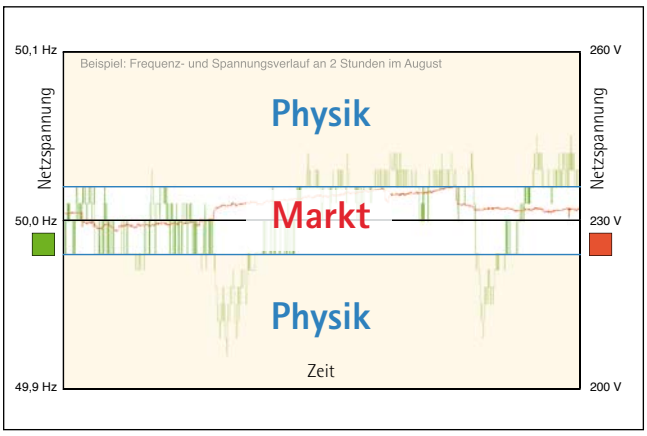
Nachdem wiederholt „smarte Akteure" mit „smarten Produkten" das Finanzsystem ruiniert haben, wäre es smart, nicht die gleichen Fehler im Stromnetz zu wiederholen. Es wäre smart, die Märkte und deren egoistische Spieler in sehr enge Schranken zu verweisen.

Vielleicht wäre es auch smart, nicht immer und überall krampfhaft das Wort „Smart" voranstellen zu wollen. Die Physik dieses Universums war noch nie dumm und das gleiche gilt auch für die Physik des Stromnetzes.

ZUM AUTOR:
▶ *Tomi Engel*
leitet den DGS Fachausschuss Solare Mobilität
tomi@objectfarm.org



Grafik 2: Die Physik der Stromnetzes „kommuniziert" auch ohne Internet mit jeder Steckdose in Europa. Wenn die Frequenz (grün) oder die Spannung (rot) nach oben ausschlagen, gibt es an diesem Ort zu viel und bei einer Abweichung nach unten zu wenig Kraftwerksleistung. Schön zu sehen (rote Ovale) sind in dieser August-Woche die im ländlichen Bayern täglich auftretenden PV-Spannungsanhebungen zur Mittagszeit. Es wäre smart, auf diese Information zu schauen, denn die Physik lügt nicht.



Grafik 3: Die Strommärkte verursachen fast zu jeder vollen Stunde, dem Ende der Handelszeiträume, messbare Probleme im Stromnetz. In der Grafik oben sind das die beiden großen Einbrüche nach unten. Um zu vermeiden, dass die Märkte (das Spiel) reale Krisen hervorrufen können, muss es verpflichtende Regeln für das Zusammenspiel im Netz geben, die sich an den Gesetzen der Physik (der Realität) orientieren. Märkte brauchen harte Grenzen.