Smart Energy Forensic

Florian Schiele
Friedrich-Alexander-Universität
Erlangen-Nürnberg (FAU)
Seminar der Hochschule Darmstadt

***Zusammenfassung*—Die fortschreitende Entwicklung unserer Städte und der Ausbau von erneuerbaren Energien bringt auch neue Anforderungen an die Energieversorgung mit sich. Eine zentrale Rolle nehmen hierbei Messeinrichtungen ein, mit denen das Stromnetz besser überwachbar wird. Diese Messeinrichtungen dienen zur Gewährleistung der Netzstabilität, zu Abrechnungszwecken, sowie zur Information der Stromkunden über deren Verbrauchsverhalten. Dieser Artikel liefert einen Überblick über etablierte Messsysteme, deren Funktionsweise und verfügbaren Messdaten. Des weiteren wird untersucht, welche forensischen Erkenntnisse aus den in Haushalten installierten Messeinrichtungen gewonnen werden können. Dieser Artikel zeigt die Erzeugung eines Nutzungsprofils eines Haushaltes welches bei forensischen Untersuchungen verwendet werden kann. Abschließend werden Methoden zur Fälschung dieser Nutzungsprofile evaluiert und vorgestellt.**

I. Einleitung

Bereits im Jahr 1882 wurde in Nürnberg mit der ersten Inbetriebnahme einer Straßenbeleuchtung die Elektrifizierung der Städte begonnen [1]. Seitdem wurde das deutsche Stromnetz bis heute mit rund 1,8 Millionen Kilometern Kabeln und Freileitungen ausgebaut [2]. Jüngste Ereignisse (z.B. Münchener Brandanschlag am 24. Mai 2021) [3] zeigen, welchen Stellenwert die elektrische Energieversorgung in unserem Leben eingenommen hat. So waren bei dem Münchener Brandanschlag rund 20 000 Haushalte und Betriebe für anderthalb Tage ohne Strom. Neben ausgefallenen Ampelanlagen und Kühlschränken konnten viele Menschen während des Stromausfalles ihrem Beruf nicht nachgehen [3].

Um die Auswirkungen derartiger Ereignisse abzumildern oder zu vermeiden setzen die Stromnetzbetreiber immer mehr Technologien ein, die defekte Kabelabschnitte und Anlagenteile automatisch erkennen und das Umschalten auf einen Reserveweg im Fehlerfall ermöglichen.

Der stark steigenden Ausbau von erneuerbaren Energieen und dezentralen Kleinstkraftwerken (z.B. Blockheizkraftwerken) birgt weitere Risiken, die die Stabilität der Stromnetze negativ beeinflussen können. Um diese Risiken zu minimieren ist eine Überwachung der Energieflüsse in allen Ebenen der Energienetze notwendig. Die Überwachung dient der Erkennung von übergreifenden und auch punktuellen Über- und Unterbelastungssituationen. Hierzu werden sowohl in den Energieerzeugungsanlagen, dem Energieübertragungsnetz und beim Endkunden Messeinrichtungen installiert. Diese Messeinrichtungen liefern Messwerte über die Höhe der Energie und über die Energieflussrichtung. Die Messwerte werden unter anderem von den Netzbetreibern zu Regelungs- und Abrechnungszwecken ausgewertet.

Dieser Artikel zeigt, zum einen welche Systeme und Betriebsmittel in Stromnetzen für die Gewinnung von Messdaten beauskunftet werden können und zum anderen welche forensischen Erkenntnisse hieraus gewonnen werden können. Hierzu werden Messdaten aus Schutzsystemen und der modernen Messeinrichtungen[1] betrachtet sowie die anfallenden Daten maschinell und in Echtzeit forensisch ausgewertet. Das Vorliegen der Messdaten ermöglicht eine automatische Reaktion auf Ereignisse im Stromnetz. Zusätzlich können durch kontinuierliches Monitoring potentielle Fehler präventiv erkannt werden, bevor es zu einem Versorgungsausfall kommt.

Der nachfolgende Artikel ist wie folgt aufgebaut: Abschnitt II beschreibt den Aufbau von Energienetzen und die verfügbaren Quellen für Messdaten. Die für eine forensische Untersuchung relevanten Messwerte werden in Abschnitt III identifiziert und validiert. Abschnitt IV evaluiert mögliche Maßnahmen zur Fälschung von Nutzungsprofilen. Abschnitt V fasst die Erkenntnisse des vorliegenden Artikels zusammen.

II. Aufbau von Energieversorgungsnetzen

Um den vorliegenden Artikel besser zu verstehen und die Nachvollziehbarkeit zu gewährleisten, ist ein Grundverständnis über den Aufbau von Energieversorgungsnetzen nötig.

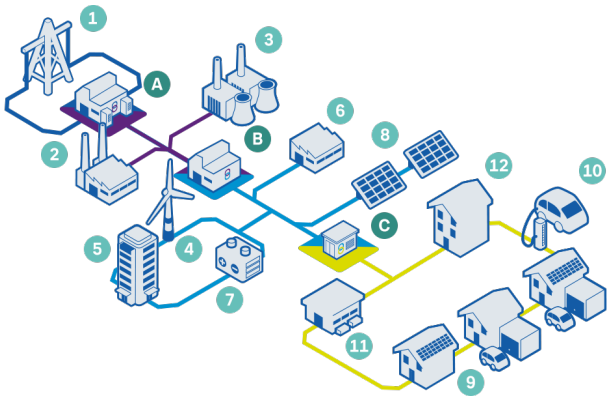


Abb. 1. Struktur Stromnetz [4]

Stromnetze sind in verschiedene Spannungsebenen eingeteilt. Von der Höchstspannungsebene über die Hoch- und Mittelspannung bis zur niedrigsten, der haushaltsüblichen Niederspannungsebene. Je höher die Spannung ist, umso verlustarmer kann die Energie übertragen werden. Dem gegenüber

[1] im Volksmund Stromzähler

stehen, physikalisch bedingt, hohe Kosten durch komplexe Anlagen, die bei der Übertragung von hohen Spannungen benötigt werden.

Abbildung 1 zeigt die Struktur eines Energieversorgungsnetzes. Die Stromerzeugung erfolgt primär mit Kraftwerken, wie in der Abbildung 1 (Position 3) dargestellt ist. Die Kraftwerke speisen in das Hochspannungsnetz mit üblicherweise einhundertzehntausend Volt (110kV) ein. Die Energie wird über Umspannwerke (B) in das Mittelspannungsnetz, üblicherweise mit einer Spannung von 10kV oder 20kV eingespeist. Hier speisen weitere Energielieferanten (z.B. Windkraftanlagen (4), Blockheizkraftwerke (7) und Solaranlagen (8)) in das Stromnetz ein. Großkunden wie Industrie (6) und Geschäftsgebäude (5) beziehen aus dem Mittelspannungs- netz Energie.

Zu den Haushaltskunden gelangt die Energie über eine Ortsnetzstation (C), die die Mittelspannung in haushaltsübliche Niederspannung (230V/400V) transformiert. Neben den klassischen Verbrauchern im Niederspannungsnetz wächst auch der Anteil der Stromkunden, die selbst erzeugte Energie, meist durch private Solaranlagen, in das Niederspannungsnetz einspeisen [4].

Um auch mit anderen Netzen Energie auszutauschen, wird das lokale Netz durch ein Umspannwerk (A) in das Höchstspannungsnetz (1) eingebunden. Hierdurch wird die Energieübertragung in andere entfernte Energienetze ermöglicht.

Vor dem Beginn der Energiewende in den 1990er Jahren, wurde der Strom ausschließlich zentral erzeugt und über das Stromnetz zum Kunden ausgeliefert. Damit war der Energiefluss in den Spannungsebenen der Mittel- und Niederspannung stets vom Umspannwerk über die Ortsnetzstationen zum Kunden. Diese seit Beginn der Energieversorgung etablierte Nutzung der Stromnetze erfuhr mit der deutschen Energiewende eine Veränderung. Abbildung 2 zeigt den Wachstum an dezentralen Erzeugungsanlagen seit den 1990er Jahren. Im Jahr 1991 waren es 17 Mrd. Kilowattstunden (kWh). Im Jahr 2020 hingegen waren es bereits 252 Mrd. kWh [5]. Das entspricht einem Beitrag von 46% des Bruttostromverbrauches[2] in Deutschland [6].

Vor der Energiewende war die Flussrichtung der Energie in den Stromnetzen konzeptionell festgelegt. Die Energie floss stets vom Energieerzeuger (z.b. einem Kraftwerk) durch das Stromnetz zu den Endkunden.

Damit sich das Energieversorgungsnetz in einem sicheren Zustand befindet, muss die verbrauchte Energie stets gleich der erzeugten Energie sein. Der Energieverbrauch durch Haushalte und Betriebe ist prognostizierbar. Auch die herkömmliche Energieerzeugung in Kraftwerken kann nach Bedarf geregelt werden. So war die Energiebilanz unter Ausschluß von erneuerbaren Energieen, insbesondere wetterabhängige Wind- und Solarenergie, stets erfüllbar.

A. Quellen für Messdaten

Zur Erhebung von Messdaten existieren mehrere Punkte im Stromnetz. In höheren Spannungsebenen (ab 110kV) sind Messungen schon seit langer Zeit etabliert, da hier die Energieflussrichtung konzeptionell nicht in jedem Betriebszustand definiert ist.

In den darunter liegenden Spannungsebenen, der Mittel- und Niederspannung, war die Energieflussrichtung hingegen konzeptionell von der Erzeugungsstelle zum Kunden eindeutig definiert. Durch den Anschluss von dezentralen Erzeugungsanlagen kann dieses Konzept allerdings nicht weiter bestehen. Deshalb werden auch die Mittel- und Niederspannungsnetze zunehmend mit Messtechnik ausgestattet. Die primäre Motivation hierbei ist, die Verfügbarkeit der Energieversorgung auf einem hohen Niveau zu halten. Dies erfolgt u.a. durch: 1) Schutzeinrichtungen, 2) Einspeisemanagement, 3) Analyse der Messwerte der Niederspannungsebene und 4) intelligente Messsysteme.

1) Schutzeinrichtungen: Eine Schutzeinrichtung wird zum Schutz von elektrischen Leitungen[3] und weiteren Anlagenteilen des Stromnetzes, wie zum Beispiel Schaltanlagen[4], eingesetzt. Hierbei werden mit einer hohen Abtastrate Messdaten über den Energiefluss der Leitung erhoben und in Echtzeit verarbeitet. Ziel ist es, bedrohliche Anomalien im Energiefluss unmittelbar zu erkennen und bei einer Detektion den überwachten Netzabschnitt vom restlichen Stromnetz zu trennen, um einen Schaden zu minimieren oder zu vermeiden [7].

Die Schutzeinrichtung besteht aus einem Messsystem und einem Auswertungssystem (Schutzgerät). Damit die Schutzeinrichtung in der Lage ist den Energiefluss zu unterbrechen, ist sie mit einem Leistungsschalter gekoppelt. Der Leistungsschalter hat die Aufgabe, die Leitung mit dem Stromnetz zu verbinden oder zu trennen [8].

Eine Anomalie kann beispielsweise, altersbedingt durch einen Kurzschluss oder aktiv durch eine Beschädigung, bedingt durch Bauarbeiten an einem Erdkabel, auftreten. Da an der Fehlerstelle große Energiemengen durch Lichtbögen freigesetzt werden können, ist es wichtig, dass die Schutzeinrichtung schnell reagiert und den Energiefluss zur Fehlerstelle unterbricht. Hiermit werden nicht nur materielle Schäden sondern insbesondere Schäden an Mensch und Umwelt begrenzt oder vermieden.

Folgend betrachtet werden zwei häufig eingesetzte Schutzkonzepte. Zum einen der in Abbildung 3a skizzierte Distanzschutz und der in Abbildung 3b skizzierte Differenzialschutz.

a) Distanzschutz: Der Distanzschutz hat einen einfachen Aufbau und besteht aus einem Schutzgerät, einer Messstelle und einem Leistungsschalter. Der Distanzschutz vergleicht ständig den gemessenen Stromfluss I der Stromleitung mit einem Einstellparameter X. Ist der Stromfluss größer als der eingestellte Parameter X, veranlasst das Schutzgerät die Abschaltung der Stromleitung über den Leistungsschalter. Der Distanzschutz kann allerdings nur den Leitungsabschnitt schützen, der in Energieflussrichtung hinter der Schutzeinrichtung liegt. Er ist damit abhängig von der Energieflussrichtung.

[2] Summe der ausgeleiferten Energie und aus Netzverlusten

[3] Erdkabel und Freileitungen

[4] Schaltanlagen sind die Knotenpunkte des Stromnetzes. Sie verbinden mehrere Leitungen und weitere Komponenten des Stromnetzes.

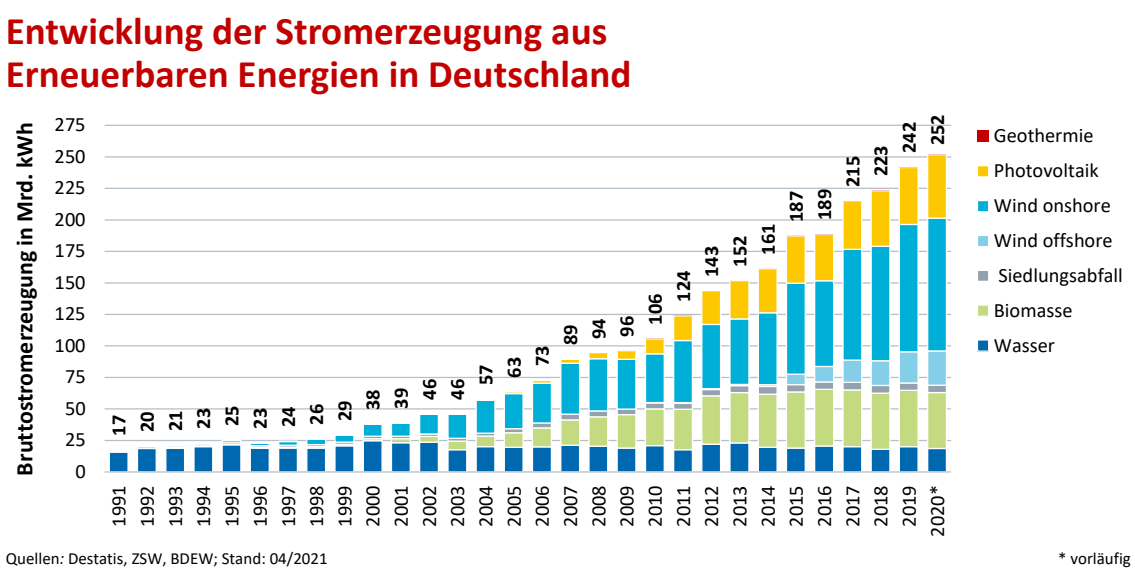
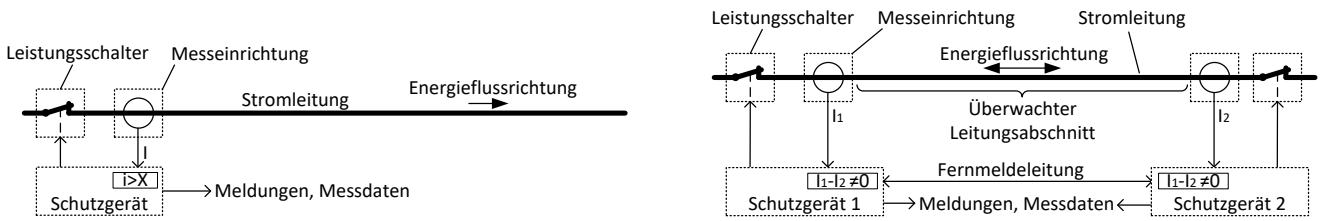


Abb. 2. Entwicklung Erneuerbare Energieen [5]



(a) Distanzschutzeinrichtung

(b) Differenzialschutzeinrichtung

Abb. 3. Arten von Schutzeinrichtungen

b) Differenzialschutz: Der Differenzialschutz hingegen ist unabhängig von der Energieflussrichtung, hat aber einen komplexeren Aufbau im Vergleich zum Distanzschutz.

Ein Differenzialschutz betrachtet immer genau den Netz- oder Leitungsabschnitt, der zwischen den Messeinrichtungen der Schutzgeräte besteht. Der Differenzialschutz kann über der in Abbildung 3b gezeigten Konfiguration auch aus mehr als zwei Schutzeinrichtungen bestehen.

Das Funktionsprinzip des Differenzialschutzes besteht nach der ersten Kirchhoffschen Knotenregel darin, dass die Energie, die in eine Leitung oder einen Netzabschnitt hineinfließt, auch wieder herausfließt. Hierzu sind alle Schutzgeräte mit einer Fernmeldeverbindung[5] verbunden.

Jedes Schutzgerät berechnet in Echtzeit die Summe aus allen aufgenommenen Stromwerten $I_1+I_2+I_n$. Im Normalzustand fließt nach Kirchhoff aus dem geschützten Netzabschnitt genau so viel Energie raus, wie rein. Folglich ist die Summe aller Ströme $I_1+I_2+I_n=0$. Tritt ein Fehler im überwachten Leitungs- oder Netzabschnitt auf, fließt an der Fehlerstelle ein Strom ab und die Differenz aller Ströme ist folglich ungleich Null. In diesem Fall lösen die Schutzgeräte über die Leistungsschalter die Abschaltung des Netzabschnittes aus.

Neben der primären Funktion der Schutzeinrichtung, dem Schutz von Leitungs- und Netzabschnitten, werden die Messdaten auch gespeichert. Insbesondere im Moment eines Fehlers sind die Messdaten (Störschriebe) zur Bestimmung des Fehlers dienlich [8].

Durch eine Anbindung der Schutzgeräte an einen zentralen Datenspeicher des Netzbetreibers können die Störschriebe dort direkt, durch Spezialisten forensisch ausgewertet werden. Die Auswertung liefert wertvolle Informationen über das Fehlerszenario. Zum Beispiel kann die Fehlerstelle geografisch eingegrenzt werden und das Entstörungsteam zielgerichtet geleitet werden. Zusätzlich können auch Rückschlüsse auf die Art des Fehlers getroffen werden.

c) Schutz im Niederspannungsnetz: Im Niederspannungsnetz treten die meisten Fehler auf. Die Häufigkeit resultiert zum einen aus der großen Anzahl von verlegten Kabeln,

[5]Lichtwellenleiter (bei Freileitungen oft im obersten Drahtseil verwoben) oder Fernmeldekabel.

als auch deren Alter und der Verlegetiefe von weniger als einem Meter.

Im Niederspannungsnetz werden hauptsächlich Schmelzsicherungen zum Schutz der Kabel und Anlagenteile eingesetzt. Der Ausfall eines Niederspannungskabels betrifft gegenüber dem Ausfall eines Mittelspannungskabels- oder Freileitung weniger Kunden.

Elektronische Schutzeinrichtungen mit Messsystemen kommen aus wirtschaftlichen Gründen im Niederspannungsnetz meistens noch nicht zum Einsatz. Somit bietet das Schutzsystem der Niederspannungsebene noch keine Quelle für Messwerte.

d) Schutz im Mittelspannungsnetz: Die am zweithäufigsten von Fehlern betroffene Netzebene ist die Mittelspannungsebene. Hier kommen häufig elektronische Schutzeinrichtungen, wie der Distanzschutz zum Einsatz. Die an den Schutzgeräten erhobenen Messwerte werden an eine zentrale Stelle des Netzbetreibers übertragen. Die Messdaten können beim Auftreten eines Fehlers zur Eingrenzung und Ermittlung der Fehlerursache herangezogen werden. Diese Technologie ermöglicht eine automatische Erkennung des defekten Leitungsabschnittes.

Netzbetreiber sind durch Vorgaben der Bundesnetzagentur und daraus folgende Maluszahlungen motiviert, die Ausfallzeiten so gering wie möglich zu halten [9].

Ein Weg dies im Mittelspannungsnetz umzusetzen, ist beim Auftreten eines Fehlers den defekten Leitungsabschnitt automatisch durch Umschaltung auf eine intakte Leitung zu umgehen. Diese Umschaltung kann vollautomatisch durch ein zentrales System geplant und durchgeführt werden.

Solche Systeme haben zur Verbesserung der Verfügbarkeit im Stromnetz beigetragen. Im Jahr 2006 war jeder Kunde auf Grund von Fehlern im Mittelspannungsnetz für durchschnittlich 18,67 Minuten spannungslos. Im Jahr 2019 waren es nur noch 10.01 Minuten [10].

2) Einspeisemanagement: Das Management der Einspeisung von erneuerbaren Energieen ist eine besondere Herausforderung. Bei kleinen Erzeugungsanlagen wie Solaranlagen und Blockheizkraftwerken, die in das Niederspannungsnetz einspeisen, müssen zur Sicherstellung der Netzstabilität Vorkehrungen zur Überwachung und Steuerung getroffen werden.

Einspeiseanlagen, die in höhere Spannungsebenen einspeisen, haben meistens einen separaten Netzanschluss an ein Umspannwerk, der durch den Netzbetreiber gemessen und kontrolliert werden kann. Bei der Einspeisung in das Niederspannungsnetz ist dies nicht der Fall. Die einspeisende Anlage teilt sich hier oft eine Stromleitung mit weiteren Verbrauchern und Einspeiseanlagen.

Um Überlastungen, z.B. durch Überspannung zu vermeiden, gilt bei Einspeiseanlagen ab 25kW die Einbaupflicht für eine Einspeisemanagementeinheit [11].

Der Netzbetreiber kann dann im Fall einer Überlastung seiner Leitungen die Einspeisung per Fernsteuerung reduzieren oder abschalten [12].

Die Einspeisemanagementeinheit stellt eine weitere Quelle für Messdaten dar. Der Netzbetreiber nutzt diese Messdaten zu Abrechnungszwecken, Untersuchungen von Netzereignissen und zur Netzplanung.

3) Messwerte des Niederspannungsnetzes: Besonders für die städtischen Netzbetreiber ist durch den Aufbau von dezentralen Erzeugungsanlagen und dem Ausbau der Ladeinfrastruktur für die Elektromobilität, die Sicherstellung der Netzstabilität eine Herausforderung. Netzbetreiber wie das Stromnetz Berlin bewältigen diese Herausforderungen unter anderem durch den Einsatz von Messtechnik im Niederspannungsnetz [4].

Messwerte, die im Niederspannungsnetz erhoben werden, können bereits Rückschlüsse auf das Verbrauchsverhalten eines Straßenzuges oder eines Mehrfamilienhauses zulassen. Da die Messwerte aus dem Niederspannungsnetz im Regelfall die Summe mehrerer Kunden ist ist es schwer, Rückschlüsse auf einen einzelnen Kunden zu ziehen. Um dies zu bewältigen müssen die Verbrauchsdaten, wie im folgenden Abschnitt beschrieben, direkt am Kundenanschluss erhoben werden.

4) Intelligentes Messsystem: Als intelligentes Messsystem wird die Kombination aus moderner Messeinrichtung und Smart-Meter-Gateway bezeichnet. Die moderne Messeinrichtung ersetzt den Ferraris Zähler[6] und misst den Energieverbrauch beim Kunden. Die moderne Messeinrichtung besitzt neben der lokalen Anzeige auch einen Speicher und eine Kommunikationsschnittstelle.

Das Smart-Meter-Gateway stellt über die Kommunikationsschnittstelle der modernen Messeinrichtung eine gesicherte Verbindung zum Messstellenbetreiber her.

Die Messwerte dieser Messeinrichtung sind von besonderem forensischen Interesse, da hier im Normalfall nur ein einzelner Haushalt gemessen wird.

Bis zum Jahr 2032 müssen alle Endverbraucher mit einem jährlichen Energieverbrauch von über 6000 kWh laut §29 Messstellenbetriebsgesetz (MsbG) mit einem intelligenten Messsystem und einer modernen Messeinrichtung ausgestattet sein. Bei Kunden mit einem Energieverbrauch bis 6000 kWh ist die Ausrüstung freiwillig [13].

Spätestens nach Ablauf der Eichung[7] der alten elektromechanischen Ferraris Zähler, müssen diese durch moderne Messeinrichtungen ersetzt werden. Das betrifft in absehbarer Zeit, mit wenigen Außnahmen[8], alle deutschen Stromkunden.

III. Messwerte aus forensischer Sicht

Haushaltsübliche elektrische Betriebsmittel, wie Fernseher, Waschmaschine, Herd und Toaster haben bestimmte elektrische Eigenschaften und Parameter, an denen Sie identifiziert werden können. Hierzu zählen insbesondere die Spannung U, gemessen in Volt (V), der Strom I, gemessen in Ampere (A) und die Leistung P, gemessen in Watt (W). Die Leistung ist das Produkt aus Spannung und Strom $P = U \cdot I$.

Die Leistung in Abhängigkeit zur Zeit, ist der zentrale Wert, der die elektrische Signatur eines Betriebsmittels maßgeblich

[6]Herkömmlicher elektromechanischer Energiezähler mit Zählrad und Zählwerk

[7]Eichung ist 16 Jahre ab Eichdatum gültig

[8]u.A. öff. Straßenbeläuchtung

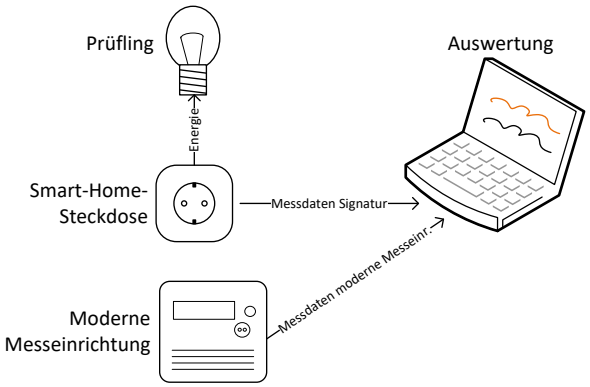


Abb. 4. Messaufbau

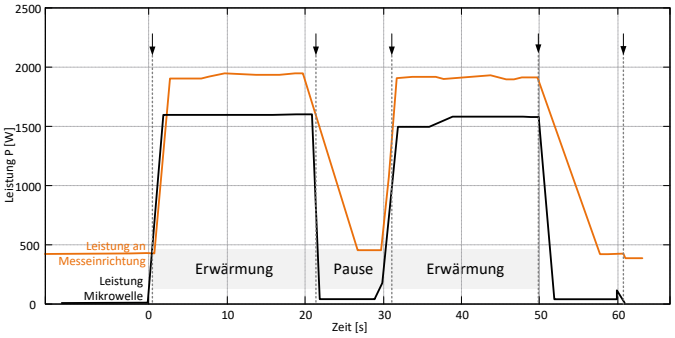


Abb. 5. Messung Mikrowelle

$\mathbf{t}$[s]	0	22	31	50	61
$\mathbf{\Delta P}$[W]	1 590	−1 560	1 318	−1 538	-105

Tabelle I. Signatur Mikrowellenofen

bestimmt. Genau diese Werte, die Leistung in Abhängigkeit zur Zeit, werden von den vorab genannten Messwertquellen mindestens erhoben.

Ob und wie ein Betriebsmittel anhand von erhobenen und gespeicherten Messwertdaten identifiziert werden kann, wird in den folgenden Abschnitten untersucht.

A. *Bestimmung Signatur*

Zunächst muss eine Datenstruktur gefunden werden, in der die gemessenen Werte gespeichert werden können. Hierzu wurden die Energieverbrauchskurven von einigen haushaltsüblichen Betriebsmitteln aufgezeichnet. Es wurde eine funksteuerbare Steckdose mit Energiemessfunktion aus dem Smart-Home Bereich mit einer modifizierten Firmware[9] ausgestattet. Die modifizierte Firmware ermöglicht das Auslesen der Energiemessdaten über ein standardisiertes Protokoll[10].

Die Firmware der Smart-Home-Steckdose sieht zur Kalibrierung einen einstellbaren Faktor vor. Der Faktor wurde mit Hilfe eines Multimeters, elektrisch bestimmt und eingestellt. Durch die Kalibrierung konnte im Messbereich zwischen 5W und 2300W eine maximale Abweichung des Messwertes von unter 5% erreicht werden. Diese Messtoleranz ist hinreichend genau für die Bestimmung der Signaturen.

Die Smart-Home-Steckdose wurde, wie in Abbildung 4 gezeigt, mit dem zu untersuchenden Prüfling und per WLAN mit einem Computer verbunden. Auf dem Computer werden die Messdaten der Steckdose in einer Datenbank[11] gespeichert. Zusätzlich wurde die Gesamtverbrauchskurve mit Hilfe der modernen Messeinrichtung des Haushaltes, in dem die Messungen stattgefunden haben ebenfalls in der Datenbank abgespeichert. Im Anschluss wurden aus den Messreihen die Verbrauchskurven geplottet und damit auch die Signatur des Betriebsmittels bestimmt. Zur grafischen Darstellung der Messreihen wurde Gnuplot[12] verwendet.

[9]https://tasmota.github.io/docs/
[10]https://mqtt.org/
[11]https://mariadb.org/
[12]http://www.gnuplot.info/

B. *Signaturen*

Die in diesem Abschnitt aufgenommenen Signaturen sollen dem Zweck der Wiedererkennung des Betriebsmittels in den Messdaten der modernen Messeinrichtung eines Haushaltes dienen. Dabei sollen der Verwendungszeitraum und ferner auch die Anwendungsart[13] nachvollzogen werden.

Zur Bestimmung der Signaturen werden die Energieverbrauchskurven zu Grunde gelegt. Aus den Verbrauchskurven können an markanten Punkten drei relevante Parameter abgelesen werden:

1) aktuelle Leistung P[W]
2) Änderung der Leistung ΔP[W]
3) Zeitspanne zwischen zwei Punkten Δt[Sekunden]

Die aktuelle Leistung zu 1) kann nur bedingt zur Identifikation beitragen da sie nur als Summe mehrerer Betriebmittel in der Gesamtverbrauchskurve vorliegt. Besser geeignet sind die Parameter zu 2) und 3), da sie sich auch in der Gesamtverbrauchskurve direkt niederschlagen und identifizieren lassen.

1) Mikrowellenofen: Zunächst wurde die Leistungskurve einer Mikrowelle mit einer angegebenen Leistung von 1500 Watt aufgenommen. Um die Auswirkung auf die Gesamtverbrauchskurve an der Messeinrichtung zu verdeutlichen, wurden beide Kurven in Abbildung 5 übereinander gelegt.

Die Leistungssprünge der Verbrauchskurve des Mikrowellenofens wurden mit senkrechten Pfeilen gekennzeichnet. Dabei wird deutlich, dass die markierten Punkte direkt der Leistungskurve der Messeinrichtung am Hausanschluss zugeordnet werden können. Folglich kann aus der Gesamtverbrauchskurve auch wieder zurück auf die Signatur des Betriebsmittels geschlossen werden.

Um aus der aufgenommenen Leistungskurve eine Signatur abzuleiten, werden die Leistungssprünge quantifiziert und in ein einer Datenstruktur tabellarisch erfasst. Hierzu werden die Zeitpunkte der Leistungssprünge und auch die Leistungsänderung an den betreffenden Stellen der Kurve erfasst.

[13]z.B. beim Wasserkocher die Menge Wasser und bei der Mikrowelle die eingestellte Leistungsstufe und Zeit

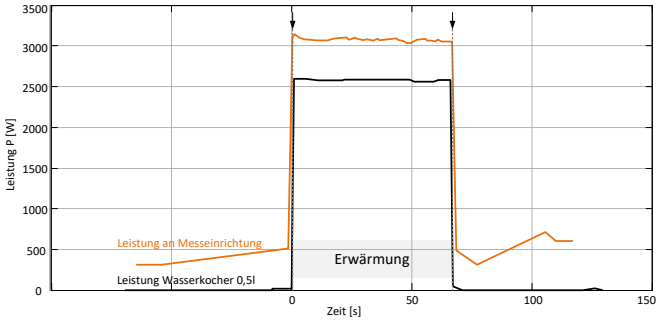


Abb. 6. Messung Wasserkocher

$\mathbf{t}[\mathbf{s}]$	0	66
$\mathbf{\Delta P}[\mathbf{W}]$	2 577	−2 534

Tabelle II. Signatur Wasserkocher

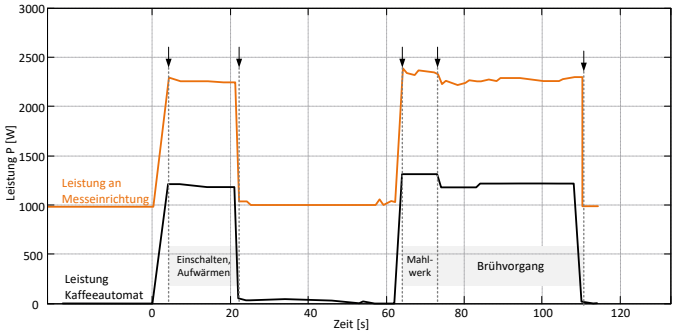


Abb. 7. Messung Kaffeeautomat

$\mathbf{t}[\mathbf{s}]$	0	17	60	70	106
$\mathbf{\Delta P}[\mathbf{W}]$	1 212	−1 129	1 313	-134	−1 190

Tabelle III. Signatur Kaffeeautomat

Für den Mikrowellenofen (1500 Watt, 60 Sekunden, Leistungsstufe 3/4 ergibt sich die in Tabelle I ermittelte Signatur. Aus der ermittelten Signatur können die vorab gewählten Einstellungen des Mikrowellenofens anhand der folgenden Betrachtung abgeleitet werden:

1) Die eingestellte Zeit lässt sich an der Zeitdifferenz zwischen dem ersten und letzten Eintrag der Signatur ablesen. In diesem Beispiel 60 Sekunden.
2) Die gewählte Leistungsstufe, hier 3/4, ergibt sich aus dem Tastverhältnis zwischen der Länge der Erwärmungsphasen und der Gesamtlaufzeit.

Diese Zusatzinformationen ermöglichen, nicht nur den Verwendungszeitraum der Mikrowelle, sondern auch die Art der Verwendung und damit das Verhalten, des Stromkunden detailreicher zu bestimmen.

2) Wasserkocher: Anschließend wurde die Signatur eines Wasserkochers mit einer angegebenen Leistung von 2850 Watt aufgenommen. Hierzu wurden $0,5$ Liter Wasser zum Kochen gebracht. Dabei wurde das Wasser von etwa $20°C$ auf etwa $100°C$ erwärmt. Die Erwärmung von $0,5l$ Wasser um 80 Kelvin benötigt rechnerisch 2784 Wattminuten. Das Messergebnis in Abbildung 6 spiegelt die Berechnung wieder. Die Einschaltzeit beträgt 1,1 Minuten und die umgesetzte Leistung beträgt etwa 2 550 Watt. Somit hat die Erwärmung $1,1\text{min.} \cdot 2\,550\text{W} = 2\,805$ Wattminuten benötigt. Die Signatur ist in Tabelle II dargestellt.

Auch hier kann neben dem Verwendungszeitraum die Art der Anwendung, der Menge des gekochten Wassers bestimmt werden.

3) Kaffeevollautomat: Bei einem Kaffeeautomaten können, wie in Abbildung 7 markiert, die einzelnen Betriebszustände anhand der Leistungskurve ermittelt werden.

Auch hier können aus der Signatur in Tabelle III einige Einstellparameter des Kaffeeautomaten nachvollzogen werden. Die Zeit, die das Mahlwerk aktiviert ist, bestimmt im Zusammenhang mit der gewählten Wassermenge maßgeblich die eingestellte Kaffeestärke. Die Zeit des Brühvorgangs kann auf die gewählte Kaffeemenge abgebildet werden.

4) Waschmaschine: Die Signatur einer Waschmaschine, gehört im Vergleich zu den hier aufgenommen Signaturen, zu den komplexeren Signaturen. Ein Waschprogramm steuert während des Waschvorganges verschiedene Komponenten der Waschmaschine an, die jeweils verschiedene Leistungsaufnahmen haben. Dadurch entsteht eine Energiesignatur mit einem vergleichsweise hohen Informationsgehalt.

In Abbildung 8 sind die Energieverbrauchskurven einer Waschmaschine und die der Messeinrichtung am Hausanschluss abgetragen. Hier wird aufgrund des großen Aufzeichnungsintervalls und der darin enthaltenen Einwirkungen von anderen Betriebsmitteln noch einmal deutlich, dass die Änderung der Leistung und die Zeit zwischen den Änderungen als Signatur zur Identifikation des Betriebsmittels herangezogen werden können.

Für die Waschmaschine (Waschgang Pflegeleicht $40°C$) ergibt sich die in Tabelle IV ermittelte Signatur.

Auch bei diesem Betriebsmittel ist die Signatur abhängig vom gewählten Waschgang.

C. Genauigkeit und Grenzen

Bisher wurden Betriebsmittel mit einer im Haushaltsbereich großen Anschlussleistung >1000 Watt, deren Leistungskurve hauptsächlich durch Sprünge und konstanten Verbrauch geprägt ist, betrachtet. Diese Klasse von Betriebsmitteln ist deutlich in der Gesamtverbrauchskurve der Messeinrichtung wiederzuerkennen. Die Sprünge sind hauptsächlich durch elektromechanische und elektrothermische Komponenten der Betriebsmittel geprägt.

Bei der Betrachtung der Leistungskurven von Betriebsmitteln mit einer geringen Leistung wie Computer oder Fernsehgerät wird klar, dass sich hier nur wenige und vor allem kleine Sprünge in der Leistungskurve abzeichnen. Aus diesem Grund ist die Detektion dieser Verbraucherklasse vergleichsweise schwierig. Insbesondere die Leistungsaufnahme eines Computers schwankt je nach Nutzung. Somit ist die Ableitung einer Signatur nur bedingt möglich.

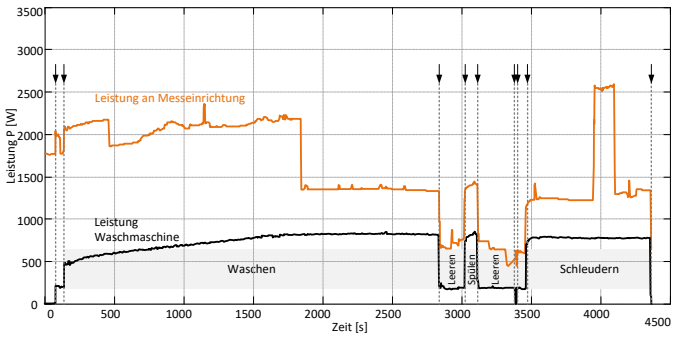


Abb. 8. Messung Waschmaschine

$\mathbf{t}[\mathbf{s}]$	0	62	2 756	2 942	3 032	3 306	3 314
$\mathbf{\Delta P}[\mathbf{W}]$	203	289	-599	550	-546	-186	186
$\mathbf{t}[\mathbf{s}]$	3 382	4 276					
$\mathbf{\Delta P}[\mathbf{W}]$	522	-678					

Tabelle IV. Signatur Waschmaschine

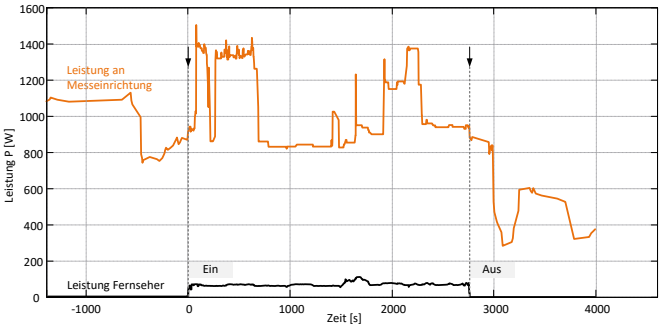


Abb. 9. Messung Fernseher

$\mathbf{t}[\mathbf{s}]$	0	2 751
$\mathbf{\Delta P}[\mathbf{W}]$	65	-65

Tabelle V. Signatur Fernseher

In der Abbildung 9 wurde die Leistungskurve eines Fernsehgerätes aufgenommen. Die Signatur in Tabelle V zeigt die Leistungssprünge beim Ein- und Ausschalten des Fernsehgerätes. Die Leistungssprünge betragen 65 Watt. Einerseits heben sich derart kleine Leistungssprünge in der Gesamtverbrauchskurve kaum hervor, andererseits gibt es im Leistungsbereich um 65 Watt viele haushaltsübliche Betriebsmittel, wie Lampen und Lüfter, die folglich eine ähnliche Signatur erzeugen würden.

Zusammenfassend kann festgestellt werden, dass die betrachtete Betriebsmittelklasse mit einem hohen Energiebedarf gut in der Gesamtleistungskurve zu identifizieren ist. Betriebsmittel mit einer geringen Leistungsaufnahme sind hingegen nur bedingt identifizierbar.

Bei der Betrachtung der Gesamtsituation der elektrischen Anlage muss zusätzlich auf Einflussfaktoren wie eine installierte Solaranlage rücksicht genommen werden. Die erzeugte Energie schlägt sich ebenfalls auf die Verbrauchskurve nieder. Insbesondere Wolken, die die Solaranlage abschatten, können sich in Form von Leistungssprüngen in der Gesamtverbrauchskurve niederschlagen. Die Höhe dieser Sprünge ist von der Sonneneinstrahlung und der Dichte der Wolken abhängig, so dass sich hier keine sichere Voraussage über den Betrag des Sprunges machen lässt. Die durch die Solaranlage verursachten Sprünge können ähnliche Signaturen wie tatsächlich vorhandene Betriebsmittel hervorrufen.

D. Forensischer Wert

Es konnte gezeigt werden, dass anhand der beim Kunden durch die Messeinrichtung aufgezeichneten Energiekurven Rückschlüsse auf die Verwendung der im Haushalt betriebenen elektrischen Betriebsmittel gezogen werden können. Hierdurch kann nun auch ein mögliches Nutzungsprofil erzeugt werden.

Das abgeleitete Nutzungsprofil könnte in einem Strafverfahren zur Überprüfung von Aussagen über die häusliche Anwesenheit und über die Tätigkeiten des Befragten herangezogen werden. Hierzu können die Ermittler die Verbrauchsdaten des Befragten vom Energielieferanten anfordern und untersuchen.

Zunächst kann der zeitlich interessante Abschnitt der Energieverbrauchskurve des Befragten, gegen einen Abschnitt zur gleichen Tageszeit an anderen Tagen, an denen er nachweislich anwesend b.z.w. abwesend war, verglichen werden. Anschließend können die angegebenen Aktivitäten des Befragten durch die in diesem Artikel vorgestellten Verfahren, untermauert oder widerlegt werden.

IV. Forensische Gegenmassnahmen

Bisher wurde gezeigt, wie aus der Leistungskurve der Messeinrichtung Rückschlüsse über den Betrieb von Verbrauchern im Haushalt gezogen werden können.

In diesem Abschnitt wird untersucht, mit welchen Ansätzen die Verbrauchermuster künstlich erzeugt werden können um die Nutzung von Haushaltsgeräten zu simulieren.

Es werden drei Ansätze verfolgt. Zum einen kann die Smart-Home- Steckdose, die schon für die Messungen genutzt wurde verwendet werden, um programmgesteuert Verbraucher ein- und auszuschalten. Ein weiterer Ansatz ist die Ausnutzung des dynamischen Energieverbrauches eines Computers mittels des Linux-Tools *stress*. Der dritte Ansatz verfolgt mittels eines Dimmers, die Leistung einer mobilen Elektroheizung zu steuern.

1) Smart-Home-Steckdose: Das programmgesteuerte Schalten von Betriebsmitteln klingt im ersten Moment naheliegend. Der praktische Versuch zeigt, dass nur eine bestimmte Auswahl von Betriebsmitteln hierzu geeignet ist. Der Wasserkocher aus der vorhergehenden Untersuchung lässt sich aus Sicherheitsgründen nur einschalten, wenn er bereits mit Energie versorgt wird. Die Mikrowelle und der Kaffeeautomat können ebenfalls nur nach lokaler Bedienung aktiviert werden. Diese Eigenschaft verhindert das Einschalten durch eine Smart-Home-Steckdose.

Hier beschränkt sich die Machbarkeit auf einfachste Betriebsmittel wie Lampen und Lüfter. Aus diesem Grund ist dieser Ansatz wenig relevant.

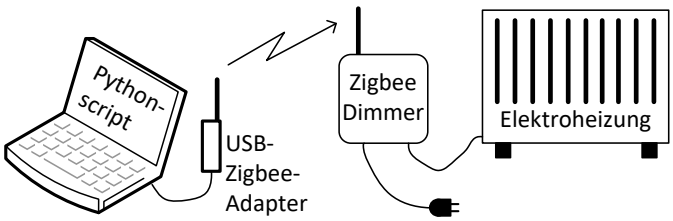


Abb. 10. Versuchsaufbau zur Erzeugung von Energiekurven

2) Leistungsdynamik Computer: Moderne Computer haben heutzutage ein großes Leistungsspektrum. Ein moderner Computer bezieht in der Leerlaufsituation eine relativ geringe Leistung. Wenn der Computer allerdings durch viele Berechnungen ausgelastet ist, steigt der Energiebedarf stark. Dieses Verhalten kann als forensische Gegenmaßnahme eingesetzt werden.

Mit dem Befehl in Listing 1 konnte der Betrieb des zuvor untersuchten Fernsehgerätes simuliert werden:

```
bash$ stress -c 16 -t 60
```

Listing 1. Aufruf stress Befehl

Der Paramater 'c' gibt an, wie viele Threads die Last erzeugen und wirkt sich somit auf die Höhe des Leistungssprunges aus. Der Parameter 't' gibt an, wie lange die Last erzeugt wird.

Mit einem üblichen Heim-PC ließen sich im Rahmen dieser Untersuchung Leistungssprünge von 65W erzeugen.

Ein Nachteil dieser Vorgehensweise ist die begrenzte Leistungsdynamik.

3) Dynamische Steuerung Elektroheizung: Die zwei bisher untersuchten antiforensischen Ansätze sind nur für wenige Simulationsfälle geeignet. Um eine für haushaltsübliche Betriebsmittel umfassende Simulation von Leistungskurven zu realisieren, wird eine variabel steuerbare Last mit ausreichend hoher Maximalleistung benötigt. Hierzu wurde eine Elektroheizung mit einer Leistung von 2000 Watt an einen Dimmer angeschlossen[14]. Durch den Dimmer kann die Leitung der Heizung in 256 Stufen zwischen 0% (Aus 0W) und 100% (volle Leistung bei 2000W) eingestellt werden. Die Auflösung beträgt $\frac{2000W}{256} = 7,8W$ und ist somit ausreichend für eine präzise Simulation. Gesteuert wird der Dimmer durch ein Python-Script, welches die Leistungssprünge aus einer Signaturtabelle ausliest und per Zigbee-Protokoll [15] an den Dimmer sendet.

Mit dem Aufbau aus Abbildung 10 ist es gelungen, die Lastprofile der zuvor untersuchten Betriebmittel, unter Ausschluss des Wasserkochers, zu generieren. Der Wasserkocher hat eine Leistungsaufnahme von rund 2580W, die die simulierbare Leistung von 2000W übersteigt. Um auch Lastkurven für leistungsstärkere Verbraucher zu generieren, kann der Simulationausfbau aus Abbildung 10 mit einer weiteren Last erweitert werden.

[14]Der Dimmer ist eigentlich für die Leuchtstärkenstellung von Halogenlampen vorgesehen

[15]Zigbee ist ein Protokoll zur Datenübertragung per Funk https://zigbeealliance.org/solution/zigbee/

V. Zusammenfassung

Die Digitalisierung der Energienetze ist für die Versorgungssicherheit wichtig. Damit dezentrale Einspeiseanlagen das Stromnetz nicht aus dem Gleichgewicht bringen, werden Steuer- und Messeinrichtungen durch die Energieversorger in den Netzen positioniert. Insbesondere die Beobachtbarkeit der Energieflüsse trägt zum sicheren Betrieb bei. Durch Messungen an verschiedenen Punkten im Stromnetz werden neue Informationsquellen für die schnelle Entstörung und auch für die digitale Forensik geschaffen.

In diesem Artikel wurde untersucht, wie Messdaten der Messeinrichtung am Hausanschluss des Kunden zur forensischen Untersuchung herangezogen werden können. Es wurde gezeigt, dass die Verwendung von einigen haushaltsüblichen Betriebsmitteln mit guter Qualität nachgewiesen werden kann. Bei einigen Betriebsmitteln konnte sogar die Verwendungsart, wie die Menge des gekochten Wassers im Wasserkocher nachvollzogen werden.

Betriebsmittel mit einer geringen Leistung sind vergleichsweise schwer zu detektieren, da sie einerseits nur eine geringe Auswirkung auf die Gesamtverbrauchskurve haben und sich andererseits in der Leistungsaufnahme voneinander kaum unterscheiden. Beispielhaft sind hier der Computer in der Office-Nutzung und das Fernsehgerät mit einem annähernd gleichen Leistungsbedarf.

Der Rollout von modernen Messeinrichtungen in den deutschen Haushalten bringt zum einen eine bessere Transparenz des Energieverbrauches für den Kunden, birgt allerdings auch einen forensischen Wert, der das Ausspähen des Verhaltens der Kunden ermöglicht.

Es konnte ausserdem gezeigt werden, wie mit marktüblichen Komponenten forensische Gegenmaßnahmen getroffen werden können um Energiekurven zu simulieren und damit Nutzungsprofile zu fälschen.

Literatur

[1] K. Strauß, *Wärmekraftwerke: Von den Anfängen im 19. Jahrhundert bis zur Endphase ihrer Entwicklung*. Berlin and Heidelberg: Springer Vieweg, 2016.

[2] Bundesverband der Energie- und Wasserwirtschaft (BDEW), "Entwicklung der stromnetze in deutschland," 2021. [Online]. Available: https://www.bdew.de/service/daten-und-grafiken/entwicklung-der-stromnetze-deutschland/ (Zugriff: 18.05.2021).

[3] Süddeutsche Zeitung, "Stromausfall in münchen," 2021. [Online]. Available: https://www.sueddeutsche.de/muenchen/muenchen-stromausfall-ermittlungen-bilder-1.5301760 (Zugriff: 10.07.2021).

[4] Stromnetz Berlin, "Das berliner stromnetz," 2021. [Online]. Available: https://www.stromnetz.berlin/technik-und-innovationen/aufbau-und-funktionsweise-stromnetz (Zugriff: 31.05.2021).

[5] Bundesverband der Energie- und Wasserwirtschaft (BDEW), "Entwicklung der stromerzeugung aus erneuerbaren energien in deutschland seit 1991," 2021. [Online]. Available: https://www.bdew.de/service/daten-und-grafiken/entwicklung-der-stromerzeugung-aus-erneuerbaren-energien-deutschland-seit-1991/ (Zugriff: 18.05.2021).

[6] ——, "Beitrag der erneuerbaren energieen zur deckung des stromverbrauchs," 2021. [Online]. Available: https://www.bdew.de/media/documents/Beitrag_EE_zur_Deckung_des_Stromverbrauchs_Vgl_VJ_online_o_quartalsweise_Ki_03052021.pdf (Zugriff: 18.05.2021).

[7] V. Crastan, *Elektrische Energieversorgung 3: Dynamik, Regelung und Stabilität, Versorgungsqualität, Netzplanung, Betriebsplanung und -führung, Leit- und Informationstechnik, FACTS, HGÜ*, 2nd ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 2018.

[8] G. Götzelmann, "Sicherer netzbetrieb durch digitale schutzeinrichtungen," *Elektrotechnik und Informationstechnik*, vol. 121, no. 10, pp. 380–382, 2004.

[9] Bundesnetzagentur, "Eckpunktepapier zur ausgestaltung des qualitätselements netzzuverlässigkeit strom im rahmen der anreizregulierung," 2021. [Online]. Available: https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Energie/Unternehmen_Institutionen/Netzentgelte/Strom/Qualitaetselement/EckpunktspapierAusgestaltungQ-Element.pdf?__blob=publicationFile&v=1 (Zugriff: 29.05.2021).

[10] ——, "Einzelstörungsdaten der gemeldeten versorgungsunterbrechungen," 2021. [Online]. Available: https://www.bundesnetzagentur.de/DE/Sachgebiete/ElektrizitaetundGas/Unternehmen_Institutionen/Versorgungssicherheit/Versorgungsunterbrechungen/Auswertung_Strom/Versorgungsunterbrech_Strom_node.html (Zugriff: 29.05.2021).

[11] Bundesamt für Justiz, "Gesetz für den ausbau erneuerbarer energien, § 9 technische vorgaben," 2021. [Online]. Available: http://www.gesetze-im-internet.de/eeg_2014/__9.html (Zugriff: 29.05.2021).

[12] ——, "Gesetz für den ausbau erneuerbarer energien, § 14 einspeisemanagement," 2021. [Online]. Available: http://www.gesetze-im-internet.de/eeg_2014/__14.html (Zugriff: 29.05.2021).

[13] ——, "Gesetz über den messstellenbetrieb und die datenkommunikation in intelligenten energienetzen, § 29 ausstattung von messstellen mit intelligenten messsystemen und modernen messeinrichtungen," 2021. [Online]. Available: http://www.gesetze-im-internet.de/messbg/__29.html (Zugriff: 18.05.2021).