Diskussionspapier

IT-SICHERHEIT DER ENERGIE-SYNCHRONISATIONS-PLATTFORM

KOPERNIKUS PROJEKTE
SynErgie
Die Zukunft unserer Energie

GEFÖRDERT VOM

Bundesministerium
für Bildung
und Forschung

KOPERNIKUS PROJEKTE
SynErgie
Die Zukunft unserer Energie

IT-Sicherheit für die Energiesynchronisationsplattform

Teil der Reihe „Diskussionspapiere V4 – Konzept der Energiesynchronisationsplattform“

Cluster Informations- und Kommunikationstechnik des Kopernikus-Projekts „SynErgie – Synchronisierte und energieadaptive Produktionstechnik zur flexiblen Ausrichtung von Industrieprozessen auf eine fluktuierende Energieversorgung“, gefördert durch das Bundesministerium für Bildung und Forschung

Stand Oktober 2021

DOI: https://doi.org/10.24406/IGCV-N-642372

Fraunhofer-Institut für Integrierte Schaltungen IIS
Nordostpark 84
90411 Nürnberg
www.iis.fraunhofer.de

Software AG
Uhlandstraße 12
64297 Darmstadt
softwareag.com

Fraunhofer-Institut für Angewandte Informationstechnik FIT
Schloss Birlinghoven
53754 Sankt Augustin
www.fit.fraunhofer.de

GEFÖRDERT VOM
Bundesministerium
für Bildung
und Forschung

AUTOREN

Fraunhofer-Institut für Integrierte Schaltungen IIS
Andreas Oeder
Karlheinz Ronge

Software AG
Jens Schimmelpfennig
Christian Winter

Fraunhofer-Institut für Angewandte Informationstechnik FIT
Raphael Ahrens

VORWORT UND DANKSAGUNG

Diese Publikation ist Teil der Reihe „Diskussionspapiere V4 – Konzept der Energiesynchronisationsplattform“, welche den Arbeitsstand des Clusters III – Informations- und Kommunikationstechnik im Kopernikus-Projekt SynErgie im Oktober 2021 dokumentiert. In dieser vierten Auflage wurde das Diskussionspapier erstmals in fünf thematisch eigenständige Papiere aufgeteilt und um eine Executive Summary ergänzt, damit wir die Informationen zielgerichtet zur Verfügung stellen können. Die Diskussionspapiere basieren auf den vorherigen Auflagen (Reinhart et al. 2020; Reinhart et al. 2018) sowie insbesondere auch auf Bauernhansl et al. (2019). Die Diskussionspapiere sollen zum Diskurs in Forschung und Praxis anregen, um so die erarbeiteten Lösungen kontinuierlich zu verbessern und weiterzuentwickeln.

Folgende Diskussionspapiere sind erschienen und wurden von den genannten Ansprechpersonen koordiniert:

- Executive Summary: Konzept der Energiesynchronisationsplattform – Diskussionspapiere
  DOI: https://doi.org/10.24406/IGCV-N-642368
  Jana Köberlein, jana.koeberlein@igcv.fraunhofer.de
- Referenzarchitektur der Energiesynchronisationsplattform
  DOI: https://doi.org/10.24406/IGCV-N-642369
  Sergio Potenciano Menci, sergio.potenciano-menci@uni.lu
- Das Energieflexibilitätsdatenmodell der Energiesynchronisationsplattform
  DOI: https://doi.org/10.24406/IGCV-N-642370
  Martin Lindner, m.lindner@ptw.tu-darmstadt.de
- Optimierung auf der Energiesynchronisationsplattform
  DOI: https://doi.org/10.24406/IGCV-N-642371
  Lukas Bank, lukas.bank@igcv.fraunhofer.de
- IT-Sicherheit der Energiesynchronisationsplattform
  DOI: https://doi.org/10.24406/IGCV-N-642372
  Andreas Oeder, andreas.oeder@iis.fraunhofer.de
- Demonstratoren der Energiesynchronisationsplattform
  DOI: https://doi.org/10.24406/IGCV-N-642373
  Andreas Schlereth, andreas.schlereth@ipa.fraunhofer.de

Verantwortlich für die Inhalte der einzelnen Diskussionspapiere sind die jeweils genannten Autor:innen.

Wir bedanken uns herzlich beim Bundesministerium für Bildung und Forschung (BMBF) für die finanzielle Unterstützung und beim Projektträger Jülich (PtJ) für die Betreuung des Kopernikus-Projektes SynErgie.

Des Weiteren bedanken wir uns bei allen Kolleginnen und Kollegen aus dem SynErgie-Projektkonsortium, die mit Ideen und kritischen Anmerkungen zur Entstehung der in diesem Diskussionspapier dargestellten Konzepte beigetragen haben. Insbesondere bedanken wir uns auch bei denen, die an der aktuellen Auflage des Diskussionspapiers nicht mehr selbst beteiligt waren:

Dennis Bauer, Martin Brugger, Volker Bühner, Eduardo Colangelo, Leon Haupt, Fabian Hering, Robert Keller, Benjamin Meyer, Lena Pfeilsticker, Jaroslav Pullmann, Christian Schmidt, Philipp Seitz, Peter Simon und Thomas Weber

Weitere Informationen zu den Kopernikus-Projekten und SynErgie finden Sie auf folgenden Webseiten:

https://kopernikus-projekte.de

https://synergie-projekt.de

KURZZUSAMMENFASSUNG

Die Energiesynchronisationsplattform (ESP) mit ihren Teilplattformen Markplattform (MP) und Unternehmensplattform (UP) nutzt IKT-Infrastruktur zum Austausch von Informationen. Dabei ist neben der Kommunikation in internen Firmennetzen auch die Nutzung öffentlicher Kommunikationsnetze ein wichtiger Bestandteil. Somit ist die ESP den Gefahren von Cyber-Angriffen ausgesetzt. Neben vertraulichen Informationen, wie Produktionsdaten, werden auch Flexibilitätspotenziale und Flexibilitätsmaßnahmen übertragen, die den Stromverbrauch oder die Stromerzeugung in den teilnehmenden Unternehmen steuern und damit einerseits den Betrieb von Produktionsanlagen beeinflussen und andererseits Rückwirkungen auf das Stromnetz haben. Daher ist ein effektiver Schutz vor Angriffen auf die ESP essentiell.

Ziel ist es, durch die Definition von IT-Sicherheitsmaßnahmen eine Risikominimierung zu erzielen. Dabei dient das Threat-Modeling der Ermittlung möglicher Angriffe. Der ermittelte Schutzbedarf wiederum richtet sich nach den möglichen Schäden, die entstehen können, wenn bei den verarbeiteten Informationen eines der Schutzziele Vertraulichkeit, Verfügbarkeit, Integrität und Nicht-Abstreitbarkeit verletzt wird. Durch die Einführung der Sicherheitslevel für die Softwarekomponenten der ESP (Services und Kernkomponenten) erfolgt schließlich eine Abstufung der IT-Sicherheitsanforderungen und damit der zu ergreifenden IT-Sicherheitsmaßnahmen, die sich an regulatorischen Rahmenbedingungen (Kritische Infrastrukturen), dem Schutzbedarf von ausgetauschten Informationen, sowie den Risiken und möglichen Schäden (insb. hinsichtlich Produktionsausfällen im Unternehmen, sowie hinsichtlich des zuverlässigen Betriebs der Stromnetze) ausrichtet. Ziel ist ein abgestuftes und jeweils am Bedarf orientiertes, notwendiges Niveau an Sicherheit.

Zur Gewährleistung des Sicherheitsniveaus, d. h. insbesondere auch zur Minimierung des Risikos bei dem Betrieb der Plattformen und aus praktischer Perspektive zur Abwehr von potentiellen Angriffen auf und über die Plattformen, wurden verschiedene technische und organisatorische Sicherheitsmaßnahmen definiert. Das Security-Life Cycle Management begleitet dabei die Plattformen in allen Entwicklungs- und Betriebsphasen. Es betrachtet die sicherheitsrelevanten Aspekte der Services und damit die Aufrechterhaltung des Sicherheitsniveaus von der ersten Idee über die Umsetzung, den Betrieb, bis hin zur Außerbetriebnahme. Dadurch wird eine kontinuierliche Berücksichtigung von Sicherheitsbelangen gewährleistet. Durch ein zugriffsbasiertes Rollenmodell werden die Aufgaben und damit die Zugriffsrechte von Rollen bestimmt. Dabei stehen eine sinnvolle Aufgabentrennung, das Need-to-Know Prinzip, sowie das Least-Privilege Prinzip im Vordergrund. Dies bedeutet, einer Rolle sollen nur die für die Aufgabe erforderlichen Rechte eingeräumt werden, damit bei Identitätsdiebstahl oder Manipulationsversuchen der mögliche Schaden eingegrenzt werden kann. Mit einer sogenannten Public-Key-Infrastruktur werden Identitäten plattformübergreifend und ggf. auch innerhalb von Plattformen bescheinigt, so dass die an einer Kommunikation beteiligten Partner und Komponenten Gewissheit über die Identität der Quellen und Empfänger ihrer Informationen haben. Auf technischer Ebene ermöglichen die von der PKI erstellten Zertifikate die Anwendungen Authentifizierung, digitale Signatur und Verschlüsselung. Für die physische und logische Infrastruktur der ESP sind ebenfalls Maßnahmen vorgesehen, etwa in Bezug auf die Netzwerkinfrastruktur, die Identitäts- und Berechtigungsverwaltung und das Logging.

INHALTSVERZEICHNIS

ABBILDUNGSVERZEICHNIS

TABELLENVERZEICHNIS

1 EINLEITUNG

1.1 Einordnung und Motivation

Die Eindämmung des Klimawandels gilt als eine der größten globalen Herausforderungen im 21. Jahrhundert (United Nations 2015). Der Anstieg der Durchschnittstemperatur auf der Erdoberfläche, insbesondere verursacht durch die zunehmende Konzentration von Kohlenstoffdioxid und anderen Treibhausgasen in der Atmosphäre, hat weitreichende Auswirkungen auf Mensch und Umwelt in allen Regionen der Welt. Es ist wissenschaftlicher Konsens, dass aufgrund des durch menschliche Aktivität verursachten Klimawandels extreme Klimaereignisse wie Hitzewellen, starke Regenfälle und Dürren häufiger und extremer werden (IPCC 2021). Diese Zunahme der extremen Wetterereignisse ist bereits heute deutlich spürbar (Mann et al. 2017). Der zwischenstaatliche Ausschuss für Klimaänderungen (IPCC) geht davon aus, dass ohne schnelle und umfassende Verringerung der Treibhausgasemissionen die globale Erwärmung von 1,5°C und 2°C im Laufe des 21. Jahrhunderts überschritten werden wird. Mit einer weiteren globalen Erwärmung werden die Veränderungen, die schon heute spürbar sind, weiter zunehmen, wobei diese bereits bei einer Erwärmung um 2°C im Vergleich zu 1,5°C deutlich häufiger und/oder ausgeprägter sein werden (IPCC 2021).
Dies führt zu hoher gesellschaftlicher Aufmerksamkeit für Klimaschutz und übt Druck auf politische und wirtschaftliche Entscheidungsträger aus, den notwendigen Rahmen für die Eindämmung des Klimawandels zu schaffen sowie die Anstrengungen für den Klimaschutz zu intensivieren. Da die Nutzung fossiler Brennstoffe wie Braunkohle, Steinkohle und Erdöl zur Energieerzeugung signifikante Mengen an Treibhausgasen freisetzt und somit ein Hauptverursacher für die Veränderung des Klimas ist, zielen Maßnahmen insbesondere auf einen nachhaltigen Energiesektor ab. Die Energieerzeugung hat heute mit knapp 29% den größten Anteil der Treibhausgasemissionen in Deutschland (Uba 2021c). Mit dem Pariser Klimaabkommen im Jahr 2015 wurde erstmals ein globaler Rahmen geschaffen, um den Herausforderungen des Klimawandels zu begegnen (United Nations 2015). Der Deutsche Bundestag hat beschlossen, seine Ziele aus dem Klimaschutzplan 2050 mit einer Novelle des Klimaschutzgesetzes noch einmal zu verstärken und strebt an, in Deutschland bis 2045 Klimaneutralität zu erreichen. Auch die Zwischen- und Sektorenziele wurden im Rahmen dessen weiter angehoben (BMU 2021). Mit dem Erneuerbaren-Energien-Gesetz (EEG) 2021 plant die Bundesregierung, die Erzeugung und den Verbrauch von Strom in Deutschland nun bereits vor 2050 vollständig zu dekarbonisieren (BMWi 2021). Im Jahr 2020 betrug der Anteil am Bruttostromverbrauch in Deutschland bereits 45,4%[2] und am Bruttoenergieverbrauch 19,6%[2] (Uba 2021a). Damit sind die Zielwerte für das Jahr 2020 zwar erreicht, dennoch liegt noch ein weiter Weg vor uns. Das Energiewirtschaftliche Institut an der Universität zu Köln (EWI) errechnete, dass das Zwischenziel eines Anteils erneuerbarer Energien am Bruttostromverbrauch von 65% im Jahr 2030 nicht erreicht werden könne. Dies begründet sich insbesondere in der Annahme eines steigenden Stromverbrauchs, getrieben durch die Sektorkopplung, welcher der prognostizierten Stromerzeugung aus Erneuerbaren gegenübergestellt wurde (Gierkink und Sprenger 2020).
Die notwendige Transformation des Energiesystems geht mit großen Herausforderungen einher. Der Anteil von Wind- und Sonnenenergie an der Bruttostrom- bzw. Bruttoenergieerzeugung aus erneuerbaren Energiequellen betrug im Jahr 2020 bereits über 70%[2] respektive etwa 40%[2] (Uba 2021b). Aufgrund der Wetterabhängigkeit der Erzeugung von Wind- und Sonnenenergie unterliegt diese erheblichen Schwankungen. Im Gegensatz zu konventionellen Kraftwerken sind diese volatilen erneuerbaren Energiequellen nicht regelbar und stellen das Stromnetz vor die Herausforderung,

[2] Vorläufige Angabe

Stromangebot und -nachfrage in Einklang zu bringen. Um Netzstabilität zu gewährleisten, unternehmen die Netzbetreiber große Anstrengungen, indem sie Reserven vorhalten und diese bei einem geringen Stromdargebot durch Wind und Sonne vorübergehend aktivieren oder bei einer Überlast treibhausgasintensive Kraftwerke abschalten. Zudem werden zusätzlich immer noch beachtliche Mengen der Stromerzeugung aus erneuerbaren Energien im Rahmen von Einspeisemanagement-Maßnahmen abgeregelt (Bundesnetzagentur 2020).

In der Vergangenheit wurden Veränderungen in der Stromnachfrage durch die Steuerung der Stromerzeugung in konventionellen Kraftwerken ausgeglichen (Papaefthymiou et al. 2018). Aufgrund der Prognoseunsicherheit und der wenig beeinflussbaren Natur erneuerbarer Energien ist dieser Mechanismus auf der Stromerzeugungsseite keine ausreichende Option mehr und erhöht den Bedarf an Flexibilität. Diese Entwicklung wird von Papaefthymiou et al. (2018) als "Flexibilitätslücke" beschrieben. Im Allgemeinen stehen vier Optionen zur Verfügung, um die notwendige Flexibilität im System bereitzustellen (Lund et al. 2015; Müller und Möst 2018)

- Übertragung: Flexibilität durch den Ausbau des Stromnetzes
- Speicherung: Flexibilität durch Speicherung
- Sektorkopplung: Flexibilität durch Energieumwandlung zwischen Energiesektoren
- Nachfrage: Flexibilität durch Demand Response (DR)

Aufgrund der hohen Kosten und mangelnden sozialen Akzeptanz des Netzausbaus (Battaglini et al. 2012; Bertsch et al. 2016), der immer noch sehr hohen Kosten für die Stromspeicherung (Lund et al. 2016) und der langsamen Fortschritte bei der Sektorkopplung, wie Power-to-Gas, Elektromobilität, etc. (Papaefthymiou et al. 2018), ist das sogenannte DR zur Anpassung der Stromnachfrage eine wettbewerbsfähige Flexibilitätsoption. DR ist eine Kategorie von Demand Side Management. Über Anreizzahlungen oder variable Strompreise bewirken DR-Maßnahmen Veränderungen der Stromnachfrage (Albadi und El-Saadany 2008; Markle-Huss et al. 2016). Motiviert durch solche Preissignale entscheiden sich teilnehmende Stromverbraucher selbstständig dafür, ihre Stromnachfrage in Zeiträumen von wenigen Minuten bis zu einigen Stunden flexibel zu gestalten (Palensky und Dietrich 2011). Realisiert wird dies durch Maßnahmen der Lasterhöhung, des Lastverzichts und der Lastverschiebung (Jazayeri et al. 2005). Bei der Automatisierung von DR zum sogenannten Automated Demand Response spielt die Informations- und Kommunikationstechnik eine maßgebliche Rolle (Bauernhansl et al. 2019).

Die Industrie stellt weltweit den größten Stromverbraucher dar, wodurch sich für diesen Sektor ein großes (theoretisches) Potenzial für DR ergibt (European Environmental Agency 2020). Das DR-Potenzial kann durch die Industrie zu vergleichsweise niedrigen Grenzkosten bereitgestellt werden (Steurer 2017). Energieintensive Unternehmen nutzen deshalb bereits DR, wenn auch noch in geringem Umfang (Papaefthymiou et al. 2018; Sauer et al. 2019b). Eine flächendeckende Nutzung in der Industrie erfordert einen neuen Ansatz der Zusammenarbeit zwischen Industrie, Stromversorgern und Netzbetreibern, was vor dem Hintergrund zunehmender Unsicherheit und Volatilität in der Stromversorgung neue Mechanismen und Interaktionsmöglichkeiten für eine wettbewerbsfähige Strombeschaffung erfordert. Um der Industrie die aktive Anpassung des Stromverbrauchs durch vereinfachte Partizipation am Stromhandel zu ermöglichen, müssen die technischen und organisatorischen Voraussetzungen geschaffen und mittels eines geeigneten Plattformökosystems umgesetzt werden, an dem alle relevanten Stakeholder beteiligt sind.

Die beschriebene Komplexität der Energiewende und die damit verbundene Herausforderung zum Ausgleich von Stromangebot und -nachfrage spiegelt sich deshalb auch in der Forschungsthematik der industriellen DR wider (Seifermann et al. 2019). Eine integrierte Betrachtung technischer, wirtschaftlicher und gesellschaftlicher Aspekte ist daher unerlässlich. Im Einzelnen sind dies

- die Untersuchung der technischen Flexibilisierungsmöglichkeit von branchenspezifischen Schlüsselproduktionsprozessen der produzierenden Industrie,
- die Betrachtung der technischen Flexibilisierungsmöglichkeit der branchenübergreifenden Produktionsinfrastruktur,
- die Erforschung einer durchgängigen Verbindung zwischen Maschine und Strommarkt sowie deren Befähigung zur automatisierten Entscheidungsfindung über Informations- und Kommunikationstechnik,
- die Analyse und Neugestaltung der regulatorischen Rahmenbedingungen des Markt- und Stromsystems zur Schaffung von wirtschaftlichen Anreizen für industrielles Demand Response,
- die Bestimmung der Höhe des Flexibilitätspotenzials sowie
- die Untersuchung ökonomischer, ökologischer und gesellschaftlicher Auswirkungen.

1.2 Das Projekt SynErgie

Das Projekt SynErgie ist Teil der Kopernikus-Projekte, eine der größten deutschen Initiativen im Rahmen der Energiewende. In einem interdisziplinären Konsortium aus Wissenschaft, Industrie und Zivilgesellschaft werden Technologien und Lösungen erarbeitet, um den Energiebedarf der deutschen Industrie effektiv mit dem volatilen Energieangebot zu synchronisieren (Sauer et al. 2019a). Die vorab genannten technischen, wirtschaftlichen und gesellschaftlichen Aspekte für DR betrachtet das Projekt SynErgie in einer analogen Struktur (siehe Abbildung 1), wobei die Informations- und Kommunikationstechnik eine Schlüsselrolle zur Verbindung der Produktion und Produktionsinfrastruktur mit dem Markt- und Stromsystem einnimmt.

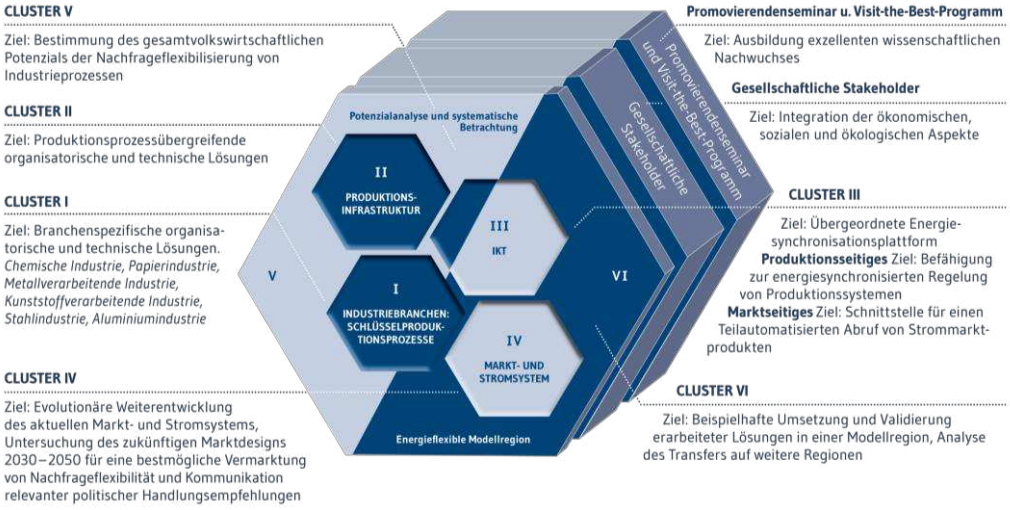

ABBILDUNG 1: STRUKTUR DES KOPERNIKUS-PROJEKTS SYNERGIE

Hierdurch können insbesondere im Bereich des industriellen DR Informationsflüsse auch über Unternehmensgrenzen hinweg definiert und aufgebaut werden. Die klassische Informations- und Kommunikationstechnik in Unternehmen wird also erweitert (Körner et al. 2019), um das Zusammenspiel diverser Optimierungsservices zu koordinieren

(Seitz et al. 2019). Darauf aufbauend wird die Automatisierung und Standardisierung (Schott et al. 2019) des gesamten Prozesses zur Energieflexibilitätsvermarktung möglich (Bauernhansl et al. 2019). Um der Bedeutung logistischer Kennzahlen für produzierende Unternehmen gerecht zu werden, ist es des Weiteren essenziell, Energieflexibilität in die Produktionsplanung und -steuerung und damit in die logistischen Zielgrößen zu integrieren (Pfeilsticker et al. 2019).

1.3 Ziele und Vision der Energiesynchronisationsplattform

Das Ziel der Energiesynchronisationsplattform (ESP) ist es, durch den Aufbau eines Plattformökosystems den gesamten Prozess des Energieflexibilitätshandels von der Maschine bis zum Energiemarkt zu automatisieren und zu standardisieren. Hierfür ist insbesondere auch die Integration von DR in die Produktionsplanung und -steuerung in produzierenden Unternehmen notwendig. Die Vision der ESP sieht deshalb vor, eine branchenübergreifende Plattform zum Energieflexibilitätshandel in Deutschland aufzubauen und damit »die« zentrale Energieflexibilitätsplattform[3] zu werden. Die ESP sowie die modular darauf aufbauenden Services zur Flexibilisierung der energieintensiven Industrie und der Flexibilitätsvermarktung ermöglichen der Industrie eine aktive Teilnahme mit möglichst niedrigen Eintrittsbarrieren an den Energiemärkten − einerseits durch eine akkuratere und schnellere Bedarfsplanung (Konsumentenrolle), andererseits durch das Anbieten von Energieflexibilitätspotenzial (Anbieterrolle). Die ESP ermöglicht damit eine ganzheitliche Betrachtung des Stromsystems, um im Sinne von automatisiertem DR eine möglichst effektive und effiziente Synchronisation von Stromangebot und -nachfrage für die Industrie zu realisieren.

Bei der ESP selbst handelt es sich nicht um eine physische Plattform. Sie beschreibt vielmehr als übergeordnetes Konzept die Zusammenarbeit zwischen den Teilplattformen Unternehmensplattform (UP) und Marktplattform (MP), was Rahmenbedingungen, Schnittstellen, Datenmodelle, Stakeholder und Sicherheitsaspekte umfasst und den gesamten Prozess des automatisierten Energieflexibilitätshandels von der Maschine bis zum Energiemarkt abbildet. Abhängig von den Gegebenheiten können die Rollen der Unternehmen jederzeit flexibel angepasst werden (Bauernhansl et al. 2019; Schott et al. 2018; Bauer et al. 2017). Die beschriebenen Eigenschaften bieten einen deutlich höheren Funktionsumfang und ein höheres Informationsangebot als aktuell bestehende Plattformen (Rösch et al. 2019).

Für die ESP wurde ein durchgängiges Konzept, einschließlich des Daten- und Informationsflusses von der Maschine bis zum Energiemarkt, entwickelt (siehe Diskussionspapier „Referenzarchitektur der Energiesynchronisationsplattform“ (Fridgen et al. 2021)). Hierfür war insbesondere die Identifikation und Entwicklung von Schnittstellen sowie die Definition eines Datenmodells für Energieflexibilität (siehe Diskussionspapier „Energieflexibilitätsdatenmodell der Energiesynchronisationsplattform“ (Buhl et al. 2021)) erforderlich. Den Kern der ESP stellen Services dar, die Daten verarbeiten, aggregieren, miteinander austauschen und Energieflexibilität bewerten und bereitstellen. Insbesondere wurden für den optimalen Betrieb der Energieflexiblen Fabrik eine Reihe von Optimierungsservices entwickelt (siehe Diskussionspapier „Optimierung auf der Energiesynchronisationsplattform“ (Schilp et al. 2021)). Das Konzept der ESP sieht dabei Erweiterungsmöglichkeiten für verschiedene Energieträger vor, auch wenn der Fokus eindeutig auf elektrischer Energie liegt. Um den Mehrwert der automatisiert gehandelten Energieflexibilität für Industrieunternehmen sowie Teilnehmer der Energiemärkte aufzuzeigen, werden verschiedene Demonstratoren konzipiert, entwickelt und umgesetzt (siehe Diskussionspapier „Demonstratoren der Energiesynchronisationsplattform“ (Bauernhansl et al. 2021)). Sie werden im Forschungsumfeld sowie, gemeinsam mit produzierenden Unternehmen und

[3] Zentrale Plattform ist an dieser Stelle im Sinne einer Meta-Plattform zu verstehen, welche bestehende Angebote integriert und nicht ablöst.

Netzbetreibern, im industriellen Umfeld und der Energieflexiblen Modellregion Augsburg aufgebaut. IT-Sicherheit muss bei allen Konzeptions- und Umsetzungsschritten eines Systems in adäquatem Maß bedacht werden sowie bei allen logischen und physischen Bestandteilen des Systems entsprechend implementiert und im operativen Betrieb aufrechterhalten werden. Zur Gewährleistung des Sicherheitsniveaus, d. h. insbesondere auch zur Minimierung des Risikos beim Betrieb der Plattformen und aus praktischer Perspektive zur Abwehr von potentiellen Angriffen auf und über die Plattformen, wurden deshalb verschiedene technische und organisatorische Sicherheitsmaßnahmen definiert (siehe Diskussionspapier „IT-Sicherheit der Energiesynchronisationsplattform“ (Oeder et al. 2021)).

Die technische Umsetzung der ESP bildet die Grundlage für eine echtzeitnahe Synchronisation flexibler Industrieprozesse mit dem volatilen Strom-/Energieangebot und damit volatilen Preisen. Abhängig vom konkreten Ziel der Umsetzung von Energieflexibilität können Unternehmen Einsparungen durch die Reduzierung der Strombeschaffungskosten und/oder der Netzentgelte sowie weiterer Umlagen erzielen oder Erlöse durch das Anbieten von Energieflexibilität für Dritte (bspw. als Systemdienstleistung) generieren. Von zentraler Bedeutung für die Akzeptanz und den Erfolg des erarbeiteten Konzepts sind auf der einen Seite die Wirtschaftlichkeit der Energieflexibilität für die Unternehmen sowie, auf der anderen Seite, die technischen Aspekte des Schutzes sensibler Unternehmensdaten, denen im Rahmen der Konzeption der ESP eine besondere Bedeutung zukommt. Die zentralen Befähiger für eine Akzeptanzerhöhung sind die Harmonisierung und Standardisierung eines erforderlichen Datenmodells und einer Schnittstelle zum sicheren Datenaustausch zwischen produzierenden Unternehmen und den Strommärkten.

1.4 IT-Sicherheit für den sicheren Betrieb der ESP

Das vorliegende Detailpapier behandelt den Schwerpunkt IT-Sicherheit. Die IT-Sicherheit ist eine wesentliche Voraussetzung für einen erfolgreichen Betrieb von IT-Systemen und deshalb zentrales Querschnittsthema des Referenzarchitekturmodells (Fridgen et al. 2021). IT-Sicherheit muss bei allen Konzeptions-und Umsetzungsschritten eines Systems in einem adäquaten Maß bedacht werden und bei allen logischen und physischen Bestandteilen des Systems entsprechend implementiert und im operativen Betrieb aufrechterhalten werden. In den vorausgegangenen Arbeiten erfolgte die Erfassung gesetzlicher Rahmenbedingungen, die Ermittlung der allgemeinen Schutzziele der Plattformen (Unternehmensplattform und Marktplattform) sowie die Benennung potenzieller Gefahren durch Cyberangriffe, gegen die die UP und MP geschützt werden müssen. Bei den gesetzlichen Rahmenbedingungen kam speziell den Anforderungen an Kritische Infrastrukturen (KRITIS) eine besondere Bedeutung zu. Es wurde entschieden, dass die ESP (und damit die UP und die MP) als KRITISready[4] entwickelt werden sollen

Der Fokus im aktuellen Dokument liegt nun auf der Konkretisierung von IT-Sicherheitsmaßnahmen. Dazu gehören zuerst einmal Methoden zur konkreten Bedrohungs- und Schwachstellenanalyse, sowie zur Ermittlung hieraus resultierender Sicherheitsanforderungen an einzelne Komponenten eines IT-Systems (Services), aber auch an das IT-System (die jeweiligen Plattformen) insgesamt. Angewandt wurden dafür die Methoden des Threat-Modelings und die Vorgehensweise zur Bestimmung der Sicherheitslevel. Mittels der Sicherheitslevel wird festgelegt, welche Anforderungen zu erfüllen sind, um einen bestimmten Grad an Sicherheit zu erlangen. Damit der Sicherheitslevel über den gesamten Lebenszyklus eines Service und in Summe der gesamten Plattform aufrechterhalten werden kann, ist

[4] KRITISready bedeutet, dass die Entwicklung der Services und der Plattformen unter Berücksichtigung der Anforderungen an Systeme und Komponenten für den Einsatz in Kritischen Infrastrukturen erfolgen soll und eine spätere Zertifizierung somit ermöglicht. Die Anforderungen beziehen sich hierbei auf die IT-Sicherheit.

ein Life-Cycle Management erforderlich. Im Rahmen des Life-Cycle Management (LCM) ist wiederum der Zugriff und die Interaktion zahlreicher Rollen für die Installation, den Betrieb und die Wartung, aber auch für die Außerbetriebnahme notwendig. Die Zugriffe erfordern ein Berechtigungsmanagement, welches über ein rollenbasiertes Zugriffsmanagement (RBAC engl. “role based acces control“) erfolgen soll. Der Identitätsnachweis, sowie der Austausch kryptographischer Schlüssel erfolgt schlussendlich über digitale Zertifikate. Nachfolgend werden diese Maßnahmen entsprechend dem aktuellen Arbeitsstand vorgestellt.

2 IT- SICHERHEIT

Die ESP stellt selbst zwar keine physikalische Plattform dar, sie besteht aber aus der Marktplattform und der Unternehmensplattform, die physikalisch existieren. Damit Flexibilität ermittelt und gehandelt werden kann, ist ein Austausch von Informationen erforderlich. Die Referenzarchitektur zeigt das Zusammenspiel der einzelnen Plattformen und Komponenten (siehe Diskussionspapier „Referenzarchitektur der Energiesynchronisationsplattform“ (Fridgen et al. 2021)). Die Kommunikation erfolgt hierfür zum Teil unternehmensintern (über nicht-öffentliche Kommunikationsnetze), speziell bei der Anbindung von Anlagen, MES und ERP Systemen an die UP aber auch extern zwischen der UP und der MP, sowie beim Zugang zu Märkten des Flexibilitätshandels oder zu externen Diensteistern (Aggregatoren, Prognosedienste und weitere). Ziel der IT-Sicherheit ist es, Maßnahmen zu definieren, die den Schutz der Daten und der Kommunikation gegenüber Cyberattacken oder Hackerangriffen in einem ausreichenden Maß sicherstellen. Dabei muss einerseits der Schutzbedarf der übertragenen und zu verarbeitenden Informationen, andererseits aber auch das Risiko eines Angriffs mit in die Betrachtungen einbezogen werden.

So nutzt die UP für die Ermittlung von Energie-Flexibilität gegebenenfalls sensible Unternehmensdaten, die je nach Detailierungsgrad Betriebsgeheimnisse offenbaren können oder der gesetzlichen Datenschutzverordnung (DS-GVO) unterliegen (Auftrags- und Kundendaten) und damit einen höheren Schutzbedarf an die Vertraulichkeit aufweisen, als beispielsweise Wetterprognosedaten. Bei der Vermarktung von Flexibilität spielen dann besonders die Authentizität, die Integrität und die Verfügbarkeit eine tragende Rolle. Dies wird besonders dann relevant, wenn die gehandelte Leistung oder jährliche Energiemenge (Strom) die Schwellwerte der KRITIS Einstufung übersteigen (Openkritis: 2021). Aber auch bei niedrigeren Leistungswerten können sich bei einer Manipulation bereits Auswirkungen auf lokale Stromnetze ergeben, die es zu vermeiden gilt.

2.1 Sicherheitslevel

Die Abstufung von zu erfüllenden Sicherheitsanforderungen in verschiedene (Sicherheits-)Klassen ist eine übliche Vorgehensweise. Dies trifft sowohl für die *IT-Sicherheit (Security*) als auch für den Bereich *Funktionale Sicherheit (Safety)* zu. Ziel dieser Abstufung ist es, das jeweils passende und notwendige Maß an Sicherheit zu definieren und umzusetzen. Dabei gilt es einerseits zu hohe Anforderungen zu vermeiden, da Sicherheit eben auch einen Kostenfaktor darstellt. Zu niedrige Anforderungen an die IT-Sicherheit bergen andererseits allerdings die Gefahr, Opfer einer Cyberattacke zu werden, wodurch Schäden verursacht werden können, die unter Umständen sogar existenzgefährdend für ein Unternehmen sind. Bei der Einstufung in eine Sicherheitsklasse werden in aller Regel der mögliche Schaden und die Eintrittswahrscheinlichkeit, also das Risiko eines ungewollten Ereignisses, betrachtet und in Relation gesetzt. Diese Vorgehensweise findet unter anderem bei der Umsetzung von Maßnahmen *zur Funktionalen Sicherheit* Anwendung (DIN EN 61508-1:2011-02). Die Norm definiert sogenannte *Safety Integrity Level* (SIL 1 bis SIL 4). Bei der Prüfung und Bewertung der Sicherheitseigenschaften von IT-Produkten kommen in vielen Bereichen die *Common Criteria for Information Technology Security Evaluation* zum Einsatz (ISO/IEC 15408-1:2009-12). Ein Bespiel im Bereich Energie ist in Deutschland das Smart Meter Gateway (Bundesamt für Sicherheit in der Informationstechnik 2021b). Bei den Common Criteria wird nach Evaluation Assurance Level (EAL) eine Abstufung des Prüfumfangs und der Prüftiefe vorgenommen. Im Bereich der IT-Sicherheit für die *industrielle Automatisierung* unterzieht sich eine steigende Anzahl an Unternehmen einer Zertifizierung nach *ISO/IEC 62443*. Die Norm gibt

entsprechende Security Level vor (DIN EN 62443-3-2:2018-10 - Entwurf). Bei den Security Level der Norm fließen die Art eines Angreifers und dessen Fähigkeiten in die Einstufung zum Sicherheitslevel mit ein. Im Zusammenspiel mit dem Reifegrad wird dann ein Protection Level definiert.

Die direkte Anwendung einer der etablierten Standards für die SynErgie Plattformen ist nicht angezeigt, da an Komponenten und Systeme im Bereich KRITIS andere Anforderungen gestellt werden, als beispielsweise im industriellen Umfeld. Im Bereich KRITIS resultieren die Anforderungen aus gesetzlichen Vorgaben, im industriellen Umfeld erfolgt hier Vieles auf freiwilliger Basis oder aufgrund von Vertragsvereinbarungen zwischen Herstellern und Kunden. Dies bedeutet, die geforderte Bandbreite ist mit den etablierten Standards nur unzureichend abzudecken. Deshalb wurden für SynErgie eigene Sicherheitslevel definiert, die sich jedoch der Vorgaben aus den erwähnten Standards bedienen. Ziel ist es für die Services der ESP den erforderlichen Sicherheitslevel zu definieren, aus dem sich dann die Sicherheitsanforderungen und zu ergreifenden Sicherheitsmaßnahmen ableiten.

Für die Einstufung in Sicherheitslevel stehen auf der einen Seite der Schutzbedarf von Informationen bzw. elektronischer Daten (im Sinne der Vertraulichkeit, Integrität und Authentizität), sowie die geforderte Verfügbarkeit der Informationen im Vordergrund. Zusätzlich ist auf der anderen Seite aber auch die Einstufung des Risikos eines Angriffs auf diese Informationen mit in die Betrachtungen einzubeziehen. Für den Schutzbedarf von Informationen wird fortan die Bezeichnung „**erforderliches Sicherheitsniveau**“ verwendet. Für die Risikobewertung wird eine **Risikoklasse** definiert. Diese beiden Parameter zusammen dienen dann zur Bestimmung des Sicherheitslevels.

Relevant für die Bestimmung des **Erforderliches Schutzniveaus** ist der Schutzbedarf der Informationen, die ein Service konsumiert, verarbeitet oder zur Verfügung stellt. Dabei erfolgt die Einstufung nach dem möglichen Schaden bei Verlust der Vertraulichkeit, Integrität[5], Verfügbarkeit und Nicht-Abstreitbarkeit. Für die Bestimmung des Erforderlichen Schutzniveaus werden insgesamt vier Klassen definiert (niedrig, mittel, hoch, sehr hoch). Dies bedeutet, es erfolgt eine qualitative Einstufung. Das Verfahren zur Einstufung des Schutzniveaus baut auf den Verfahren des NIST CDC auf und ergänzt diese um die Bewertung der Nicht-Abstreitbarkeit (NIST (CDC) FIPS 199) und (NIST (CDC) FIPS 200) Folgende Kriterien sind bei der Bestimmung des erforderlichen Schutzniveaus mit einzubeziehen:

- Möglicher Schaden (Schadenshöhe) bei Verletzung der Grundwerte, sowohl finanzieller aber auch anderer Art für das Unternehmen (Imageschaden, Unzufriedenheit der Kunden bei nicht-einhalten eines Liefertermins)
- Auswirkungen auf das Stromnetz (abhängig von Energiemenge, Leistung, zeitlichen Faktoren)
- Regulatorische Vorgaben (bspw. DSGVO. KRITIS, IT-Sicherheitsgesetz)
- Anforderungen aus Branchenstandards

[5] Integrität von Informationen beinhaltet auch die Authentizität

In die **Bestimmung einer Risikoklasse** fließen die Wahrscheinlichkeit einer Bedrohung (eines Angriffes), sowie die Fähigkeiten des potenziellen Angreifers ein. Auch hier wurden insgesamt vier Klassen definiert (niedrig, mittel, hoch, sehr hoch). Folgende Kriterien sind bei der Bestimmung der Risikostufe mit einzubeziehen:

- Potenzial eines Angreifers und damit Stärke eines möglichen Angriffs
- Wahrscheinlichkeit und Häufigkeit eines Angriffs
- Einsatzumgebung (öffentliches oder privates Kommunikationsnetz)

Die Bestimmung des **erforderlichen Schutzniveaus** und der **Risikostufe** muss für jede Komponente, bzw. jeden Service durchgeführt werden. Die Bestimmung des Risikos eines Angriffes ist dabei mitunter nicht trivial. Ausschlaggebend ist hier neben der Branche, in dem das Unternehmen tätig ist, auch die im Unternehmen vorhandene IT-Infrastruktur und das Unternehmen selbst. Bei der Einstufung können deshalb nur Annahmen getroffen werden, die beim Einsatz der Plattform (in aller Regel betrifft dies die Unternehmensplattform) noch einmal verifiziert werden müssen.
Die Bestimmung des Sicherheitslevel (SL) erfolgt nach Bestimmung des **erforderlichen Schutzniveaus** und der **Risikostufe** in der SL-Matrix Der Schnittpunkt in der SL-Matrix nach Abbildung 2 zeigt dann den erforderlichen Sicherheitslevel. Die Bestimmung sollte im Rahmen des Security Life Cycle Managements spätestens in der Entwurfsphase erfolgen (siehe Kapitel 2.6 Life-Cycle-Management).

		Risikostufe				
		Niedrig	Mittel	Hoch	Sehr hoch	
Erforderliches Schutzniveau	Sehr hoch	SL 2 (SL 3 bei KRITIS)	SL 3	SL 4	SL 4	KRITIS
	Hoch	SL 2 (SL 3 bei KRITIS)	SL 3	SL 3	SL 4	
	Mittel	SL 2	SL 2	SL 3	SL 3	Nicht-KRITIS
	Niedrig	SL 1	SL 2	SL 2	SL 2	

ABBILDUNG 2: SL-MATRIX ZUR BESTIMMUNG DES SICHERHEITSHEITSLEVEL

Wie in der SL-Matrix ersichtlich, wird eine Unterscheidung getroffen, ob ein Service im Umfeld KRITIS eingesetzt wird oder nicht. Für den Einsatzbereich KRITIS wird vorgegeben, dass das erforderliche Schutzniveau mindesten die Stufe hoch erfüllen muss. Der minimale SL für den Einsatz im Umfeld KRITIS soll SL 3 sein. Soll ein Einsatz im nicht- KRITIS Umfeld erfolgen, so ist bei einem erforderlichen Schutzniveau von hoch oder sehr hoch und niedriger Risikostufe auch SL 2 ausreichend.

Für die Sicherheitslevel wurden sowohl Anforderungen an die IT-Sicherheit als auch funktionale Anforderungen festgelegt. Die Anforderungen, die für einen Sicherheitslevel erhoben werden, basieren auf den Anforderungen der IEC 62443, dem BSI Grundschutz‘, sowie den Vorgaben des BDEW zu Kritischen Infrastrukturen.

TABELLE 1: SICHERHEITSLEVEL UND RESULTIERENDE ANFORDERUNGEN

SL	Anforderungen an IT-Sicherheit	Funktionale Anforderungen
SL0	Es sind keine Maßnahmen zum Schutz gegen Angriffe notwendig	Ein Schutz von Informationen ist nicht notwendig. Es bestehen geringe Anforderungen an die ordnungsgemäße Funktion. Ein Ausfall oder eine Fehlfunktion haben keine nennenswerten Auswirkungen
SL-1	Schutz gegen gelegentliche und zufällige Verstöße durch Angreifer mit geringen Fähigkeiten	Der Schutz von vertraulichen Informationen muss geringen Anforderungen genügen. Informationen sollten korrekt sein. Kleinere Fehler können toleriert werden. Fehler, die die Aufgabenerfüllung erheblich beeinträchtigen, müssen jedoch erkennbar oder vermeidbar sein. Längere Ausfallzeiten, sind zu vermeiden. Der Schutz personenbezogener Daten muss gewährleistet sein.
SL-2	Schutz gegen vorsätzliche Verstöße durch einfache Mittel mit geringem Ressourcenaufwand, generischen Security-Kenntnissen und geringer Motivation	Der Schutz vertraulicher Informationen muss mittleren Anforderungen genügen und in kritischen Bereichen stärker ausgeprägt sein. Die verarbeiteten Informationen müssen korrekt sein, auftretende Fehler müssen erkennbar und vermeidbar sein. Längere Ausfallzeiten sind nicht akzeptabel. Der Schutz von vertraulichen Daten muss gewährleistet sein.
SL-3	Schutz gegen vorsätzliche Verstöße durch hochentwickelte Mittel mit moderatem Ressourcenaufwand und Expertenwissen, die mit klar definierten Zielen effektiv, aber kostenorientierte Angriffsszenarien entwickeln und mit moderater Motivation vorgehen	Der Schutz vertraulicher und systemrelevanter Informationen muss hohen Anforderungen genügen. Die verarbeiteten Informationen müssen in hohem Maße korrekt sein, auftretende Fehler müssen erkennbar sein und es müssen Maßnahmen ergriffen werden bei Fehlfunktionen den Betrieb aufrecht zu erhalten oder Ausfallzeiten kurz zu halten.
SL-4	Schutz gegen vorsätzliche Verstöße durch hochentwickelte Mittel mit erweitertem Ressourcenaufwand, höchsten Fähigkeiten, die gegen ein spezifisch ausgewähltes Ziel vorgehen und über nahezu unbegrenzte finanzielle Mittel verfügen (Staatliche Organisationen)	Der Schutz vertraulicher und systemrelevanter Informationen muss höchsten Anforderungen genügen Die verarbeiteten Informationen müssen in höchstem Maß korrekt sein. Ausfallzeiten sind nicht akzeptabel.

Im Projekt erfolgte die Einstufung aller verfügbaren und hinreichend konkret spezifizierter Kernkomponenten und Services der ESP. In Summe waren dies 26 sogenannte „Artefakte“. Die ermittelten SLs entsprechen dabei dem aktuellen Kenntnisstand und dem Stand der Entwicklung. Im Rahmen des Security Life Cycle Managements können äußere Umstände, wie die Zunahme oder die Qualität von Cyber-Angriffen dazu führen, dass beispielsweise die Risikostufe eine Anpassung erfahren muss, was die Anpassung des Security Level zur Folge haben kann, bzw. der Service mit seinem ursprünglich festgelegten SL nicht mehr für den Einsatz im jeweiligen Bereich geeignet ist. Ebenso kann bei einem Service, der initial für die Verarbeitung von Daten mit einem niedrigen Schutzbedarf ausgelegt war, durch Beaufschlagen von Daten mit einem hohen Schutzbedarf das ursprünglich festgelegte Schutzniveau nicht mehr ausreichen. Dies bedeutet also, ähnlich wie die Gültigkeit einer Zertifizierung befristet erfolgt, unterliegt die Einstufung in einen SL einer zyklischen Kontrolle und gegebenenfalls einer Neubewertung und Anpassung.

Für die Kernkomponenten der Unternehmensplattform und der Marktplattform zeigen Tabelle 2 und Tabelle 3 die ermittelten Sicherheitslevel, die diese erfüllen müssen.

TABELLE 2: SICHERHEITSLEVEL DER KERNKOMPONENTEN DER UNTERNEHMENSPLATTFORM

Artefakte der Unternehmensplattform	Art	Sicherheitslevel
Marktplatz für UP-Services (Company Portal)	Technische Kernkomponente	SL 3
Vermarktungskomponente (ehemals Schnittstelle zur Marktplattform)	Technische Kernkomponente	SL 3
Manufacturing Service Bus (MSB – Middleware, IaaS Interface)	Technische Kernkomponente	SL 3
Smarter Konnektor	Technische Kernkomponente	SL 3 (ggf. SL 4, wenn höchste Verfügbarkeit gefordert ist)
Energieflexibilitätsmanagementservice (EFMS)	Technische Kernkomponente	SL 3

TABELLE 3: SICHERHEITSLEVEL DER KERNKOMPONENTEN DER MARKTPLATTFORM

Artefakte der Marktplattform oder Externe Services	Art	Sicherheitslevel
Marktplattform (Service Discovery etc.)	Technische Kernkomponente	SL 3

Für die UP gilt, dass speziell die Anforderungen an die Verfügbarkeit, sowie die Integrität und in einzelnen Fällen die Nicht-Abstreitbarkeit die höchste Priorität zugemessen wird. Die Vertraulichkeit von Daten spielt besonders dort eine Rolle, wo ein Service über ein MES System oder eine ERP auf vertrauliche Daten zugreift. Dort sollte die Regel gelten, dass die Filterung von Daten bereits an der Quelle erfolgen sollte. Über die tatsächliche Vertraulichkeit dieser Daten kann zum aktuellen Zeitpunkt jedoch keine belastbare Aussage getroffen werden. Hiervon betroffen sind in aller Regel besonders die Optimierer. Durch die Aggregation und Abstraktion von Lastprofilen in den EFDMs werden Rückschlüsse auf sensible Informationen bereits in einem hohen Maße unterbunden. Besonders, wenn die Generierung von EFDMs bereits im Smarten Konnektor erfolgt. Die Verfügbarkeit gewinnt dann an Priorität, wenn eine vermarktete Flexibilität auch tatsächlich umgesetzt werden soll. Dabei sind nicht nur finanziellen Aspekte aus der Vermarktung der Flexibilität für das Unternehmen selbst ausschlaggebend, sondern, abhängig von der tatsächlich vermarkteten Stromleistung bzw. Energiemenge auch die Auswirkungen auf die Stromnetze. Höchste Priorität und damit auch die höchsten SLs werden dann folglich gefordert, wenn die Schwellwerte der Bemessungsgrenzen für Kritische Infrastrukturen überschritten werden. Die Integrität der Daten ist sowohl bei der Angebotserstellung als auch bei der Umsetzung als hoch einzustufen.

2.2 Threat-Modeling

Bei der Software-Entwicklung geht es zuallererst darum, eine Software zu entwerfen, welche die vorgegebenen Aufgaben erfüllt. Was die Aufgaben einer Software sind wird in den Anforderungen festgehalten, die mit verschiedensten Requirements Engineering Prozessen ermittelt werden. Threat-Modeling ist ein Prozess zur Bestimmung der Sicherheitsanforderungen.

Das *Threat modeling manifesto* definiert Threat-Modeling folgendermaßen (Braitermann et al. 2020)

> *Bei der Bedrohungsmodellierung (Threat-Modeling) werden Darstellungen eines Systems analysiert, um Bedenken hinsichtlich der Sicherheits- und Datenschutzmerkmale aufzuzeigen.*
> *Wenn wir ein Bedrohungsmodell (Threat-Model) erstellen, stellen wir vier Schlüsselfragen auf höchster Ebene:*
> *Woran arbeiten wir? Was kann schief gehen? Was werden wir dagegen tun? Haben wir unsere Arbeit gut genug gemacht?*

Im Gegensatz zu anderen Methoden der Anforderungsermittlung liegt der Fokus des Threat-Modelings auf der Fragestellung, welche Gefahren bei der Verwendung der Software auftreten können. Als Gefahr versteht man dabei alle ungewollten Ereignisse und Interaktionen, welche eine negative Auswirkung haben können. Erst mit dem Wissen über die möglichen Gefahren, befasst man sich mit den verbundenen Risiken und den Gegenmaßnahmen, welche die Risiken reduzieren und die potenziellen Schäden mindern.

Um die Gefahren zu ermitteln, benötigt man ein solides Verständnis über die Funktionsweise der Software und über das Umfeld, in dem diese eingesetzt wird. Hierzu reicht es nicht aus den Quellcode zu betrachten, sondern es muss zusätzlich geklärt werden:

- Wer mit dem System interagiert? Das bezieht sowohl die Benutzer als auch andere Software-Systeme mit ein.
- Wie die Software ausgeführt wird? Handelt es sich um eine Desktop-Anwendung, einen Betriebssystem-Dienst oder eine Server-Anwendung?
- Wie die Software angebunden ist? Kann die Software mit anderen Prozessen, Betriebssystem-Diensten, Server im LAN oder WAN kommunizieren?
- Wie und wer kann mit der Software interagieren? Öffnet die Software einen Netzwerk-Port, einen IPC-Endpunkt oder eine manuelle Eingabe?
- Wie sensible sind die Informationen, die durch die Software verarbeitet werden?

Diese Fragen lassen sich mit der Funktionsbeschreibung der Software nicht beantworten. Der Gründe dafür sind unter anderem,

- dass eine Software meist mehr Funktionen anbietet als in einer Installation genutzt werden
- die Anbindung und Interaktionsmöglichkeit beschränkt werden kann (z.B. durch eine Firewall, ein VPN, das Betriebssystem, die Konfiguration der Software)
- die Benutzer der Software nicht bestimmt werden können und
- die zu verarbeitenden Informationen nicht bekannt sind.

Zur Beantwortung dieser Fragen ist es hilfreich, ein Modell der Software zu erstellen, in dem nicht nur die Interna der Software repräsentiert werden, sondern auch das Umfeld, in dem die Software ausgeführt wird. Zur Modellierung der Software können verschiedene Beschreibungen angewendet werden, solange die Interaktionen mit den Akteuren und die Interna der Software modelliert werden können. Die geläufigen Beschreibungssprachen sind UML-Sequenz-

Diagramme und Datenflussdiagramme (DFD), aber auch Zustandsdiagramme, *Message Sequence Charts* und *Business Process Model and Notation (*BPMN) können verwendet werden. Dabei hängt es von der Software und dem Umfeld ab, welche Beschreibungssprache den Sachverhalt am besten beschreibt. Bei einer Software mit vielen Funktionen oder einem komplexen Umfeld empfiehlt es sich, mehrere Modelle zu erstellen, wobei auch verschiedene Beschreibungssprachen verwendet werden können.

Nachdem ein Modell der Software erstellt wurde, beginnt die Analysephase des Threat-Modelings. Ziel dieser Phase ist es Fehlverhalten der Software zu finden, welche beim Betrieb der Software auftreten können. Was ein Fehlverhalten ist hängt von der Software und des Umfeldes ab, in dem die Software eingesetzt wird. Sobald ein Fehlverhalten eine negative Auswirkung haben könnte, wird sie als Bedrohung[6] klassifiziert. Am Ende der Analysephase hat man eine Liste der Bedrohungen für die analysierte Software.

Die einfachste Form der Analyse ist ein einfaches Brainstorming mit den Stakeholdern, bei dem die Beteiligten ihre Bedenken gegenüber der Software einbringen können. Dieser einfache Ansatz hat aber das Problem, dass zum einen nicht immer alle Stakeholder zur Verfügung stehen. Zum anderen liegt der Fokus der Stakeholder eher auf den Aufgaben, welche die Software erledigen soll, weniger auf dem was nicht passieren darf. Um dem entgegenzuwirken, wurden verschiedene formalere Methodiken entwickelt, welche in der Analysephase eingesetzt werden können, wie STRIDE (Kohnfelder und Garg 1999; Shostack 2014), PASTA (UcedaVelez und Morana 2015), TRARA (Wynn et al. 2011) und Trike (Larcom und Eddington 2005)und viele andere mehr (Shevchenko et al. 2018). Für das Projekt SynErgie kamen STRIDE und PASTA in die engere Auswahl.

Die älteste dieser Methodiken ist STRIDE und ihre Spezialisierungen STRIDE-per-Element und STRIDE-per-Interaction (Kohnfelder und Garg 1999; Shostack 2014). STRIDE steht für die sechs möglichen Fehlerklassen (Kohnfelder und Garg 1999; Shostack 2014)

- **S**poofing - Vortäuschen einer fremden Identität
- **T**ampering - Manipulation von Daten auf der Festplatte, dem Netzwerk oder wo anders
- **R**epudiation - Abstreitbarkeit einer Handlung
- **I**nformation disclosure - Einsicht in Informationen durch unautorisierte Dritte
- **D**enial of service - Herbeigeführter Ausfall einer Funktion der Software
- **E**levation of privilege - Erlauben von Handlungen durch unautorisierte Dritte

Bei der Anwendung von STRIDE werden alle Elemente des Modells betrachtet und je Element wird die Frage gestellt, ist eine diese Fehlerklassen hier anwendbar? Sobald ein Fehler gefunden wurde und dieser als Bedrohung eingestuft werden kann, wird dieser in die Liste der Bedrohungen aufgenommen. Häufig muss bei STRIDE die Liste der Bedrohungen am Ende der Analysephase nochmal auf Duplikate hin überprüft werden, da viele Fehler über mehrere Fehlerklassen gefunden werden können. Die Liste wird im Anschluss nach dem potentiellen Schaden sortiert, welchen die Bedrohungen verursachen könnten.

Eine neuere Methodik ist PASTA (Process for Attack Simulation and Threat Analysis), deren Fokus auf einem deutlich formelleren Vorgehen liegt und dabei die Modellierung miteinschließt.

PASTA ist in sieben Schritte unterteilt (UcedaVelez und Morana 2015)

[6] aus dem englischen Threat übersetzt

1. Define Objectives - Festlegen der Ziele der Software, sowie der gesetzlichen Vorgaben
2. Define Technical Scope - Beschreibung des technischen Umfeldes
3. Application Decomposition - Modellierung des Systems
4. Threat Analysis - Ermittlung von Bedrohungen aus vergangenen internen und externen Ereignissen und Angriffsbibliotheken
5. Vulnarability & Weakness Analysis - Sammlung von Schwachstellen im Design und in den verwendeten Komponenten
6. Attack Modeling - Beschreibung von möglichen Angriffen auf Basis der gefundenen Bedrohungen und Schwachstellen
7. Risk & Impact Analysis - Bewertung der gefundenen Angriffe nach ihrem Risiko und dem möglichen Schaden

PASTA hat den Vorteil, dass in den Schritten 1, 2, 4 und 5 die potenziellen Angriffsflächen der Software, die möglichen Angreifer und deren Ziele dokumentiert werden. Aber den Nachteil, dass es schwierig anzuwenden ist, wenn die Umsetzung der Software, das Umfeld, in dem sie ausgeführt wird oder die möglichen Angreifer und deren Ziele nicht klar definiert werden kann. Zusätzlich hat PASTA einen höheren Arbeitsaufwand im Vergleich zu STRIDE (Shevchenko et al. 2018).

Nach der Analysephase beginnt die Abwehrphase, in der die Bedrohungsliste beginnend mit der größten Bedrohung bearbeitet wird und für jede Bedrohung die möglichen Gegenmaßnahmen betrachtet werden. Dabei muss der Aufwand, welcher durch die Umsetzung der Gegenmaßnahmen entsteht, gegen die Risiken und den Schaden der Bedrohung abgewogen werden. Eine Gegenmaßnahme kann dabei sowohl eine Veränderung der Software bedeuten (z.B. Verbesserung der Zugriffskontrolle) als auch eine Veränderung in der Umgebung (Zugang zur Software ist nur noch aus einem internen Netz möglich.). Sollte der zu erwartende Schaden oder das Risiko sehr gering sein, ist es auch durchaus möglich, keine Gegenmaßnahme zu treffen.

Sobald die Gegenmaßnahmen umgesetzt sind, beginnt die Introspektionsphase, in der das Modell, die Bedrohungen und die Gegenmaßnahmen nochmal betrachtet werden. Dabei wird überprüft, ob und wie die Gegenmaßnahmen die Software oder das Umfeld beeinflussen, wodurch sich wiederum die Bedrohungen verändern. An dieser Stelle könnte man wieder bei der Modellierung anfangen. Die Introspektionsphase gibt aber auch die Gelegenheit das Vorgehen zu evaluieren.

In SynErgie wurden für 20 Software-Komponenten Threat-Models erstellt. Jede Komponente ist entweder Teil der Unternehmensplattform, der Marktplattform oder ein Service, welcher auf einer der beiden Plattformen ausgeführt wird. Für die Threat-Models wurde von allen Entwicklungsteams STRIDE eingesetzt. Für die Modellierung wurden ausschließlich Datenflussdiagramme verwendet. Der Grund dafür liegt darin, dass keins der Teams bereits Erfahrungen im Threat-Modeling hatte und daher pro Team ein Workshop durchgeführt wurde. Der Fokus lagt bei den Workshops auf STRIDE in Verbindung mit Datenflussdiagrammen, da STRIDE weniger formell und daher schneller zu erlernen ist und Datenflussdiagramme, im Gegensatz zu anderen Beschreibungssprachen, nur aus fünf Elementen bestehen[7]. Dies erleichterte die Einarbeitung für die Teams.

[7] Datenflussdiagramme sind nicht wie UML und BPMN standardisiert, daher variiert die Zahl der Elemente je nach Autor und der Art zu zählen zwischen vier und zwölf.

Es wurde aber den Teams die Möglichkeit gelassen etwaige existierende Diagramme wieder zu verwenden, um schneller in die Analysephase zu kommen. Die Teams führten dann selbständig eine Analysephase durch, was folgende Gründe hat: Zum einen werden die Teams dazu gebracht, darüber nachzudenken wie das Umfeld ihrer Komponente aussehen wird. Zum zweiten müssen sich die Teams mit möglichen Fehlern und Bedrohungen, denen ihre Komponente standhalten muss, auseinandersetzen. Zum dritten, die Teams sind diejenigen, welche ihre Software am besten verstehen und daher bessere Modelle erstellen und bei der Fehlersuche besser mit den Details vertraut sind.

Die Threat-Models der Teams wurden dann zentral nach der Analyse der Teams gesammelt und vereinheitlicht und nochmal analysiert, um dann in die Abwehrphase überzugehen. In der Abwehrphase wurden Gegenmaßnahmen gefunden, von denen möglichst viele Teams gleichzeitig profitieren. Auf diese Maßnahmen wird im folgenden Abschnitt eingegangen.

2.3 Maßnahmen

Aus den Sicherheitslevel und dem Threat-Modeling leiten sich die Anforderungen an die IT-Sicherheit ab, die letztendlich durch das Ergreifen geeigneter Maßnahmen zu einer Reduzierung führen, Opfern einer Cyber-Attacke zu werden. Eine umfangreiche Sammlung an sicherheiterhöhenden Maßnahmen wird im Security-Life-Cycle Management detailliert beschrieben. Beim aktuellen Stand der Projektarbeit sind die Anforderungen hierzu beschrieben, ein Auszug davon ist in Abschnitt 2.6 Life-Cycle-Management in diesem Dokument aufgeführt. In diesem Abschnitt soll nun auf die wichtigsten Erkenntnisse noch einmal eingegangen werden.

2.3.1 Filterung der Daten an der Datenquelle – Vererbung von Anforderungen

Eine Erkenntnis der durchgeführten Workshops zu Sicherheitslevel und Threat-Modeling war, dass die Schnittstellen zu den ERP und MEP Systemen zu einem Großteil noch nicht völlig bekannt sind. Ebenso ist damit nicht bekannt, welchen Vertraulichkeitsgrad die Daten und Informationen haben, die der UP zur Verfügung gestellt werden. Dabei sollte das Prinzip der Datensparsamkeit zur Anwendung kommen. Dies bedeutet, dass Daten, die in die UP eingespeist werden, nur die zwingend erforderlichen Informationen enthalten sollen, die ein Service für die Erfüllung seiner Aufgabe benötigt. Die Daten sollten – sofern dies möglich ist – bereits an der Datenquelle entsprechend gefiltert und soweit abstrahiert oder anonymisiert werden, dass die Anforderungen an die Vertraulichkeit und dementsprechend die erforderlichen Maßnahmen überschaubar und handelbar bleiben. Ansonsten könnte die Anforderung einer Ende-zu-Ende Verschlüsslung von Daten erforderlich sein, was durch den MSB erschwert wird.

2.3.2 Nutzerauthentifizierung über einen zentralen SSO-Service mit der Möglichkeit zur Anbindung an existierende Benutzerverwaltungssysteme

Viele Services müssen einen Benutzer authentifizieren. Um die Angriffsfläche zu verkleinern, ist es ratsam die Authentifizierung auf einen Single-Sign-On-Service auszulagern. Dadurch werden an weniger Orten sensible Daten wie Passwörter gespeichert und zusätzlich wird der Entwicklungsaufwand verringert.

2.3.3 Zentrales Logging in der Unternehmensplattform

Innerhalb der Unternehmensplattform muss ein zentraler Log-Server vorgesehen werden, damit die Anbindung der Plattform an die Unternehmens-IT leichter von statten geht.

2.3.4 Einheitliche Format für Log-Nachrichten

Für die Log-Nachrichten soll ein einheitliches Format definiert werden. Dieses dient der Übersichtlichkeit und erleichtert eine automatisierte Auswertung und Analyse von Einträgen.

2.3.5 Bessere Unterstützung für ein automatisiertes Deployment

Viele Services auf der UP bieten eine Web-Schnittstelle an, mit welcher der Service im laufenden Betrieb neu konfiguriert werden kann. Dies verursacht zwei Probleme. Zum einen kann eine solche Web-Schnittstelle nicht ohne weiteres automatisch ausgerollt werden, zum anderen benötigt diese Web-Schnittstelle eine Authentifikation und Autorisierung, welche innerhalb des Service umgesetzt werden muss. Es ist daher empfehlenswert, anstelle dessen eine Konfigurationsdatei zu verwenden, die durch die Authentifikation und Autorisierung des Betriebssystems geschützt werden kann. Eine Konfigurationsdatei lässt sich auch einfacher in CI/CD-Pipelines verwenden.

2.3.6 Signieren der EFDM-Nachrichten

Innerhalb der UP werden Informationen zwischen Services über den MSB ausgetauscht, dadurch hat man keinen Ende-zu-Ende gesicherten Kanal zwischen den involvierten Services. Was geschützt ist, ist die Kommunikation zwischen dem Service und dem MSB. Viele Services vertrauen aber darauf, dass der MSB ihnen nur Informationen und Nachrichten zustellt, die von bestimmten Service kommen (z.B. Smarter-Konnektor schickt EFDMS-Nachricht an die Optimierer). Dabei ist aber nicht ausgeschlossen, dass der MSB als „Confused Deputy“ (Hardy 1988) handelt.

Ein ähnliches Problem existiert bei der Verbindung zwischen den EFDM erstellenden und verarbeitenden Services und dem EFMS. Um das Problem zu umgehen, existieren zwei Möglichkeiten.

1. Entweder müssen Direktverbindungen zwischen den Services möglich sein, so dass ein Service beim Verbindungsaufbau den anderen authentifizieren kann oder
2. Nachrichten, die über den MSB versandt werden, müssen vom Sender vor dem Versand signiert werden und die Empfänger müssen diese Signatur überprüfen.

2.3.7 Testdaten für das EFDM

Für die Übertragung des EFDM wird das EFDM ins JSON-Format serialisiert. JSON ist der Defacto-Standard für die Übertragung von Daten im Web geworden. Allerdings hat der JSON-Standard einige Unklarheiten und Fallstricke. Man nehme zum Beispiel dieses JSON-Objekt.

```
{
  "id" = "0000",
```

```
  "id" = "1111"
}
```

Abhängig davon, wie ein Service dieses Objekt interpretiert, ist die `id` entweder `1111` oder `0000`. Das wird dann zu einem Sicherheitsproblem, wenn verschiedene Services unterschiedliche `id`-Felder verwenden.
Um solchen Problemen zuvorzukommen, sollte eine Datenbasis an validen und nicht validen Testdaten für das EFDM erstellt werden. Mit solchen Testdaten können dann alle Services, welche EFDMs empfangen, auf deren Konformität mit dem EFDM-Format überprüft werden.

2.3.8 Kontinuierliche Integration der Software-Komponenten

Beim Review der Threat-Models ist es offensichtlich geworden, dass es bei so einem großen Projekt zu Missverständnissen bzgl. Komponenten unterschiedlicher Teams kommen kann. Solche Missverständnisse schwächen die Verlässlichkeit der Software, können aber auch zu Sicherheitslücken führen. Dies hat sehr individuelle Gründe, denen aber mit einer koordinierten kontinuierlichen Integration entgegengewirkt werden kann. Regelmäßige Integrationen erlauben es, Missverständnisse früher zu erkennen und die betroffenen Stakeholder zu identifizieren.

2.4 Beschreibung der Rollen und des Rechtekonzepts

Ein weiteres Sicherheitsmerkmal ist die Umsetzung eines geeigneten Rechte- und Zugriffsmanagement. Für die ESP und ihre Teilplattformen wurde ein rollenbasiertes Rechtekonzept gewählt.

Basis eines rollenbasierten Rechtekonzepts ist die Definition von Rollen, denen ganz spezifische Aufgaben übertragen werden und die hierfür erforderlichen Rechte eingeräumt werden. Je feingranularer die Definition der Rollen erfolgt, desto übersichtlicher ist die Vergabe der notwendigen Rechte. Die Besetzung der Rolle erfolgt dann durch die Zuweisung der Rolle zu einer Stelle, also letztendlich einem Mitarbeiter. Ein Rollenkonzept ermöglich natürlich, dass eine Person mehrere Rollen in einem Unternehmen übernimmt. Dabei gilt es aber abzuwägen, ob bestimmte Kombinationen von Rollen ein potenzielles Risiko darstellen können. Ein Anwendungsentwickler sollte nicht gleichzeitig der Test-Manager sein. Ebenso kann eine Rolle aber auch mehreren Mitarbeitern zugeordnet werden.

Aus der Aufgabenbeschreibung der Rolle resultieren die notwendigen Berechtigungen. Für SynErgie wurden bereits in den Arbeiten zu Phase 1 Stakeholder oder Akteure benannt, die nun als Basis für die Rollen dienen. Zusätzlich wurden diese durch Rollen ergänzt, die sich aus dem Security Life Cycle Management als notwendig ergeben. Bei der Definition von Rollen und der Vergabe von Rechten gilt es einige Regeln zu beachten. In Tabelle 4 werden einige grundlegenden Empfehlungen aufgeführt, die bei der Definition von Rollen beachtet werden sollten.

TABELLE 4: EMPFEHLUNGEN ZUR ROLLENDEFINITION

Empfehlungen zu Rollendefinitionen
Rollen sollen dem Need-to-Know Prinzip entsprechen
Anwendung des Least-Privileg Prinzips – Die Rolle soll nur die für seine Aufgabe notwendigen Rechte erhalten

Nutzer, Geräte und Anwendungen werden den Rollen zugeordnet
Rollenkonflikte werden bei der Rollenzuordnung geprüft und aufgelöst
Rollenzuordnungen zu Stellen werden zeitlich befristet
Ausscheidende Mitarbeiter, Altgeräte und zu löschende Anwendungen werden von ihren Rollen getrennt, d.h. die Zuordnung wird aufgelöst.
Bei den Rollen sollen System- und Fachaufgaben getrennt werden
Rollen werden nach dem 4-Augen Prinzip definiert
Die Rollenzuordnung wird regelmäßig geprüft und aktualisiert
Es gibt einen Freigabe-Workflow für Benutzer, Geräte, Anwendungen, Clouds, Rollen und Privilegien
Für tragende Rollen erfolgt eine angemessene Sicherheitsüberprüfung
Die Besetzung von Rollen erfordert eine Beurteilung der Vertrauenswürdigkeit und der Befähigung

Zusätzlich sind bei der Besetzung von Rollen bei Kritischen Infrastrukturen die Anforderungen aus dem internationalen Standard ISO/IEC 27001 Anhang A (DIN EN ISO/IEC 27001:2017-06) zu beachten, die sich speziell auch mit dem Thema der Sicherheitsüberprüfung und Beurteilung der Befähigung beschäftigen.

Nachfolgend werden einige ausgewählte Rollen der Marktplattform und der Unternehmensplattform beschrieben, die für das Deployment und den Betrieb zuständig sind. Die Rollen werden dabei, wie in Abbildung 3 dargestellt, in sechs Kategorien unterteilt.

ABBILDUNG 3: KATEGORISIERUNG DER ROLLEN DER UP UND MP

Infrastrukturbetreiber

Der Infrastrukturbetreiber stellt die Infrastruktur und Umgebung (Server, Cloud) für den sicheren Betrieb der Plattform bereit. Die Rolle ist optional. Sofern der Plattformbetreiber die Plattform auf seiner eigenen Infrastruktur betreibt, übernimmt der Plattformbetreiber die Funktion des Infrastrukturbetreibers. Zu den Pflichten des Infrastrukturbetreibers gehört der sichere und zuverlässige Betrieb, der Schutz der Infrastruktur gegen Cyberangriffe, die Verfügbarkeit der Infrastruktur entsprechend vereinbarter SLAs.

Plattformbetreiber

Der Plattformbetreiber ist verantwortlich für den operativen (inhaltlichen) Betrieb der jeweiligen Plattform (MP oder UP). Für den operativen Betrieb sind weitere, hierarchisch untergeordnete Rollen erforderlich. Die für die IT-Sicherheit relevanten Rollen sind administrative Rollen wie Administratoren und Identitätsmanager.

Die Rollen der Administratoren gelten beim Deployment und Betrieb als tragende Rollen. Ihnen obliegt die Verantwortung Services zu installieren, einen eingebundenen Service zu administrieren, erforderliche Zugriffsrechte einzuräumen und den Datenaustausch zu konfigurieren. Aus diesem Grunde lautet die Empfehlung, die Administratorenrollen zu untergliedern, um einen möglichen Schaden im Falles eines erfolgreichen Spoofing- oder Elevation of Privilege Angriffs oder durch einen korrumpierten Administrator zu begrenzen.

Administratorrollen der Markplattform:

- Root CA Admin: verantwortlich für die Administration der Root-CA
- Sys Admin: Administration der IT-Infrastruktur und der Betriebssysteme
- Operativer Admin: Administration und Wartung der Marktplattform und der Services der Marktplattform
- User Manager: im Prinzip ein Administrator, dem die Verwaltung der Nutzer (Service-Nutzer und Service Anbieter) obliegt

Administratorrollen der Unternehmensplattform:

- Sys Admin: Administration der IT-Infrastruktur und der Betriebssysteme
- Services Kurator: Buchung von Services am Marketplace und Aufnahme in das Repository der Unternehmensplattform
- Service Integrator: Installation der Services aus dem Repository und Konfiguration der Datenflüsse zwischen den Services der Unternehmensplattform über den Data Integration Flow des MSB
- Services Admin: Konfiguration der spezifischen Services der Unternehmensplattform über das Konfigurations-Interface der Services
- IAM Manager: Legt Nutzer im System der Unternehmensplattform an, erteilt die erforderlichen Berechtigungen und hält diese aktuell

Nutzer – Anwenderrollen

Als Nutzer sind die Anwender der Unternehmensplattform benannt, die im Rahmen ihrer betrieblichen Aufgabenbeschreibungen die UP und die Services zur Unterstützung ihrer Tätigkeiten nutzen. In den Diskussionen und Workshops zeigte sich, dass eine Beschreibung der einzelnen Anwenderrollen nur exemplarisch erfolgen kann, da diese eben sehr unternehmensspezifisch sind. Allgemein können dies Energie-Manager, Produktionsplaner, Maschinen-Operatoren, Flex-Händler, Energie-Einkäufer, Energie-Verkäufer usw. sein. Aus Sicht der IT-Security und

des Rechtekonzepts lässt sich zum aktuellen Zeitpunkt festhalten, dass diese Rollen nur auf die für den Aufgabenbereich relevanten Services und Informationen Zugriff erhalten sollten. Wichtig für die IT-Security ist, dass die Zugriffsrechte und Ausführungsrechte, die den Anwendern eingeräumt werden, so eingerichtet werden, dass das Least-Privilege Prinzip und das Need-to-Know Prinzip eingehalten wird. Eine Rolle soll jedoch herausgegriffen werden, da diese aktuell die Entscheidung darüber trifft, welche Inserate auf welchem Markt angeboten werden sollen:

- Flex-Manager: Ist als Entscheider bei der Unternehmensplattform dafür verantwortlich, ob ein Flexibilitätsinserat das Unternehmen „verlässt" und somit am Strommarkt angeboten wird

Resilienz und Angriffsabwehr

Damit den Anforderungen des neu verabschiedeten IT-Sicherheitsgesetztes IT-Sig 2.0 (Bundesrepublik Deutschland 2021) und der heraus resultierenden BSI-KritisV (Stand 10/2021 gibt es noch keine an IT-Sig 2.0 angepasste Version) für KRITIS entsprochen wird, ist es zukünftig erforderlich, beim Einsatz der ESP (in der Hauptsache der Unternehmensplattform) im Bereich KRITIS Maßnahmen zur Früherkennung von Cyber-Angriffen und zur Angriffsabwehr zu ergreifen. Im Falle erfolgreicher erheblicher Sicherheitsvorfälle muss eine Meldung an die Meldestelle des BSI erfolgen. Aber auch aus betrieblicher Sicht ist es sinnvoll sich mit der Angriffsabwehr und Notfallplänen und einer schnellen Wiederherstellung von Systemen, im Falles eines erfolgreichen Cyber-Angriffs, auseinanderzusetzen. Für diese Aufgaben wurden aktuell drei Rollen definiert, die exemplarisch sind und im Unternehmen konkretisiert werden sollten. Diese Rollen gehören dem Computer Security Incident Response Team, oder abgekürzt CSIRT, an.

- IT-Sicherheits Operator: Überwacht die ordnungsgemäße Funktion der Plattform und der Services, ist für die Erkennung von ungewöhnlichem Verhalten zur Früherkennung von Cyber-Attacken verantwortlich und übernimmt die Aufgaben, die aus den Anforderungen des IT-Sicherheitsgesetzes 2.0 zur frühzeitigen Angriffserkennung und Abwehr für KRITIS erforderlich sind. Er übernimmt bei KRITIS die Meldung erheblicher Sicherheitsvorfälle an die Meldestelle des BSI.
- Incident Manager: Ist verantwortlich für die Aufrechterhaltung des Betriebs und die effektive Durchführung des Incident-Management-Prozesses
- Backup Manager: Ist verantwortlich für die Planung und Durchführung regelmäßiger Backups und für die Festlegung der Intervalle. Zusammen mit dem Incident Manager sorgt er dafür, dass nach einem Ausfall der Plattformen die Aufnahme des Betriebs schnellstmöglich wieder erfolgen kann.

Märkte und Netze

Für die Beschreibung der Marktrollen und der Rollen des Netzbetriebs wird derzeit auf die Rollenbeschreibungen des BDEW (Bundesverband der Energie- und Wasserwirtschaft e.V. (BDEW) 2019) und der ENTSO-E (ENTSO-E 2020) verwiesen. Ob es im Rahmen eines lokalen Strommarktes zu weiteren Rollendefinitionen kommen wird, muss dann geklärt werden, wenn dieser Strommarkt weiter spezifiziert ist. Aktuell erfolgt die Kommunikation zu externen Rollen der Flexibilitätsvermarktung über die Vermarktungskomponente der Unternehmensplattform.

2.5 Nutzung von kryptographischen Zertifikaten in der ESP

Kryptographische Zertifikate beruhen auf asymmetrischer Kryptographie. Daher wird kurz auf deren Grundlagen eingegangen. Asymmetrische Kryptographie ermöglicht eine Vielzahl von Anwendungen, insbesondere Verschlüsselung und Signatur von Daten sowie Authentifizierung von Personen und Systemen. Diese Art von Kryptographie beruht auf Schlüsselpaaren, wovon stets ein Schlüssel geheim ist, d.h. nur der besitzenden Entität bekannt ist, und der zugehörige öffentliche Schlüssel einem beliebig großen Kreis interessierter Entitäten bekannt gemacht werden kann. Je nach Anwendungsfall reicht dieser Kreis von einzelnen Personen und Systemen bis hin zur Weltöffentlichkeit.

Da öffentliche Schlüssel per se nicht die Information beinhalten, wem diese gehören, gibt es kryptographische Zertifikate zu öffentlichen Schlüsseln. Diese nennen die besitzende Instanz in Verbindung mit dem öffentlichen Schlüssel und beglaubigen dies mit einer kryptographischen Signatur. Die Signatur hängt wiederum vom Schlüsselpaar der beglaubigenden Instanz ab. Das Problem der nachweisbaren Schlüsselzuordnung scheint damit zunächst nur verlagert zu sein, wird mit Zertifikaten aber gelöst, wie nachfolgend dargestellt.

Im Kontext von Zertifikaten spielen Zertifizierungsstellen (engl. „Certificate Authority“, CA), die kryptographische Zertifikate ausstellen, eine zentrale Rolle. Beim Erstellen von Zertifikaten nutzt die CA ein CA-Zertifikat, um Signaturen für die auszugebenden Zertifikate zu erzeugen. CA-Zertifikate sind hierarchisch organisiert und Ausgangspunkt einer Hierarchie ist jeweils ein sogenanntes Wurzelzertifikat, das nicht von einem anderen Zertifikat, sondern mit seinem zugehörigen privaten Schlüssel signiert wurde. In der Hierarchie unter einem Wurzelzertifikat (bzw., wenn man bei der Baummetapher bleibt, *über* einem Wurzelzertifikat) befinden sich meist auf mehreren Ebenen weitere CA-Zertifikate, sogenannte Zwischenzertifikate. Am Ende der Hierarchie stehen die Anwendungszertifikate, sogenannte Blattzertifikate, welche keine CA-Funktionalität besitzen. Letztendlich werden somit über eine solche Hierarchie auf Basis eines einzigen Wurzelzertifikats viele Schlüssel nachweisbar der jeweiligen besitzenden Instanz zugeordnet.
In Anwendungssystemen sind typischerweise einige Wurzelzertifikate als Vertrauensanker hinterlegt, so dass die Systeme sämtliche darunter befindlichen, gültigen Zertifikate für die angegebenen Zwecke wie z.B. Signaturen oder Authentifizierung akzeptieren. Ein Zertifikat ist gültig, wenn der momentane Zeitpunkt, wie er über die Systemuhr bestimmt wird, in dem im Zertifikat angegebenen Gültigkeitszeitraum liegt und das Zertifikat nicht widerrufen wurde. Für die Bekanntgabe widerrufener Zertifikate gibt es etablierte technische Mechanismen, nämlich Zertifikatswiderrufslisten (engl. „Certificate Revocation List“, CRL) und das Online Certificate Status Protocol (OCSP).
Eine Zertifikatshierarchie und die weiteren hier genannten Technologien und Systeme bilden eine sogenannte Public-Key-Infrastruktur (PKI). Als technischer Standard für eine PKI und insbesondere für die Struktur von Zertifikaten hat sich die ITU Recommendation X.509 durchgesetzt.

2.5.1 Struktur der SynErgie-PKI und Anwendungsmöglichkeiten

Die ESP von SynErgie hat eine eigene PKI. Die zentrale Zertifizierungsstelle mit dem Wurzelzertifikat wird auf der Marktplattform (MP) betrieben. Direkt unter dem Wurzelzertifikat befinden sich zwei Zwischenzertifikate. Mit dem einen Zwischenzertifikat stellt die CA weitere Zwischenzertifikate für an der ESP teilnehmende energieflexible Unternehmen aus. Ebenso unter dem Wurzelzertifikat befindet sich ein Zwischenzertifikat, womit die MP wiederum

Zwischenzertifikate für an der MP teilnehmende Services ausstellt. Sowohl die Unternehmen als auch die marktseitigen Services können mit ihren Zwischenzertifikaten eine eigene CA betreiben. Die Struktur der SynErgie-PKI ist in Abbildung 4 dargestellt. Gezeigt werden in der Abbildung auch die Zertifikate der sogenannten OCSP-Responder auf Seiten der Marktplattform, womit die OCSP-Funktionalität zum Prüfen des Widerrufsstatus von Zertifikaten umgesetzt wird.

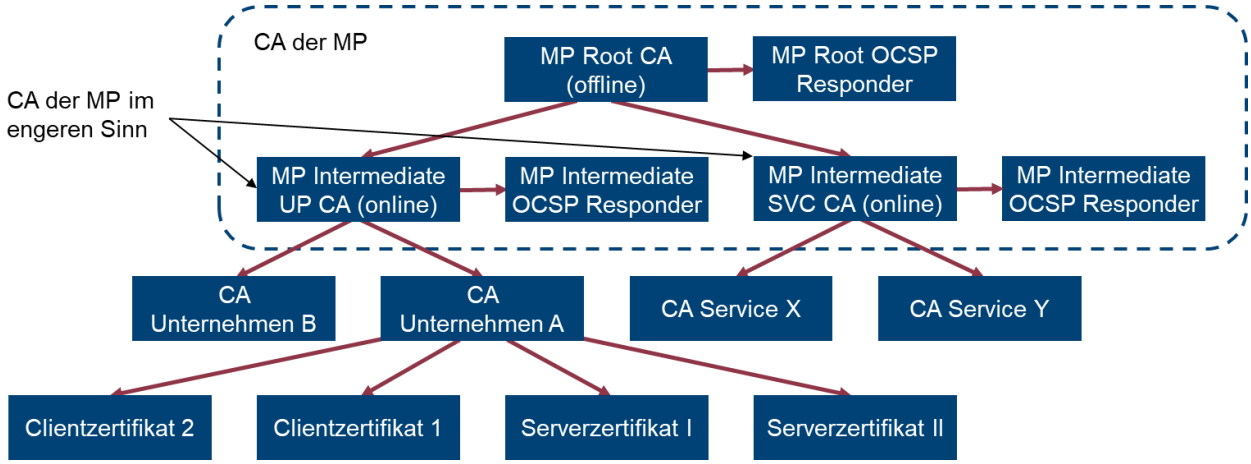

ABBILDUNG 4: AUFBAU DER SYNERGIE-PKI

Marktseitige Services können auf die Zertifikatshierarchie, die von der Marktplattform bereitgestellt wird, zurückgreifen, müssen dies aber nicht. Da jeder Service ein Zwischenzertifikat erhält, kann dieser für verschiedene Zwecke davon abgeleitete Blattzertifikate erzeugen. Hier gibt es mindestens drei Anwendungsmöglichkeiten:

- Der Service kann sich mit einem abgeleiteten Blattzertifikat gegenüber den Nutzern ausweisen.
- Der Service kann Nutzern dedizierte Anwendungszertifikate zum Authentifizieren ausstellen.
- Der Service kann Nutzern dedizierte Anwendungszertifikate zum Signieren von Daten ausstellen.

Außerdem, bzw. genauer gesagt als Ergänzung oder Alternative zu den zwei letztgenannten Punkten, kann der Service Nutzer und Daten auf Basis von Zertifikaten akzeptieren, die von einem Unternehmens-Zwischenzertifikat abgeleitet sind. Hierfür ist es nicht nötig, dass der Service eine Zertifizierungsstelle betreibt, jedoch aber, dass das Unternehmen eine Zertifizierungsstelle betreibt.

Auf Unternehmensseite gibt es ebenfalls verschiedene Anwendungsmöglichkeiten zum Betrieb einer Zertifizierungsstelle innerhalb der SynErgie-PKI, basierend auf dem Zwischenzertifikat, welches sie von der Marktplattform erhalten. Hierbei ist die marktseitige Nutzung von Zertifikaten und die unternehmensinterne Nutzung von Zertifikaten zu unterscheiden. Wie im vorigen Absatz bereits angedeutet, können marktseitige Services die folgenden Möglichkeiten anbieten oder auch vorschreiben:

- Je nach Vorgabe des marktseitigen Service müssen Unternehmen sich mit einem Zertifikat ausweisen. Dazu können oder müssen sie je nach Vorgabe ein Zertifikat nutzen, das von ihrem Unternehmens-Zwischenzertifikat abgeleitet ist.

- Evtl. müssen Unternehmen Daten, die sie an einen Service schicken, wie z.B. EFDM-Objekte, digital signieren, wozu sie je nach Vorgabe des Service ein Zertifikat nutzen können oder müssen, das von ihrem Unternehmens-Zwischenzertifikat abgeleitet ist.

Services haben auch die Möglichkeit, Unternehmen für die zwei genannten Zwecke, wie oben dargestellt, mit Zertifikaten zu versorgen, die vom Service-Zwischenzertifikat abgeleitet sind.

Unternehmensintern kann ebenfalls die SynErgie-PKI verwendet werden. Hier ist es den Unternehmen generell freigestellt, ob und wie Zertifikate für welche Zwecke eingesetzt werden. Hinsichtlich der Referenzarchitektur der Unternehmensplattform (UP) sind aktuell folgende Aussagen zum Einsatz von Zertifikaten möglich:

- Für die Authentifizierung von Services und Personen innerhalb der UP wird aktuell LDAP verwendet und ein Wechsel zu OpenID Connect ist geplant. Zertifikate sind daher nicht für die Authentifizierung innerhalb der UP vorgesehen.
- Es werden derzeit Umsetzungsvarianten zum Signieren von EFDM-Objekten innerhalb der UP diskutiert. Hierfür könnten Zertifikate genutzt werden, die vom SynErgie-Zwischenzertifikat des Unternehmens abgeleitet sind.

2.5.2 Deployment

Bei der Erzeugung von Schlüsseln und Zertifikaten sind eine Reihe von Sicherheitsmaßnahmen zu beachten, die direkten Einfluss auf die Systemarchitektur, die Betriebsprozesse und die Implementierung der nötigen Services haben. Dies wurde bei der Implementierung der Zertifizierungsstelle für die Marktplattform und bei der Implementierung des CA-Service für Unternehmensplattformen berücksichtigt.

Generell sollten private Schlüssel direkt auf dem System, auf dem sie verwendet werden sollen, erzeugt und sicher verwahrt werden. Eine Ausnahme bilden eingebettete Systeme mit geringem Funktionsumfang, wo eine Erzeugung von Schlüsseln nicht möglich ist. Hier können Schlüssel auf einem anderen Gerät erzeugt und in einer geschützten Umgebung auf das Zielgerät aufgespielt werden.

Hervorzuheben ist auch, dass beim Ausstellen eines Zertifikats durch eine Zertifizierungsstelle nicht der private Schlüssel des zu erstellenden Zertifikats benötigt wird. Stattdessen wird der private Schlüssel des signierenden Zertifikats benötigt, worüber die Zertifizierungsstelle bereits verfügt. Von außen werden nur die Informationen benötigt, die im Zertifikat zu beglaubigen sind, d.h. insbesondere der öffentliche Schlüssel, Angaben zur besitzenden Entität, der Verwendungszweck des Zertifikats und der Gültigkeitszeitraum (siehe unter Abschnitt 2.5.3 für weiterführende Erläuterungen). Dementsprechend wird der private Schlüssel des zu erstellenden Zertifikats nicht übertragen und auch nicht von der Zertifizierungsstelle erzeugt, sondern vorab von der Stelle, die das Zertifikat beantragen möchte. Der eigentliche Antrag geschieht mit einem sogenannten Certificate Signing Request (CSR), der im Wesentlichen den öffentlichen Schlüssel und die Angaben zur besitzenden Entität enthält und mit dem zugehörigen privaten Schlüssel signiert ist. Die Signatur stellt sicher, dass der CSR nur von der Stelle erzeugt werden kann, die tatsächlich über den privaten Schlüssel verfügt und dass die Inhaltsdaten des CSR gegen Manipulation geschützt sind. Die Signatur stellt

jedoch nicht sicher, dass die Inhaltsdaten korrekt sind, insbesondere, dass die beantragende Stelle diejenige ist, die sie vorgibt zu sein.
Den vorhergehenden Erläuterungen entsprechend sind die Zertifizierungsdienste von MP und UP so implementiert, dass sie CSRs entgegennehmen und basierend darauf Zertifikate erstellen. Zudem sind die Dienste durch Authentifizierungsmechanismen geschützt, sodass nur berechtigte Stellen Zertifikate beantragen können, wobei Zertifikate nur auf den Namen der jeweiligen Stellen ausgestellt werden.

Die Erzeugung eines CSR obliegt der beantragenden Stelle. Möchte beispielsweise ein Unternehmen an der SynErgie-PKI teilnehmen, muss es dafür ein Zwischenzertifikat von der Zertifizierungsstelle der Marktplattform beziehen. Hierzu führt es die folgenden Schritte aus:

1. Zunächst erstellt das Unternehmen einen privaten Schlüssel und den dazugehörigen öffentlichen Schlüssel.
2. Den öffentlichen Schlüssel und weitere Informationen fügt das Unternehmen in einen CSR ein und signiert diesen mit dem privaten Schlüssel.
3. Für die Zertifikatsanfrage muss das Unternehmen neben dem CSR auch ein Zertifikatsprofil angeben, welches den Verwendungszweck des Zertifikats festlegt. Nach aktueller Architektur ist hier der Zweck Zwischenzertifizierungsstelle fest vorgesehen.
4. Zur Authentifizierung der Zertifikatsanfrage nutzt das Unternehmen den Aktivierungscode, den es bei der Registrierung auf der Marktplattform per Post erhalten hat. Mit diesem Aktivierungscode berechnet es einen sogenannten HMAC über die Zertifikatsanfrage und verknüpft die Anfrage damit nachweislich mit der eigenen Identität.
5. Das Unternehmen schickt die Zertifikatsanfrage bestehend aus CSR und Profilwahl zusammen mit dem HMAC an die Zertifizierungsstelle der MP.
6. Während das Unternehmen auf die Antwort wartet, validiert die Zertifizierungsstelle den HMAC, prüft die Signatur des CSR und überprüft, ob der im CSR angegebene Unternehmensname mit dem Unternehmensnamen übereinstimmt, welcher zu dem verwendeten Aktivierungscode gehört. Falls alle Prüfungen positiv verlaufen, erstellt die CA der MP ein Zertifikat für das Unternehmen.
7. Das Unternehmen empfängt das neue Zertifikat von der Marktplattform.

Da das genutzte Profil vorgibt, dass das Zertifikat für eine Zwischenzertifizierungsstelle gedacht ist, kann das Unternehmen mit dem Zertifikat und dem zugehörigen privaten Schlüssel nun eine eigene Zertifizierungsstelle betreiben und damit selbst Zertifikate für verschiedene Anwendungszwecke in internen Systemen, sowie für die Kommunikation mit weiteren ESP-Diensten (siehe Abschnitt 2.5.1) ausstellen.

Besonders wichtig ist der Schutz des privaten Schlüssels des Wurzelzertifikats einer PKI. Daher wurden hierfür bereits beim Aufbau der SynErgie-PKI besondere Maßnahmen ergriffen. Die wesentliche Anforderung hier ist, dass der private Schlüssel des Wurzelzertifikats „offline“ ist, d. h. nicht auf einem mit dem Internet verbundenen System vorgehalten wird. Daher wurden ganz zu Beginn des Aufbaus der SynErgie-PKI dieser Schlüssel und das zugehörige Wurzelzertifikat nicht auf der Marktplattform, sondern auf einem dedizierten System erstellt. Die Marktplattform hat im weiteren Verlauf lediglich die privaten Schlüssel für ihre beiden Zwischenzertifikate (siehe Abschnitt 2.5.1) sowie die zugehörigen CSRs erzeugt. Diese CSRs wurden manuell auf das dedizierte System der Wurzel-CA übertragen. Dort wurden im nächsten Schritt die Zwischenzertifikate für die Marktplattform erstellt. Diese Zwischenzertifikate und das

Wurzelzertifikat (natürlich ohne den privaten Schlüssel) wurden anschließend für die weitere Nutzung und Veröffentlichung auf die Marktplattform übertragen. Damit hatte die Wurzelzertifizierungsstelle ihre Aufgaben bis auf Weiteres, d.h. bis in mehreren Jahren die Erneuerung der Zwischenzertifikate nötig wird, erfüllt. Daher wurde ihr privater Schlüssel in einem verschlüsselten Offline-Speicher archiviert und das System wurde außer Betrieb genommen (vgl. Abschnitt 2.6.8).

2.5.3 Attribute

Die von der Marktplattform erstellten Zertifikate enthalten zunächst die Standardattribute von X.509-Zertifikaten. Dies sind im Wesentlichen Identitätsattribute, kryptographische Parameter, Angaben zum Verwendungszweck der Zertifikate (etwa Authentifizierung oder Signatur) und der Gültigkeitszeitraum. Damit wird die Zertifizierungsstelle der MP dem Zweck gerecht, Identitäten zu beglaubigen. Darüber hinaus kennzeichnen die Zwischenzertifikate der MP durch ihre Namen, ob ein darunter ausgestelltes Zertifikat einem Serviceanbieter oder einem Servicenutzer (d.h. einem energieflexiblen Unternehmen) gehört. Weitere Attribute hingegen, die über die Standard-Attribute von X.509-Zertifikaten hinausgehen, werden von der CA der MP nicht in den ausgestellten Zertifikaten hinterlegt.

Die MP ist serviceagnostisch und wird daher nicht dafür genutzt, servicespezifische Attribute, etwa ein servicespezifisches Berechtigungsmanagement, zu implementieren. Andernfalls müsste eine enge architektonische und operative Verzahnung der MP mit den Services umgesetzt werden und die Services wären an die MP gebunden. Bei einer Implementierung des Berechtigungsmanagements über die Zertifizierungsstelle der MP müssten die Services zudem Konfigurationsmöglichkeiten direkt in der CA erhalten oder es müssten andere Prozesse zum Festlegen der Attribute etabliert werden. Zudem müssten Zertifikate bei jeder Attributsänderung, also ggf. häufig, widerrufen werden. Auf Unternehmensseite ist es den Unternehmen generell freigestellt, ob und wie Zertifikate für welche Zwecke eingesetzt werden und welche Attribute dazu ggf. in Zertifikaten hinterlegt werden.

2.6 Life-Cycle-Management

Die Services der Unternehmensplattform und der Marktplattform unterliegen, wie jedes andere Produkt auch, einem Lebenszyklus. Dieser beginnt bei der ersten Idee und endet bei der Entsorgung bzw. bei der Deinstallation des Service. Damit die geforderte Sicherheit über alle Lebensphase eines Produkts sichergestellt werden kann, bedarf es Vorgaben und Maßnahmen für die jeweiligen Lebensphasen zu definieren und umzusetzen. Das Security Life Cycle Management befasst sich hierbei mit der IT-Sicherheit der Services der ESP. Durch Security LCM soll sichergestellt werden, dass die Sicherheit der Services während des gesamten Lebenszyklus auf dem erforderlichen Sicherheitslevel gehalten werden. Das Security LCM beginnt mit der Definition von Anforderungen und dem Einsatzgebiet, welche ein Hersteller oder ein Kunde eines Service festlegt, über den Entwicklungs- und Freigabeprozess, das Deployment und über das Update-Management im Betrieb und endet mit der sicheren Deinstallation und dem Löschen von vertraulichen Informationen (inkl. einer Datensicherung sofern erforderlich) sowie dem Löschen von Berechtigungen.

Da das Sicherheitskonzept in SynErgie auf den definierten Sicherheitslevels aufbaut, ist es nur konsequent, dass die Anforderungen im Security LCM in den Lebensphasen, je nach angestrebtem Sicherheitslevel, variieren. Als Basis für die Festlegung der unterschiedlichen Lebenszyklen wurde die Vorgehensweise nach dem Security Development Lifecycle Management (SDL) der Firma Microsoft® herangezogen (Microsoft 2021). Die Anforderungsbeschreibungen selbst erfolgten basierend auf einer Auswahl weiterer Standards und Empfehlungen zum Life-Cycle Management.

Dabei wurden folgenden Standards oder Empfehlungen mit einbezogen und eigene Ergänzungen und Anpassungen vorgenommen:

- NIST – Lifecycle Management nach NIST SP.800-160 (Ross et al. 2018), SP.800-100 (Bowen et al.)
- BSI: IT-Grundschutz-Bausteine und Guideline zu Common Criteria, insbesondere Assurance class "Life-Cycle Support (ALC) (Bundesamt für Sicherheit in der Informationstechnik 2021a)
- OWASP: SDLC -Software Development Lifecycle (OWASP SDLC 2021); SAMM (Software Assurance Maturity Model) (OWAPS SAMM 2.0) und Application Security Verification (OWASP Security Qualitative Metrics 2021)

Die Gesamtheit der betrachteten Lebenszyklen eines Service im Security LCM zeigt Abbildung 5.

ABBILDUNG 5: LEBENSPHASEN EINES SERVICE DER ESP

Das Security LCM definiert für jede Lebensphase Anforderungen, die sich nach gefordertem Sicherheits-Level unterscheiden können. Anforderungen und resultierende Maßnahmen, die für höhere SLs als verbindlich gelten und umzusetzen sind, können auch für niedrigere SLs umgesetzt werden, sind dann aber optional. Da die Überprüfung der definierten Anforderungen in der Praxis nur im Rahmen einer Überprüfung durch eine autorisierte Stelle oder eine Zertifizierung tatsächlich möglich wäre, ist die Durchsetzung und Verifikation der Umsetzung derzeit noch offen. In jeder Lebensphase sollte beim jeweiligen Unternehmen der eigene Prozess zur IT-Sicherheit hinsichtlich der Einhaltung der im Security LCM benannten Anforderungen überprüft werden. Im Falle einer Zertifizierung nach etablierten IT-Sicherheitsstandards sind die hierfür notwendigen Maßnahmen ohnehin umzusetzen und nachzuweisen.

Allgemeine Ziele von (Security) Life Cycle Management:

- Schutz des Kunden durch sichere Software
- Reduzierung der Anzahl an Schwachstellen und Verringerung des Schweregrads von Vorfällen
- Berücksichtigung von Compliance-Anforderungen
- Proaktiv, vorausschauend Anforderungen definieren
- Eliminieren von Redundanzen, Koordination der Prozesse und Steigerung der Produktivität
- Kostenreduktion: Fehlerbehebung nach dem Release sind deutlich teurer als während der Entwicklung
- Steigerung des Vertrauens

Fasst man die wichtigsten Regeln und Konzepte der Security- und Privacy-Prinzipien zusammen und lässt diese in die Prozesse des LCM mit einfließen, erhält man bereits eine fundierte Basis für die IT-Sicherheit der Services und Plattformen. In Tabelle 5 werden die Prinzipien zusammengefasst dargestellt:

TABELLE 5: PRINZIPIEN EINER SICHEREN ENTWICKLUNG

Prinzip	Beschreibung
Security by design	Sicherheitsbelange bereits in der Planungsphase betrachten
Security by default	Standardeinstellungen möglichst konservativ wählen (z.B. Privilegien möglichst niedrig einstellen) Selten benutzte Funktionen standardmäßig deaktivieren
Security in deployment	Sichere Verteilung und Installation; Nutzung vertrauenswürdiger Quellen Mitgelieferte Dokumentationen und Tools sollen bei der optimalen Einrichtung unterstützen
Communications (Security)	Offen mit möglichen Sicherheitslücken umgehen und Endanwendern schnell Patches oder Workarounds zur Verfügung stellen
Privacy by design	Datenschutzbelange der Software bereits in der Planungsphase berücksichtigen
Privacy by default	Standardeinstellungen hinsichtlich Sammlung, Speicherung und Weitergabe von personenbezogenen konservativ wählen
Privacy in deployment	Offenlegung der Datenschutzmechanismen, um es Administratoren zu ermöglichen, die internen Datenschutzrichtlinien des Unternehmens umzusetzen
Communications (Privacy)	Datenschutzerklärungen transparent formulieren Ein Team für Datenschutzvorfälle einrichten

Bei den nachfolgenden Ausführungen handelt es sich um eine kurze Zusammenfassung der erarbeiteten Ergebnisse. Für die Entwicklungsphasen werden zusammengefasst die wichtigsten Anforderungen aufgezeigt, die im Rahmen des Life-Cycle-Managements und des Schutzbedarfskatalogs erarbeitet wurden.

2.6.1 Anforderungsphase

In der Anforderungsphase werden die funktionalen Anforderungen und hinsichtlich IT-Security nicht-funktionale Anforderungen ermittelt. Ebenso werden gesetzliche Anforderungen aufgenommen. Die Definition der Produktanforderungen läuft oft auf einen Kompromiss zwischen den geschäftlichen Anforderungen eines Kunden und dem erforderlichen Sicherheitsniveau zum Schutz seiner Vermögenswerte hinaus. Dies kann nur durch das Sammeln und gründliche Analysieren von marktbasierten Anforderungen, geltenden Gesetzen und Vorschriften sowie Standards und Best Practices erreicht werden.

2.6.2 Entwurfsphase

In der Entwurfsphase erfolgen die Planung und die Konzeption. Neben der rein funktionalen Beschreibung eines Service wird hier die Bestimmung des notwendigen Sicherheitslevels, basierend auf der Einstufung des erforderlichen Schutzbedarfs der zu verarbeitenden Daten und des Risikos (Risikoanalyse), durchgeführt. Ebenso erfolgt hierbei die Bedrohungsmodellierung (Threat-Modeling). Daraus leiten sich nachfolgend die Anforderungen für die zu ergreifenden IT-Sicherheitsmaßnahmen und die zu treffenden Anforderungen an den Lebenszyklus eines Service ab. Am Ende der Entwurfsphase steht eine Grobspezifikation zur Verfügung.

2.6.3 Entwicklungsphase

Die Entwicklungsphase umfasst sowohl die Erstellung der Feinspezifikationen als auch die Implementierung selbst. Im Rahmen der Entwicklung erfolgt ebenfalls die Auswahl von einzusetzender Drittsoftware (Bibliotheken) und die Auswahl der Entwicklungswerkzeuge. Die Implementierung folgt dabei den Vorgaben der Programmierrichtlinien, wobei sich die Secure Coding Standards auf die Vermeidung von Programmierfehlern konzentrieren Die Vorgaben sind hierbei abhängig vom jeweiligen erforderlichen Sicherheitslevel. Ebenso ist die Durchführung von Codeüberprüfung und eine erste entwicklungsbegleitende Durchführung von Tests (Unit-Tests, Modultests) Bestandteil dieser Phase. Dabei gilt es die Awareness von Mitarbeitern durch Schulungen zu fördern. Je nach vereinbartem Sicherheits-Level ist die Durchführung von Code-Analysen und die Auswahl und Pflege der Entwicklungswerkzeuge einzuhalten.

2.6.4 Überprüfung und Freigabe

Das Secure Life Cycle Management fokussiert in der Testphase auf das (Ab-)Testen von geforderten Sicherheitsfunktionen. Das rein funktionale Testen eines Service (Test der Anwendung) ist Teil der „normalen“ Software-Entwicklung. Im Secure LCM werden die in der Entwurfsphase definierten Maßnahmen zur IT-Sicherheit überprüft. Auch hier kann zwischen eher funktionalem Testen und nicht-funktionalem Testen unterschieden werden. Funktionales Testen beträfe hier beispielsweise die Überprüfung von Login-Verfahren, Auswahl der spezifizierten Krypto-Algorithmen, während das nicht-funktionale Testen die Robustheit beispielsweise gegen Angriffen im Fokus hat. Am Ende der Verifikation steht die Freigabe des entwickelten Service durch den Hersteller. Sollte eine Zertifizierung erforderlich sein, ist diese ebenfalls in dieser Phase durchzuführen. Je nach Sicherheits-Level kann eine Hersteller-Signatur der Software gefordert sein. Die Testtiefe und der Testumfang ist abhängig vom jeweiligen Sicherheitslevel.

2.6.5 Ausbringung

Im Secure LCM stehen die Verfahren zum sicheren Bezug inklusive einer möglichen Freigabe durch einen Service-Provider und der Vertrieb im Vordergrund. Hierzu gehört auch die Prüfung der Authentizität einer Software. Der Freigabeprozess sollte abhängig vom erforderlichen Sicherheits-Level sein. Dies kann von einer einfachen Überprüfung der grundlegenden Funktionen und Interfaces bis zu einem Code-Review und einer Zertifizierung und Signatur durch den Service-Provider reichen. Neben der IT-Sicherheit müssen hierbei aber auch Fragen der Haftung und der Verantwortlichkeiten geklärt werden, wie auch die Wege oder Varianten des Deployments. Dabei gilt es Vorgaben zu Restriktionen zu bestimmen: Installation nur von einer vertrauenswürdigen Quelle oder in der Verantwortung des Betreibers auch von anderen Quellen.

2.6.6 Sicheres Deployment – Abschließende Sicherheitsüberprüfung / Zertifizierung

Die abschließende Sicherheitsüberprüfung konzentriert sich in erster Linie auf die Bewertung der Produktreife durch einen Service Provider oder Betreiber eines App-Stores, einschließlich der Fragen, die mit seiner Sicherheit zusammenhängen, und, falls erforderlich, auf die Zertifizierung eines Produkts durch den App-Store Betreiber, sowie auf die weitere Entscheidung, ob ein Produkt durch ihn auf den Markt gebracht werden soll oder nicht. In wieweit eine Sicherheitsprüfung und Zertifizierung durch den Service Provider erfolgt ist noch nicht final entschieden.

TABELLE 6: AUSZUG DER ANFORDERUNGEN IN DER AUSBRINGUNGSPHASE

Nr.	Beschreibung	SL1	SL2	SL3	SL4
D.1 [8]	Zusammenstellung von Releases (Überprüfung der Kompatibilität von unterschiedlichen Software-Ständen einzelner Services); Gesamtpaket		O[9]	M[10]	M
D.2	Durchführung von Integrationstests durch den Service Provider		O	M	M
D.3	Umsetzung eines Secure-Deployments (automatisiert, zertifikatsbasiert)		O	M	M
D.4	Update und Patch-Management (Sicherheitsupdates)		O	M	M
D.5	Zertifizierung und Vergabe eines Sicherheits-Labels[11]			O	O

2.6.7 Betrieb und Wartung

Der sichere Betrieb beginnt mit dem Prozess der Installation, des Einbindens oder Anbindens eines Service in oder an eine der Plattformen der ESP. Dazu ist ergänzend ein Identitäts-Management, ein Key-Management oder ein Zertifikatsmanagement, je nach Sicherheits-Level, erforderlich. Ebenso sind Dokumentationen zum Service notwendig, die einem Nutzer oder dem Administrator die Inbetriebnahme und Konfiguration erleichtern und diese sicher machen. Weiterhin ist für den sicheren Betrieb ein Event-Logging-Mechanismus hilfreich, wenn es um die Nachvollziehbarkeit von Fehlfunktionen oder um die Früherkennung von Angriffen geht. In einer weiteren Stufe wäre Monitoring zu nennen. Monitoring unterscheidet sich vom reinem Logging durch die Analyse und Auswertung der erfassten Daten. Einerseits ist damit eine Nachvollziehbarkeit von Fehlfunktionen möglich, aber Monitoring und Analyse zählen auch zu den wichtigsten Mitteln der Früherkennung von Angriffen. Sie sind damit ein Instrumentarium zur Abwehr von Angriffen. Angriffe erfolgen oft in mehreren Schritten. Wird der erste Schritt erkannt, der zumeist eine erste Analyse möglicher Schwachstellen ist, können frühzeitig Maßnahmen zur Abwehr des nachfolgenden eigentlichen Angriffes eingeleitet werden.

Update-Management: Da sich Angriffsvektoren und die Fähigkeiten von Angreifern im Leben einer Anwendung laufend ändern, ist die Aufrechterhaltung der Sicherheit ein dynamischer Prozess, der ständig Anpassungen unterliegt. Dazu ist es erforderlich, dass der Software Hersteller regelmäßig überprüft, ob es Sicherheitsvorfälle bei der eingesetzten

[8] D steht für Phase Deployment
[9] O steht für optional
[10] M steht für mandatory
[11] Die Entscheidung, ob im Rahmen des SynEnergie eine Zertifizierung erfolgt ist derzeit noch nicht beschlossen

Software gibt oder ob es bei eingesetzter Fremdsoftware zu Sicherheitsvorfällen kam. Lücken sind durch ein Patch- oder Update Management zu schließen. Dafür braucht es entsprechenden Support.

Alarm-Management: Je nach Sicherheitslevel ist ein Alarmmanagement erforderlich, um bei unerwarteten Ereignissen einen Alarm auszulösen, damit notwendige Maßnahmen eingeleitet werden können. Im Falle der Kritischen Infrastrukturen ist hierzu auch die Gesetzeslage zu betrachten und es muss die entsprechende Behörde (BSI) informiert werden, wenn es zu schwerwiegenden sicherheitsrelevanten Vorfällen kam.

Notfall-Management: Ein zusätzlicher Faktor ist ein Notfall-Management im Fehlerfall. Im Kontext der Verfügbarkeit soll das Notfallmanagement sicherstellen, dass eine N-1 Sicherheit besteht, sofern die Verfügbarkeit essentiell ist, ein Notbetrieb ermöglicht wird oder sonstige Maßnahmen eingeleitet werden können, die schwerwiegende Auswirkungen abschwächen oder sogar vermeiden können.

Sichere Konfiguration: Fast jedes Out-of-the-Box-Produkt muss ordnungsgemäß konfiguriert werden, um in der Produktionsumgebung zu funktionieren. Danach muss das Produkt überwacht und bei Bedarf aktualisiert werden (z. B. aufgrund der Veröffentlichung einer neuen Version des Produkts, der Notwendigkeit, aufgedeckte Codierungsfehler oder Schwachstellen zu korrigieren), um weiterhin das erforderliche Sicherheitsniveau zu gewährleisten.

TABELLE 7: AUSZUG DER ANFORDERUNGEN IN DER BETRIEBSPHASE

Nr.	Beschreibung	SL1	SL2	SL3	SL4A
OP.1 [12]	Betrieb und Anbindung an eine PKI (Unterstützung Zertifikatsmanagement)		O	M	M
OP.2	Betrieb und Anbindung an eine zentrale CA für die Marktplattform und die Unternehmensplattform (Zertifikatsmanagement externe Services)		O	M	M
OP.3	Betrieb und Anbindung an Sub-CAs in den Unternehmen für Zertifikatsmanagement (UP Services)		O	M	M
OP.4	Management für Sicherheits-Patches und Updates; Betrieb Updateserver; Informationsplattform, …			M	M
OP.5	Anbindung an ein ESP Meldesystem für Bugs / Sicherheitsvorfälle		O	M	M
OP.6	Monitoring von ungewöhnlichen Ereignissen, als präventive Maßnahmen für Angriffsversuche		O	M	M
OP.7	Alarmmanagement zur Einleitung von Notfallmaßnahmen		O	M	M

[12] OP steht für Phase Operation (Betrieb)

TABELLE 8: AUSZUG DER ANFORDERUNGEN IN DER BETRIEBSPHASE - NOTFALLMANAGEMENT

Nr.	Beschreibung	SL1	SL2	SL3	SL4
OP.8	Erstellung von Notfallplänen und Umsetzung von Maßnahmen in Notfällen (speziell auch zum Thema KRITIS)		O	M	M
OP.9	Betrieb eines Secure Backupkonzept zur Wiederherstellung nach einem Angriff			M	M
OP.10	Anbindung an ein Behördenmeldesystem zur Meldung von Vorfällen (speziell im Falle KRITIS)			M	M
OP.11	Betrieb eine Meldesystems (Hersteller oder App-Store Betreiber) zur Meldung von Fehlern		M	M	M

2.6.8 Außerbetriebnahme

Bei der Außerbetriebnahme ist ein besonderes Augenmerk darauf zu legen, dass schützenswerte Daten einerseits nicht verloren gehen (Datensicherung und Aufbewahrung), sofern diese aus unterschiedlichsten Gründen weiterhin benötigt werden (gesetzliche Aufbewahrungspflicht, Firmen-Know-how, etc.), aber andererseits auch nicht in falsche Hände geraten (Mediensanitisierung). Dies gilt auch für Zertifikate, Secret Keys, lokal gespeicherte Passwörter oder Zugangsdaten. Ebenso wichtig ist ein geordneter Abmeldeprozess eines Service vom System, damit dieser nicht von einem Angreifer genutzt werden kann, um sich Zugang zum System zu verschaffen.

Wenn es an der Zeit ist, ein Produkt zu entsorgen (aufgrund seiner Veralterung, einer notwendigen Aktualisierung oder aus anderen Gründen), müssen geschützte Informationen weiterhin sicher aufbewahrt werden. Um dies richtig anzugehen, sollte ein Entsorgungsprozess geplant und im Voraus durchdacht werden, wobei auf Sicherheitsmaßnahmen geachtet werden sollte, die zur Erhaltung wertvoller Informationen, zum sicheren Löschen und Bereinigen von Medien sowie insgesamt zur Entsorgung von Hard- und Software angewendet werden sollten.

TABELLE 9: AUSZUG DER ANFORDERUNGEN IN DER AUSSERBETRIEBNAHME

Nr.	Beschreibung	SL1	SL2	SL3	SL4
DEC.1 [13]	Datensicherung – Bewahrung von Daten	O	O	M	M
DEC.2	Sichere Mediensanitisierung (sicheres Vernichten von vertraulichen Daten, Secrete Keys, Zertifikaten)		O	M	M
DEC.3	Gesicherter Abmeldeprozess		O	M	M
DEC.4	Sichere Entsorgung von Hardware- und Software			M	M

[13] DEC steht für Phase Decommissioning (Außerbetriebnahme)

3 FAZIT UND AUSBLICK

Das Detailpapier vermittelt einen Einblick in die Arbeiten und daraus resultierende Erkenntnisse zur IT-Sicherheit im Projekt SynErgie. Die IT-Sicherheit ist eine der wesentlichen Voraussetzung für die Akzeptanz und einen erfolgreichen Betrieb der Unternehmensplattform und der Marktplattform. Der Sektor Energie zählt zu den Kritischen Infrastrukturen. Ziel der Arbeiten ist es, bereits bei der Referenzarchitektur und der Entwicklung der Plattformen und Services die erforderlichen Prozesse und Maßnahmen zum Erzielen der erforderlichen IT-Sicherheit mit zu betrachten und umzusetzen, und damit dem Prinzip des „Security by design“ gerecht zu werden. Die Zielsetzung ist, dass die beiden Plattformen der ESP (Marktplattform und Unternehmensplattform) KRITISready entwickelt werden sollen, damit der Einsatz bei KRITIS möglich ist und eine erforderliche Zertifizierung dadurch erleichtert wird. Die aktuelle Version des Diskussionspapiers stellt nun konkrete Maßnahmen vor, die in den Entwicklungsprozessen zukünftig umgesetzt werden sollen.

Dazu wurde mit dem Threat-Modeling eine Methode zur Gefahren- und Schwachstellenanalyse vorgestellt, die bereits in der Entwurfsphase bei der Bestimmung der Sicherheitsanforderungen anzuwenden ist und nicht nur isoliert die Software, sondern auch das Umfeld mit betrachtet, in der die Software eingesetzt werden soll. Die Bestimmung des Sicherheitslevels erfolgt ebenfalls in der Entwurfsphase. Zur Bestimmung wird die Kritikalität von Informationen hinsichtlich Vertraulichkeit, Integrität, Authentizität, Verfügbarkeit und Nicht-Abstreitbarkeit betrachtet, wobei der mögliche Schaden beim Verlust dieser als Kriterium dient. Hinzu kommt das Risiko eines möglichen Angriffs, wobei auch hier das Umfeld analog zum Thread-Modeling mit betrachtet werden muss. Beide Methoden zusammen geben somit die Anforderungen an die IT-Sicherheit und damit an die erforderlichen Maßnahmen vor.

Mittels des Security Life-Cyle Managements werden die Anforderungen in den verschiedenen Lebenszyklen vorgegeben, die dazu dienen den Sicherheitslevel über den gesamten Lebenszyklus einer Komponente oder eines Service aufrecht zu erhalten. Da sich die Fähigkeiten von Angreifern kontinuierlich verbessern und auch die Angriffsziele (Branchen, Firmen) sich ständig ändern, müssen die Voraussetzungen, die zur Einstufung in einen Sicherheitslevel führten, zyklisch überprüft werden, ebenso wie die umgesetzten Maßnahmen.

Die Definition von Rollen und ein Rechtekonzept sind ein weiterer Baustein eines Sicherheitskonzepts. Zusammen mit den Plattformverantwortlichen erfolgte die Definition der zentralen Rollen, die Zugriffe auf die Plattformen oder Services haben müssen. Dabei fand zum aktuellen Zeitpunkt eine Fokussierung auf Administration und Betrieb statt. Teil des Sicherheitskonzepts ist es, eine eindeutige Trennung zwischen Betreiberrollen (Plattform as a Service, Infrastructure as a Service), Administratorenrollen und Nutzerrollen vorzunehmen. Durch eine restriktive Rechtevergabe kann so der mögliche Schaden, der von einer Rolle ausgehen kann, stark begrenzt werden.

Der aktuelle Stand der Arbeiten dient als Basis für die nachfolgenden Arbeiten, bei denen eine weitere Vertiefung und Konkretisierung der Maßnahmen erfolgt. Den Entwicklern werden hierzu zukünftig Hilfsmittel in Form einer Prozessbeschreibung zum Life-Cycle Management und eines Security-Guide zur Verfügung gestellt. Einer der Kernpunkte wird zukünftig das Deployment von Services sein. Hier gilt es Fragen zu beantworten, wie offen ein System im angestrebten Umfeld sein darf und wie restriktiv Anforderungen an die IT-Sicherheit gegenüber Softwareherstellern und Vertriebswege eingefordert werden müssen und können.

LITERATURVERZEICHNIS

Albadi, M. H.; El-Saadany, E. F. (2008): A summary of demand response in electricity markets. In: *Electric Power Systems Research* 78 (11), S. 1989–1996. DOI: 10.1016/j.epsr.2008.04.002.

Battaglini, A.; Komendantova, N.; Brtnik, P.; Patt, A. (2012): Perception of barriers for expansion of electricity grids in the European Union. In: *Energy Policy* 47, S. 254–259. DOI: 10.1016/j.enpol.2012.04.065.

Bauer, D.; Abele, E.; Ahrens, R.; Bauernhansl, T.; Fridgen, G.; Jarke, M. et al. (2017): Flexible IT-platform to Synchronize Energy Demands with Volatile Markets. In: *Procedia CIRP* 63, S. 318–323. DOI: 10.1016/j.procir.2017.03.088.

Bauernhansl, T.; Bauer, D.; Abele, E.; Ahrens, R.; Bank, L.; Brugger, M. et al. (2019): Industrie 4.0 als Befähiger für Energieflexibilität. In: A. Sauer, E. Abele und H. U. Buhl (Hg.): Energieflexibilität in der deutschen Industrie. Ergebnisse aus dem Kopernikus-Projekt - Synchronisierte und energieadaptive Produktionstechnik zur flexiblen Ausrichtung von Industrieprozessen auf eine fluktuierende Energieversorgung - SynErgie. Stuttgart: Fraunhofer Verlag, S. 245–312.

Bauernhansl, T.; Sauer, A.; Kaymakci, C.; Schlereth, A.; Schilp, J.; Kalchschmid, V. et al. (2021): Demonstratoren der Energiesynchronisationsplattform. Diskussionspapiere V4. Online verfügbar unter https://doi.org/10.24406/IGCV-N-642373.

Bertsch, V.; Hall, M.; Weinhardt, C.; Fichtner, W. (2016): Public acceptance and preferences related to renewable energy and grid expansion policy: Empirical insights for Germany. In: *Energy* 114, S. 465–477. DOI: 10.1016/j.energy.2016.08.022.

BMU (2021): Novelle des Klimaschutzgesetzes vom Bundestag beschlossen. Hg. v. Bundesministerium für Umwelt, Naturschutz und nukleare Sicherheit. Online verfügbar unter https://www.bmu.de/pressemitteilung/novelle-des-klimaschutzgesetzes-vom-bundestag-beschlossen, zuletzt geprüft am 13.10.2021.

BMWi (2021): Gesetz zur Änderung des Erneuerbare-Energien-Gesetzes und weiterer energierechtlicher Vorschriften. Gesetzentwurf der Bundesregierung. Hg. v. Bundesministerium für Wirtschaft und Energie. Online verfügbar unter https://www.bmwi.de/Redaktion/DE/Artikel/Service/gesetz-zur-aenderung-des-eeg-und-weiterer-energierechtlicher-vorschriften.html, zuletzt geprüft am 21.10.2021.

Bowen, P.; Hash, J.; Wilson, M.: Information security handbook: a guide for managers. Online verfügbar unter https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-100.pdf, zuletzt geprüft am 11.10.2021.

Braitermann, Z.; Shostack, A.; Marcil, J.; Vries, S. d.; Michlin, I.; Wuyts, K.; Hurlbut, R. (2020): Threat Modeling Manifesto. Online verfügbar unter https://www.threatmodelingmanifesto.org/, zuletzt aktualisiert am 27.11.2020, zuletzt geprüft am 15.10.2021.

Buhl, H. U.; Duda, S.; Schott, P.; Weibelzahl, M.; Wenninger, S.; Fridgen, G. et al. (2021): Energieflexibilitätsdatenmodell der Energiesynchronisationsplattform. Diskussionspapiere V4. Online verfügbar unter https://doi.org/10.24406/IGCV-N-642370.

Bundesamt für Sicherheit in der Informationstechnik (2021a): IT-Grundschutz-Bausteine (Edition 2020). Online verfügbar unter https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/IT-Grundschutz-Bausteine/2020/Bausteine_Download_Edition_2020_node.html, zuletzt aktualisiert am 26.01.2021, zuletzt geprüft am 15.04.2021.

Bundesamt für Sicherheit in der Informationstechnik (2021b): Übersicht Schutzprofile und TR - Übersicht Schutzprofile und Technische Richtlinien. Online verfügbar unter https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Smart-metering/Uebersicht-Schutzprofile-und-TR/uebersicht-schutzprofile-und-tr.html, zuletzt aktualisiert am 08.10.2021, zuletzt geprüft am 12.10.2021.

Bundesnetzagentur (2020): Quartalsbericht Netz- und Systemsicherheit - Gesamtes Jahr 2019. Bonn: Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen. Online verfügbar unter https://www.bundesnetzagentur.de/SharedDocs/Mediathek/Berichte/2020/Quartalszahlen_Gesamtjahr_2019.pdf, zuletzt geprüft am 18.09.2020.

Bundesrepublik Deutschland (2021): Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme, zuletzt geprüft am 08.10.2021.

Bundesverband der Energie- und Wasserwirtschaft e.V. (BDEW) (2019): Rollenmodell für die Marktkommunikation im deutschen Energiemarkt. Online verfügbar unter https://www.bdew.de/media/documents/Awh_20190507_Rollenmodell-MAK-Version1-2-END.pdf, zuletzt geprüft am 31.08.2020.

DIN EN 61508-1:2011-02: Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme - Teil 1: Allgemeine Anforderungen (IEC 61508-1:2010); Deutsche Fassung EN 61508-1:2010. Online verfügbar unter https://www.beuth.de/de/norm/din-en-61508-1/135302584, zuletzt geprüft am 11.10.2021.

DIN EN 62443-3-2:2018-10 - Entwurf: Sicherheit für industrielle Automatisierungssysteme - Teil 3-2: Sicherheitsrisikobeurteilung und Systemgestaltung (IEC 65/690/CDV:2018). Berlin. Online verfügbar unter https://www.beuth.de/de/norm-entwurf/din-en-62443-3-2/294546806, zuletzt geprüft am 07.10.2021.

DIN EN ISO/IEC 27001:2017-06: Informationstechnik - Sicherheitsverfahren - Informationssicherheitsmanagementsysteme - Anforderungen (ISO/IEC 27001:2013 einschließlich Cor 1:2014 und Cor 2:2015). Online verfügbar unter https://www.beuth.de/de/norm/din-en-iso-iec-27001/269670716, zuletzt geprüft am 07.10.2021.

DS-GVO: VERORDNUNG (EU) 2016/ 679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES - vom 27. April 2016 - zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/ 46/ EG (Datenschutz-Grundverordnung). In: DSGVO. Online verfügbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016R0679&from=DE, zuletzt geprüft am 11.10.2021.

ENTSO-E (2020): The harmonised electricity market role model. Online verfügbar unter https://www.entsoe.eu/Documents/EDI/Library/HRM/Harmonised_Role_Model_2020-01.pdf, zuletzt geprüft am 31.08.2020.

European Environmental Agency (2020): Final energy consumption by sector and fuel. Unter Mitarbeit von Stephanie Schilling. Hg. v. European Environmental Agency. Kopenhagen. Online verfügbar unter https://www.eea.europa.eu/data-and-maps/indicators/final-energy-consumption-by-sector-9/assessment-4, zuletzt aktualisiert am 17.01.2019, zuletzt geprüft am 10.07.2019.

Fridgen, G.; Potenciano Menci, S.; van Stiphoudt, C.; Schilp, J.; Köberlein, J.; Bauernhansl, T. et al. (2021): Referenzarchitektur der Energiesynchronisationsplattform. Diskussionspapiere V4. Online verfügbar unter https://doi.org/10.24406/IGCV-N-642369.

Gierkink, M.; Sprenger, T. (2020): Die Auswirkungen des Klimaschutzprogramms 2030 auf den Anteil erneuerbarer Energien an der Stromnachfrage. Energiewirtschaftliches Institut an der Universität zu Köln (EWI) gGmbH. Online verfügbar unter https://www.ewi.uni-koeln.de/cms/wp-content/uploads/2021/07/200106_EWI-Analyse-Anteil-Erneuerbare-in-2030_final.pdf, zuletzt geprüft am 13.10.2021.

Hardy, N. (1988): The Confused Deputy: (or why capabilities might have been invented). In: *ACM SIGOPS Operating Systems Review* 22 (4), S. 36–38.

IPCC (2021): Climate Change 2021: The Physical Science Basis. Contribution of Working Group I to the Sixth Assessment Report of the Intergovernmental Panel on Climate Change. Summary for Policymakers. In Press. Unter Mitarbeit von Masson-Delmotte, V., P. Zhai, A. Pirani, S. L. Connors, C. Péan, S. Berger, N. Caud, Y. Chen, L. Cambridge University Press.

ISO/IEC 15408-1:2009-12: Informationstechnik - IT-Sicherheitsverfahren - Evaluationskriterien für IT-Sicherheit - Teil 1: Einführung und allgemeines Modell (15408-1 - 2009-12). Online verfügbar unter https://www.beuth.de/de/norm/iso-iec-15408-1/125041003, zuletzt geprüft am 11.10.2021.

Jazayeri, P.; Schellenberg, A.; Rosehart, W. D.; Doudna, J.; Widergren, S.; Lawrence, D. et al. (2005): A Survey of Load Control Programs for Price and System Stability. In: *IEEE Trans. Power Syst.* 20 (3), S. 1504–1509. DOI: 10.1109/TPWRS.2005.852147.

Kohnfelder, L.; Garg, P. (1999): The threats to our products. In: *Microsoft Interface, Microsoft Corporation* 33.

Körner, M.-F.; Bauer, D.; Keller, R.; Rösch, M.; Schlereth, A.; Simon, P. et al. (2019): Extending the Automation Pyramid for Industrial Demand Response. In: *Procedia CIRP* 81, S. 998–1003. DOI: 10.1016/j.procir.2019.03.241.

Larcom, B.; Eddington, M. (2005): Trike v1 methodology document. In: *Draft, work in progress*.

Lund, H.; Østergaard, P. A.; Connolly, D.; Ridjan, I.; Mathiesen, B. V.; Hvelplund, F. et al. (2016): Energy Storage and Smart Energy Systems. In: *International Journal of Sustainable Energy Planning and Management* 11, S. 3–14. DOI: 10.5278/IJSEPM.2016.11.2.

Lund, P. D.; Lindgren, J.; Mikkola, J.; Salpakari, J. (2015): Review of energy system flexibility measures to enable high levels of variable renewable electricity. In: *Renewable and Sustainable Energy Reviews* 45, S. 785–807. DOI: 10.1016/j.rser.2015.01.057.

Mann, M. E.; Rahmstorf, S.; Kornhuber, K.; Steinman, B. A.; Miller, S. K.; Coumou, D. (2017): Influence of Anthropogenic Climate Change on Planetary Wave Resonance and Extreme Weather Events. In: *Scientific Reports* 7, 1-10. DOI: 10.1038/srep45242.

Markle-Huss, J.; Feuerriegel, S.; Neumann, D. (2016): Decision model for sustainable electricity procurement using nationwide demand response. In: Tung X. Bui und Ralph H. Sprague (Hg.): Proceedings of the 49th Annual Hawaii International Conference on System Sciences (HICCS). 5-8 January 2016, Kauai, Hawaii. Koloa, HI, 1/5/2016 - 1/8/2016. Piscataway, NJ: IEEE, S. 1010–1019.

Microsoft (2021): Microsoft Security Development Lifecycle (SDL) – version 5.2. Online verfügbar unter https://docs.microsoft.com/de-de/previous-versions/windows/desktop/cc307748(v=msdn.10), zuletzt aktualisiert am 11.10.2021, zuletzt geprüft am 11.10.2021.

Müller, T.; Möst, D. (2018): Demand Response Potential: Available when Needed? In: *Energy Policy* 115, S. 181–198. DOI: 10.1016/j.enpol.2017.12.025.

NIST (CDC) FIPS 199: Standards for Security Categorization of Federal Information and Information Systems. NIST Computer Security Division (CSD). Online verfügbar unter https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf, zuletzt geprüft am 11.10.2021.

NIST (CDC) FIPS 200: Minimum Security Requirements for Federal Information and Information Systems. NIST Computer Security Division (CSD), zuletzt geprüft am 11.10.2021.

Oeder, A.; Ronge, K.; Schimmelpfennig, J.; Winter, C.; Ahrens, R. (2021): IT-Sicherheit der Energiesynchronisationsplattform. Diskussionspapiere V4. Online verfügbar unter https://doi.org/10.24406/IGCV-N-642372.

Openkritis: (2021): Neue KRITIS-Anlagen und Schwellenwerte im IT-SiG 2.0. Online verfügbar unter https://www.openkritis.de/it-sicherheitsgesetz/kritis-anlagen_kritisv_itsig20.html, zuletzt aktualisiert am 17.09.2021, zuletzt geprüft am 08.10.2021.

OWAPS SAMM 2.0: OWASP SAMM v2.0 - Core Model Document. Online verfügbar unter https://raw.githubusercontent.com/OWASP/samm/master/Supporting%20Resources/v2.0/OWASP-SAMM-v2.0.pdf, zuletzt geprüft am 26.03.2021.

OWASP SDLC (2021): OWASP in SDLC. Online verfügbar unter https://owasp.org/www-project-integration-standards/writeups/owasp_in_sdlc/, zuletzt aktualisiert am 23.02.2021, zuletzt geprüft am 03.03.2021.

OWASP Security Qualitative Metrics (2021): OWASP Security Qualitative Metrics. Online verfügbar unter https://owasp.org/www-project-security-qualitative-metrics/SECURITY-QUALITATIVE-METRICS.html, zuletzt aktualisiert am 12.03.2021, zuletzt geprüft am 25.03.2021.

Palensky, P.; Dietrich, D. (2011): Demand Side Management: Demand Response, Intelligent Energy Systems, and Smart Loads. In: *IEEE Trans. Ind. Inf.* 7 (3), S. 381–388. DOI: 10.1109/TII.2011.2158841.

Papaefthymiou, G.; Haesen, E.; Sach, T. (2018): Power System Flexibility Tracker: Indicators to track flexibility progress towards high-RES systems. In: *Renewable Energy* 127, S. 1026–1035. DOI: 10.1016/j.renene.2018.04.094.

Pfeilsticker, L.; Colangelo, E.; Sauer, A. (2019): Energy Flexibility – A new Target Dimension in Manufacturing System Design and Operation. In: *Procedia Manufacturing* 33, S. 51–58. DOI: 10.1016/j.promfg.2019.04.008.

Reinhart, G.; Bank, L.; Brugger, M.; Hieronymus, A.; Köberlein, J.; Roth, S. et al. (2020): Konzept der Energiesynchronisationsplattform. Diskussionspapier V3. Online verfügbar unter http://publica.fraunhofer.de/documents/N-602416.html.

Reinhart, G.; Bank, L.; Brugger, M.; Roth, S.; Simon, P.; Bauernhansl, T. et al. (2018): Konzeption Der Energiesynchronisationsplattform. Diskussionspapier V2.

Rösch, M.; Bauer, D.; Haupt, L.; Keller, R.; Bauernhansl, T.; Fridgen, G. et al. (2019): Harnessing the Full Potential of Industrial Demand-Side Flexibility: An End-to-End Approach Connecting Machines with Markets through Service-Oriented IT Platforms. In: *Applied Sciences* 9 (18), S. 3796. DOI: 10.3390/app9183796.

Ross, R.; McEvilley, M.; Oren., J. (2018): Systems security engineering: considerations for a multidisciplinary approach in the engineering of trustworthy secure systems, volume 1. Gaithersburg, MD. Online verfügbar unter https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v1.pdf, zuletzt geprüft am 11.10.2021.

Sauer, A.; Abele, E.; Buhl, H. U. (2019a): Einleitung. In: A. Sauer, E. Abele und H. U. Buhl (Hg.): Energieflexibilität in der deutschen Industrie. Ergebnisse aus dem Kopernikus-Projekt - Synchronisierte und energieadaptive Produktionstechnik zur flexiblen Ausrichtung von Industrieprozessen auf eine fluktuierende Energieversorgung - SynErgie. Stuttgart: Fraunhofer Verlag, S. 4–8.

Sauer, A.; Abele, E.; Buhl, H. U. (Hg.) (2019b): Energieflexibilität in der deutschen Industrie. Ergebnisse aus dem Kopernikus-Projekt - Synchronisierte und energieadaptive Produktionstechnik zur flexiblen Ausrichtung von Industrieprozessen auf eine fluktuierende Energieversorgung - SynErgie. Stuttgart: Fraunhofer Verlag.

Schilp, J.; Bank, L.; Köberlein, J.; Bauernhansl, T.; Sauer, A.; Kaymakci, C. et al. (2021): Optimierung auf der Energiesynchronisationsplattform. Diskussionspapiere V4. Online verfügbar unter https://doi.org/10.24406/IGCV-N-642371.

Schott, P.; Ahrens, R.; Bauer, D.; Hering, F.; Keller, R.; Pullmann, J. et al. (2018): Flexible IT platform for synchronizing energy demands with volatile markets. In: *it - Information Technology* 60 (3), S. 155–164. DOI: 10.1515/itit-2018-0001.

Schott, P.; Sedlmeir, J.; Strobel, N.; Weber, T.; Fridgen, G.; Abele, E. (2019): A Generic Data Model for Describing Flexibility in Power Markets. In: *Energies* 12 (10), S. 1893. DOI: 10.3390/en12101893.

Seifermann, S.; Abele, E.; Sauer, A.; Bauer, D. (2019): Integrierte Betrachtung technischer, wirtschaftlicher und gesellschaftlicher Aspekte industriellen Demand-Side Managements. In: *Internationaler ETG-Kongress 2019: Das Gesamtsystem im Fokus der Energiewende. 08. und 09. Mai 2019, Esslingen am Neckar. - Frankfurt am Main*.

Seitz, P.; Abele, E.; Bank, L.; Bauernhansl, T.; Colangelo, E.; Fridgen, G. et al. (2019): IT-based Architecture for Power Market Oriented Optimization at Multiple Levels in Production Processes. In: *Procedia CIRP* 81, S. 618–623. DOI: 10.1016/j.procir.2019.03.165.

Shevchenko, N.; Chick, T. A.; O'Riordan, P.; Scanlon, T. P.; Woody, C. (2018): Threat modeling: a summary of available methods. Carnegie Mellon University Software Engineering Institute Pittsburgh United.

Shostack, A. (2014): Threat Modeling: Designing for Security. 1st: Wiley Publishing.

Steurer, M. (2017): Analyse von Demand Side Integration im Hinblick auf eine effiziente und umweltfreundliche Energieversorgung. Univ. Stuttgart, Diss., 2017.

Uba (2021a): Anteil erneuerbarer Energien am Bruttostromverbrauch und am Bruttoendenergieverbrauch. Umweltbundesamt. Online verfügbar unter https://www.umweltbundesamt.de/sites/default/files/medien/384/bilder/dateien/de_indikator_ener-04_erneuerbare-energien_2021-03-16.pdf, zuletzt geprüft am 13.10.2021.

Uba (2021b): Erneuerbare Energie in Zahlen. Umweltbundesamt. Online verfügbar unter https://www.umweltbundesamt.de/themen/klima-energie/erneuerbare-energien/erneuerbare-energien-in-zahlen#uberblick, zuletzt geprüft am 13.10.2021.

Uba (2021c): Treibhausgas-Emissionen in Deutschland seit 1990 nach Kategorien der UNFCCC-Berichterstattung. Umweltbundesamt. Online verfügbar unter https://www.umweltbundesamt.de/sites/default/files/medien/361/bilder/dateien/2021-03-15_thg_crf_plus_1a_details_ci_1990-2019_vjs2020.pdf, zuletzt geprüft am 13.10.2021.

UcedaVelez, T.; Morana, M. M. (2015): Risk Centric Threat Modeling: process for attack simulation and threat analysis: John Wiley & Sons.

United Nations (2015): Transforming our world: The 2030 Agenda for sustainable development. New York: United Nations. Online verfügbar unter https://sustainabledevelopment.un.org/content/documents/21252030%20Agenda%20for%20Sustainable%20Development%20web.pdf, zuletzt geprüft am 05.08.2019.

Wynn, J.; Whitmore, J.; Upton, G.; Spriggs, L.; McKinnon, D.; McInnes, R. e. a. (2011): Threat assessment & remediation analysis (tara): Methodology description version 1.0. MITRE CORP. Bedford, MA.