OIAZ
166 WISSENSCHAFT & PRAXIS
September 2021

ÖSTERREICHISCHE
INGENIEUR-UND
ARCHITEKTEN-ZEITSCHRIFT

The JOURNAL of OIAV

SICHERE IT-ARCHITEKTUREN UND METHODEN FÜR DIGITALISIERTE ENERGIESYSTEME

Christian Neureiter, Günther Eibl & Dominik Engel

ABSTRACT

The digitization of the power grid is creating new challenges. In order to master the complexity of digitized power systems, which almost always represent "systems of systems", new approaches are needed. "Systems Engineering" as an interdisciplinary approach provides the tools to address these challenges, and to consider important aspects, such as IT security or the protection of personal data, already at the architectural level.

KURZFASSUNG

Durch die Digitalisierung des Stromnetzes ergeben sich neue Herausforderungen. Um die Komplexität digitalisierter Energiesysteme zu beherrschen, die fast immer „Systems of Systems" darstellen, werden neue Herangehensweisen benötigt. „Systems Engineering" als interdisziplinärer Ansatz liefert die Werkzeuge um diese Herausforderungen zu adressieren, und wichtige Aspekte, wie z.B. die IT-Sicherheit oder den Schutz persönlicher Daten, bereits auf Architekturebene zu berücksichtigen.

Die voranschreitende Digitalisierung des Stromnetzes stellt dieses insbesondere aus architektonischer Sicht vor neue Herausforderungen. Aus einer ehemaligen Top-Down Architektur wird ein verteiltes System mit interagierenden Teilnehmer_innen. Systemisch betrachtet wandelt sich das Stromnetz von einem ehemals vernetzten und komplizierten System zu einem komplexen System. Basierend auf der Klassifikation nach Haberfellner et al. [1] lässt sich das einerseits durch den Anstieg beteiligter Komponenten sowie deren Diversität, und andererseits durch eine veränderbare bzw. veränderliche Topologie argumentieren.

Darüber hinaus ist das Stromnetz Teil eines sogenannten „System of Systems" [2] [3] in dem sich einzelne Teilnehmer_innen freiwillig zu einer Kooperation entschließen, um einen übergeordneten Nutzen zu erzielen. Ein Beispiel hierfür ist das sogenannte „Demand Side Management", in dem durch besondere Anreize (z.B. flexible Preismodelle) Verbraucher_innen zu einem netzdienlichen Verhalten animiert werden sollen. Als Beispiel ist hierfür das Preis-gesteuerte Laden von Elektrofahrzeugen zu nennen. Hierbei reagiert das Stromnetz auf hohe Lasten durch einen höheren Strompreis, wodurch Fahrzeuge gegebenenfalls den Ladevorgang

verschieben. Problematisch wird dieses Szenario allerdings, wenn z.B. nach einer längeren Phase mit hohem Preis dieser wieder gesenkt wird und eine Vielzahl an Fahrzeugen gleichzeitig den Ladevorgang fortsetzen. Der sprunghafte Anstieg des Verbrauchs würde wiederum zu einer entsprechenden Antwort des Stromnetzes führen (noch höherer Preis), was wiederum ein Aussetzen des Ladevorgangs nach sich ziehen kann. Im schlimmsten Fall könnte es hier zu einem Aufschwingen des Stromnetzes mit weitreichenden Konsequenzen kommen. Ein Ausweg hierfür wäre eine harte Abschaltung einzelner Teilnehmer_innen bzw. eine Begrenzung der zur Verfügung gestellten Ladeleistung. Aus energiepolitischer Sicht wäre das aber kontraproduktiv, und es gilt, Lösungen für den verlässlichen Betrieb im Systemverbund zu finden.

Das geschilderte Szenario illustriert ein sogenanntes „emergentes Verhalten" als typische Charakteristik für System-of-Systems. Es lässt sich weder auf der einen, noch auf der anderen Seite lösen, sondern erfordert eine gemeinsame Betrachtung des Systemverbundes. Die inhärente Komplexität dieses Verbundes benötigt aber Methoden, um Komplexität aus architektonischer Sicht in den Griff zu bekommen.

Dabei sind zwei Aspekte zu trennen. Zum einen geht es um die Frage der interdisziplinären Zusammenarbeit über Domänengrenzen hinweg. Das beginnt bei vermeintlich einfachen Themen wie einer gemeinsamen Sprache, zieht sich fort über abgestimmte Prozesse und landet bei interoperablen und kompatiblen Entwurfsmethoden. Zum anderen stellt sich die Frage, wie Komplexität architektonisch behandelt werden kann.

Für die Beantwortung der ersten Frage lohnt sich ein Blick in das wissenschaftliche Fachgebiet „Systems Engineering". Systems Engineering als interdisziplinärer Ansatz widmet sich der Frage, wie komplexe, technische Systeme in großen Projekten realisiert werden können. Neben fundamentalen Engineering Prozessen, wie z.B. im ISO Standard 15288 [4] beschrieben, liefert diese Disziplin eine Vielzahl an Ansätzen und Methoden.

Für die Beantwortung der zweiten Frage kann das menschliche Gehirn als Inspiration dienen. Um die Komplexität der echten Welt erfassbar zu machen, stützen wir uns hier auf die zwei Paradigmen „Abstraktion" und „Separation of Concerns".

Modellierung, als „Abstraktion auf relevante Aspekte" ist in technischen Disziplinen Teil des Alltags. Es gibt Modelle für die Beschreibung elektrischer Schaltungen, mechanischer Konstruktionen oder Software. Die Herausforderung liegt hier nicht im Mangel geeigneter Modelle begründet, sondern in der Integration dieser zu einem großen Ganzen - über Disziplinen- und Domänengrenzen hinweg.

Als Analogie kann hierfür das Internet dienen. Kompatibilität der einzelnen Systeme im Internet wird primär über den sogenannten ISO/OSI Stack [5] ermöglicht. Dieser Stack allokiert die Hauptfunktion des Internets („dezentrale Kommunikation") auf unterschiedliche Schichten, von denen jede eine spezielle Teilaufgabe übernimmt. Die unterste Schicht regelt beispielweise wie die logischen Elemente „1" und „0" auf physikalischer Ebene repräsentiert werden, die übergeordneten Schichten regeln in weiterer Folge die Korrektur von Bit-Fehlern, das Strukturieren in Datenpakte, die Transportsicherung und so weiter.

Ein vergleichbares Konzept ist für die Architektur des Stromnetzes anzustreben. Auf einer obersten Schicht können beispielsweise Geschäfts- und Unternehmensarchitekturen modelliert werden. Dies betrifft sowohl Unternehmens-interne als auch Unternehmens-übergreifende Prozesse, wie z.B. die Interaktion zwischen Netz- und Ladestationsbetreiber. Weiters kann auf dieser Ebene abgeleitet werden, welche (Teil-) Systeme existieren und wie diese miteinander interagieren. Da auf dieser Ebene unterschiedliche Stakeholder aus den verschiedenen Disziplinen involviert sind, ist eine gemeinsame Sprache Voraussetzung. Mit dem „Smart Grid Architecture Model" (SGAM) [6] gibt es hier für das intelligente Stromnetz auch bereits eine interessante, wenn auch noch unvollständige Basis.

Für die weitere Dekomposition einzelner Komponenten, wie z.B. einer Ladestation, ist insbesondere das Konzept der Objekt Modellierung zu nennen. Analog der Funktionsweise des Gehirns ermöglichen hierbei sogenannte „General Purpose Modelling Languages" wie z.B. SysML [7] die Dekomposition größerer Systeme in kleinere Einheiten einerseits, und die „Komposition" (den Zusammenbau) dieser Einheiten andererseits. Hervorzuheben ist hierbei, dass dieser Ansatz nicht nur auf eine strukturelle Zerlegung beschränkt ist, sondern auch die funktionale Komposition ermöglicht.

Diese Möglichkeit ist insbesondere relevant, als auf dieser Basis auch eine weiterführende Validierung stattfinden kann. Z.B. kann das Modell eines Teils des Stromnetzes mit dem vielfach instanziierten Modell elektrischer Fahrzeuge im Rahmen einer Co-Simulation verbunden werden. Somit kann das Verhalten des Gesamtverbundes analysiert werden, noch bevor dieser realisiert wurde.

Voraussetzung hierfür ist allerdings sowohl eine semantische und syntaktische, als auch eine technische Kompatibilität der einzelnen Modelle.

Das Ergebnis der Objektmodellierung sind somit einzelne „Design Elemente", die an die entsprechenden Entwicklungsteams weitergereicht werden, wo in weiterer Folge das detaillierte Design sowie die Implementierung realisiert werden können.

Wichtige Aspekte, wie die IT-Sicherheit und die Wahrung des Datenschutzes, können so bereits auf Architekturebene berücksichtigt werden. Gerade für Methoden der IT-Sicherheit und Wahrung der Privatsphäre erhöht die Integration auf Architekturebene die Wirksamkeit enorm, wird doch so die Herangehensweise von „security by design" und

„privacy by design“ erfüllt [9]. Während der Zugang, ein System im Nachhinein sicher und datenschutzkonform zu machen, meist mühsam und fehlerbehaftet ist, ist dieser Zugang tauglicher, um komplexe IT-Systeme und die darin verarbeiteten Daten zu schützen. So konzentrieren sich etwa traditionelle security Methoden darauf, den Angreifer aus dem System auszusperren, während sich neue, „resiliente“ Ansätze auch die Frage stellen, wie man einen Angreifer, der bereits im System ist, behandeln muss. Das reicht von der Erkennung des Einbruchs mit der Beurteilung, welche Teilsysteme infiltriert wurden über die Minimierung des Schadens etwa durch Segmentierung des Informationsnetzes und die Erstellung von backup-Systemen bis hin zur Planung von situationsabhängigen Abwehrmaßnahmen.

Die skizzierte Vorgehensweise zur Erstellung von Systemarchitekturen ist Voraussetzung für eine ganzheitliche Betrachtung des Stromnetzes, insbesondere im Verbund mit interagierenden Systemen. Wohlgemerkt steht hierbei nicht nur der Entwurf, sondern insbesondere die Validierung des Gesamtsystems bzw. eines ganzen Systemverbundes im Fokus. Es gilt die Prämisse: wenn sich Systeme vernetzen, dann müssen auch die zugehörigen Entwurfsmodelle und darüber hinaus die entwerfenden Organisationen kompatibel zueinander sein. Dieses Prinzip der Spiegelung von Organisation und Architektur ist auch als „Conway’s Law“ benannt und wurde bereits 1968 postuliert [8].

Das Ziel interoperabler Systeme und Organisationen ist Stand heute noch nicht erreicht, die Richtung wurde aber bereits eingeschlagen. Und der gerade stattfindende Rollout von Elektromobilität und allen damit einhergehenden Konsequenzen erhöht hierfür nochmals deutlich die Geschwindigkeit.

LITERATURVERZEICHNIS

[1] R. Haberfellner, O. L. de Weck, E. Fricke, and S. V¨ossner, Systems Engineering. Grundlagen und Anwendung. Orell F¨ussli, 2012.

[2] M. W. Maier, “Architecting principles for systems-of-systems,” Systems Engineering, vol. 1, no. 4, pp. 267–284, 1998.

[3] D. DeLaurentis, “Understanding Transportation as a System-of-Systems Design Problem,” in 43rd AIAA Aerospace Sciences Meeting and Exhibit. Reno, Nevada, 2005.

[4] International Organization for Standardization (ISO), ISO/IEC 15288:2015 Systems engineering - System life cycle processes, Std., 2015.

[5] International Organization for Standardization (ISO), ISO/IEC ISO/IEC 7498-1:1994. Open Systems Interconnection- Basic Reference Model 1994

[6] Smart Grid Coordination Group, “Smart Grid Reference Architecture,” CEN-CENELEC-ETSI, Tech. Rep., 2012

[7] Object Management Group, “OMG Systems Modeling Language (OMG SysML) Version 1.3,” Tech. Rep., 2012.

[8] Conway, Melvin E. “How do committees invent.” Datamation 14, no. 4 (1968): 28-31.

[9] Cavoukian, A., Polonetsky, J., & Wolf, C. (2010). SmartPrivacy for the Smart Grid: embedding privacy into the design of electricity conservation. Identity in the Information Society, 3(2), 275–294. Retrieved from http://dx.doi.org/10.1007/s12394-010-0046-y

AUTOREN

Christian Neureiter
Günther Eibl
Dominik Engel
Fachhochschule Salzburg