DISASTER RESEARCH DAYS 2020

DCNAustria
Disaster Competence Network Austria

WEBINAR SERIES
OCTOBER
13 — 22

Book of Abstracts

Konferenzband

From Ecology to Cyberresilience: an interdisciplinary application of resilience principles for smart grid designs

KEVIN MALLINGER,
ALEXANDER SCHATTEN,
JOHANNA ULLRICH

Organisation(en):
SBA Research

kmallinger@sbaresearch.org, aschatten@sbaresearch.org, jullrich@sbaresearch.org

Abstract

Critical infrastructures that perpetuate modern societies form a complex systemofsystems which usually stays invisible to us. This is true for information systems (e.g. accounting systems) and traditional critical infrastructures as well. However, digitization increasingly intertwines ICT and critical infrastructure. The resulting complexity of hierarchical and hyperconnected systems that build and rely on each other, display emergent behavior that individuals are unable to monitor and control anymore. Symptoms of these effects can be observed e.g. in high maintenance costs, publicized data breaches, largescale security incidences and the increasing risk of critical supply chain losses. As the technological ability to create safe and resilient systems is mostly at hand, we investigate how design principles facilitate new narratives for handling critical infrastructures and enable the application of available resiliencedesigns and techniques.

Our proposition is that these sociotechnical systems are better understood as complex ecosystems and thus a lot can be learned from biological ecosystem principles. Thus, in this paper, we use smart power grids as an example to outline how design principles of ecological resilience research might be an applicable and supporting framework for cyberresilience and infrastructure resilience research. Furthermore, we investigate how practical resilience techniques taken from the MITRE taxonomy can be integrated to support the framework. In order to reduce the complexity of the topic, we focus on the architectural implications of the discussed principles and examples.

Introduction

Digitization effected most technological fields in the 21st century by improving engineering techniques, production processes, and for our case most importantly, by connecting individual systems to hyperconnected, softwaredefined systemofsystems. The increasing ways of human interactions with these systems added another layer of complexity and further increased the difficulty to overlook and handle cyberecosystems. Thus, it is not surprising to observe the same phenomena in our usecase, the evolution of the power grid. Our current systems are grounded on an isolated design that is over 100 years old but are now transitioning to a digitized and hyperconnected smart grid (Li et al. 2013). This will enable the connections of decentralized energy producers and consumers, improve efficiency, and enhance the ability to detect threats. However, the complexity of these systems will open up an increased attack surface for (cyber)attacks. Beyond that, emergent errors are harder to predict, failures cascade faster and threaten the international power grid system. The lack of resilience within such systems impacts depending systems and creates external costs for society – the latter not only in a short term economic sense, but even more importantly by harming the trust we put in digital technologies and the ability to maintain critical functions for society. In terms of production and distribution of electricity, outages of a power plant or the loss of power grids can cost society billions of euros (Li et al. 2013). Especially since the cyberattack on the Ukrainian power grid in 2015 (EISAC 2016), it is known that such attacks are feasible and can have devastating effects. The open availability of worms, malware, or botnets (Dabrowski et al. 2017) on the internet leads to easier execution of such attacks and constitutes an increasing threat to the energy sector and society.

Consequently, in order to effectively manage the transition to a hyperconnected infrastructure, a framework is needed (Yan et al. 2013) that at the same time takes the inherent properties of complex systems into account but is simple enough to deduce a clear, actionable guideline for handling errors, threats and emergent behavior. Finding and describing core principles is therefore of great importance for the stability of such software defined infrastructures. In the classical field of cybersecurity there are only few such superordinate structures and for the new research field of cyberresilience, mainly the MITRE taxonomy (Bodeau et al. 2013). Although the taxonomy provides clear derivations of actions, with 19 design principles and 15 specific techniques, it is quite extensive and somewhat difficult to understand for people without an advanced technological background. As mechanisms that foster stability, survival and safety seem equally applicable to the individual, society, nature, and technical systems (Cavelty et al. 2015), we draw inspiration from a discipline that successfully managed to derive actionable guidelines for handling complex systems; namely, the ecological resilience research.

In this abstract, we want to investigate briefly, i) if the seven principles from ecological resilience research are a useful framework for managing complex cyberphysical systems, ii) which MITRE techniques complement ecological resilience design principles, and iii) how these principles might enhance the stability of smart grids. The meanings of the ecological principles cannot be assumed to be identical and need to be redefined in the context of cyberresilience. Therefore, the individual principles might be interpreted in a different way than that of ecology. As cyberresilience designs and techniques are mostly focusing on the software architecture level, the abstract will discuss the implications on the smart grid exclusively from an architectural point of view. Structurally, the seven individual principles are defined and described, their architectural implications are discussed and exemplified by general resilience and MITRE techniques that foster a resilient design for smart grids.

Background

The research term resilience was introduced to the scientific community in 1973 by Crawford Holling, as he published his paper on the resilience and stability of ecological systems (Holling 1973). From there on, it pathed it way from ecology to a multitude of sciences and is getting increasingly prominent in the 21. century, and eventually, influenced the creation of the new research field cyberresilience. The effort to define a first taxonomy by the MITRE corporation should foster an increased understanding of that new field. It was created as an extended engineering framework that addressed a broader range of threats than that of the cyber domain alone. It is intended to apply to systemsofsystems that include cyberphysical constituents with a specific focus on critical operations (Bodeau et al. 2013). We therefore use this framework as a comparison to the ecological principles.

By the systemic approach and the associated principles – as used in complex science studies – such as emergence, nonlinearity, uncertainty, critical thresholds, connectivity, hierarchy & panarchy (Ladyman et al. 2013), the ecologically based construct of resilience offers an elegant way to cope with complex and sometimes unpredictable environments. Since systemic effects are the primary focus of this paper, we define resilience as the capacity of a system to continually change and adapt yet remain within critical thresholds (Folke et al. 2010).

This definition acknowledges the possibility to mitigate adverse events through systemic effects and feedback loops but also the ability of systems to adjust to changing environments. In the first case, resilience describes i) the ability to adapt while providing systemimmanent properties, ii) the controlled failure of system(s), and iii) in the event of a system failure, the rapid restoration of properties. The second considers the changes in the system environment so that i) problems intrinsic to the system do not arise, ii) emerging problems are intercepted and mitigated, and iii) longterm threat scenarios are integrated into the systems design.

Application

The first ecological principle, maintain diversity and redundancy, can be interpreted as variety (how many different elements), balance (how many representatives of each element) or disparity (how different the elements are from one of each other) (Stirling 2007). As it enables us to react to changes and disturbances, diversity has proven effective to increase a system's resilience. Therefore, it is a critical design principle to avoid largescale cyberattacks, as only a

part of the overall system can be affected. This is still an inherent problem for smartgrids, as has been shown by a Spanish smart metering system that used the same encryptionscheme for all meters. Once these smartmeters were breached by a bruteforce attack, they could be used as an entry point to launch an attack against the whole power system (Mahmud et al. 2015). To avoid such threats, different notions of diversity can be used (e.g. intrusiontolerant architectures, nvariant systems, massivescale software diversity, dynamic diversity, synthetic diversity). This is an incremental part of the MITRE taxonomy as well as in ecology, as it avoids the risk of a monoculture, in which the compromise of one component can propagate to all other such components (Bodeau & Graubart 2017).

The same ecological and engineering principle is used for the design of power grids by applying the N1 criteria that dictates that a continuous power flow is guaranteed in case of a failure of one of the network's components (Reichl et al. 2016). Thereby, it not only concentrates on the availability of a diverse set of physical structures, but also integrates several perspectives that include a profound risk assessment, interTSO coordination (transmission system operator) (see principle broaden participation) and efficient modelling and routing of the power flow (see principle manage connectivity) that correspond to the multiperspective view of diversity in ecological designs.

The second principle, manage connectivity, refers to the way in which parts of a system interact with each other (i.e. exchange information, transfer material, transform energy, etc.). The avoidance of system failures or the fast revival of networks are key areas of resilience research and are necessary to tackle a variety of challenges in power grids.

One of the most critical challenges is the development from a centralized power generation system to a decentralized, complex, and multiagent system. Thereby, the integration of regenerative producers into the energy system demands methods that foster smart management and enables peertopeer energy transactions. The MITRE taxonomy gives advice on how to design resilient connections (e.g. adaptive response, analytic monitoring) but doesn't address the scope of these challenges, as it focusses mainly on the agility of systems in the context of compromised systems.
As the ecological principles extend the focus not only on smallscale systems but integrate the complex adaptive environment (see CAS principle) it pivots the focus on managing the interconnections of individual systems. For power grid network communication, software defined networks (SDN) are one way to practically apply this principle within its broad scope. SDNs can be employed to manage the communication entities of smart grids and can be used for load balancing and shifting, dynamically adjusting routing paths, monitoring traffic flows and fast failure detection (Rhemani et al. 2019).

The third principle, manage slow variables and feedbacks, defines the temporal dimension of the architecture. As in nature and for any given information system, slow variables typically determine the underlying structure, while the dynamics of the system arise from interactions and feedbacks between fast variables that respond to the conditions created by the slow variables (Biggs et al. 2015).

This is often overlooked in the design phase, but quite important on the long run, as the postponed management of legacy systems is complex, time consuming, expensive, and prone to failures.

This is also the case in the grid system as the transition from analog handling of power grids to software defined, hyperconnected smart grids generated a gap between the physical and the software realm. Novel attacks (e.g. botnets) can exploit the slow response times of physical assets and closedloop feedback structures to destabilize the whole system (Dabrowski et al. 2017).

The MITRE taxonomy addresses this aspect partly (see Table 1) but lacks focus on emergent phenomena within the system, which arise through longterm changes and feedbacks. The ecological principle specifically highlights such emergent properties and points out complex feedback loops that might arise within in the system but also by combining legacy systems with new technologies. Thus, by translating this principle to the mentioned problem, selfregulating systems must be designed (see also CAS) that do not reinforce the feedbacks and foster a resilient management system.
The fourth principle, foster complex adaptive systems (CAS) thinking, describes the diverse interaction of components, that are individually and collectively adaptive to change, enabling them to selforganize and evolve, and often yielding emergent properties at different scales (Biggs et al. 2015).

The power grid slowly evolved from a local design, to a national and finally, to an international construct, without changing the technical presumptions and management narratives accordingly. The resulting complexity of this digitized power grid causes unintended behavior (e.g. oscillation) (ENTSOE 2016) and makes it as a CAS partly unpredictable. Therefore, the hyperconnected smart grid should be able to reshape itself nimbly to meet tactical goals (e.g. energy demand, system stability) but also in the context of environmental changes (e.g. attacks, disasters). This development sets the requirement of selfadaptive software and adaptation of security mechanisms that can also be found in the MITRE taxonomy (Evesti & Ovaska 2013).

In ecology, CAS can create dependencies horizontally, vertically but also on a temporal dimension. This fosters a mindset that complexity can only be managed by integrating all perspectives and thereby, creating a natural balance. As in nature, smart grids can be designed to pursue such a balance to (unintended) changes by using complex algorithms, local data processing, decentralized control, twoway electricity transmission, and reliabilityefficiency driven response, which are also the basis for selfhealing processes (Dabrowski et al. 2017; Wang et al. 2015).

The fifth principle, encourage learning, represents the constant need to revise existing knowledge to enable adaptative capabilities in complex systems, as well as to maintain critical services in the face of disturbance and change (Biggs et al. 2015). This principle encourages to continuously improve learning processes, to broaden the technological knowledge but also to integrate extended dependencies (e.g. versatile user behaviour) and novel approaches (e.g. game theory) to measure variables that might influence smart grids (Xue & Yu 2017).

Learning has to start with the situational awareness of system elements, threats, and missions' dependencies on system elements (e.g. performance monitoring) which is also addressed by the MITRE framework (Bodeau et al. 2013). As used in ecological research to better understand CAS, novel monitoring and prediction methods are found in the area of deep learning, machine learning and artificial intelligence. These methods can be used to profile the activity of users, devices, applications, and networks. They seek to detect anomalous patterns or unusual behavior, that may arouse suspicion (Eleks 2018), and are powerful tools in softwaredefined, smart power grids (Rehmani et al. 2019).

The sixth principle, broaden participation, which is used in ecological resilience research as a prerequisite to better manage CAS, affects the discussed architectural perspective only indirectly. By broadening the focus and bringing in expertise from other disciplines, a holistic research focus can be aspired, and more elaborated solutions can be found. This is still a problem for power grids, as the specific models and architectures are not publicly available and hinders scientific analysis and development from researchers of other fields. In the MITRE taxonomy, this perspective is only indirectly included by fostering diversity (Table 1) but lacks the inclusion of positive effects of increased participation.

As power grids are connected internationally, the collective coordination and response by diversity of stakeholders and nations is thought to increase the resilience and to build trust and relationship. This improves the legitimacy of the knowledge base and decision making, helps to promote the understanding of system dynamics, and improves the capacity of a management system to detect and interpret shocks and disturbances (Biggs et al. 2015).

The seventh principle, promote polycentric governance systems, is not only valid for governance, but for polycentric systems in general. As inspired by nature, polycentric systems favor higher diversity, increased communication while building in modularity and redundan-

Ecological resilience design principles	MITRE Techniques													
	adaptive response	analytic monitoring	coordinated defense	deception	diversification	dynamic positioning	dynamic	non-persistence	privilege restriction	realignment	redundancy	segmentation	substantiated	unpredictability
Diversity/Redundancy	B		B/U	B	B/U	B		B			B/U	B/U		B
Manage Connectivity	B/U	U	B	U	U			U	U	U		U	U	U
Slow Variables & Feedbacks		U					U			U				
Complex Adaptive Systems	U	U	U	B/U	U	U	U	U		U		U		B/U
Learning	B	U	B				B/U			B			U	
Broaden Participation	B		B		B						B			
Polycentric (Governance) Systems	B		B		B/U	B/U		U	U	B	B/U	B/U		

Table 1: Ecological resilience design principles (DP) and their mutually complementing techniques (U = DP uses technique; B = DP as basis or support for technique) (own illustration)

cy (Biggs et al. 2015). Due to the remote control of high amounts of power consumption, the smart grid is considered to be vulnerable to direct cyberattacks aiming to destabilize the system (Dabrowski et al. 2017). Therefore, the principle can also be interpreted as to avoid single points of failures and will be an incremental part in the upcoming energy transition. By looking at the MITRE taxonomy, several designs can be pointed out (e.g. diversification, segmentation) that foster such decentralized architectures but should further be inspired by ecological insights.

Other MITRE techniques support ecological principles as well but haven't been included due to spatial limitations. An overview can be found in Table 1.

Conclusion

By considering the seven ecological resilience principles in the design of systems and systemofsystems, the general application of such foster an extended narrative and practical applications to create a more agile and safer environment not only against cyberattacks, but in case of natural disasters, disturbances and internal failures as well. As many technological solutions already exist to create agile structures, the integration of advanced perspectives tackles an underlying problem, why such designs haven't been thoroughly planned. It appears that the research field of software engineering made significant advancements in the last years to create an elaborated framework for handling complex cyber systems that is, at least partly, lacking in critical infrastructure engineering. Nevertheless, the MITRE taxonomy focusses much on the technical aspects of resilience but does not include hierarchical management structures. The ecological resilience principles extend that framework by integrating temporal, social, organizational and human factors that mutually support each other. This perspective helps to outline the importance of a holistic strategy to tackle complex and multidimensional challenges as can be seen in the development of the smart grid system.

It could also be shown that the proposed ecological framework not only incorporates existing techniques (e.g. MITRE taxonomy), but also includes design and management principles, such as slow variables, CAS, broaden participation and learning, that initially might not have been considered as important for handling complex systems. By referring to wellknown natural processes, its descriptions are easy to understand for managing complex systems. As superordinate principles they are supported by technological resilience techniques on how to design and maintain agile cyberphysical systems but also create an overall environment that favors the deployment of such techniques.

References

Biggs R., Schlüter M. & Schoon M. (eds.) (2015): Principles for Building Resilience. Sustaining Ecosystem Services in SocialEcological Systems. – Cambridge.

Bodeau D., Brtis J., Graubart R. & Salwen J. (2013): Resiliency Techniques for Systemsof-Systems. Extending and Applying the Cyber Resiliency Engineering Framework to the Space Domain. (=MITRE Technical Report 130515).

Bodeau D. & Graubart R. (2017): Cyber Resiliency Design Principles. Selective Use Throughout the Lifecycle and in Conjunction with Related Disciplines. (=MITRE Technical Report MTR 170001).

Cavelty M., Kaufmann M., Kristensen K. (2015): Resilience and (in)security: Practices, subjects, temporalities. – Security Dialogue 46 (1).

Dabrowski A., Ullrich J. & Weippl R. E. (2017): Grid Shock: Coordinated LoadChanging Attacks on Power Grids. Annual Computer Security Applications Conference (ACSAC) 2017, S. 112.

Eleks (2018): Why adaptive security architecture will become a new standard. https://eleks.com/blog/adaptivesecurityarchitecturebecomenewstandard/?utm_source=medium&utm_medium=refferal&utm_campaign=RepublAdaptiveSecBlog (Last viewed on 09.01.2020).

EISAC (2016): Analysis of the Cyber Attack on the Ukrainian Power Grid; https://ics.sans.org/media/EISAC_SANS_Ukraine_DUC_5.pdf (01.10.2020).

ENTSOE (2017): Analysis of CE InterArea Oscillations of 1st December 2016. – ENTSOE SG SPD Report.

Evesti A. & Owaska E. (2013): Comparison of Adaptive Information Security Approaches. –ISRN Artificial Intelligence 2013.

Folke C., Carpenter R. S., Walker B., Scheffer M., Chapin T. & Rockström J. (2010): Resilience Thinking: Integrating Resilience, Adaptability and Transformability. – Ecology and Society 15 (4): S. 20.

Holling C. (1973): Resilience and Stability of Ecological Systems. – Annual Review of Ecology and Systematics 4: 123.

Ladyman J., Lambert J. & Wiesner C. (2013): What is a complex system? – European Journal for Philosophy of Science 3 (1): S. 3367.

Li X., Liang X., Lu R., Shen X., Lin X. &Zhu H. (2012): Securing smart grid: cyber attacks, countermeasures, and challenges. – IEEE Communications Magazine 50 (8): S. 3845.

Linkov I., Eisenberg D., Plourde K., Seager T., Allen J. & Kott A. (2013): Resilience metrics for cyber systems. – Environment Systems and Decisions 33: S. 471476.

Mahmud R., Vallakati R., Mukherjee A., Ranganathan P. & Nejadpak A. (2015): A Survey on Smart Grid Metering Infrastructures: Threats and Solutions. – IEEE International Conference on Electro/Information Technology (EIT), Dekalb: S. 386391.

Rehmani M. H., Davy A., Jennings B. & Assi C. (2019): Software Defined Networks based Smart Grid Communication: A Comprehensive Survey. IEEE Communications Surveys & Tutorials 21 (3): S. 26372670.

Reich. J., Cohen J. J., Moeltner K. & Schmidthaler M. (2016): Electricity supply security, service valuation, and public perception of energy infrastructure. Kroos D., Schweitzer D., Leroy C., Andreini E., Baltasar B., Boston T. & Keršnik M. (eds.) Protecting Electricity Networks from Natural Hazards. – Vienna, Austria.

Stirling A. (2007): A general framework for analyzing diversity in science, technology and society. – Journal of the Royal Society Interface4: S. 707719.

Wang Z., Chen B. & Chen C. (2015): Networked Microgrids for SelfHealing Power Systems. – IEEE Transactions on Smart Grid 7 (1): S. 310319.

Xue Y. & Yu Y. (2017): Beyond Smart Grid – A CyberPhysicalSocial System in Energy Future. – Proceedings of the IEEE 105 (12): S. 22902292.

Yan Y., Qian Y., Sharif H. & Tipper D. (2012): A Survey on Cyber Security for Smart Grid Communications. IEEE Commmunications Surveys Tutorials 14 (4), S. 9981010