Proceedings of the 35th European Safety and Reliability & the 33rd Society for Risk Analysis Europe Conference
Edited by Eirik Bjorheim Abrahamsen, Terje Aven, Frederic Bouder, Roger Flage, Marja Ylönen
 Published by Research Publishing, Singapore.
doi: 10.3850/978-981-94-3281-3_ESREL-SRA-E2025-P3481-cd

Exploring and Developing Resilience Training Scenarios for Security of Electricity Supply

Tom Ivar Pedersen

Energy Systems, SINTEF Energy Research, Norway. E-mail: tom.ivar.pedersen@sintef.no

Maren Istad

Energy Systems, SINTEF Energy Research, Norway. E-mail: maren.istad@sintef.no

Oddbjørn Gjerde

Energy Systems, SINTEF Energy Research, Norway. E-mail: oddbjorn.gjerde@sintef.no

Tor Olav Grøtan

Software Engineering, Safety and Security, SINTEF Digital, Norway. E-mail: tor.o.grotan@sintef.no

Stine Skaufel Kilskar

Software Engineering, Safety and Security, SINTEF Digital, Norway. E-mail: stine.s.kilskar@sintef.no

The electric energy sector faces large challenges and needs for digital transformations. The introduction of intermittent renewable energy resources, increased demand, and new energy consumption patterns influence grid stability and security of supply. Moreover, the strained geopolitical situation implies new threats and digital vulnerabilities to a complex system comprising a mix of new and old technologies. Existing regimes, design, and operational principles (e.g., "N-1") are challenged by the urge to facilitate a higher utilization of the existing grid. A more risk-based approach is suggested to face these challenges. In other sectors, the disappointments and shortcomings of anticipation-based risk management have incited a strong interest in resilience approaches. The successful adoption of methods for enhancing the cyber-resilience of the electric energy sector requires that the approaches are adopted to its unique characteristics. However, cyber resilience is not confined to cyber security but includes, from a sociotechnical perspective, countering of digital vulnerabilities in the context of security of supply. Moreover, we see resilience as an adaptive capacity both residing in normal operation and invoked at boundary conditions. Resilience is thus a process and practice, not only observable outcomes. Hence, resilience is an inherent ability that manifests itself at boundaries and margins of operation. These boundaries are not static but influenced by past actions and future strategies. This paper aims to enable distribution system operators (DSOs) to understand and benefit from their adaptive history, grasp their precariously vulnerable present, and envisage their resilient future. The primary method is training on scenarios that clarify boundary conditions for DSOs and foster inherent resilience, supported by a proper learning and strategizing environment using the Training for Operational Resilience Capabilities framework. This paper gives an example of such a scenario.

Keywords: Sociotechnical cyber resilience, adaptive capacity, security of electricity supply, resilience training, training scenarios.

1. Introduction

As illustrated by the ongoing war in Europe, the security of electricity supply is more crucial than ever. At the same time, we are facing a climate crisis which necessitates a rapid decarbonizing of society. Electrification is one of the most important means for achieving this decarbonization. The transition to smart grids is an important enabler for electrification but will potentially introduce new cyber vulnerabilities. Consequently, both the character of, as well as the demands for the electric energy system are changing.

This paper argues that the use of resilience training on challenging scenarios is a good approach for enabling distribution system operators (DSOs) of an increasingly more interconnected and complex grid to gradually build the necessary adaptive capacity for ensuring security of supply throughout this transition.

The rest of this paper is organized as follows. The next section presents forces driving the ongoing digitalization of the electricity grid and the consequences of this development. It also describes how resilience engineering principles may be adopted by the DSOs. Section 3 gives a brief introduction to the Training for Operational Resilience Capabilities (TORC) framework. An example TORC scenario representative of the challenges ahead is presented in Section 4. The paper is rounded off with discussions and a conclusion in Section 5 and 6, respectively.

2. Background

2.1. Digitalization of the electricity grid and security of supply

The term digitalization is in this paper used in line with (Parviainen et al. 2017, 64), as "changes in ways of working, roles, and business offering caused by adoption of digital technologies in an organisation, or in the operation environment of the organisation". Digitalization of electricity grids involves introducing digital components, systems and tools in e.g., substations and control rooms (Swain et al. 2022), creating new ways of working, such as in determining the condition of components, making

operational decisions (Torres Olguin et al. 2024), or doing maintenance (Alvarez-Alvarado et al. 2022).

Digitalization is however a double-edged sword. On the one hand, it enables a more flexible and smarter grid where automated systems, for example protection, recovery, monitoring and decision making, can be implemented. On the other hand, it introduces new vulnerabilities, new modes of failure and new requirements for expertise (Ghiasi et al. 2023). Balancing these two sides is not only a question of whether a fully digitalized grid will be secure or not. Research on the relationship between risk and change management shows that there may be significant risks that can be attributed to the transformation process itself, e.g., (Kilskar and Antonsen 2017). Hence, digitalization is a process, not a product, involving the continuous merging of old and new technologies and practices. For the electricity sector, this transformation risk also comprises a shift from facing a relatively stable risk picture which the sector has managed quite successfully, to encountering a novel and unfamiliar risk picture.

The critical knowledge gap is therefore not merely about specific digital risks per se, nor any idealized, theoretical response to them in security terms. The most pressing gap is about how DSOs can develop the necessary capabilities to deal with digitalization as a transformation process into new territories of novel and emergent risks, maintaining an adaptive capacity that is sensitive to not only expected and unexpected events in the general sense, but also to fundamental surprise in which basic assumptions are contested. Such capabilities cannot be developed in a void, they must be sensitive to the local organizational context and be anchored in the "hard" issues of digitalization. E.g., in the electricity grid, industrial control systems are key elements commonly labelled "operational technologies" (OT). By digitalization, IT and OT are no longer separate domains – they are increasingly fused together into what has been called "the new battlefront of cyber security" (Piggin 2014, 70). This IT/OT challenge is common for many critical sectors, but the electricity grid stands out due to the constant need for balancing energy consumption and production at large, availability of sufficient power, and quality (e.g., voltage, frequency).

Bochman (2018) argues that the electricity sector should refrain from utilizing some of the opportunities of digitalization, due to cyber security challenges that it is just not prepared for. Nevertheless, the current geopolitical situation and surge for more renewable energy, and the accentuated demand for security of supply in a rapidly changing energy system, renders Bochman's option irrelevant; digitalization is instrumental for the necessary transformation of the energy system.

This development introduces new vulnerabilities from IT-related technical issues to new opportunities for malicious actors to disrupt power supply. From the perspective of the DSOs, malicious acts from an advanced persistent threat, and non-malicious events caused by poor design, implementation, or technical failure may have the same symptoms and consequences (at least at the outset), making it hard for the DSO to separate these two types of events. As the boundaries between these types of events are indefinite, a flexible approach to handle and prepare for this is needed.

Hence, the electricity sector faces what Woods and Alderson (2021) denote a strategic agility gap, with the additional aspect that consequence of lagging behind may be immediate loss of power supply, with huge consequences for other critical infrastructures at the mercy of energy supply. To close this gap, there is a need for building knowledge on how DSOs can develop the necessary adaptive capabilities that can support security of electricity supply throughout the digital transformation process.

While replacing analogue measurement and control of grid components with digital solutions and signals is a matter of technical innovation, it is important that controlling the risks involved is not only seen as a technical challenge (Antonsen et al. 2021). Rather, the risks of a sociotechnical nature must also be considered. E.g., the role of risk assessment and management in procurement processes, the formal organization within the DSO and the relationship with suppliers of components and services, issues related to professional jargon, organizational cultures and competence, and implications for the management of emergencies and crisis situations.

Digital transformation of electricity grids amplifies technological and organizational complexity. Facing this, traditional approaches based on anticipating failure scenarios and planned measures to deal with foreseen failures are likely to fall short as it will be increasingly hard to predict the ways the grid may be disturbed and impact the security of electricity supply, e.g., (Sperstad, Kjølle, and Gjerde 2020). This calls for an approach where the ability to anticipate and prepare is complemented with the ability to be resilient toward disruption and surprise, to counter the emerging strategic agility gap (Woods and Alderson 2021).

2.2 Resilience as adaptive capacity: a path for closing the potential agility gap

"Resilience" – increasingly popular in safety and security discourses in recent years – is a polysemic term, comprising a wide variety of meanings. IEEE (2018) defines resilience of a *system* as "*the ability to withstand and reduce the magnitude and/or duration of disruptive events, which includes the capability to anticipate, absorb, adapt to, and/or rapidly recover from such an event*." This can be paraphrased through popular terms like "robustness", "rebound" or "build back better" being added to the designed technical and operational capabilities of a system. However, there is nothing in this definition explicitly pointing beyond protection from recurring or imagined disturbances, based on projections from existing practices. In which case, arguably, the notion of "resilience" is reduced to an epiphenomenon, a new label attached to the expected outcome from mere reinforcement of existing principles and practices (Pettersen and Grøtan 2024).

Exemplifying this somewhat simplistic and reductionist comprehension of resilience, the US DoE C2M2 Model argues that "*operational resilience focuses on the organization's ability to manage operational risk*" (DOE 2022, 86). Accordingly, it does not explicitly address the potential human contribution to resilience beyond the

role of complying to the rules and logic derived from risk management practices. Presumably, this reflects that from a risk management perspective, it is intuitive to conceive resilience as a mere supplement to emergency response and business continuity planning in terms of a reinforced capacity related to planned or designed recovery and restoration during and after unwanted events.

In contrast, over the last two decades, the coining of "Resilience Engineering" (RE) has signified an attempt to encircle and craft distinct sociotechnical principles and practices enabling effective responses to the fundamental challenge of complexity and surprise. This attempt is however not confined to a traditional safety or security scope. RE aims to be a paradigm for managing risk and reliability that focuses on how to help sociotechnical systems to "*cope with complexity under pressure to achieve success*" (Hollnagel, Woods, and Leveson 2006, 6), by *engineering an adaptive capacity* (Woods 2015). This paradigm emphasizes complexity as a source of small and large disturbances, but also as a conveyor of (potential) capabilities to make situational adaptations in response. These capabilities rest on distinct principles and practices that are sensitized to recognize and transcend the inherent boundaries of preparedness in the traditional sense. The main interest is thus not on the specific adaptations per se, but on being poised to adapt (Woods 2018). As condensed by Woods and Alderson (2021), "*resilience is a verb in the future tense*" – resilience is thus not a possession or noun, but an activity. Hence, attention is directed towards sociotechnical practices and interactions needed for emancipation from the confines of past presumptions. Key traits in this may be initiative, reciprocity, timing and other means to avoid becoming "stuck and stale" in outdated models and patterns (Woods and Alderson 2021).

Due to the potentially huge societal consequences of electricity grid outage, the impact of security of supply through the digitalized grid is beyond the notion of security or safety "case" in the traditional sense. Rather, it may be paraphrased RE-wise as "coping with complexity under pressure to maintain supply", from which attention is drawn to agility. Accordingly, grid operators must aim for a level of resilient performance that requires more than just relabelling the outcome of existing practices.

At a theoretical level, it is meaningful to separate the above comprehensions of resilience into separate categories or theories (Grøtan, Antonsen, and Haavik 2022), analytically separating resilience *as result* from resilience *as process and practice*. Moreover, as for the petroleum industry, and at a pragmatic level (Pettersen and Grøtan 2024), it is necessary to acknowledge that several resilience "theories" are useful. The practical implication from such a research position is that the practices creating the potential for adaptive capacity in the RE sense are embedded and entangled in other practices. Discovering the adaptive potential within these composite practices is therefore not a simple matter of "seeing is believing", but also the other way around. In other words, "seeing" also requires "believing", or at least sensitization to the possibility of interpreting practices from an RE perspective.

An RE-inspired interpretation of (entangled) practices will imply recognition of the "robust yet fragile" theorem (Woods 2015) claiming that apparent success through robustification and risk-based planning may be deceptive, rendering the system fragile ("stuck and stale") when unexpected and disrupting events occur. Moreover, it follows from this that the concept of practical drift (Dekker 2011) is not unilaterally negative in the sense of signifying a deviation, but also a consequence of silent but effective adaptations. However, without a sustained forward-looking monitoring of adaptive capacity, adaptive drift may also unwarily bring the system into unforeseen and possibly fatal vulnerabilities (Dekker 2019).

Anyway, an important aspect of the RE-related theory/perspective is to gather knowledge about the way sociotechnical systems really work when coping with variability, disruption, and surprise. A key to identify the silent adaptive practices, coined as the *rudiments* of adaptive capacity (Grøtan, Antonsen, and Haavik 2022) is the appreciation of the distinction between "work-as-imagined" (WAI) and "work-as-done" (WAD) (Dekker 2011). This distinction also has important implications for digital transformation processes as it highlights that the introduction of new technology can have unforeseen and unpredictable consequences.

Based on this theoretical positioning, we can derive an idealized path for closing the agility gap through developing an adaptive capacity based on the observable rudiments of resilience in a digitalized grid:

Table 1 Idealized Path

Idealized Path step	Description	Attribution
IP1	Assess the limits of prepared resistance to disturbances	WAI
IP2	Identify and describe the rudiments of resilience engaged in coping with variability and disruptions	WAD
IP3	Monitor exposure (by operation or training) of the system to additional stressors that may stretch the rudiments into what Woods (2018) coins "graceful extensibility" of current rules and practices	WAD
IP4	Work out strategies to ensure that episodes of graceful extensibility with generic potential are fed back into the formal organizational operational repertoire	WAI/WAD
IP5	Establish organizational structures that orchestrate implementation of the previous steps with the scope of upholding a sustained adaptive capacity (Woods 2018)	WAI/WAD

For the latter (IP5), it is important to be aware of the reductionist, the moral and the normative traps, which Dekker (2019, 418–22) urge resilience *scholars* to avoid. In

our view, these traps are at least equally important to address for real organizations.

A key presumption behind this idealized path is that the rudiments of resilience in the RE sense are residing tacitly in normal operation, entangled with many other practices. If not appreciated organizationally and managerially, the rudiments *may* still silently contribute to a modest degree of resilience in grid operations. In the opposite case, they *may* be guided and nurtured into more powerful graceful extensibility at more challenging boundary conditions and even be carefully orchestrated into sustained adaptive capacity.

In this paper we will limit our scope to demonstrate how a training-by-gaming approach may be used to operationalize the three first steps of the path.

3. Methodology

On this background of an electric power grid going through a digital transformation, we describe a case of non-firm connections to the electricity grid which illustrates the complexity of data dependence and need for adaptive capacity in the digitalized grid.

Further, we demonstrate that the Training for Operational Capabilities (TORC) training-by-gaming approach can stage this case for implementation of the first three steps of the idealized path towards sustained adaptive capacity. Based on this, we will argue in Sec. 5 that this training scenario is suitable to raise awareness of the need for adaptive capacity, and how the results can be nurtured and developed further with TORC support.

The TORC game and its artifacts have previously been presented in (Grøtan 2020). Since then, a digital version of the original board game has been made[a], enabling easier scenario setups and facilitation of training sessions, improved recording of training data, and playing the game without physical presence.

TORC is designed to 1) challenge the boundaries of robustness towards projected events 2) trigger, reveal and enhance samples and rudiments of adaptive capacity, 3) engage participants in prospecting adaptive capacities, including assessing its boundaries and limits.

One "round" of the game is driven by the introduction of a stressor by the facilitator who is framing and setting the scene. The subsequent stages of a round involve discussions and actions related to becoming aware of what is going on and what could be done to gather more information (*awareness*); making sense of the situation, plausible explanations and what happens if no action is taken (*sense making*); different alternatives for action (*anticipation*); before deciding what to do (*decision*) and following up the situation (*monitoring*).

A training scenario typically consists of several such rounds. The sequence of stressors, and the presence/offering of predefined "action cards" available at each round will in general reflect the training objective of the organization to which the participants belong. The amount of and degree of detailing of action cards can vary substantially, from rehearsing robustification and planned rebound, to challenging the participants at the boundaries of preparedness to investigate the potential adaptive capacity residing among the participants and their affiliated organizational context.

For the latter type, which corresponds with the scope of this paper, the progression will follow this scheme: The first stressor will typically invoke predefined actions cards to familiarize the participants with the situation and activate the present organizational preparedness level. The next stressor will typically demonstrate the limits of these preparations and make visible the need to modify or rearrange the present preparations, while the succeeding stressors will seek to trigger the rudiments of resilience presumed to be inherent in the organization. Hence, this directly supports the idealized path described above. At this stage, the skilled facilitator might bring in new stressors to trigger specific capacities or combinations, with or without facilitating a discussion on the present findings with the participants. It follows from this that the relevance of predefined action cards will diminish with the number of stressors employed, however TORC is designed with the purpose of participants proposing defining new action cards "en route".

4. Example of TORC scenario: Non-firm connections to the electricity grid

4.1 Background on non-firm connections

The distribution grid has traditionally been relatively static, passive and manually operated, in the sense that few changes in grid topology (switching operations) have been performed, and few remotely controlled components have been available. With an increasing load demand and a large share of intermittent renewable energy sources (IRES), e.g., solar power voltaic (PVs) and wind power, there is an increasing need for more dynamic, remote and active management of the grid to balance production and consumption at all times (Torres Olguin et al. 2024). Active management of consumption, by disconnecting or reducing the load of individual customers, is expected to become increasingly important going forward (Gopstein et al. 2021). This is often referred to as *demand response*.

Several different types of mechanisms for demand response have been proposed and tested in recent years (ACER 2023). As DSOs are regulated monopolies with obligations to serve the connected customers, available measures for demand response are highly dependent on the regulations imposed on them. In Norway, provisions have been made for DSOs and new customers to enter into agreements where the DSOs can disconnect or limit the costumers' load under certain predefined conditions (NVE 2024). This is often referred to as *non-firm connections*. These types of agreements are typically used when a firm connection of new consumption or production to the existing grid is not operationally justifiable.

So far, few agreements with non-firm connections have been made, and events where these costumers have had to be disconnected have been rare. However, many

[a] https://torc.no

DSOs are currently facing a large number of requests for increased load from both new and existing customers. As the DSOs are under pressure not to delay the electrification and introduction of IRES that are necessary to decarbonize society, they have incentives to allow for an increase in non-firm connections pending the building of new grid capacity.

As the number of non-firm connections increases, automated solutions and processes will be needed to disconnect or reduce the load of these customers. Several trade-offs related to cost, reliability, and security must be considered when designing these solutions, for example, how to communicate with the customer assets (i.e., using optical fibre-cables or wireless solutions); or whether the procurement, installation, and maintenance of the assets located at the customer is to be done by the DSO or the customer.

Until now, DSOs have normally had full control over all the assets in their grids, and communication has normally taken place via dedicated optical fibre cables. If non-firm connection agreements are to be rolled out to a large number of customers, the traditional technical solutions for controlling assets in the grid will be too expensive. Wireless communication can be cheaper to install but may also introduce new vulnerabilities and interdependencies.

4.2 Example scenario description

The rest of this section shows how a TORC scenario related to non-firm connections can be structured. As pointed out by Grøtan et al. (2016) it is important that the participants can relate the scenarios to everyday operations and past incidents in their organization. Thus, it is recommended that the scenario, stressors, and action cards are adjusted to the operational context of the participants when this information is available to the TORC training facilitator. In this scenario, a relatively simple system has been chosen to ensure that the introduction of the scenario to the participants can be done effectively. However, some details have been added to set the scene for possible cyber events as the TORC training progresses. E.g., remote monitoring of some of the assets and wireless communication, which enables adversarial techniques T0822 and T0860 as defined in the MITRE ATT&CK framework, respectively[b]. See the MITRE ATT&CK Industrial Control System (ICS) Matrix and reports on the 2015 Ukraine electric power grid attack, e.g., (Beach-Westmoreland and Styczynski 2016) or (Lee, Assante, and Conway 2016), for an overview of other adversarial tactics and techniques relevant for this scenario. Moreover, technical failures and communication errors, that can be challenging to distinguish from the acts of malicious actors, may also be included in the scenarios. See, e.g., IEC TR 61850-90-12 (IEC 2020) for introduction to some of these types of non-malicious cyber events.

4.2.1 Scenario introduction

Imagine that a Norwegian DSO has entered into a large number of non-firm connection agreements with customers such as electric vehicle charging stations, commercial buildings, agriculture, and industrial companies. To manage this, the DSO has introduced automated solutions to reduce the load or disconnect these customers when necessary to prevent overloading the grid and customer outages.

The example scenario is a substation having customers with both non-firm and firm connections. The substation is equipped with overload protection. When the substation overload protection is activated, all the downstream customers lose power. Instead of overloading and disconnecting customers; reduction or disconnection of load with non-firm connections can be made, but this involves using assets located at the customer and relaying on wireless communication, which introduces new vulnerabilities for the DSO.

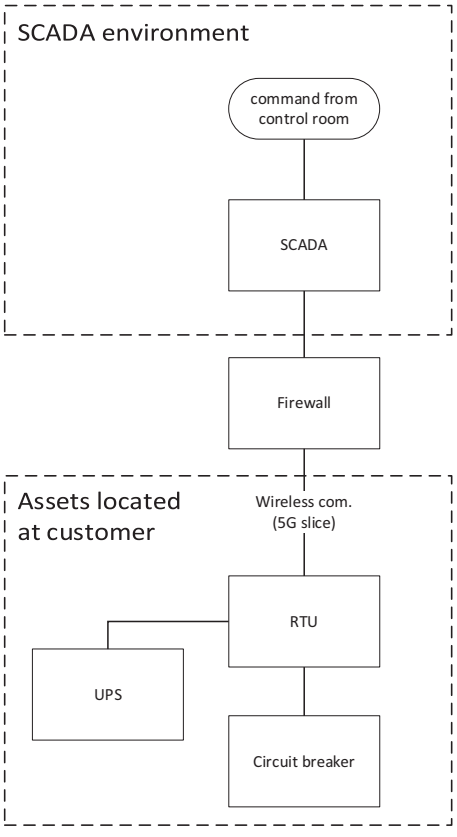

Fig. 1 Illustration of system architecture for disconnection of customers with a non-firm connections agreement.

Fig. 1 illustrates the system architecture for controlling customers with a non-firm connection agreement. It is assumed that commands to disconnect the customers are sent from the DSO's SCADA system through a firewall and to a Remote Terminal Unit (RTU) located at the customer. The RTU is powered by an Uninterruptible Power Supply (UPS) and controls a circuit breaker that can be used to disconnect the customer. Communication between the DSO

[b] https://attack.mitre.org/techniques/ics/

and the RTU at the customer is done through a slice in the public 5G telecommunication network. The circuit breaker belongs to the customer and is located on the customer's premises. The customer can choose which type of circuit breaker to install if it meets the specifications defined by the DSO. The DSO does not have routines for checking and maintaining the circuit breaker; this is the customer's responsibility. The UPS and the RTU belong to the DSO and are locked in a room that customers and other third parties cannot access. The UPS has remote diagnostics functionality, e.g., for monitoring battery status. Remote monitoring of the UPS is available through a web interface provided by the UPS manufacturer. It is possible to update setpoints, alarm limits, and firmware for the RTU remotely.

Table 2: Suggested Stressors and actions cards for the example scenario. In the table the text inside [brackets] indicates additional information that may be provided to the participants in the TORC-game. In addition to the suggested action cards, the players can in all stages decide to do no action, i.e., "wait and see", or to suggest new action cards.

Stressors (with affiliation with Idealized Path (IPx), see Table 1	**Stage**	**Possible action cards**
Stressor 1: Warning (IP1) The DSO receives a notification from a trusted source, e.g., from the energy sector Computer Emergency Response Team (KraftCERT), that some other DSOs have recently experienced events related to customers with non-firm connections. These events have so far had no consequences other than that the DSOs have had to dispatch technicians to restart and/or replace certain hardware components. For several of these events, specific technical failures have been reported as the cause of the incidents. However, a common root cause has not been identified for these events.	Awareness	• Contact KraftCERT • Contact certain customers with non-firm connection agreements to check whether "something is going on"?
	Sense making	• Obtain more information about the events from KraftCERT • Arrange meeting with internal IT and OT experts, technicians or control room staff regarding experiences with incidents related to non-firm connections
	Anticipation	• Update the requirements for technical solutions for demand management of customers with non-firm connections • Carry out inspection of selected customers with non-firm connection agreements
	Decision	*No new cards at this stage*
	Monitoring	• Introduce regular reporting/metrics for incidents related to management of non-firm connections
Stressor 2: Risk of overload (IP2) The loading of a substation in the example scenario is approaching its rated capacity. Several customers with non-firm connections are supplied from this substation. [Details regarding the margin before reaching the substation load limit may be presented in the form of graphs or visualized in a manner similar to what shown on the screens in the DSO control room.]	Awareness	• Check the time series for load at the relevant substation and the margin to the limit for activation of overload protection • Check the weather forecast or other sources of what is the expected development in load in the coming hours
	Sense making	• Forecast whether, and if so, when, the load is expected to reach the substation's rated capacity • Get overview of what types of customers that are supplied by this substation, including non-firm connections
	Anticipation	• Disconnect one or several non-firm customer(s) • Allow for intermittent overloading of substation
	Decision	*No new cards at this stage*
	Monitoring	• Monitor load and transformer temperature in the substation
Stressor 3: Load is not reduced as expected when disconnecting customer (IP3) The control room operator has remotely disconnected one, or several, non-firm customer(s). However, the load at the substation is not reduced as expected. [If the game participants have not chosen to disconnect at least one non-firm customer in the previous decision stage, Stressor 2 is repeated with a further increase in load]	Awareness	• Check SCADA and other data sources in available in the control room for assessing whether the customer(s) has/have actually been disconnected • Contact the disconnected customer(s)
	Sense making	• Assess whether load increases from other customers have offset the disconnected customer(s)
	Anticipation	• Disconnect multiple other non-firm customers • Dispatch technician to substation to manually disconnect non-firm customers • Dispatch technician to inspect the assets at non-firm customer(s)
	Decision	*No new cards at this stage*
	Monitoring	• Use dispatched technician to monitor the state of the substation or assets at non-firm customer
Stressors 4 and onward: (IP4/IP5) The facilitator may continue to introduce stressors depending on the aims of the TORC game. As an increasing number of stressors are introduces the operational contexts will reach, and surpass, the boundaries of normal operation. Failure of customer assets and the situations where the customer is unavailable and/or does not understand the ongoing situation, can increase the stress for the DSO personnel. Thus, as the game progresses the players will increasingly have to formulate their own actions cards as procedures based on experience and anticipation-based risk management become less relevant.		

4.2.2 Stressors and actions cards

Table 2 shows the initial stressors for the example scenario. The intention of the first stressors is to act as "warm up"-rounds to let the participants get familiar with the TORC game while handling stressors that are within the boundaries of normal operations.

As the participants get familiar with the TORC game, more challenging stressors and scenarios that, to a larger degree, test the potential adaptive capacity of the organization are introduced. See (Grøtan et al. 2016) or Appendix A in (Costantini and Raffety 2021) for inspiration for development for further stressors and scenarios.

5. Discussion

This paper presents an example TORC scenario related to customers with non-firm connections. Disconnection of non-firm customers is primarily relevant when load demand is high. Thus, it is when there are few "reserves" in the system and the consequences of power outages are large that disconnection is relevant. This type of demand management system may therefore be a well-suited target for malicious, hybrid-threat actors wanting to disturb or disrupt the power system. The scenario presented in Sec. 4 also exemplifies more generic challenges and trade-offs related to ensuring security of supply in a more digital and actively managed grid.

We argue that a resilience engineering approach to these challenges need to be developed beyond the current state of the art within the sector. E.g., Panteli et al. (2017) describe a metric for how an electricity system can "bounce back" from technical and operational disturbances. This resembles the basic idea of resilience as outcome but needs to be extended into adaptive capacity, recognizing resilience as a process. To advance, scientific investigation and organizational development need to be sensitized to the resilient practices already residing tacitly in the sector's people and organizations. Experience-based operational knowledge residing in these systems should be combined with knowledge about the evolution of electricity systems over a long period of time, including the impact of a constant mix of old and new technology. Such insight will be foundational for new methods seeking foresight about the implications of innovation and decisions regarding security of supply.

As technological change increases in pervasiveness and speed, such methods will be important for both research and practice. From an industry perspective, enhanced adaptive capacities will also enable the industry's capacity to deal with the inherent risks of digital transformation. This should include whether and how redundant fallback options (e.g., the ability to operate the grid manually in case of IT failure) should be preserved or established in the digitalization process. Such a knowledge foundation should be based on the framing of digitalization as a continuous process of organizational adaptation and balanced intake of technology, dealing with surprise and paradox in a resilient manner. This involves complementing the considerations of technological readiness level (TRL) of new solutions, with knowledge about what may be coined an "organizational readiness level" (ORL), addressing organizational maturity in terms of structures, capacity, and competence. The TORC training approach, facilitating an idealized path (Table 1) to sustained adaptive capacity, is a promising avenue which has been exemplified in this paper.

From a societal perspective, the primary knowledge need lies in systematizing knowledge about how critical infrastructures can be digitalized in a safe, secure, and efficient manner. Currently, we suspect that the interest in digitalization is larger than the insight into what it really means, and the risks it may entail. To overcome this, it is important to avoid that companies starts from a void. This requires concepts, models and methods for safe and secure digitalization enabling experience transfer across industries, and a more cumulative knowledge-building than what is the case today. Application of resilience training scenarios may contribute to this knowledge-building and help the employees in the DSOs gaining insight into resilience concepts and how to use and adapt these concepts.

6. Conclusion

Based on the presumption that the future grid incorporating active controls will be both more complex and more vulnerable to digital threats, we have argued that cyber resilience in the form of "real-time" adaptive capacity will be needed to avoid frequent needs for rebounds after grid outages. Moreover, we have shown how a specific case of demand management of customers with non-firm connection agreements can be used to develop such adaptive capacities through the TORC approach. We have provided the specification of a training scenario with presumed sequential stressors and some useful resources made available for the participants. However, the needed ("graceful") extension of the operational repertoire at boundaries of preparedness require that participants also acquire the skills to use these resources purposefully, and develop additional, situated practices through actual training exposing them to more complex, real scenarios. This will be the subject of further research.

Acknowledgement

This research is funded by the project Theoretical Advances of Cyber Resilience – Practice, Governance and Culture of Digitalization (TECNOCRACI), funded by the Research Council of Norway, grant no. 303489.

References

ACER. 2023. "Demand Response and Other Distributed Energy Resources: What Barriers Are Holding Them Back?" https://www.acer.europa.eu/sites/default/files/documents/Publications/ACER_MMR_2023_Barriers_to_demand_response.pdf.

Alvarez-Alvarado, M. S., D. L. Donaldson, A. A. Recalde, H. H. Noriega, Z. A. Khan, W. Velasquez, and C. D. Rodriguez-Gallegos. 2022. "Power System Reliability and Maintenance Evolution: A Critical Review and Future Perspectives." *IEEE Access* 10:51922–50. https://doi.org/10.1109/ACCESS.2022.3172697.

Antonsen, S., T. O. Grøtan, O. Gjerde, and M. Istad. 2021. "Security of Electricity Supply in the Transition Toward Smarter Grids." In *Proceedings of the 31th European Safety and Reliability Conference*. Angers, France.

Beach-Westmoreland, N., and J. Styczynski. 2016. "When The Lights Went Out." Booz Allen Hamilton. https://www.boozallen.com/content/dam/boozallen/documents/2016/09/ukraine-report-when-the-lights-went-out.pdf.

Bochman, A. 2018. "The End of Cybersecurity." *Harvard Business Review*.

Costantini, L. P., and A. Raffety. 2021. "Cybersecurity Tabletop Exercise Guide." National Association of Regulatory Utility Commissioners (NARUC). https://www.naruc.org/cpi-1/critical-infrastructure-cybersecurity-and-resilience/cybersecurity/cybersecurity-manual/.

Dekker, S. 2011. *Drift into Failure: From Hunting Broken Components to Understanding Complex Systems*. London: CRC Press. https://doi.org/10.1201/9781315257396.

———. 2019. *Foundations of Safety Science: A Century of Understanding Accidents and Disasters*. Routledge.

DOE. 2022. "C2M2 Cybersecurity Capability Maturity Model Ver. 2.1." https://www.energy.gov/sites/default/files/2022-06/C2M2%20Version%202.1%20June%202022.pdf.

Ghiasi, M., T. Niknam, Z. Wang, M. Mehrandezh, M. Dehghani, and N. Ghadimi. 2023. "A Comprehensive Review of Cyber-Attacks and Defense Mechanisms for Improving Security in Smart Grid Energy Systems: Past, Present and Future." *Electric Power Systems Research* 215 (February):108975. https://doi.org/10.1016/j.epsr.2022.108975.

Gopstein, A., C Nguyen, C O'Fallon, N. Hastings, and D. A. Wollman. 2021. "NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 4.0." 1108rev4. https://www.nist.gov/publications/nist-framework-and-roadmap-smart-grid-interoperability-standards-release-40.

Grøtan, T. O. 2020. "Training for Operational Resilience Capabilities (TORC); Advancing from a Positive First Response." In *Proceedings of the 30th European Safety and Reliability Conference and the 15th Probabilistic Safety Assessment and Management Conference*. Venice, Italy: Research Publishing.

Grøtan, T. O., S. Antonsen, and T. K. Haavik. 2022. "Cyber Resilience: A Pre-Understanding for an Abductive Research Agenda." In *Resilience in a Digital Age*, edited by F. Matos, P. M. Selig, and E. Henriqson, 205–29. Contributions to Management Science. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-85954-1_12.

Grøtan, T. O., J.K.J. van der Vorm, D. Zuiderwijk, D. van der Beek, I. Wærø, L. Macchi, T. E. Evjemo, and G. Veldhuis. 2016. "Guidelines for the Preparatory Work Needed to Implement a TORC Training Program."

Hollnagel, E., D. D. Woods, and N. Leveson. 2006. *Resilience Engineering: Concepts and Precepts*. Ashgate Publishing, Ltd.

IEC. 2020. "Communication Networks and Systems for Power Utility Automation – Part 90-12: Wide Area Network Engineering Guidelines." IEC TR 61850-90-12.

IEEE. 2018. "The Definition and Quantification of Resilience." Technical report PES TR 65.

Kilskar, S. S., and S. Antonsen. 2017. "Endring, sikkerhet og ledelse." In *Sikkerhet og ledelse*, 261–79. Gyldendal Akademisk.

Lee, R. M., M. J. Assante, and T. Conway. 2016. "Analysis of the Cyber Attack on the Ukrainian Power Grid." SANS Institute. https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2016/05/20081514/E-ISAC_SANS_Ukraine_DUC_5.pdf.

NVE. 2024. "Connection with conditions of disconnection [In Norwegian: 'Tilknytning med vilkår om utkobling']." https://www.nve.no/reguleringsmyndigheten/regulering/nettvirksomhet/nettilknytning/dette-er-leveringsplikten/tilknytning-med-vilkaar-om-utkobling/.

Panteli, M., P. Mancarella, Dimitris N. Trakas, E. Kyriakides, and N. D. Hatziargyriou. 2017. "Metrics and Quantification of Operational and Infrastructure Resilience in Power Systems." *IEEE Transactions on Power Systems* 32 (6): 4732–42.

Parviainen, P., M. Tihinen, J. Kääriäinen, and S. Teppola. 2017. "Tackling the Digitalization Challenge: How to Benefit from Digitalization in Practice." *International Journal of Information Systems and Project Management* 5 (1): 63–77.

Pettersen, S., and T. O. Grøtan. 2024. "Exploring the Grounds for Cyber Resilience in the Hyper-Connected Oil and Gas Industry." *Safety Science* 171:106384.

Piggin, R. 2014. "Industrial Systems: Cyber-Security's New Battlefront [Information Technology Operational Technology]." *Engineering & Technology* 9 (8): 70–74.

Sperstad, I. B., Gerd H. Kjølle, and O. Gjerde. 2020. "A Comprehensive Framework for Vulnerability Analysis of Extraordinary Events in Power Systems." *Reliability Engineering & System Safety* 196 (April):106788. https://doi.org/10.1016/j.ress.2019.106788.

Swain, A., E. Abdellatif, A. Mousa, and P. W. T. Pong. 2022. "Sensor Technologies for Transmission and Distribution Systems: A Review of the Latest Developments." *Energies* 15 (19): 7339. https://doi.org/10.3390/en15197339.

Torres Olguin, R. E., I. B. Sperstad, R. Rana, S. H. Jakobsen, M. Z. Degefa, G. Vist, M. F. Eliassen, B. Sloth, Å. Vatne, and L. Bergfjord. 2024. "Rethinking Distribution Network Operational Planning with Flexibility Resources." In *CIGRE Session Proceedings 2024*. CIGRE.

Woods, D. D. 2015. "Four Concepts for Resilience and the Implications for the Future of Resilience Engineering." *Reliability Engineering & System Safety* 141:5–9.

———. 2018. "The Theory of Graceful Extensibility: Basic Rules That Govern Adaptive Systems." *Environment Systems and Decisions* 38 (4): 433–57.

Woods, D. D., and D. L. Alderson. 2021. "Progress toward Resilient Infrastructures: Are We Falling behind the Pace of Events and Changing Threats?" *Journal of Critical Infrastructure Policy* 2 (2): 5–18. https://doi.org/10.18278/jcip.2.2.2.