What Could Possibly Go Wrong? Smart Grid Misuse Case Scenarios

Inger Anne Tøndel*, Ravishankar Borgaonkar*, Martin Gilje Jaatun*, and Christian Frøystad†
**SINTEF Digital*, Trondheim, Norway
(ingeranne.tondel,ravi.borgaonkar,martin.g.jaatun) at sintef.no
†*Secure Practice*, Trondheim, Norway
christian at securepractice.no

***Abstract*—The modernisation of the power grid is ongoing, and the level of digitalisation of the power grid in, say, ten years may be quite different than today. Cyber security needs will change correspondingly. In this paper we utilise a qualitative research approach to explore misuse cases related to three main areas of modernisation that we envision for the next ten year period: 1) managing flexibility in the TSO-DSO relation, 2) smart distribution grids, and 3) microgrids. The misuse cases represent potential security challenges to be considered when working on modernising the grid, however they are not exhaustive. The misuse cases presented in this paper can contribute to identifying security requirements, thus reducing associated cyber risks, and assist in development of new cyber security mechanisms for the next-generation power grid employing digitally-connected, self-healing, and automation characteristics.**

***Index Terms*—Misuse Cases, attacks, Smart Grid, Cyber-physical Security**

I. Introduction

Modernisation of the power system, with a smarter distribution grid, more flexibility and the use of microgrids, brings about large potential benefits. At the same time, the digitalisation and interconnectedness increase the risks of cyber attacks. Cyber attacks are performed on the information that reside or flow in the system. Still, such attacks can have physical consequences in cyber-physical systems such as smart grids.

This paper aims to give an overview of potential misuse cases in the future power grid. With misuse cases, we mean scenarios that show how the future power grid can be misused by threat actors performing various types of cyber attacks, and explain what consequences this may result in [1]. We have selected three primary areas to focus our contribution where we envision changes to be extensive and where potential consequences of cyber security attacks may be severe:

- integration of flexible resources in the grid, resulting in a need to change the interaction between Distribution System Operators (DSOs) and the Transmission System Operators (TSOs) in order to manage a grid where flexibility is distributed
- a smart distribution grid, with monitoring and control capabilities throughout
- microgrids

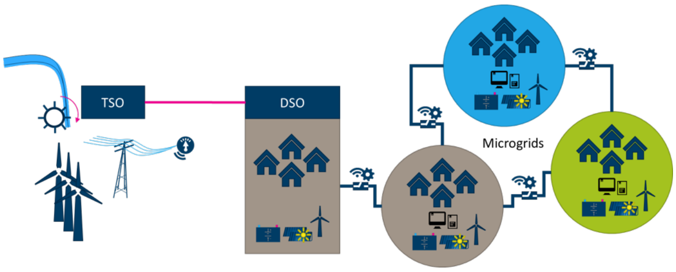

Fig. 1. Overview of the power generation, transmission and distribution landscape

These areas have been selected in line with major research topics for the modernisation of the research grid in Norway[1]. Fig. 1 gives a high-level overview of these areas, showing the integration of the more traditional model where generated power is moved from TSOs towards DSOs, in combination with flexible loads at the DSO level and even microgrids that can operate autonomously.

This paper is organised as follows. Section II explains the method used to identify and select the misuse cases presented in this paper. The presentation of the misuse cases is divided into sections based on the overall modernisation areas they relate to: Section III cover the DSO-TSO interaction, Section IV cover the operation of the distribution grid and Section V cover microgrids. Section VI concludes the paper.

II. Research Method

This work is concerned with future smart grid solutions, and the scenarios take into account technologies that may not yet be wide-spread in the power industry. To cope with the need to think ahead and deal with uncertainty, we used a variety of methods to get the necessary background to identify misuse cases. This included workshop with industry participants, discussions with power system researchers, and literature providing visions for the future grid and describing potential cyber attacks. The work on misuse cases was highly iterative, integrating input from all these sources to identify

[1] As defined by the Centre for Intelligent Electricity Distribution, one of the Centres for Environmental-Friendly Energy Research in Norway (https://www.sintef.no/cineldi)

and improve upon misuse cases and select a set of misuse cases for presentation.

In June 2018, we organised a workshop with 11 participants. Participants included representatives from DSOs and regulators in addition to researchers. In the workshop we identified potential misuse cases through brainstorming. The misuse cases that were considered most important by participants were documented in more detail in the workshop, identifying the associated future power grid assets, the threat actors, assumptions, preconditions, how it may come about, and potential consequences. The brainstorming results and the misuse cases that were discussed in the workshop have been used as a basis for some of the misuse cases found in this paper.

During 2019, we performed group interviews with researchers from the three main modernisation areas we focused on (TSO-DSO interaction, smart distibution grids, and microgrids) in order to understand their visions for the future and thoughts on potential future smart grid solutions. We identified and described potential misuse cases based on these group interviews and validated with the researchers. Two to three researchers from each area were involved in this work.

In parallel with the work on misuse cases, colleagues were working on identifying scenarios for future smart grid operation [2] and on identifying driving forces and miniscenarios as a part of a foresight process to understand potential future developments of the power grid [3]. The work presented in this paper on misuse cases benefited from the results of these other activities and also provided input to them. In addition, we have identified literature on cyber security threats relevant for the modernisation areas covered in this paper, and have used them as input in the scenario work.

Selected misuse cases have, towards the later stages of the process, been discussed and validated with representatives from the industry (one vendor, one DSO).

The list of misuse cases is not meant to be exhaustive, but instead to illustrate risks related to cyber security that should be considered during the design of future power grid systems. We have deliberately left out security and privacy issues that are confined to the Advanced Metering Infrastructure (AMI) system as this is covered extensively in other publications [4]–[7]. However, the impact a compromised AMI might have on the overall grid is not excluded. Additionally, we have left out issues related to planning, as these have a less direct impact on the grid than issues related to operations.

III. Misuse cases for managing flexibility in the TSO-DSO relation

Traditionally, large hydropower plants in the transmission network were the only power producers in the Norwegian grid. Now, more production is connected at lower voltage levels, such as small hydro in the high voltage distribution network and solar power at end-consumer level. In addition, end-users invest in electrical vehicles, a potential flexible resource. Hence, the flow of energy is changing from one-directional to bi-directional. This impacts how the TSO and the DSOs need to cooperate in order to ensure grid stability. Changes are needed for several reasons:

- Grid stability is traditionally a responsibility of the TSO. Now the DSOs will have some role to play in this task as well even though it's still the legal responsibility of the TSO.
- Flexible resources that can be used to ensure grid stability will not necessarily be directly under the control of the TSO.
- The flexible resources that are introduced into the grid are more numerous than the traditional resources used for grid stability, thus a new approach is needed to utilise these.
- Some services utilizing flexible resources might require a control signal (could e.g. be the power price) to tell them what action to take in ensuring grid stability.

The details of how this TSO-DSO interaction will be handled in the future power grid is as of now unclear, this includes the extent to which the TSO should have insight into the distribution grid. In the misuse cases concerning TSO-DSO interaction for managing flexibility in the modernised power grid, we have considered that this interaction may be realised in different ways, e.g. with varying degrees of information exchange and use of control signals. The assumptions made are detailed in each misuse case.

A. Misuse cases concerning the communication of control signals for flexible resources

As already explained, we can assume that in the future there will be a large amount of flexible resources that are controlled via some form of signal. This signal may come in varying forms, e.g., via price signals or via direct commands, either stemming from the TSO, an aggregator, or the DSO. It is not yet clear how such signals will be sent. Control signals can be attacked in different ways: they can be modified, stopped or eavesdropped on. This is further detailed in the following misuse cases.

1) Disturb grid stability by hijacking control signals to flexible energy resources: An attacker manipulates or inserts false signals that control flexible energy resources. To do this, the attacker needs to have gained access to messages sent to flexible resources and be able to send such messages. The main point of attack is the control signal sent from the TSO.

Example:

1) The threat actor gains access to the communication network used for relaying control signals/messages to and from the flexible resources
2) The threat actor observes the communication until he's able to understand the format and how to form his own control signals/messages
3) The threat actor manipulates existing control signals/messages or creates his own before sending them to the flexible energy resources or the control system

Grid stability can potentially be disturbed – as an attacker can modify control signals or send false signals so that a large amount of flexible resources turns on/off in a way that can cause instability to the grid.

2) Denial of Service on the control signals to flexible energy resources: Flexible energy resources will in the future rely on control signals to decide when to perform changes to their provided services in order to enhance grid stability. If these control signals become unavailable, stability of the grid may be disturbed. Control signals that rely on internet connection will be vulnerable to Denial of Service (DoS) attacks that lead to downtime on the network connectivity, either by a massive influx of network packets that exhaust the resources of network gear, such as routers and firewalls, or by application layer attacks that exploit vulnerabilities in protocols or applications to cause network downtime.

Example:

1) A threat actor gains access to the communication network used for relaying control signals/messages to and from the flexible resources
2) The threat actor floods the network with network packages, overloading the network equipment
   OR
   The threat actor floods each flexible energy resource with random signals/messages, making the resource incapable of receiving legitimate control signals/messages

Consequences include potential disturbance of grid stability -– as an attacker disturbs the control signals in such a way that the energy production/consumption is no longer adapted to the needs, resulting in potential blackout or overload situation.

3) Gain access to confidential information on grid structure by eavesdropping on communication between the TSO and the DSO: This misuse case explains a situation where an attacker eavesdrops on signals that is necessary for TSO-DSO interaction, and thereby gains access to confidential information about the structure of the grid. This information can be used to plan further attacks on the grid, which might vary from simple attacks for personal gain to complex acts of war like the attacks on Ukraine in 2015 and 2017 [8]. To do this, an attacker needs to have gained access to messages that contain information that can be used to understand how the grid is structured, and any encryption of these messages must be broken. The main point of attack is the status messages sent from the DSO to the TSO, but control messages may also be a source for information about the grid.

Example:

1) A threat actor gains access to the communication network used for exchanging information between the TSO and the DSO
2) The threat actor observes the information over time, trying to gain insight into the topology of the power grid

Consequences include an attacker potentially getting access to details about the grid, and this information can be used to launch other attacks, both physical and digital.

B. Misuse cases concerning attacks on the flexible resources themselves

In the future it can be envisioned that a high amount of flexible energy resources is connected to the grid, and that most of these flexible resources are not under the control of the DSO or the TSO. Thus, the way these flexible resources are protected against cyber security attacks is not under the control of DSOs or TSOs. It is unclear whether attacks on a limited number of such devices will have significant impact on grid stability, however if a very large amount of these devices are compromised, this can potentially impact the grid as well. Below we explain misuse cases related to this.

1) Hijacking of controllers on flexible energy resources: In the future, flexible energy resources may be connected over the Internet for monitoring or controlling purposes. However, if the flexible resources are not secured properly, an unauthorized actor may compromise the IT systems used in flexible energy resources so that they fail to respond to control messages, fail to communicate their status, or communicate the wrong status. The IT systems at the controllers of the flexible resources can be compromised by malware remotely if connected over the Internet, or through the local network, for example via a USB stick. Consequently, some unauthorised actor disables one or more flexible energy sources, thus removing or reducing the intended flexibility in the grid.

Example:

1) A threat actor inserts malware into an update meant for the controller OR a threat actor infects portable equipment used in connection with the controller with contagious malware
2) The malware gives the threat actor control over the flexible energy resources

Consequences include potentially disturbing grid stability – as an attacker can compromise controllers at flexible resources to send fake signals or disconnect them from the grid. If enough resources are affected, the result could be blackouts depending on the local situation.

2) Coordinated load-changing attacks originating from compromised consumer IT devices: An unauthorized actor could compromise consumer IT devices such as computers and printers to build a botnet. A recent research paper demonstrated that between 2.5 and 9.8 million compromised IT systems are enough to launch a noteworthy attack against the European synchronous grid [9]. Recent research demonstrated impact of such a botnet against the normal operation of the power grid [10]. Attackers could exploit a botnet to disrupt grid frequency, line failures and cascades, failure in tie-lines and eventually increasing the operating cost of grid.

Example:

1) A threat actor gains control over many consumer IT-devices
2) The threat actor synchronously makes all the devices suddenly require lots of power – thus causing a significant spike in power demand

Potential consequences include pushing the power grid into an unstable state by triggering automated load-shedding or tie-line tripping. Attacks originating from compromised high wattage IoT devices could result in local outages and potentially large-scale blackouts in the power grid, and increase the operating cost of the grid.

C. Misuse case on compromising the restoration functionality

The restoration functionality in relation to the TSO/DSO relation concerns the balancing act of restoring enough energy production before applying load and not applying too much load too fast which would destabilise the grid.

Compromising the restoration functionality could disturb the restoration and delay restoration of power indefinitely. The attack could be targeting either the production side, the distribution side, the TSO organisation and coordination, or the communication between the entities.

Example:

1) Power is lost in the whole country
2) A threat actor gains access to the communication network between the TSO and the DSO
3) The threat actor manipulates the communication between the TSO and DSO so in such a way that balanced consumption and production is not reached

Possible consequences include disturbing the restoration, and delaying restoration of power indefinitely.

IV. Misuse cases for smart distribution grids

Future smart distribution grids will have the instrumentation necessary for state estimation. The instrumentation of the distribution network can be considered to include sensors in the homes, in form of AMI systems – this is already used by several DSOs. In addition, the abilities to perform control actions digitally will be increased. One may even envision self-healing in parts of the DSO network. With increased monitoring and control capabilities, the types of consequences that one may experience from cyber-attacks on the distribution network systems will be different than today. The reliance on availability and integrity of the state information may also increase.

Fig. 2 gives some examples of how instrumentation could be applied in the power grid. Examples include sensors along power/transmission lines, automated and/or remotely operated circuit breakers and access to distributed flexible power resources, as well as utilization of newer communication technologies such as 5G.

The misuse cases described in the following concern:

- attacks on the overall state estimation
- attacks on smart grid components
- attacks on self-healing functionality
- AI/machine learning

Attacks on the control center itself are not covered.

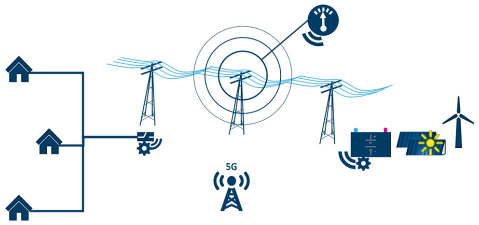

Fig. 2. Increased instrumentation in smart grids

A. Misuse case related to state estimation: Injection of false measurement data

Performing false injection attacks on state estimation is considered an advanced type of attack that requires persistence and skills from attackers. An attacker needs to gain knowledge of the current configuration/topology of the distribution system they want to attack (this may imply attacking the control system in order to get access to updated system topology information) and be able to manipulate meter measurements in a consistent way. This can be done using different tactics:

- Physically tamper with meters/sensors
- Malicious software on meters/sensors
- Modify data packets containing meter readings

The difficulty of doing this depends on the protection of the meters/sensors. Since it is envisioned that AMI can be used as a sensor, many of the sensors will be located outside of the physical control of the distribution company. Getting physical access to a high number of meters will be challenging and take a lot of effort. However, if an attacker manages to digitally attack many meters, this may be feasible to do if the meters are connected to the internet and are vulnerable for such attacks. Alternatively, one can envision an attacker trying to replay old data packets containing measurement data, either to hide another (physical) attack on the grid or to replay an earlier fault condition. This is only possible if the system does not have mechanisms to detect replay attacks.

Example:

1) The attacker gains access to an unprotected substation
2) The attacker attaches a portable computer to the internal substation network, ensuring all communication must go via this computer
3) The attacker will read all messages from sensors used for state estimation, and modify sensor values to systematically show lower values

Wrong data from enough of the sensors can result in wrong decisions that harm the power delivery. One motivation for an attacker is sabotage (or to hide sabotage), another could be financial gain [11] by tampering with metering data.

B. Misuse cases concerning attacks on smart grid components

Malware may infect many smart grid components, and may in extreme cases cause network blackouts, as in Ukraine [8]. Additionally, a complex digital system such as that in a smart distribution grid risks being misconfigured, and this can lead to vulnerabilities that facilitate attacks. Malware infections and misconfigurations may occur due to several reasons, and the following misuse cases outline some possible ways this can happen.

1) Malware infection inadvertently made possible by the DSO: Human operators at the DSO can have behaviour that increases the risk of being infected by malware. The following represent some ways this may happen:

- Inadvertent malware installation: Human operators may inadvertently install malware due to clicking on links in phishing emails (as in Ukraine [8]). In this misuse case a human operator has access to the internet from DSO equipment, uses this internet access to read email and gets tricked into inadvertently installing malware.
- Unsafe use of removable media: Human operators may use removable media in an unsafe manner (as in Stuxnet [12]). In this misuse case removable media is infected with malware. When this removable media is connected to DSO equipment, this equipment may become infected with malware.
- Lack of patching: Internet-exposed equipment may have unpatched vulnerabilities (as in NHS [13]), and these vulnerabilities make the equipment vulnerable to malware that utilizes this vulnerability.

Example:

1) Operator finds a shiny new USB memory stick in the parking lot
2) Operator inserts USB stick in DSO network computer to check contents
3) BadUSB [14] malware immediately infects computer, but shows no symptoms
4) Infected computer surreptitiously scans DSO network, and spreads to other computers
5) Malware opens a backdoor through the firewall
6) At time Y, the attacker connects to the network through the backdoor, and starts shutting down equipment
7) Blackout ensues

Malware, once present on a system, can do anything a human user with corresponding privileges can do without having physical access. In the Ukraine incident, attackers piggybacked on legitimate VPN connections from infected office computers, and installed malware on RTUs that rendered them inoperable after the attack activation [8], forcing a manual reset and reinstallation requiring physical presence.

2) Malware in delivered equipment from the vendor: This misuse case describes how equipment can be delivered with general malware or with a backdoor that allows for unauthorized access to the equipment because the supply chain has been compromised. This may happen in several ways, e.g.:

- Insider at a supplier: An employee at a supplier installs a backdoor that allows for remote control and extraction of information, e.g. makes it possible to access a substation. This can happen at the initiative of the insider, or the employee may be extorted to do this. The DSO in the end is not aware of this backdoor into their system.
- Test access functionality is not removed: To allow easy testing of the equipment, the vendor implements functionality to access the equipment remotely and this functionality is not removed before the equipment is delivered to the DSO due to neglect. Thus, the equipment ends up having a backdoor into the system that the DSO is not aware of.
- Vendor that cannot be trusted: The vendor implements a backdoor into the component on purpose (e.g. due to ties to foreign powers). Thus, the vendor (and others the vendor may serve/cooperate with) ends up having a mean to access the system where the equipment is installed.
- Infected equipment is moved: Equipment that has been used somewhere else, and has been infected with malware, is moved into the DSO network without the malware being detected.
- Equipment is infected at the supplier: Malware in the supplier environment (e.g. in the test network) spreads to the delivered equipment before it is received by the DSO. The malware is not detected by the DSO before the equipment is installed in the DSO system.

Example:

1) Attacker compromises vendor X and replaces firmware on PLCs with trojanized versions.
2) A new PLC from vendor X is installed in the DSO network.
3) PLC works fine for the first weeks
4) At time Y, the PLC from vendor X stops accepting commands, and can no longer be controlled

The consequences of such a misuse case depends on what type of equipment is infected, and may include the following:

- Malware can be spread in the network
- Equipment will not work as intended, e.g. use processing power, reduced performance of the communication network and equipment
- If ransomware, encrypted and thus unresponsive equipment (controls PLCs)
- Disturb or hinder monitoring and control of the process network
- Data loss – e.g. information about the whole Industrial Control System

Further consequences could include installation of a back door which can be used in subsequent coordinated attacks, plus information gathering that may be useful for further attacks.

3) Malign software update is installed on equipment in the DSO network: This misuse case describes how a vendor's approach to deliver software updates can be compromised so that malign software updates are delivered and installed into the DSO network. The consequences of this attack depend on the type of equipment that is attacked, how many components are affected (e.g. whether the DSO network has much of this equipment, and whether all/some/one of this equipment receives the malicious update) and what the malicious update does.

Example:

1) A vendor uses a website to distribute software updates to its customers.
2) This website has vulnerabilities that allows an attacker to upload files
3) The attacker creates trojanized versions of several firmware updates to vendor's equipment, and uploads these to the vendor website with the current date.
4) The DSO update manager discovers that there are new updates available for the vendor's equipment, and downloads the trojanized updates (there is nothing to tell that the updates are malign)
5) The update process places malware in the DSO network, and on the vendor's equipment
6) The attacker gets real-time access to the DSO network and the vendor's equipment in that network

If only the devices that are updated with the malicious software update are affected, the consequences are likely to be local outages, increased manual workload and potentially the cost of replacing any affected equipment. If the update succeeds in having a propagating effect (worm), the consequences will be more significant, potentially giving the threat actor control of the whole grid. For both alternatives, there could also be fires, personnel injuries, components no longer fulfilling their purpose, and incorrect information being reported to the control centre.

4) Temporary access rights are not removed: Vendors get remote access rights to the system for a task and for a certain time period, but if this access is not removed when it should no longer be needed, it represents a security risk. This can include opening a port for the vendor in the firewall or giving vendors a username or password to the system. If the password in addition is of low quality (e.g. test123) to allow for easy use by the vendor, this increases the risk of an attack, also during the period of authorised access.

Example:

1) Remote access rights are opened up for vendor, allowing to connect through the firewall with a remote desktop application
2) Vendor selects a password which is easy to remember: ”test123”
3) Vendor performs its tasks
4) Nothing happens for a month, remote access rights are forgotten by vendor and DSO
5) Vendor is infected by targeted malware which searches for access to SCADA systems
6) Malware determines access to DSO, and starts trying to log in using common passwords
7) The password test123 is quickly found, and malware reports back to attacker
8) The unauthorised access rights are misused.

Potential consequences may include:

- Adversaries getting access to information
- Sabotage
- Unauthorized configuration changes
- New accounts on the system
- Adding of more backdoors
- Hindered access for legitimate users of the system
- Further infiltration the network

5) Misconfigurations: Manual configuration of equipment carries with it the risk that parts of the system is misconfigured. Misconfigured equipment may represent security vulnerabilities that may be exploited by external attackers. Misconfiguration is common in cases of manual configuration, as shown by Wool [15] in the case of Firewalls – there is no reason to believe that the situation for other complex equipment is any different.

Possible consequences include SCADA equipment such as PLCs not functioning correctly, or not at all.

C. Malicious manipulation of the FLISR (self-healing) functionality

Fault Localization, Isolation and Service Restoration (FLISR or self-healing) [16] enables disconnection of transmission or distribution segments with errors, and automatic reconfiguration of the grid to minimize the number of segments left without power. The self-healing function is maliciously manipulated either by providing false data preventing correct self-healing in the face of an outage, or by providing false data during normal operations resulting in an outage due to unneeded self-healing operations. The following example will illustrate the latter case.

Example:

1) A threat actor forges a signal from Breaker 2 (see Fig. 3 b) below) that the breaker has tripped due to line failure
2) FLISR system believes network from Breaker 2 and up to be without power
3) Threat actor forges a last-gasp signal from Breaker 3 indicating that the failure lies between Breaker 3 and Breaker 2
4) FLISR system triggers Breaker 3
5) Threat actor forges another last-gasp signal from Breaker 2 indicating that the failure lies between Breaker 2 and Breaker 3
6) FLISR system triggers breaker 2
7) FLISR system reconfigures network by closing the normally-open point (NOP).
8) Network segment between Breaker 3 and Breaker 2 is left without power, even though no failure has occurred.

Potential consequences may include outage due to self-healing being prevented from healing the grid, or from self-healing being manipulated to cause the outage.

D. Abusing Artificial Intelligence/machine learning algorithm

A malicious actor manipulates machine learning algorithms used to control the power grid. This could cause unexpected situations to occur, like the automated system shutting off power in an area when there is no need or the system could avoid isolating a fault, causing an unnecessarily large area to be affected. The manipulation could either be done at the algorithm level, provide fake data or slightly change the provided data. Example:

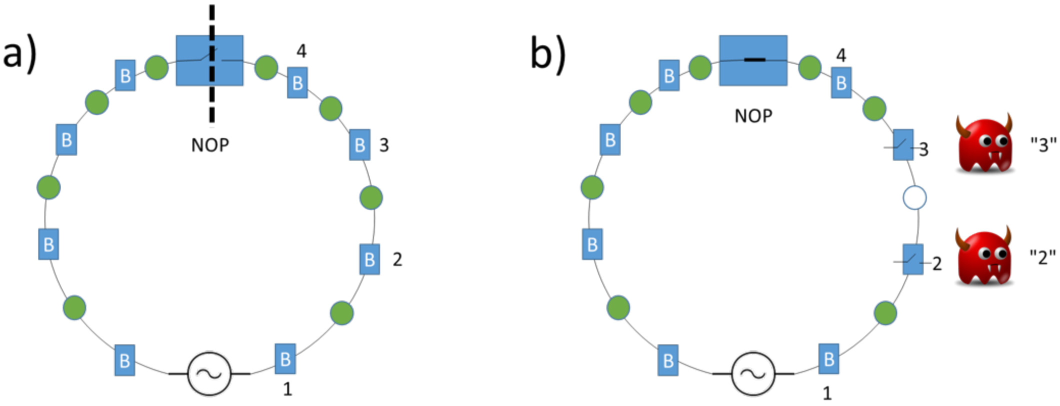

Fig. 3. a) Self-healing configuration b) Self-healing manipulated by attacker

1) The algorithm is trained with normal data and not able to detect anomalies etc.
2) A threat actor gains access to the communication channel and injects commands in a pattern confusing the artificial intelligence algorithm
3) The artificial intelligence algorithm perceives something other than the reality as happening, thus making decisions harmful to the grid stability rather than stabilizing

These attacks may have impact on the resilience aspects of the power grid, resulting in potential disruption of the energy services.

V. Misuse cases related to microgrids

Microgrids are envisioned as the basic core technology that will assist in realizing tomorrow's smart grids. According to The U.S. Department of Energy [17], a microgrid can be defined as - a group of interconnected loads and distributed energy resources (DER) with clearly defined electrical boundaries, that can be not only connected to the traditional grid but also disconnected to operate in island mode to function autonomously. Microgrids can come in a variety of network architectures; they can be isolated islands that are totally self-sufficient, they can be interconnected with other microgrids forming an enclave, and they can have the option of being connected to the main grid if the power consumption increases or there is a need for load balancing.

In microgrids, distributed generations, loads and energy storage devices are constantly being connected and disconnected. Therefore, all infrastructure elements need to be monitored to ensure safe operation. Accordingly, in the future microgrids may utilize more information and communication technologies (ICT) to enable advanced system monitoring and control. For example, microgrids rely on cyber-physical systems in order to integrate different types of microgrid network domains used in solar, storage, and fuel sources.

The various misuse cases discussed above can be applicable to microgrids as well, for example, malware related attacks, misconfiguration of IT systems used within control systems of the microgrid. In the future, artificial intelligence and machine learning techniques may pave the way in transforming microgrids into self-healing systems [18]. Accordingly, abusing AI and ML algorithms type of misuse cases as discussed in section IV-D are valid for microgrids. Though misuse cases discussed above may be similar, their impact on the overall smart-grid architecture may be different.

A. *False data injection attacks in microgrids*

In the future, microgrids may be connected to and separated from other microgrids and the distribution network when needed for better fault handling. While connected, microgrids can exchange status information with other microgrids and with the DSO network. The inverter controllers in microgrids play a major role in performing important functions such as island or connected mode operation, frequency/voltage regulation, etc. Further, information from different interconnected nodes and DERs need to be sent to the control management system of a microgrid. An adversary may attempt to modify this information or inject false data by compromising ICT resources at interconnected loads and DER (such as a computer connected with the Internet, IoT devices, etc.) or via attacking over-the-air interface of WIFI or cellular network. In the past, similar attacks demonstrated impact on voltage stability within the microgrid [19].

Example:

1) An attacker gets access to the wired or wireless communication channel to intercept and modify the data
2) A compromised sensor or IT system can be used to send false data to other connected devices or systems

The aforementioned attacks affect the control system of microgrids and result in increased energy loss. Such data integrity attacks may be used to fake connected or island mode to the DSO to induce voltage stability issues within the smart grid itself.

B. *DoS attacks in microgrids*

In the future, the use of cloud computing or software-defined technology may play a significant role and there may be public Internet-based connectivity between operational technology and information technology in microgrids [20]. In addition, due to the requirement of interconnectivity within microgrid domains, the risk of Denial of Service (DoS) attacks increases. In the past, several researchers have demonstrated such types of DoS attacks. Typically, an adversary attempts to exhaust IT resources within control central of microgrids by sending a lot of unwanted messages or exploiting vulnerabilities in the network or system. This is done in order to disable normal services of microgrid operations. Such types of DoS attacks can be detected to prevent service interruption [21]. However, intermediate types of DoS attacks are difficult to detect and could be used by adversaries to bypass existing protection systems. The impact of DoS-attacks and intermediate types of DoS-attacks would be similar on stability and cyber-physical security of microgrids.

Example:

1) An adversary uses wireless attacks (over cellular or WiFi) to send malicious or legitimate packets to the connected sensors. Consequently, the sensors would not be able to share information with the control center.
2) In case some IT infrastructure of microgrid domain is connected over the public Internet, such type of connectivity could be attacked to cause a denial of service scenario.

Normal services of a microgrid in the island or connected mode would be affected due to this attack due to unavailability of network connectivity. Without a functioning communications network, the real-time data required to manage the energy exchange will not be available. In addition, it may have an impact on the overall grid as communication channels (wired or wireless) are unavailable to report the status of microgrid operations due to the attack.

VI. Concluding remarks

This paper has presented misuse case scenarios related to three overall areas: managing flexibility in the TSO-DSO relation, smart distribution grids and microgrids. The misuse cases represent potential security challenges to be considered when working on modernising the grid, however they are not exhaustive. Future work can include improving the misuse case scenarios as more details on the future solutions become available. More important is however to take such scenarios into account when working on future solutions, so that the risks associated with these and other misuse case scenarios can be reduced.

Acknowledgment

This work was supported by the FME CINELDI research centre, funded by the Research Council of Norway, grant number 257626 (www.sintef.no/projectweb/cineldi). Thanks to the power system researchers and industry representatives that provided input to this work. Thanks to Marie Elisabeth Gaup Moe for contributing to the identification and selection of the misuse cases, and thanks to Henning Taxt for providing comments on an earlier version of this paper.

References

[1] C. Frøystad, I. A. Tøndel, M. G. Jaatun, R. Borgaonkar, and M. Moe, "Misuse cases – an overview," FME CINELDI, Tech. Rep., 2018.

[2] A. Z. Morch, M. Istad, K. Ingebrigtsen, S. Garnås, J. Foros, and B. M. Mathisen, "Use cases for future (2030-2040) smart distribution grid operation," CINELDI, Trondheim, Tech. Rep., 2018.

[3] T. S. Hermansen, H. Vefsnmo, G. H. Kjølle, and K. Sand, "Driving forces for intelligent distribution system innovation-results from a foresight process," in *Proceedings of 25th International Conference and Exhibition on ELECTRICITY DISTRIBUTION*, CIRED. AIM, 2019. [Online]. Available: https://www.cired-repository.org/handle/20.500.12455/507

[4] K. Bernsmed, M. G. Jaatun, and C. Frøystad, "Is a smarter grid also riskier?" in *Security and Trust Management. STM 2019*, 2019.

[5] M. B. Line, A. Zand, G. Stringhini, and R. Kemmerer, "Targeted Attacks Against Industrial Control Systems: Is the Power Industry Prepared?" in *Proceedings of the 2Nd Workshop on Smart Energy Grid Security*, ser. SEGS '14. New York, NY, USA: ACM, 2014, pp. 13–22. [Online]. Available: http://doi.acm.org/10.1145/2667190.2667192

[6] M. B. Line, I. A. Tøndel, and M. G. Jaatun, "Cyber security challenges in smart grids," in *2011 2nd IEEE PES International Conference and Exhibition on Innovative Smart Grid Technologies*, Dec 2011, pp. 1–8.

[7] I. A. Tøndel, M. G. Jaatun, and M. B. Line, "Threat Modeling of AMI," in *"Proceedings of the 7th International Conference on Critical Information Infrastructures Security (CRITIS 2012)"*, 2012.

[8] A. Cherepanov and R. Lipovsky. (2017) Industroyer: Biggest threat to industrial control systems since stuxnet. WeLiveSecurity by eset. [Online]. Available: https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/

[9] A. Dabrowski, J. Ullrich, and E. R. Weippl, "Grid shock: Coordinated load-changing attacks on power grids: The non-smart power grid is vulnerable to cyber attacks as well," in *Proceedings of the 33rd Annual Computer Security Applications Conference*, 2017, pp. 303–314.

[10] S. Soltan, P. Mittal, and H. V. Poor, "Blackiot: Iot botnet of high wattage devices can disrupt the power grid," in *27th USENIX Security Symposium (USENIX Security 18)*, 2018, pp. 15–32.

[11] S. Sridhar, A. Hahn, and M. Govindarasu, "Cyber–physical system security for the electric power grid," *Proceedings of the IEEE*, vol. 100, no. 1, pp. 210–224, 2011.

[12] N. Falliere, L. O. Murchu, and E. Chien. (2011) W32.Stuxnet Dossier. [Online]. Available: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

[13] J. Ehrenfeld, "WannaCry, cybersecurity and health information technology: A time to act," *J Med Syst*, vol. 41, p. 104, 2017. [Online]. Available: https://doi.org/10.1007/s10916-017-0752-1

[14] F. Griscioli, M. Pizzonia, and M. Sacchetti, "Usbcheckin: Preventing badusb attacks by forcing human-device interaction," in *2016 14th Annual Conference on Privacy, Security and Trust (PST)*. IEEE, 2016, pp. 493–496.

[15] A. Wool, "A quantitative study of firewall configuration errors," *Computer*, vol. 37, no. 6, pp. 62–67, 2004.

[16] M. G. Jaatun, M. E. G. Moe, and P. E. Nordbø, "Cyber security considerations for self-healing smart grid networks," in *2018 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)*, June 2018, pp. 1–7.

[17] D. T. Ton and M. A. Smith, "The us department of energy's microgrid initiative," *The Electricity Journal*, vol. 25, no. 8, pp. 84–94, 2012.

[18] A. Chaouachi, R. M. Kamel, R. Andoulsi, and K. Nagasaka, "Multiobjective intelligent energy management for a microgrid," *IEEE Transactions on Industrial Electronics*, vol. 60, no. 4, pp. 1688–1699, 2013.

[19] M. Ma and A. Lahmadi, "On the impact of synchronization attacks on distributed and cooperative control in microgrid systems," in *2018 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*. IEEE, 2018, pp. 1–6.

[20] Nokia, "Adopting SDN for microgrid communications," https://www.engerati.com/microgrid/adopting-sdn-for-microgrid-communications/, Tech. Rep.

[21] Symantec, "Attack: SCADA Control MicroSystems ClearScada DOS." [Online]. Available: https://web.archive.org/web/20170703160508/https://www.symantec.com/security_response/attacksignatures/detail.jsp?asid=24137