Is a Smarter Grid Also Riskier?

Karin Bernsmed[1], Martin Gilje Jaatun[1], and Christian Frøystad[2]

[1] SINTEF Digital, Trondheim, Norway {karin.bernsmed,gilje}@sintef.no
[2] Secure Practice, Trondheim, Norway

Abstract. The smart grid evolution digitalizes the traditional power distribution grid, by integrating information communication technology into into its operation and control. A particularly interesting challenge is the integration of grid topology monitoring and decision support systems with the remote control of breakers in the grid and at the subscribers' premises. In this paper we outline and discuss the results from a recent information security risk assessment of such an integrated system.

Keywords: smartgrid, cyber security, risk assessment

1 Introduction

Energy supply is vital for almost all parts of our daily lives. Failure in the delivery of power will have direct consequences for all sectors in our society and for the digital systems that these sectors rely on. Today, it is already common practice to use Information and Communication Technology (ICT) to support the operation and control of electric power transmission systems and the SCADA systems that supervise them. To meet the modern society's demand for efficient and reliable power supply, SCADA systems are increasingly being interconnected with other systems, such as Distribution Management Systems (DMS), Geographical Information Systems (GIS), Network Information Systems (NIS) and systems for Customer Relationship Management (CRM). In addition, the introduction of the Advanced Metering Infrastructure (AMI) with smart electricity meters, which will provide the power utility companies with information on the current status of the power distribution grid, will also increase the reliance on ICT in this sector.

Increased digitalization and integration of these systems into an envisioned smart grid will yield increased utility, but will potentially also bring increased risk [4]. In particular the increased complexity will make it difficult to understand how the different parts interact, and this will also increase the risk of technical failures, human errors and cyber security threats.

In this paper we outline results from a information security risk assessment of the integration of AMI, DMS and SCADA systems that we performed on behalf of the Norwegian Water Resources and Energy Directorate[3] during the fall of 2018. The focus of the risk assessment was not on the security of the individual

[3] https://www.nve.no/english/

systems per se (this has already been covered in numerous publications; cf. next section), but rather on new threats and risks that may materialize when these systems become more closely integrated. Further, our analysis focuses on risks that stem from breaches of information security, i.e. attacks; we have not included random failures and other types of unwanted events in our study.

The paper is organised as follows. Section 2 provides an introduction to the threat picture faced by the energy sector today, as well as an overview over existing studies of threats and risks related to smart grid security. Section 3 explains the methodology that have been used to perform the risk assessment. In Section 4 we outline the system that has been our target of evaluation. Section 5 and Section 6 outline the assets and the evaluation criteria that we have used in the risk assessment. Section 7 contains the risk identification, analysis and evaluation and Section 8 provides a set of countermeasures that can be implemented to mitigate the most serious risks. Finally, in Section 9 we conclude our work.

2 Background

The Stuxnet attack against uranium enrichment centrifuges in the Iranian Bushehr nuclear power plant [3] was the first publicly known external cyber attack against industrial control systems. At the time, the power distribution industry professed confidence that a similar incident could not happen in their systems [11], but only a few years later saw the Dragonfly campaign targeting industrial control systems in the power sector [15]. Dragonfly was primarily an information gathering exercise, but in December 2015 the gloves came off when almost a quarter of a million Ukrainians suddenly found themselves without power for more than 6 hours due to a cyber attack on several Ukranian Distribution System Operators (DSOs). The trick was repeated one year later by the Industroyer malware [1], blacking out parts of Kiev for an hour.

Nowadays, cyber security is high on the agenda, both for the industry as well as in the academic community. Pièvre-Cambacédès et al. [11] review 21 "myths" about cyber security that exist in the power industry. The very first one is the common perception that the different control systems are isolated. According to the authors, most systems are already (to a varying degree, of course) connected in one way or the other. In the paper, the authors also neutralize the common belief that cyber security incidents will not impact operations. An interview study of power distribution system operators (DSOs) from 2014 indicates that, even though the power industry is very well prepared for traditional threats, such as physical attacks, they are not yet ready to meet targeted cyber attacks.

Security threats and challenges to smart grids have been highlighted by, for example, Goel and Hong [5], Hawk and Kaushiva [6], Sanjab et.al. [12] and Cleveland [2] (the last one already in 2008). An excellent overview and classification of threats to smart grid cyber securiy is provided by Otuoze et.al. [10]. While the scope of these articles do not cover all parts of the system that we have assessed, the threats identified has been a valuable input in our study when identifying risks to the integrated system.

3 Methodology

The risk assessment presented in this paper has been performed in accordance to ISO/IEC 27005 Information Security Risk Management standard [7]. The standard prescribes five different steps; 1) Context establishment, which includes understanding the system that is to be assessed, defining the scope of the analysis, identifying assets and agreeing on scales and acceptance criteria for risk assessment and evaluation, 2) Risk identification, which includes identifying threats and understanding how these threats may lead to unwanted events, 3) Risk analysis, which includes assessing the consequence and likelihood of each of the identified risks, 4) Risk evaluation, which includes comparison of risk analysis results with risk criteria to determine which risks should be considered for treatment, and 5) Risk treatment, which includes identifying and selecting means for risk mitigation and reduction.

Since our assessment concerns an envisioned system rather than an existing one, lots of effort was put into the context establishment phase; more specifically to define what such a system would look like and agreeing on the scope of the analysis. To gather necessary information, we arranged a workshop with key stakeholders from the energy sector, which included participants from energy producers and suppliers, Distribution System Operators (DSOs), vendors of relevant equipment as well as representatives from the national regulatory body. In this workshop we used the world café methodology[4] to facilitate the discussion and to gather the stakeholders' perspectives on how the integration of AMI, DMS and SCADA will manifest. We also briefly discussed what are the critical assets that will need to be protected and what risks the stakeholders envision with this future system.

To identify risks, we then performed a thorough walk-through of all the identified assets, in which we analyzed their need for confidentiality, integrity and availability, where in the system they will be stored, how they will processed and used, and how they will be transmitted between the different parts of the system. Using Microsoft STRIDE [13] we were then able to identify a number of relevant threats. The vast body of existing literature on AMI and SCADA security (cf. Section 2) was also of great help in this process. Since ISO/IEC 27005 is a generic standard, applicable to any kind of domain, we also needed to adapt the risk evaluation step to the domain at hand. More specifically, we used a existing guidance document for risk assessment of AMI and its adjacent systems [9] to derive the scales for consequence and likelihood evaluation and the risk evaluation criteria that we later relied on in our assessment.

Finally, when all the steps in the risk assessment were completed, we sent a draft report to a selected number of stakeholders from the workshop, to gain their feedback on the identified risks, the risk acceptance criteria and the list of countermeasures that we had proposed for mitigating the unacceptable high risks.

[4] `http://www.theworldcafe.com/key-concepts-resources/world-cafe-method/`

4 System Description

The scope of the analysis presented in this paper is the integration of AMI, DMS and SCADA systems in the context of power grid operation. Here we first present an overview over the individual subsystems (Section 4.1- 4.3) before we outline the integrated system that has been assessed (Section 4.4). We will refer to this integrated system as *Integrated DMS, AMI and SCADA (IDAS)*.

4.1 DMS

The Distribution Management System (DMS) is a map application with an overlay network topology, which provides the grounds for predicting consequences of planned and unplanned breaker operations in the SCADA system, and for assessing the severity of failures and downtime of the different links and components in the power distribution grid. The main purpose of the DMS is hence to facilitate a better understanding of potential changes to the grid. At the DMS operation centre, the Shift Operation Manager is the sole person authorized to approve changes to the grid and he/she is also responsible for making sure that such changes are reflected in the DMS. The DMS receives incoming data in terms of state information from the automatic and/or remotely controlled breakers in the SCADA system, but at the time of writing, it is very rare that a DMS has implemented outbound communication, i.e. transmission of breaker operation commands from DMS to SCADA[5].

Data from the DMS is also replicated and transmitted as status information to 3rd party actors and other types of systems. DMS also receives information from other sources, such as the AMI Head End System (see Section 4.3), however, such data is not processed automatically; instead it is sent to the Shift Operation Manager who manually reviews it and decides whether the DMS should be updated or not.

4.2 SCADA

Supervisory Control And Data Acquisition (SCADA) resides between the physical and the digital world. A SCADA system consists of a collection of hardware (Programmable Logical Controllers (PLCs), servers and switches) and software that monitors and controls (parts of) the power distribution grid. Per today, it is straightforward to retrofit sensors in the SCADA system whenever needed, but the use of actuators is less common. All transformer substations in the SCADA network have already been automated, but so far is has not been considered worth the effort to automate the smaller components. Hence, today the majority of the power distribution grid is still operated manually, i.e. not controlled by the SCADA system, which means personnel need to be dispatched to execute changes in, for example, the switches in the grid.

[5] Systems that control SCADA operations are subject to dedicated legislation, which today in practice is considered a showstopper in most European countries.

4.3 AMI

The Advanced Metering Infrastructure (AMI) measures the power consumption of the individual households in the power distribution grid by collecting and analyzing data from smart meters installed at the subscribers' premises. The AMI can also log and report events, such as local earth faults, and send and receive control messages; the most controversial one being the envisioned breaker operation that will shut down the power supply to one or more subscribers. The smart meters are in most cases connected to a central Head End System (HES) through local master nodes. The master nodes are connected to the HES through the mobile network (GPRS, 4G, 3G or 2G), while the remaining smart meters (slave nodes) are connected to the master node through a mesh based network. Note that there are also other ways to connect the smart meters to the HES, for example by installing a dedicated transmitter that nearby smart meters can connect to, or by installing radio communication equipment in the smart meter themselves.

4.4 Integrated DMS, AMI and SCADA (IDAS)

Increased integration of the power distribution grid indicates that existing systems are tied more closely together. This becomes particularly interesting when systems that have been designed to avoid being classified as "operation control systems" (such as the DMS) are being connected with existing operation control system (such as SCADA). Closer integration between AMI, DMS and SCADA means that DMS is being more closely connected the power distribution grid operations, in addition to its current status as a segregated system whose main purpose is to provide increased situation awareness. In case the integration of these three subsystems are performed to such a degree that the new system-of-systems can do both the job of the DMS, as well as sending control signals to SCADA and AMI, such an integrated system would also fall into the category of "operation control systems". In this paper, we refer to this future integrated system as "IDAS" (Integrated DMS, AMI and SCADA).

Note that these systems have already, in some cases, been partly integrated; there exist installations where the HES in the AMI delivers data to the DMS (the HES is then often implemented as a cloud service), and where the SCADA system delivers sensor data and breaker status data to the DMS.

Fig. 1 outlines the state-of-the-art in the energy sector where most actors already operate a DMS. The purple dashed line shows where IDAS will manifest, in terms of closer integration of systems and functionality. The purple arrows show communication to and from IDAS. As can be seen in the figure, integration of data from AMI is expected to be more direct and possibly also automatic. At the same time, IDAS will be allowed to control the SCADA system directly. These changes increase the attack surface for all the systems that used to be more separated. In the not-so-distant future, we may also envision the IDAS as a system-of-systems that automatically manages the existing tasks of the human operators at DMS, AMI HMI and SCADA HMI.

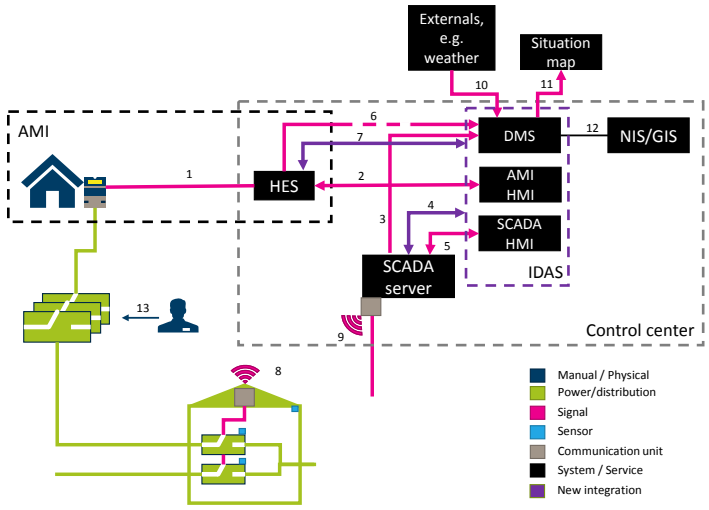

Fig. 1. System overview

The different communication interfaces are identified by numbers in Fig. 1, and are detailed as follows:

1. **Smart Meter – HES** (bidirectional): The smart meter periodically sends meter readings to HES, including eventual error messages. In the case of power cut, a "last gasp" diagnostic message is sent, and some meters can also send updated information after power cut. The HES sends control messages to the smart meter. The HES can request readings outside the planned interval, activate breaker function, and set limit on allowed consumption before breaker is automatically activated (throttling function).
2. **HES – AMI HMI** (bidirectional): HES offers an API for interaction. The DSOs can either use the interface offered by HES, or implement their own.
3. **SCADA server – DMS** (unidirectional): SCADA transfers status information on breakers and sensors in the grid to DMS.
4. ***SCADA server – IDAS*** (bidirectional): IDAS transfers control signals to SCADA to effectuate physical changes in the grid. This implies that breakers may alter state.
5. **SCADA server – SCADA HMI** (bidirectional): SCADA HMI is the user interface to the SCADA controller. All state information is sent from SCADA server to SCADA HMI, and commands are sent from SCADA HMI to SCADA-server.
6. **HES – DMS** (unidirectional): HES transfers alarms from the grid so that they may be put in an operational context in DMS.
7. ***HES – IDAS*** (bidirectional): Operation of breaker and throttling for each individual smart meter.

8. **Substation – SCADA Server** (unidirectional): Sensor data (humidity, temperature, door open/closed, etc.), measurement on transformer load, and state of breakers.
9. **SCADA Server – Substation** (unidirectional): Control signals for operation of breakers.
10. **External entity (e.g., weather service) – DMS** (unidirectional): Relevant updates from external sources such as weather information to DMS.
11. **DMS – Situation map** (unidirectional): DMS transfers relevant data (i.e., data to be published)
12. **DMS – NIS/GIS** (bidirectional): DMS is based on the NIS/GIS data base, hence will changes made in the DMS interface be reflected in the NIS/GIS data base, and vice versa.
13. **Service technician – manual breaker** (manual): Manually changing the state of breakers.

5 Primary and supporting assets

ISO/IEC 27005 stipulates that the risk assessment should focus on assets. The standard distinguishes between *primary assets*, which are the information and services that are crucial for the business operation, and *supporting assets*, which are related IT infrastructure and human resources that also will need to be protected in order to ensure the confidentiality, integrity and availability of the primary assets. The focus of our analysis is mainly information security. As described in the previous three subsections, closer integration of AMI, DMS and SCADA will entail that breaker operations (or "ops") will be pushed from DMS to SCADA, which is new compared to today's situation. In addition, the status of the breakers in the power distribution network will form the basis for (possible automated) decisions in the IDAS. We have therefore identified three primary assets, which we call "SCADA Breaker ops", "SCADA Breaker status" and "AMI Breaker ops". These are further described in Table 1. In addition, we have identified twelve supporting assets, which, if manipulated or misused, may affect the primary assets. These are:

- AMI Breaker status: reports breaker status for individual power consumers. Manipulation of AMI status reports may lead to a misconception of the status of the grid, leading to the execution of erroneous SCADA breaker operations that, in worst case, can have harmful consequences.
- Sensor data: reports the status (power output, temperature, wind, humidity, wear out, etc) of different parts of the power distribution grid. Sensor data is aggregated in the network and transmitted to the SCADA server, which in turn forwards the data to the SCADA HMI and the DMS. Sensor data can be correlated with breaker status to detect deviations in the network. Manipulation of sensors may be used to avoid the detection of malicious breaker operation commands or and breaker status reports.
- NIS/GIS data: imported to the DMS and used to model and visualize the topology of the power distribution network. Correct topology information

is a necessity for the usage of breaker status in decision making and for performing remote execution of breaker operations.
- AMI measurements: reports power consumption and events to the HES. This information is used to support AMI breaker operations (P3).
- Authentication credentials: need to be protected to ensure that only authorized personnel have access to the AMI and SCADA HMIs.
- Encryption keys: used to ensure confidentiality protection of data in transit and stored data. Encryption is currently implemented in smart meters, the HES, the SCADA servers and the PLCs.
- System documentation: contains detailed information about the IDAS architecture, functionality and current configuration. Should be kept confidential.
- Head End System (HES): collects data from smart meters and receives and forwards control commands to the smart meters. Protecting the HES is necessary to secure the execution of AMI breaker commands.
- SCADA server: the heart of the SCADA system. Transmits commands to the remotely controlled breakers and collects sensor data from the grid.
- IDAS software: provides monitoring and control of the complete power distribution grid, including the ability to execute changes to the grid and to control smart meters.
- Software/firmware updates: all updates to any part of the system need to be protected and controlled.
- Network communication infrastructure: need to be available and have sufficient capacity to ensure that control commands can reach the breakers and that sensor data and breaker status can reach the SCADA server.

Table 1: Description of primary assets

Id	Primary asset & rationale	C	I	A	Storing	Processing	Communication
P1	**SCADA Breaker ops.** A remotely executed command that changes the state of a breaker in the power distribution grid. Unauthorized breaker operations may disconnect (parts of) the grid. Such events may require the operator to disable remote control altogether and revert to manual control of the grid.	yes	yes	yes	n/a	Processed by SCADA HMI and IDAS (receive decisions from the Shift Operation Manager), SCADA server (receives commands from SCADA HIM or DMS and forward them to the breakers) and remote breakers (receive commands and changes the state of the breakers).	Transmitted from IDAS or SCADA HMI to SCADA server and further to the PLC (using cable or wireless).

Table 1: Description of primary assets

Id	Primary asset & rationale	C	I	A	Storing	Processing	Communication
P2	**SCADA Breaker status.** A (real-time) status report of the breakers in the power distribution grid. User by the operation central. Breaker status is important because it 1) can be used by unauthorized persons to survey the grid, 2) erroneous breaker status may lead to the execution of erroneous actions from the control center that damages the grid, and 3) lack of updated breaker status may in worst case cause operators to execute unnecessary change sin the grid, or changes that may have adverse safety effects	yes	yes	yes	DMS (stored until the next update) and SCADA (stored continuously)	Processed by sensors at the breakers (generates and transmits status of automatized breakers), SCADA server (receives signals from sensors at breakers and forwards these to the SCADA HMI) and SCADA HMI and IDAS (displays information to the operators).	Transmitted from the breaker sensors to the SCADA server over cable or 4G, and further to the SCADA HM and IDAS (over cable).

Table 1: Description of primary assets

Id	Primary asset & rationale	C	I	A	Storing	Processing	Communication
P3	**AMI Breaker ops.** Manipulation of AMI breaker operations could lead to loss of power for one or more subscribers. Unavailability of this function will require personnel to be dispatched to manually connect or disconnect the subscriber. In the longer term, unavailability may also prevent serious failures at subscribers to be isolated form the rest of the grid.	no	yes	yes	n/a	Processed by HES, IDAS and the smart meters.	Transmitted from HES to smart meters over through master nodes, mesh network or dedicated transmitters (cf Section 4.3). The communication link will be encrypted. NB: AMI breaker operations will allegedly never be broadcasted; only unicast will be implemented.

6 Risk assessment criteria

Risk assessment in accordance to ISO/IEC 27005 [7] includes the identification and assessment of unwanted events, which in the scope of our study include threats that cause a breach of confidentiality, integrity or availability of the three primary assets "SCADA Breaker ops", "SCADA Breaker status" and "AMI Breaker ops" that we have identified[6]. Further, risk is a combination of likelihood and consequence. The threats have therefore been assessed in terms of what *impact* they will have on the relevant stakeholders, which in our case is the DSOs, the power consumers (subscribers) and the society overall, and the *likelihood* that the threat will occur. In the energy sector, reliable power supply should always be included as a dimension of impact [9]. Here we have also included safety and economy as additional dimensions when assessing the impact of each identified threat. Likelihood is a notoriously difficult dimension to assess in a security risk assessment. Here we have made a qualitative assessment based on "expert opinion", which takes into account how easy/difficult it would be to perform the

[6] Note that some of the threats will also implicitly affect the supporting assets

attack, whether there exist any security mechanisms that could prevent, detect and/or react to such a threat, and whether such events have been observed in the past.

The scale that was used to assess likelihood is:

1. Unlikely
   - Expected to occur less than every 10th year.
   - Security mechanisms exist and are expected to work as intended.
   - Existing security mechanisms can only be circumvented by resourceful insiders with thorough knowledge of the system.
   - External attackers need to have advanced technical skills and help from insiders.
   - There are no known examples of this attack.
2. Less likely
   - Expected to occur once a year.
   - Security mechanisms exist and are expected to work as intended.
   - Existing security mechanisms can be circumvented by insiders with some knowledge of the system.
   - External attackers must be resourceful and have detailed knowledge of the system.
   - Similar attacks have occurred in other sectors and may, in theory, also be applied in the energy sector.
3. Possible
   - Expected to occur several times a year.
   - Security mechanisms are not fully implemented or do not work as intended.
   - Existing security mechanisms can easily be circumvented by insiders.
   - External attackers need some knowledge of the system. There may be existing exploit tools that can be used to perform the attack.
   - Such attacks have been observed in the energy sector before.
4. Likely
   - Expected to occur several times a month.
   - Security mechanisms do not exist, or can be easily circumvented by either insiders or external attackers.
   - The attack can be performed without any specific knowledge of the system.
   - The incident may be caused by negligence, either by own personnel or attackers.
   - Such incidents are common in the energy sector.

The scale that was used to asses impact is:

1. Minor
   - Minor or insignificant impact on the subscribers.
   - No interruption of power supply.
   - No damage to equipment.
   - Insignificant economic loss.

2. Moderate
   - Local impact affecting a small number of subscribers.
   - A limited number of subscribers lose power for a limited amount of time.
   - Minor damage to equipment.
   - Small (recoverable) economic loss
3. Major
   - Serious consequences in a local community.
   - Loss of power for a long period of time for a limited number of subscribers.
   - Damages to the grid and/or on personnel
   - Major economic loss
4. Critical
   - Essential services, such as health care or other critical infrastructure, are affected.
   - Loss of power for large parts of the grid during a long period of time
   - Severe damages to equipment and/or loss of human life
   - Irreparable economic loss.

The risk of each identified incident have then been calculated as likelihood $\times$ impact and evaluated as

- High (red) for values between 12-16,
- Medium high (orange) for values between 8-9,
- Medium low (yellow) for values between 4-6,
- Low (green) for values between 1-3,

7 Risk identification, analysis and evaluation

We have identified 11 threats that may have direct consequences for primary assets; these are detailed in Table 2. For each identified threat, we indicate whether it affects Confidentiality (C), Integrity (I) or Availability (A) of the affected primary asset(s). We also calculate the risk using the scales outlined in the previous section.

Table 2: Threats with direct consequences for the primary assets

ID	Threat	Pri. asset(s)	C	I	A	Consequence	Impact	Likelihood	Risk
R1	Eavesdropping of commands that modify state of breakers, or status messages from remotely controlled breakers in the distribution grid	SCADA Brk. ops (P1) SCADA Brk. status (P2)	X			Mapping of network topology, communication pattern analysis	1	3	3
R2	Unauthorized entities send fake commands with breaker operations to remotely controlled breakers in the distribution grid	SCADA Breaker ops (P1)		X		Can disconnect (parts of) distribution grid, as well as inflict damage on equipment and grid that leads to greater and more long-lasting power cuts. In the worst case, this can lead to disconnection of large areas, including hospitals and other critical infrastructures.	4	3[7]	12
R3	Denial of service attack against the communication link to a single or a few remotely operated breakers in a limited area of the distribution grid	SCADA Brk. ops (P1) SCADA Brk. status (P2)			X	Reduced overview of status, delay in ability to make changes in the distribution network (due to need for sending out personnel)	1	2[8]	2
R4	Targeted attack against SCADA servers so that breakers in the distribution grid cannot be remotely controlled	SCADA Breaker ops (P1) SCADA Breaker status (P2)			X	Significantly reduced overview of status in own grid, delay in ability to make changes in the distribution grid (due to need for sending out personnel to observe and make changes)	2	2	4

Table 2: Threats with direct consequences for the primary assets

ID	Threat	Pri. asset(s)	C	I	A	Consequence	Impact	Likelihood	Risk
R5	Attack against central communication infrastructure that prevents communication with remotely operated breakers	SCADA Breaker ops (P1) SCADA Breaker status (P2)			X	Significantly reduced overview of status in own network, delay in ability to make changes in the distribution network (due to need for sending out personnel to observe and make changes)	2	3	6
R6	Reporting of false breaker status to the SCADA server	SCADA Brk. status (P2)		X		Can spur grid changes that may cause damage to the grid or people	3	3[9]	9
R7	Unauthorized entities perform changes in the DMS part of IDAS that lead to undesirable SCADA breaker operations are effectuated	SCADA Breaker ops (P1) SCADA Breaker status (P2)		X		Can disconnect (parts of) grid, cause damage to equipment and grid that leads to major and long-term power loss. In worst case blackouts in larger areas, including hospitals and other critical infrastructure.	4	3[10]	12
R8	Denial of service attack that affects communication link to one or more subscribers in the grid	AMI Breaker ops (P3)			X	Breaker functionality and throttling is expected to be rarely used per subscriber, but loss of communication link may cause reduced overview of own grid. Delays in restoration due to use of manual labor to make changes.	1	4[11]	4
R9	An unauthorised entity gains control over the AMI breaker functionality for a single subscriber	AMI Breaker ops (P3)		X		A single subscriber disconnected.	1	2	2

Table 2: Threats with direct consequences for the primary assets

ID	Threat	Pri. asset(s)	C	I	A	Consequence	Impact	Likelihood	Risk
R10	An unauthorised entity gains control over the AMI breaker functionality for a group of subscribers	AMI Breaker ops (P3)		X		Arbitrary number of subscribers disconnected	4	2^{12}	8
R11	An unauthorised entity immobilises an arbitrary number of smart meters ("bricking")	AMI Breaker ops (P3)		X	X	Loss of overview in the grid, loss of ability to disconnect subscribers with serious errors. Loss of DSO revenue, and extra maintenance cost	2	2	4

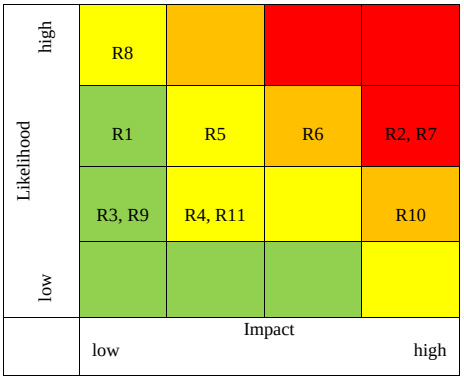

Fig. 2. An overview of the risks identified for the IDAS.

Figure 2 shows an overview over the risks. As can be seen, two risks are unacceptably high:

- R2: Unauthorized entities send fake commands with breaker operations to remotely controlled breakers in the distribution grid.
- R7: Unauthorized entities perform changes in the DMS part of IDAS that lead to undesirable SCADA breaker operations are effectuated.

The severity of these threats are comparable with the incidents that occurred in Ukraine in 2015 and 2016 [8] and may cause a loss of power for large parts of

the grid during a long period of time, possibly also affecting essential services, such as health care and other critical infrastructure.

Two risks have also been assessed as medium high:

- R6: Reporting of false breaker status to the SCADA server.
- R10: An unauthorised entity gains control over the AMI breaker functionality for a group of subscribers.

These threats will only have consequences for local communities. The effect will hence be less severe than if the attacker have had direct access to the execution of SCADA breaker operations (as in R2 and R7).

The rest of the identified risks were considered to be either medium low (yellow) or low (green). It is therefore not necessary to treat these, but as will be discussed below, some of the countermeasures that we propose to mitigate the four higher risks will also reduce the likelihood or impact for some of these lower risks.

We have also identified the following threats to the supporting assets:

T12 Unauthorised entities can read meter values from the smart meter (AMI meter data – S4)
T13 Manipulation of meter values (AMI meter data – S4)
T14 Eavesdropping on messages that contain breaker status (Status AMI breaker – S1)
T15 Reporting fake breaker status to HES (Status AMI breaker – S1)
T16 Field Area Network (FAN) access used to break into central systems (HES and beyond) and subsequent unauthorised modification of HES Software (HES – S10)
T17 Unauthorised eavesdropping on sensor data (Sensor data – S2)
T18 Unauthorised manipulation of sensor data (Sensor data – S2)
T19 Unauthorised access to NIS/GIS (NIS/GIS data – S3)
T20 Unauthorised manipulation of NIS/GIS (NIS/GIS data – S3)
T21 Unauthorised access due to data breach involving authentication information (Authentication information – S7)
T22 Unauthorised access due to weak authentication (Authentication information – S7)

[7] Observed in Ukraine in the case of fully integrated DMS and SCADA.
[8] The major DSOs in Norway are required to have redundant communication in their SCADA system, which implies that fault in a single communication link will not cause a failure.
[9] Observed, e.g., in Stuxnet.
[10] If today's DMS is integrated unchanged with IDAS, the likelihood will be higher due to DMS having more contact points to the outside world, and lower security requirements.
[11] With use of combined communication technology (radio, cellular, copper, etc.) communication failures must be expected.
[12] Lower likelihood of finding many keys for group disconnection, than to find a single key to disconnect one subscriber. There is no function for group disconnection in AMI, but seems easy to script if keys are available

T23 Data breach involving encryption keys (Encryption keys – S8)
T24 Broken encryption due to use of weak encryption algorithms (Encryption keys – S8)

The assessment of these secondary threats will depend on the actual implementation in each DSO's distribution grid, so we have not ventured to make guesses at likelihood or impact, and hence do not attempt to rank the risks to the secondary assets. However, needless to say, these will also need to be protected in order to ensure the security of the primary assets.

8 Recommended security countermeasures

The recommended security countermeasures are

- Implement authenticity, integrity and confidentiality protection of all SCADA breaker operations and SCADA status reports. This can be achieved by, for example, setting up secure sessions between the communicating entities. For connectionless communications, each single message needs to be protected. This will reduce R1, R2 and R6.
- Ensure that only authorized actors have access to the AMI breaker functionality. This can be achieved by following the instructions in the guidance report [14]. This will reduce R9 and R10.
- Define and enforce procedures and criteria for user access control to all systems and equipment that will be part of IDAS (DMS, AMS-HMI and SCADA HMI). This will reduce R7.
- Use independent and redundant communication links, preferably over different media (wireless/fiber/etc) and delivered by different service providers. This will reduce R3, R5 and R8.
- Perform hardening of the SCADA server, i.e., remove unnecessary services and configure the remaining ones to the highest possible security level. This will reduce R4 and R5.
- Implement segmentation of the SCADA network, by splitting the logical network into two or more different security zones. This will reduce R3, R4 and R5.
- Install a firewall between IDAS and the outside network. This will reduce R3 and R4.
- Set up an Intrusion Detection System that monitors the SCADA server and its inbound and outbound connections. This will reduce R4.
- Introduce a regime for signing and verifying all software updates and patches of the SCADA server. This will reduce R11.
- Perform regular vulnerability scanning of the different parts of the IDAS, including any external services. This will reduce all the identified risks.
- Perform a penetration test of the different subsystem in IDAS, including any external services. This will reduce all the identified risks.
- Use whitelists to control all incoming connections from external systems. This will reduce all the identified risks.

– Use digital certificates for secure communication and ensure that all root certificates are securely stored. This will reduce R1, R2, R6, R9, R10 and R11.

The above list is not meant to be a silver bullet; the proposed countermeasures will mitigate the most pressing risks, but in the end it is up to the stakeholders in the energy sector to decide what risks are unacceptable and what countermeasures that are worth investing in.

9 Conclusion

Increased integration of AMI, DMS and SCADA means that systems that originally were designed as separate entities now are being connected and will be dependent on each other. This is particularly challenging when systems that are have been designed with the intention of avoiding falling into the category of "operation control systems" suddenly are connected with such systems. In this paper we have assessed risks that stem from threats to SCADA breaker operations, SCADA breaker status reports and AMI breaker operations. Our assessment shows that the highest risks with an integrated system are related to the execution of unauthorized SCADA breaker operations, which in worst case can have severe consequences on our whole society. The proposed list of security countermeasures is meant to serve as a starting point for stakeholders who want to implement a more integrated system, but we emphasize that the details of each new architecture needs to be thoroughly scrutinized in order to ensure that it is sufficiently secure. It would also be useful to pay more attention to the risk of cyber security threats causing *black swans*, i.e. unexpected events that are hard to predict but that may have severe safety consequences. Such events are typically not picked up by an information security risk assessment like the one that we have presented in this paper.

Acknowledgments

This paper is based on a risk assessment assignment performed for NVE, and further developed as part of the RCN CINELDI project.

References

1. Cherepanov, A., Lipovsky, R.: Industroyer: Biggest threat to industrial control systems since stuxnet. WeLiveSecurity by eset (2017), `https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-\-stuxnet/`
2. Cleveland, F.: Cyber security issues for advanced metering infrastructure (AMI). pp. 1 – 5 (08 2008)

3. Falliere, N., Murchu, L.O., Chien, E.: W32.Stuxnet Dossier (2011), \url{http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf}
4. Frøystad, C., Jaatun, M.G., Bernsmed, K., Moe, M.: Ros-analyse ams-dms-scada – risikoanalyse av økt integrasjon mellom ams, dms og scada. Tech. Rep. 2018:01083, SINTEF Digital (2018), \url{http://publikasjoner.nve.no/eksternrapport/2018/eksternrapport2018_15.pdf}
5. Goel, S., Hong, Y.: Security Challenges in Smart Grid Implementation. Springer, London (2015)
6. Hawk, C., Kaushiva, A.: Cybersecurity and the smarter grid. The Electricity Journal 27(8), 84 – 95 (2014), http://www.sciencedirect.com/science/article/pii/S1040619014001791
7. ISO: Information technology – security techniques – information security risk management. ISO/IEC Standard 27005:2018 (2018), https://www.iso.org/standard/75281.html
8. Lee, R.M., Assante, M.J., Conway, T.: Analysis of the cyber attack on the ukrainian power grid, defense use case. SANS ICS and E-ISAC white paper (2016), \url{https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf}
9. Norges vassdrags- og energidirektorat: Veiledning i risiko- og sårbarhetsanalyser for kraftforsyningen. Tech. rep., Norges vassdrags- og energidirektorat (2010), \url{http://publikasjoner.nve.no/veileder/2010/veileder2010_02.pdf}
10. Otuoze, A.O., Mustafa, M.W., Larik, R.M.: Smart grids security challenges: Classification by sources of threats. Journal of Electrical Systems and Information Technology 5(3), 468 – 483 (2018), http://www.sciencedirect.com/science/article/pii/S2314717218300163
11. Pietre-Cambacedes, L., Tritschler, M., Ericsson, G.N.: Cybersecurity myths on power control systems: 21 misconceptions and false beliefs. IEEE Transactions on Power Delivery 26(1), 161–172 (Jan 2011)
12. Sanjab, A., Saad, W., Güvenç, I., Sarwat, A.I., Biswas, S.: Smart grid security: Threats, challenges, and solutions. CoRR abs/1606.06992 (2016), http://arxiv.org/abs/1606.06992
13. Shostack, A.: Experiences threat modeling at microsoft. In: Proceedings of the Workshop on Modeling Security (MODSEC08). CEUR Workshop Proceedings (2008), http://ceur-ws.org/Vol-413/paper12.pdf
14. Skapalen, F., Jonassen, B.: Veileder til sikkerhet i avanserte måle- og styringssystem. Tech. rep., Norges vassdrags- og energidirektorat (2012), https://www.nve.no/Media/5525/veiledertil-sikkerhet-i-ams.pdf
15. Symantec Security Response: Dragonfly: Cyberespionage attacks against energy suppliers (2014), \url{https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/Dragonfly_Threat_Against_Western_Energy_Suppliers.pdf}