"© 2020 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works."

Cyber-Security Gaps and Reasons in a Digital Substation: From Sensors to SCADA

Athar Khodabakhsh,
Sule Yildirim Yayilgan
NTNU
Gjovik, Norway
athar.khodabakhsh@ntnu.no
sule.yildirim@ntnu.no

Siv Hilde Houmb,
Nargis Hurzuk
Statnett
Oslo, Norway
siv.houmb@statnett.no
nargis.hurzuk@stanett.no

Maren Istad,
Jørn Foros
Sintef Energy
Trondhiem, Norway
maren.istad@sinteff.no
jorn.foros@sinteff.no

***Abstract*—Development of digital substations provides power industrial operation, real-time functionalities and information access. However, the main challenge in DS is to ensure security, availability, and reliability of power systems as in conventional systems in addition to interoperability capability for different vendors. DS development is rather new in Norway and in an R&D Digital Substation pilot project ECODIS[1], Statnett[2] is investigating new functionality advantages and associated costs with IEC 61850 process bus technology. This paper examines cyber-security gaps in power infrastructure, including vulnerabilities introduced through digitalization of substations.**

Abbreviations:
CT: Current Transformer
DS: Digital Substation
DoS: Denial-of-Service
GOOSE: Generic Object Oriented Substation Event
HMI: Human Machine Interface
IEC: International Electrotechnical Commission
IED: Intelligent Electronic Devices
LAN: Local Area Network
MitM: Man-in-the-Middle
MMS: Manufacturing Messaging Specification
MU: Merging Unit
NCIT: Non-Conventional Instrument Transformer
RTU: Remote terminal Units
SCADA: Supervisory Control and Data Acquisition
SV: Sampled Values
VT: Voltage Transformer
WAN: Wide Area Network

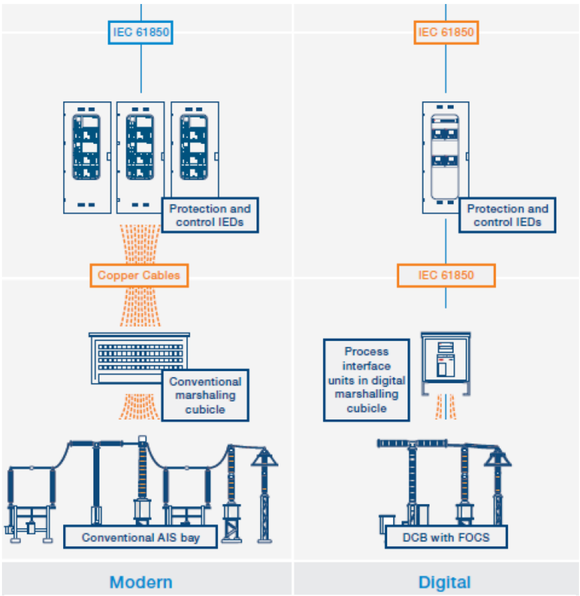
IEC 61850
Protection and control IEDs
Copper Cables
Conventional marshaling cubicle
Conventional AIS bay
Modern
IEC 61850
Protection and control IEDs
IEC 61850
Process interface units in digital marshalling cubicle
DCB with FOCS
Digital

Fig. 1. Depiction of substation digitalization adopted from ABB.

I. Introduction

DS based on IEC 61850 process bus technology is a new concept in Norway and involves replacing most of hardwired copper connections in the substation with process bus technology over fiber cabling, as shown in Figure 1. DS consists of several physical and cyber infrastructures in switchyard and substation buildings. In a DS instantaneous values of analogue signals (voltage, current, etc.) are sampled and digitalized [1]. In the ECODIS project, the objective is to gain experience with NCIT and process bus as well as evaluating interoperability with IEDs from different vendors [2]. There are three pilot sites in the project: Furuset substation owned by Statnett SF - Statelig Foretak, Hafslund and Skagerak substations.

The project seeks to increase utilization of DS, firstly, by demonstrating in three pilots the possibility to utilize SVs to implement additional functionalities in real-time. Secondly, it aims at building a platform in the laboratory environment for investigating different aspects of IEC 61850 including interoperability and cyber-security. Thirdly, the project aims to increase competence in DS of the transmission and distribution system operators in Norway. Findings from this project lay the foundation for implementing real-time functionalities for condition monitoring, and for facilitating an effective deployment of DS for power systems in Norway [3].

Cyber-attacks on power systems such as the Ukraine Power Grid Attack in 2015, showed the vulnerabilities of commu-

[1] Engineering and Condition monitoring in Digital Substation (ECODIS) is a project funded by Research Council of Norway (NFR), Innovation Project for the Industrial Sector - ENERGIX program, project number 296550, coordinated by Statnett R&D group.

[2] Statnett is the system operator of the Norwegian power system.

This is the accepted version of an article published in 2020 9th Mediterranean Conference on Embedded Computing (MECO)
http://dx.doi.org/10.1109/MECO49872.2020.9134350

"© 2020 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works."

nication framework in modern power systems. For detecting attacks, measures are required to enable the system with proper response and minimize consequences of intrusions [4]. For instance, an attacker can reprogram devices, inject malicious data into communication network between sensors and controllers, or inject false control commands to force an action and take the physical plant into potentially unsafe state [5]. Consequently, we focus on the cyber-security issues in DS due to: 1) Critical infrastructure and substation control systems should be protected and preserved from cyber-attacks. 2) In a DS, utilities have the IEC 61850 station based solution in operation for many years. The process bus is rather new where the risk of remote attacks has increased as we have the IP based communication to the process level component as well. 3) The increase in design complexity in cyber-physical system may introduce potential software vulnerabilities that can be exploited to launch remote attacks over a network [6], [7], i.e. the attacker may not require physical access to the system. 4) Other weaknesses can happen by improper authentication, verification of data, credential management, configuration and maintenance of software, and access control.

In this paper, two research questions are addressed: 1) What are the cyber-security attack types in DS? 2) Where and how could such attacks occur? We investigated the vulnerabilities that arise by deployment of process bus technology, threats in process level to physical equipment, and in station levels toward IT infrastructure and software. Section 2 describes a generic system architecture in DS. Section 3 explores cyber-attack types and discusses a threat scenario. Section 4 maps the potential cyber-attacks that are studied in Section 3 to DS, focusing on the pilots in the ECODIS project. Section 5 concludes the study and highlights future research.

II. System Architecture of a DS

Transition from modern to digital substation involves the replacement of conventional devices with process interfaces in additon to replacing most of hardwired copper connections in the substation with process bus technology [8], as shown in Figure 1. Due to the scope of our project, we focus on the part of the DS which covers the process bay and station levels. Physical infrastructure components as shown in Figure 2, in process level are CT, VT, MU, breakers, sensors, etc. and cyber infrastructure includes communication network, IEDs, switches, software (e.g. SCADA system) and hardware in the station level. Functionality description of each component in a DS are listed below.

Communications The types of communication devices and networks used in DS are:

- **Gateway** is a network device that allows data to flow from one network to another.
- **Switch** is a network device that is used for switching packets to receive and forward data to the destination devices.
- **WAN** is the network which is accessible through the gateway.

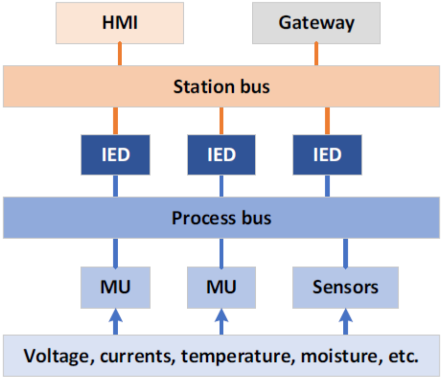

Fig. 2. Communication structure of an IEC 61850 substation.

- **Process and Station Buses** in a DS, Client/Server communication is used between IEDs and SCADA system via the station bus. The technology used for this communication is defined in IEC 61850-8-1 as MMS. The communication between switchyard and relay house is also through optical fiber, using IEC 61850 process bus.
- **LAN/Ethernet** is the local network in DS. Certain services e.g. remote access solutions are available through this network.

HMI is the graphical interface between the human operator and the controller (all the physical devices) of an industrial system for interaction and communication between them.

SCADA is a centralized system used for monitoring and controlling of a plant. It is a supervisory system for gathering data about industrial processes and sending commands for controlling.

IED is microprocessor-based device that is used by the electric power industry to control power system switching devices.

MU is a device that enables the implementation of an IEC61850 process bus by converting the analog signals from the conventional CT/VT into IEC61850 SVs for metering, protection, and control purposes.

CT/VT are devices that constantly interact with physical environment and communicates with the controller via a shared process bus.

These components are vulnerable to cyber threats and are required to be secured in order to prevent, mitigate, and handle cyber-attacks [9] to ensure power system's availability and preserve reliability.

III. Common Types of Cyber-Attacks on a DS

While the DS structure from different vendors may vary in automation level and security concerns (e.g. unauthorized access), the below lists a set of common cyber threats:

- **DoS attack**: The attacker tries to make the network inaccessible to the intended users by flooding the network with traffic. The attacker can achieve this by:
  - buffer overflow attacks: sending more traffic to the server than what it can handle.

This is the accepted version of an article published in 2020 9th Mediterranean Conference on Embedded Computing (MECO)
http://dx.doi.org/10.1109/MECO49872.2020.9134350

"© 2020 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works."

- **Communication network attacks**: These networks are vulnerable and required to be secured from threats. Weak firewall, network design, and component configurations can make the system insecure. Once a system is connected to WAN using TCP/IP transport layer networking, a user on any other system on the network, regardless of how many other computers are between them, could potentially gain access to the target system [5].
  - **Scanning ports and network monitoring**: The attacker scan the network and devices such as switches, IEDs, relays, and SCADA system to find open ports to gain access to the substation.
  - **Intrusion into the local network**: The attacker impacts HMI/SCADA systems by:
    - accessing SCADA console in administrative-level that are protected only by login ID/password.
    - accessing confidential information,
    - accessing sensory data,
    - sending false command to control the network and the electronic equipment (relays, IED, etc.),
    - false-data injection,
    - memory corruption and accessing data from the memory,
    - user credential management or modifying ID/password files.

  Depending on the system design and the OS of the servers, the results of these attacks might be the loss of a particular component or it could spread across the whole system.
- **Malware injection**: The attacker injects malicious software such as ransomware and worms into the software components of DS. Such malicious software can easily penetrate into local network.
- **Intrusion into the physical site**: An engineer or a technical staff with malicious purposes intrude into the DS as follows:
  - connecting a mobile device to Internet carried by a personnel,
  - injecting infected USB or laptop,
  - information distortion,
  - controlling devices manually,
  - controlling functionality of devices.
- **Spoofing attack**: The attacker or malicious program acts on behalf of another person/device to perform actions in the system or gain access to sensitive data.
- **MitM attack**: The attacker gains unauthorized access on communication network or between sensors and controllers by spoofing SV stream, MMS, and GOOSE messages which will cause failure or undesirable operations in the system.
- **Human-factor based attacks**: In order to secure a DS, the personnel who are allowed to enter the physical substation (plant manager and engineers) should be authorized and have limited role-based access to the components in accordance to their levels of authority. However, an employee may have several roles which will lead to vulnerabilities in the DS. Assigning multiple roles to the same person often ends up with a permission mix that could give unintended authorized access, either through combination of permissions across roles or due to being assigned a role with more permissions than needed. An employee might disable or damage the cyber or physical system by *accidental action* or *intentional action* referred as an "inside job". These actions might happen by former employees of vendors with potentially dangerous knowledge as well.

A. An attack scenario in DS

The purpose of a cyber-attack on a SCADA system could range from hackers trying to prove they can get through a system's defenses to cause damage to components. Possibly someone might set up an attack for espionage industrial purposes or to generate "false" information to the SCADA system [5]. The most serious threats are those that intend to either seriously disable the system (which could include generating false data so that operators are unaware of problems developing) or those attempting to take control of the system to cause damage to the process or equipment by sending out improper control commands [10].

IV. Cyber-Attack Map for a Pilot DS

In Figure 3, we provide a cyber-attack map based on the DS architecture for our pilots. An attacker may scan the network to find open ports, listen to the network traffic, access sensory data, stop/change the functionality, reprogram devices, and gain access to devices' memory. These attacks require high-level access and a fair degree of system knowledge and expertise. Below, we explain component-wise vulnerabilities and map the common cyber-attacks to DS, pointing where and how attacks can happen.

- **Communication Network** An attacker may find and exploit vulnerabilities in the communication networks in the form of listening to network traffic, falsifying communication data (MitM) and via DoS attack.
- **Switch** An attacker may control switches on either of the buses, manipulate switch traffic, and/or connect infected device through USB/Test-Set.
- **HMI/SCADA** An attacker may inject malware to the SCADA system. In most cases, the attacker would need to gain access to credentials and login to gain access to the SCADA system. If the attacker gains access, it could be possible to take control of the system, manipulate SCADA software, stop functionailities, access data on servers and sensory data.
- **IEDs** An attacker may gain access to an IED by obtaining login credentials. If so, the attacker may reprogram IED, access data on IED, and/or stop/change device functionalities.
- **MUs** An attacker might gain access to a MU device, manipulate analog data received from NCIT, and/or stop and/or control functionality.

This is the accepted version of an article published in 2020 9th Mediterranean Conference on Embedded Computing (MECO)
http://dx.doi.org/10.1109/MECO49872.2020.9134350

"© 2020 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works."

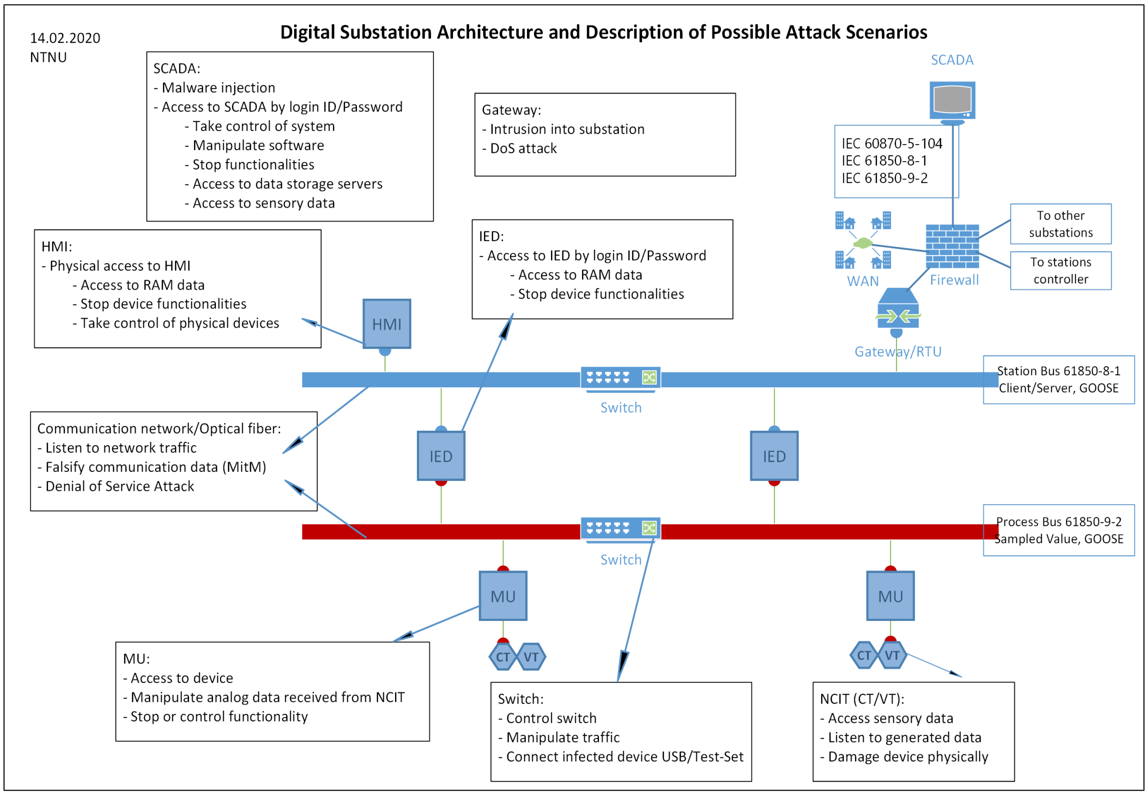
14.02.2020
NTNU
Digital Substation Architecture and Description of Possible Attack Scenarios
SCADA:
- Malware injection
- Access to SCADA by login ID/Password
- Take control of system
- Manipulate software
- Stop functionalities
- Access to data storage servers
- Access to sensory data
Gateway:
- Intrusion into substation
- DoS attack
SCADA
IEC 60870-5-104
IEC 61850-8-1
IEC 61850-9-2
To other substations
To stations controller
WAN
Firewall
Gateway/RTU
HMI:
- Physical access to HMI
- Access to RAM data
- Stop device functionalities
- Take control of physical devices
HMI
IED:
- Access to IED by login ID/Password
- Access to RAM data
- Stop device functionalities
Switch
Station Bus 61850-8-1
Client/Server, GOOSE
Communication network/Optical fiber:
- Listen to network traffic
- Falsify communication data (MitM)
- Denial of Service Attack
IED
IED
Switch
Process Bus 61850-9-2
Sampled Value, GOOSE
MU
MU
CT
VT
CT
VT
MU:
- Access to device
- Manipulate analog data received from NCIT
- Stop or control functionality
Switch:
- Control switch
- Manipulate traffic
- Connect infected device USB/Test-Set
NCIT (CT/VT):
- Access sensory data
- Listen to generated data
- Damage device physically

Fig. 3. The component-wise map of potential cyber-attacks to Digital Substation.

- **Physical Devices (CT/VT)** An attacker might gain access to sensory data, listen to measured values, and/or damage device physically. The impact of an attack could range from impacting sensors by sending corrupted measurements (e.g., sensor spoofing) or cause minor disruptions in performance to a complete takeover of the system. Sensors are also vulnerable to physical attacks.

V. Conclusion and Future Work

In this paper, we have discussed potential cyber-attacks to DS and provided a component-wise map of cyber-attacks to DS pilots in ECODIS project. The digital substation is based on the IEC 61850 standard where MUs digitize analog data coming from sensors, CT/VT. Then digital data is conveyed further to IEDs through the process bus. Furthermore, data is transferred from IEDs into the station bus and from there, data is utilized by local HMIs and the SCADA system. Access to SCADA requires passing through the gateway, otherwise, it is likely to attack DS via any of the mentioned components e.g. MU, IED, buses, switches, etc.

Our literature review resulted in the common cyber-attack types listed and explained in Section 2. We have also provided an attack scenario in DS. Our conclusion regarding the second research question is that each of the components in DS e.g. HMIs, SCADA, IED, Sensor, and MUs can become access points for cyber-attacks. Conclusively, even though using firewalls and/or encryption solves the cyber-attack problem partially, they are not the sole solutions and still attacks are possible. As future work, we will study asset management for DS and simulate cyber-attack scenarios to evaluate their consequences in DS.

References

[1] R. Loken and N. Hurzuk, L. Stensrud, B. Ohrn, F. Simensen and et al., *Experience with process bus in Statnett R&D project Digital substation*, CIGRE, 2018.

[2] L. Stensrud, B. Ohrn, R.S. Loken, N. Hurzuk, A. Apostolov, Testing of Intelligent Electronic Device (IED) in a digital substation. The Journal of Engineering, 2018(15), pp. 900-3, 2018.

[3] Engineering and Condition Monitoring of Digital Substations (ECODIS), available online: https://www.sintef.no/en/projects/ecodis/.

[4] A. Klien, *New approach for detecting cyber intrusions in IEC 61850 substations*, OMICRON electronics GmbH, Austria, 2019.

[5] W. T. Shaw, *SCADA System Vulnerabilities to Cyber Attack*, Electric Energy T&D Magazine FRÉDÉRIC ALLARD, 2004.

[6] R. Ivanov, M. Pajic, I. Lee, *Attack-resilient sensor fusion for safety-critical cyber-physical systems*, ACM Transactions on Embedded Computing Systems (TECS), vol. 15(1), pp. 1-24, 2016.

[7] K. Bernsmed, M. G. Jaatun, C. Frøystad, *Is a Smarter Grid Also Riskier?*, In International Workshop on Security and Trust Management, pp. 36-52, Springer, Cham, 2019.

[8] M. G. Jaatun, M. E. G. Moe, M. Istad, *Cybersikkerhet i digitale tansformator-stasjoner, Forprosjekt*, 2019.

[9] S. Sridhar, A. Hahn, M. Govindarasu, *Cyber–physical system security for the electric power grid*, Proceedings of the IEEE, vol. 100(1), pp. 210-224, 2012.

[10] N. Moreira, E. Molina, J. Lazaro, E. Jacob, A. Astarloa, *Cyber-security in substation automation systems*, Renewable and Sustainable Energy Reviews, vol. 54, pp. 1552-62, 2016.

This is the accepted version of an article published in 2020 9th Mediterranean Conference on Embedded Computing (MECO)
http://dx.doi.org/10.1109/MECO49872.2020.9134350