Master's thesis

NTNU
Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Dept. of Information Security and Communication Technology

Iver Hesby Hurum

ABAC for Power Grid Substation Systems and Equipment

Master's thesis in Information Security
Supervisor: Siv Hilde Houmb
Co-supervisor: André Jung Waltoft-Olsen
June 2022

NTNU
Norwegian University of Science and Technology

Iver Hesby Hurum

ABAC for Power Grid Substation Systems and Equipment

Master's thesis in Information Security
Supervisor: Siv Hilde Houmb
Co-supervisor: André Jung Waltoft-Olsen
June 2022

Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Dept. of Information Security and Communication Technology

NTNU
Norwegian University of
Science and Technology

ABAC for Power Grid Substation Systems and Equipment

Iver Hesby Hurum

Supervised by
Siv Hilde Houmb
and André Jung Waltoft-Olsen

Norwegian University of
Science and Technology

Master Thesis
Master in Information Security
iverhh@ntnu.no
30 ECTS
Department of Information Security and Communication Technology
NTNU Gjøvik, 2022

Avdeling for informasjonssikerhet
og kommunikasjonsteknologi
NTNU Gjøvik
Postboks 191
2802 Gjøvik
Norge

Department of Information Security
and Communication Technology
NTNU Gjøvik
Box 191
N-2802 Gjøvik
Norway

Abstract

OT devices, like the ones found in Substation Automation Systems (SAS), were originally not designed with online security in mind. Connecting Industrial Control Systems (ICS) to the Internet gives the flexibility of monitoring, performing maintenance and controlling legacy devices remotely. Unfortunately, this introduces some security concerns, as SAS gets exposed to new vulnerabilities. According to security companies in this field of research, uncontrolled access to ICS is the greatest vulnerability in OT systems.

Statnett is the responsible system operator of the Norwegian power grid and is dependent on a secure day-to-day operation. In their current access control, an actor who is authenticated by the system, can acquire all rights to all protected resources, at every hour of the day, and even during emergencies.

In this project, we propose an ABAC solution that enforces a granular access policy in power grid SAS and equipment, which determines which subjects are authorized to access which resources, and what actions they can perform under some given environment conditions. ABAC is the next generation of access control because it is situational aware, but it has not gained a foothold in the research community yet. Our new results focus on how to implement an ABAC solution in ICS and how it can be configured to meet the security requirements of Statnett's SAS.

Sammendrag

OT enheter, slik man finner i transformatorautomatiseringssystemer (SAS), var opprinnelig ikke designet med sikkerhet i tankene. Ved å koble industrielle kontrollsystemer (ICS) til Internett får man fleksibilitet til å monitorere, utføre vedlikehold og kontrollere disse enhetene fjernstyrt. Uheldigvis introduserer dette nye sikkerhetsbekymringer, fordi SAS dermed blir eksponert for nye sårbarheter. I følge sikkehetseksperter innen dette forskningsområdet, er ukontrollert tilgang til ICS den største sårbarheten i OT systemer.

Statnett er den ansvarlige driftsaktøren for det norske kraftnettet og er helt avhengige av en sikker drift i det daglige. I deres nåværende aksesskontroll, kan en aktør som har blitt autentisert av deres system innhente alle tilgjengelige rettigheter over de beskyttede ressursene, samt få det til dette til alle døgnets tider, selv under krisesituasjoner.

I dette prosjektet foreslår vi en ABAC-løsning som pålegger granulære retningslinjer for aksess i kraftsystemene, som bestemmer hvilke subjekter som er autorisert til å aksessere hvilke ressurser, og hvilke handlinger de kan utføre under hvilke situasjoner. ABAC er nestegenerasjons aksesskontroll fordi den er situasjonsbevisst, men det har ikke blitt anvendt i noe særlig grad innen forskningsmiljøet ennå. Våre nye resultater fokuserer derfor på hvordan man kan implementere en ABAC-løsning for ICS og hvordan denne kan bli tilpasset til å møte sikkerhetskravene hos Statnett sine SAS.

Acknowledgements

First and foremost, I would like to express my deepest appreciation to my supervisor Siv Hilde Houmb for her outstanding guidance, patience and feedback sessions during this project. Without her, I would not have been able to get this thorough understanding of the power grid industry, nor had the necessary skills to carry out this project.

Special thanks must also be directed to André Jung Waltoft-Olsen for being an excellent co-supervisor on this project. His proof-reading, critical questions and cheerful mood has really helped me during this project, and it has been a pleasure working with him.

Lastly, I would like to acknowledge the core stakeholders in Statnett that took their time off to participate in my interview sessions. Your contribution helped me to achieve more credible results.

Contents

List of Figures

1 Introduction

This chapter contains what topic is covered by the project, a problem description, justifications and motivation, research questions and the planned contributions of the Master thesis.

1.1 Topic Covered By the Project

Statnett is a state-owned association that is responsible for building, operating and maintaining the Norwegian power grid [6]. They manage over 11000 km of high-voltage power lines, 166 substations and 1400 km of land- and underwater cables that is interconnected to Sweden, Denmark, Finland, Russia, Germany, the Netherlands and United Kingdom [A][7]. Equipment found in the switchyard in the substations plays essential roles in the power distribution. Interruption of substation operation, e.g. a cyber attack, can result in a total blackout in a community. A recent example of unauthorized power grid access took place in Kiev in 2015, causing 230.000 inhabitants to be left with no power [8].

In order to enhance the security of Statnett's substation automation systems and equipment, this project aims to propose an implementation of Attribute-Based Access Control (ABAC) on their systems, as well as substations in general. ABAC is an authorization mechanism that determines which attributes the *subjects* must have in order to access which *resources*, and what *actions* they can perform under which *environment* conditions. Any subject that wants to access the substation automation systems and equipment must have their access request evaluated by an authorization engine. Only if the request is permitted by the authorization engine, the subject will be allowed to perform the requested action on the resource in question.

1.2 Keywords

CCS Concepts [9]:

- **Security and privacy** → **Security services**; *Access control, authorization*
- **Security and privacy** → **Systems security**; *File system security, information flow control*
- **Computer systems organization** → **Real-time systems**; *Real-time operating systems*
- **Applied computing** → Enterprise computing; *IT architecture*

Additional keywords

ABAC, substation automation systems, authorization, XACML, ALFA

1.3 Problem Description

Operational Technology (OT) systems were originally designed to run in isolated environments [10]. Industrial Control Systems (ICS) were responsible for monitoring, maintaining and controlling the industrial process in the OT systems. By connecting the ICS to the Internet makes it more flexible for operators to control the industrial process remotely. Since OT systems run on legacy software, connecting them to the Internet introduces new

vulnerabilities. According to Kaspersky and Checkpoint [11][12], uncontrolled access to ICS is the greatest vulnerability in OT systems. Hence, the security standard IEC 62351 requires Role-Based Access Control (RBAC) to be applied as an authorization mechanism on substations.

Today's problem on Statnett's substations, is that an operator can establish a remote access to the ICS to perform some actions, but there is no existing security mechanism that restricts the access. Therefore, once an operator have obtained access to the system, they have acquired all available system rights. Regardless of time of day, the remote access can be initiated whenever an operator decides, even during emergency situations.

1.4 Justification, Motivation and Benefits

The problem described in Section 1.3 is a security concern because no one should be able to obtain all available rights over a protected resource. For instance, if an operator in Statnett just needs to read the the current power output on a distribution line on the substation for monitoring purposes, the operator should not be able to perform other types of actions on the system, e.g. performing line switching in the switching yard. Additionally, should the operator be able to establish a remote connection to the automation system outside working hours or during an emergency situation? This problem needs to be addressed in order to lower the risk of uncontrolled access in Statnett's substation automation systems (SAS).

Yalcinkaya et al. have already identified the security concerns of connecting ICS to the Internet [13]. Exactly how they have implemented and configured the ABAC system with some test cases have *not* been described in detail. However, this project will focus more on the holistic implementation and application of the ABAC system, which will help the research field to reproduce this thesis' results in a similar industrial environment. The primary stakeholders for this project are Statnett and NTNU. To the best of our knowledge, research covering access control for ICS is insufficient to solve our problems. Therefore, the stakeholder's main benefit is the research contribution to closing the literature gap by proposing how the next generation of access control can improve security in critical infrastructures.

The overall Return On Investment (ROI) of this project is considered as high because the ABAC solution has to be custom made with access policies to function in Statnett's substations. In other words, this project applies Statnett's use cases to concretize an ABAC solution, but the produced results can also be generalized to fit other Transmission System Operators (TSOs) and Distribution System Operators (DSOs). More information about the ABAC solution is specified in Section 4.5.

1.5 Research Questions

This Master thesis aims to discuss and find answers to the following research questions:

1. Why is RBAC not sufficient in power grid systems even though it is a requirement from IEC 62351?
2. What are the use cases where Statnett need access control?
3. How can we propose an ABAC solution for Statnett's substation automation systems and equipment? How can the solution be generalized to provide value to other TSOs and DSOs?

1.6 Planned Contributions

In accordance with the research questions 1-3, this Master thesis aims to propose an ABAC solution based on the use cases where Statnett needs access control. The *new* results produced from this thesis are the actual implementation of the ABAC solution, as there are no current guide or existing solution that describes the technical aspects of such a solution. As briefly touched in Section 1.4, Yalcinkaya et al. [13] have already identified the problem, but does not go into the technical details of how to implement the ABAC solution [13]. NIST's guide to ABAC only contains definitions and considerations to an enterprise, yet does not discuss the technical aspects either [14]. The lack of reproducibility in the above-mentioned reports enforces this thesis to focus on the technical implementation aspects, as well as developing custom access control policies to the use cases in question.

Other planned contributions involves literature studies on substation systems, IEC 60870-5-104, IEC 61850 and IEC 62351, in accordance with the task description [A].

2 Background

This chapter explains what a power grid substation is, what equipment can be found there, and how they are networked to provide power to the consumers. The chapter also conducts literature studies of relevant substation standards and protocols, as well as highlighting the key differences between various information security access control models.

2.1 Substation Systems

A high voltage transformation station, or *substation*, is an electric installation that interconnects transmission and distribution lines [1]. Transmission lines are high voltage lines that originates from a power station, where electricity is generated. Since energy generation usually takes place far away from end consumers, the electricity is transferred at high voltages, up to 420 kV in overhead lines, to reduce energy loss [15]. One of the main purposes of a substation is to step down the voltage from one level to another, to ultimately make the electricity usable for industries and homes. We differ between Transmission System Operators (TSO) and Distribution System Operators (DSO). In regards to the Norwegian power grid system, Statnett acts as the only TSO, whereas Hafslund, Elvia, Fjordkraft, etc. functions as DSOs.

Voltage transformation happens in multiple stages: From the power station to the TSO (high voltage), between the TSO and DSO (middle voltage), between the DSO and the directly connected end consumer (low voltage). The DSO is normally stationed in close proximity to the end consumer. Figure 1 illustrates this supply chain.

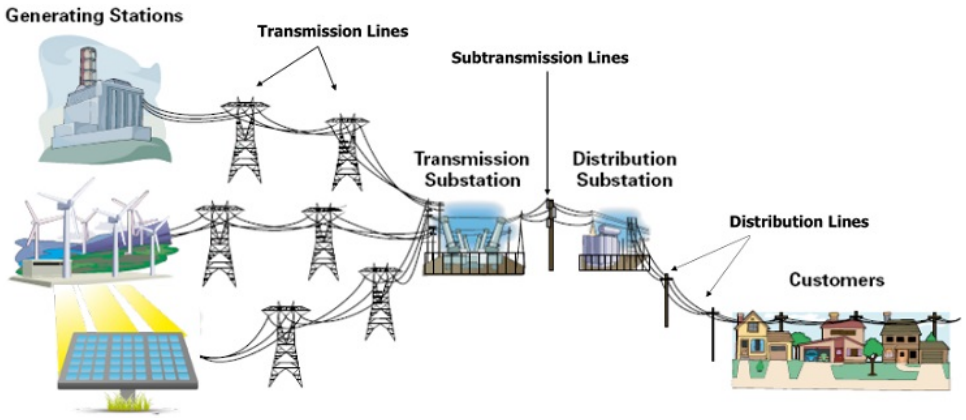


Figure 1: Supply chain and voltage step-down [1].

A substation can also be constructed to work as a switching station [16]. Their purpose is to connect and disconnect transmission lines in the power grid utility system. A switching substation serves as junction point where several individual transmission lines congregates. Not all transmission lines have to be connected to the power grid at the same. Depending on the total power draw of the power grid utility system, transmission

lines can be connected or disconnected by line switching in order to meet the current power flow requirements. A switching substation is also ensuring redundancy when an incident occurs, e.g. a tree that is falling over a power line causing regional outage. By simply connecting another transmission line to the affected region, the inhabitants and power consumers will still have electricity available. Simultaneously, maintenance crew can be assured that the affected power line is physically disconnected when trying to repair the damages. The act of power line switching can be done in two ways: manually and physically by a substation operator, or automatically through SAS.

2.1.1 SAS

Voltage step-down and line switching are the primary operations on a substation. These operations can be controlled through secondary substation components, called substation automation systems (SAS). SAS are dedicated software that is running on Intelligent Electronic Devices (IEDs) [16]. The IEDs are hardware components found in the substation's main control facility building that are used to send and receive signals to the primary installations in the substation, e.g. the switchyard and the voltage transformers (ref. Section 2.1.2). In other words, via the interface of the IEDs, SAS manages the data acquisition process; monitoring and control; and various alarming functions related to the primary high voltage equipment. Controlling and monitoring the substation is taken care of by an operator through a graphical interface in the control facility building, or by a remote SCADA operator. Section 2.1.3 describes in detail how a substation is remotely controlled.

2.1.2 Substation Equipment

A substation may be divided into three individual logical levels where different equipment and interfaces can be found, namely the switchyard-, bay- and station level [16]. The following overview describes what equipment and which processes that are located on each level:

Switchyard level

The primary equipment on a TSO substation refers to the high voltage apparatus operating from 52 kV and above, such as [1][16]:

1. Switching gear
   - Circuit breakers
   - High voltage fuses
   - Disconnectors
   - Earthing switches
2. Instrument transformers
   - Voltage transformers
   - Current transformers
3. Power transformers

Bay level

The bay level is defined as the intervening site between the switchyard and the small control room located in the switchyard (must not be confused with the main control facility

building outside of the switchyard) [1][16]. Data transfers between the switchyard level and the bay level is managed by Merging Units (MU's) or IED's for monitoring and operational purposes. This data transfer can be referred to as the *process bus*. MUs measure analogue data from the primary equipment and converts it a binary data representation, whereas IED's are the modern way of sending and receiving signals on a modernized and digital substation, standardized by the communication protocol IEC 61850 [17]. More information about IEC 61850 is found in Section 2.2.2. A rundown of the various equipment found on the bay level are listed as follows:

1. Switching transients
   - Operation of disconnector
   - Operation of circuit breaker
2. Lightning protection
   - Lightning arresters
3. Earthing systems
4. Measures to reduce electromagnetic effects
5. Switchyard control room
6. The Bay Controller (BC)
7. Intelligent Electronic Devices (IEDs)
8. Process bus to communicate with the switchyard level

Station level

A substation is controlled and monitored on the station level [16]. This is where we find the main control house of the substation. The main control house is located outside of the high voltage switchyard, but inside of the fenced substation facility. Inside the building, in the control room, we find a Human-Machine Interface (HMI). The HMI is the master work place of the local substation operators, where they can perform line switching, monitoring or other SAS control operations. The HMI is therefore a physical installation that consists of hardware and software components.

A Station Controller (SC) is also present in the control room. This is an industrial computer or IED that works as the central processor of the substation, supplementing functionality and coordination of the Bay Controllers (BCs). A station LAN serves Ethernet connectivity throughout the main control building, as well as ensuring time synchronization between substation equipment. The Station Controller is connected to the HMI and participates in the logic of switching transmission lines in the switchyard. Since the Station Controller is one of the most vital IEDs on the substation, its configuration is usually duplicated to a standby station controller to provide redundancy and strengthen the availability. As operations of substations are gradually starting to become more digitized and centrally operated, remote access the local HMI and the industrial systems must be accommodated.

2.1.3 Remote Substation Access

Substations can be remotely controlled by a control center when equipped with Supervisory Control and Data Acquisition (SCADA) systems [16]. The Station Controller, Remote Terminal Units (RTUs) and various IEDs on a substation works as *slave devices* as they are sending and receiving signals to the remote *master* control center through IP based fiber optic communication. Statnett has regional control centers that follows this master / slave relationship. The master control center allows a SCADA operator to perform switchgear operations, conduct measurements of gauging instruments, event handling and alarming on the substations in the given control domain. The IP communication between the substation and the control center follows the standard OSI reference model for data transfers. This automation concept is therefore based on four hierarchical and logical levels:

1. The remote control level
2. The station level
3. The bay level
4. The process level

The communication between each logical level is managed by IEDs.

A SCADA or maintenance operator achieves remote access by connecting to the interface of the substation's gateway by utilizing a Privileged Access Management (PAM) solution [18][19]. The PAM solution provides a secure connection to the substation's critical industrial control systems (ICS). Since substations are configured individually by different system vendors, and IEDs are configured in Substation Configuration Language (SCL), the substation gateway needs to perform a protocol conversion to be able to communicate with the remote control center [16]. The gateway is located at the station level, managed my the Station Controller's CPU.

In terms of Statnett's digital substations, normal SCADA operations and external maintenance crew can connect to the ICS on the substation through their PAM solution, illustrated by Figure 2:

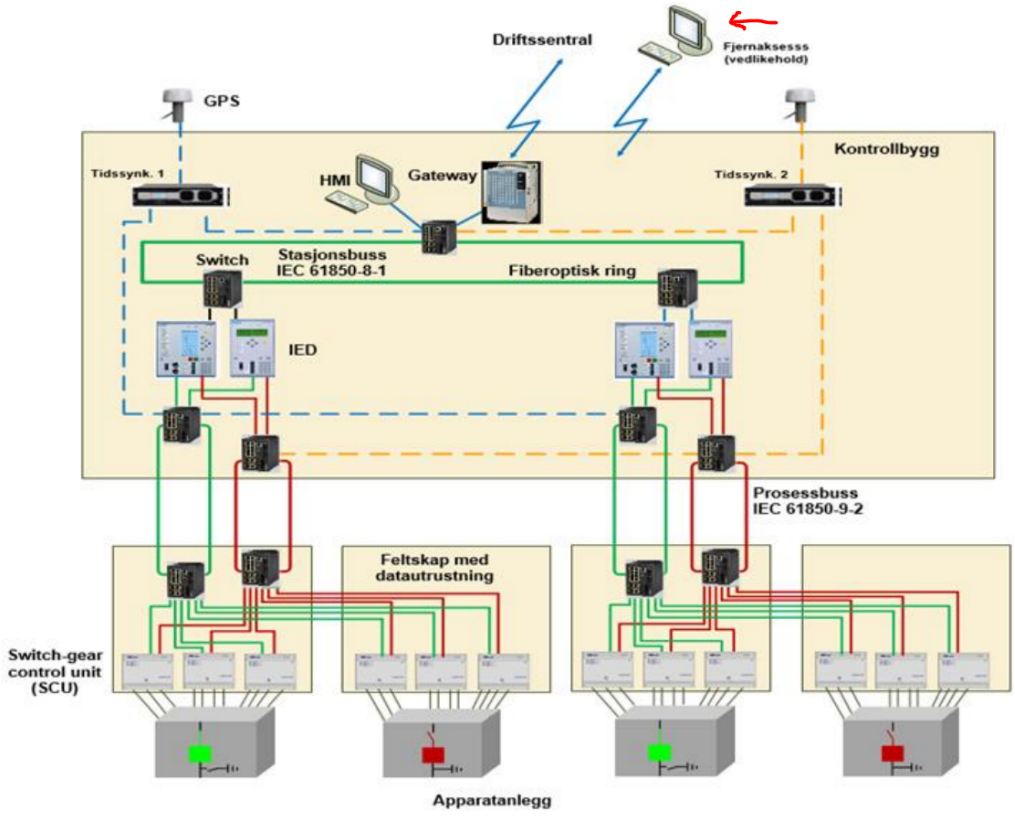


Figure 2: Illustration of the SAS model of Statnett [2]. The red arrow is drawn by the author of this thesis and highlights the remote substation access.

2.2 Literature Studies of Relevant Standards

This section studies how TCP/IP based communication can be enabled between a remote control station and a substation in IEC 60870-5-104, and how automation systems can be implemented to increase efficiency in IEC 61850. Ultimately, IEC 62351 defines how the activities from the standards above should be secured in order to achieve cyber resilience on substations.

2.2.1 IEC 60870-5-104

IEC 60870-5-104 (IEC 104) is a network transmission protocol that supplements the underlying IEC 60870-5-101 (IEC 101) standard [20]. These standards are both *companion standards* of part 5 of IEC 60870, which specifies how telecontrol messages can be sent between two electrical power systems [21]. Companion standards are standards that are cross-referencing each other. In short, IEC 101 describes how monitoring and control functions can be supported between a substation and a remote control center (SCADA) over a serial connection. The purpose is to automate the monitoring and basic control functions on the substation. IEC 104 defines how IEC 101 can be extended with standard communication profiles over an Ethernet connection (TCP / IP network, or Point-to-Point link) [22][23]. It specifies how the OSI referencing layers L1 to L4 should be utilized to enable full network access. The complete network access is used between the substation IEDs, gateway and RTU, to the remote control center, and ensures a connection-oriented

data transmission over TCP. IEC 104 is based on the master / slave principle, where the particular substation acts as the slave. Whereas fiber optic LANs are configured on substations, the communication with the remote control center is through WAN. With complete network access between a substation and a remote control center, several other substation functions can be automated: alarming, event logging, remote maintenance, HMI interface, etc.

2.2.2 IEC 61850

IEC 61850 is a communication standard that specifies how information should be transferred between different substation equipment on a given substation, e.g. IEDs and protection devices, or to the remote control center. Several parts of the standard, also called *publications*, have been added since its release in 2003. Nowadays, there are 26 active parts in the standard [24]. The purpose of the standard is to avoid proprietary communication protocols, which means that a vendor of substation equipment should not have their own way of implementing substation automation systems. IEDs from one vendor must be able to work with IEDs from another vendor. Complying to IEC 61850 makes it more convenient for engineers and system vendors to have the running substation configuration up to date, as well as ensuring seamless interoperability between the equipment.

Besides the purpose of preventing vendor lock-in, the standard focuses heavily on reliability and availability [16]. A substation must be able to operate in a normal manner even if some SAS components fails. This implies that critical SAS components must have redundancy, most preferably configured by the "hot-hot" and "hot-standby" principle. In other words, if an essential SAS component fails, the standby component has to resume the operation without service disruption. Additionally, if an emergency occurs, it must be possible to override interlocking SAS components manually by the substation operator.

Real-time communication

The standard specifies that communication between substation automation systems must have no more latency than 3 ms [16][24]. Since TCP / IP based communication tends to take more time than this, three other protocols have been established to serve this purpose. Each protocol works at their own logical level on the substation:

1. MMS (Manufacturing Message Specification)
   - Used on the *station level*.
   - Operates between the remote controlled SCADA system, the gateway and the IEDs.
   - Works by the master / slave principle, where the database in the SCADA system tries to replicate the current real-world from the reporting substations.
   - The MMS service is considered to transmit medium important information.
2. GOOSE (Generic Object-Oriented Substation Event)
   - Used on the *bay level*.
   - Operates between multiple IEDs on the process bus in order to distribute critical information quickly among them, such as status of switchgear or control commands.

- Each IED has its own local buffer to correctly process the information it is receiving by the GOOSE protocol.
- Works by the master / slave principle.

3. SV (Sampled Values)
   - Used on the *switchyard level*.
   - Ensures swift and reliable communication between the high voltage equipment, such as the voltage- and current transformers.
   - Works by the client / server principle, as merging units (MUs) records an obtained value after measuring high voltage apparatus, then adds the value to its own local buffer, then sends it to an IED on the bay level.
   - The IED on the bay level is the listening device. A time stamp value is passed simultaneously to the IED for packet validation, to ensure the information is up to date.
   - (Digital substations does not utilize analogue MUs anymore. IEDs have therefore replaced them completely at the switchyard level.)

Substation Configuration Language

IEC 61850-6, or part 6 of the standard, defines the programming language for IEDs, called Substation Configuration Language (SCL) [16][17]. SCL is already based on XML, which makes the configuration of substation equipment human friendly to write, as well as quick to compile and run for the IEDs. Another advantage is that SCL ensures interoperability between applications from different external vendors, avoiding IEDs to be programmed in other programming languages. When all vendors are using the same configuration language, the complexity to get all IEDs to communicate together decreases.

The SCL configuration is stored in an SCL file. IEC 61850-7-2 covers that this file determines which real-time communication protocol the particular IED should be using (MMS / GOOSE / SV) by the `Communication` field, and which other IEDs it can communicate with in the `IED` field. The communication between the IEDs works in a similar way as subnets in an enterprise network. Since MMS, GOOSE and SV have different encoding rules, the `Data-type templates` field specifies how the received bit stream should interpreted, e.g. divide the incoming bit stream into 8 bit octets. ASN.1, BER and DER are the current encoding rules used by the established IED communication.

IEC 61850-8-1 specifies in detail how information can be exchanged by using MMS or GOOSE on the logical station bus, whereas IEC 61850-9-2 defines how information should be exchanged using the SV technique.

Conformance tests, substation communication and network guidelines

In order to validate the configured substation automation system, engineers will find how to perform conformance tests in IEC 61850-10. Here, performance parameters are checked to confirm that it is compliant to the 3 ms latency requirement [17].

IEC 61850-90-1 is a guideline for how communication is established across substa-

tions. It complements the information exchange defined in IEC 60870-5-104 (ref. Section 2.2.1).

IEC 61850-90-4 is a network guideline addressing the pros and cons of different network topologies [16]. It also stresses the importance of network redundancy.

2.2.3 IEC 61850 vs IEC 60870-5-104

Even though both IEC 61850 and IEC 104 are communication standards for the same electrical power installations, IEC 104 is more generic and bases its references to the OSI model, whereas IEC 61850 adds more details to the different types communication (MMS / GOOSE / SV) between IEDs and other equipment on the substation. IEC 61850 is about information mapping between IEDs on a local substation, and IEC 104 is about the connection and communication with the remote master control center.

2.2.4 IEC 62351

IEC 62351 is a series of standards that aims to address the lack of security mechanisms in, among others, IEC 104 and the IEC 61850 series. The standard requires that the four central information security principles of *confidentiality*, *integrity*, *availability* and *non-repudiation* (accountability) must be taken care of in order to have a secured end-to-end system [3]. For each information security principle, IEC 62351 proposes security mechanisms and measures that mitigates the risk of compromise, as seen by Figures 3-6:

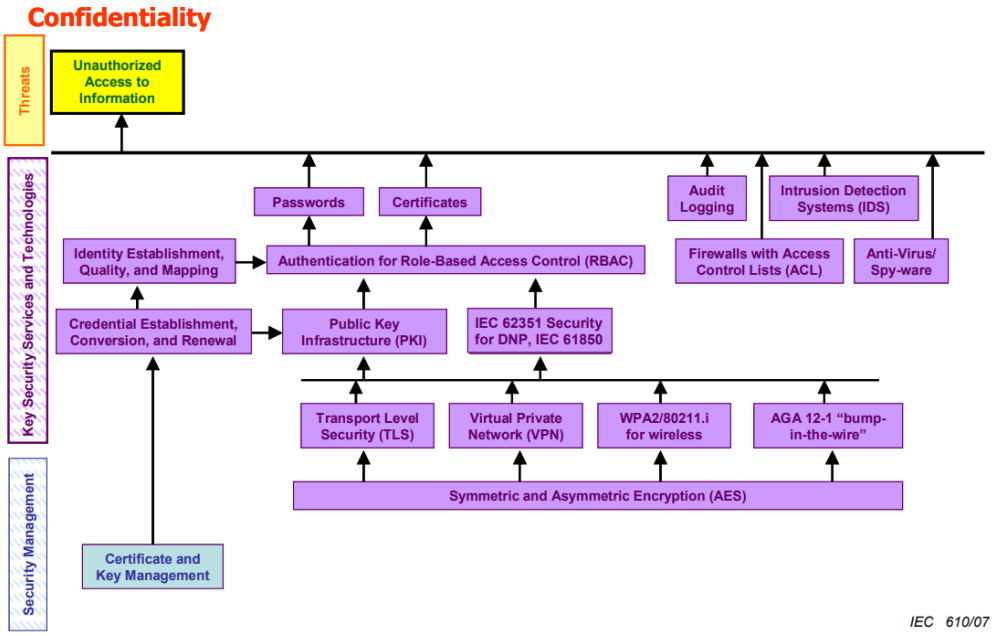


Figure 3: Security measures for confidentiality, IEC 62351-1 [3].

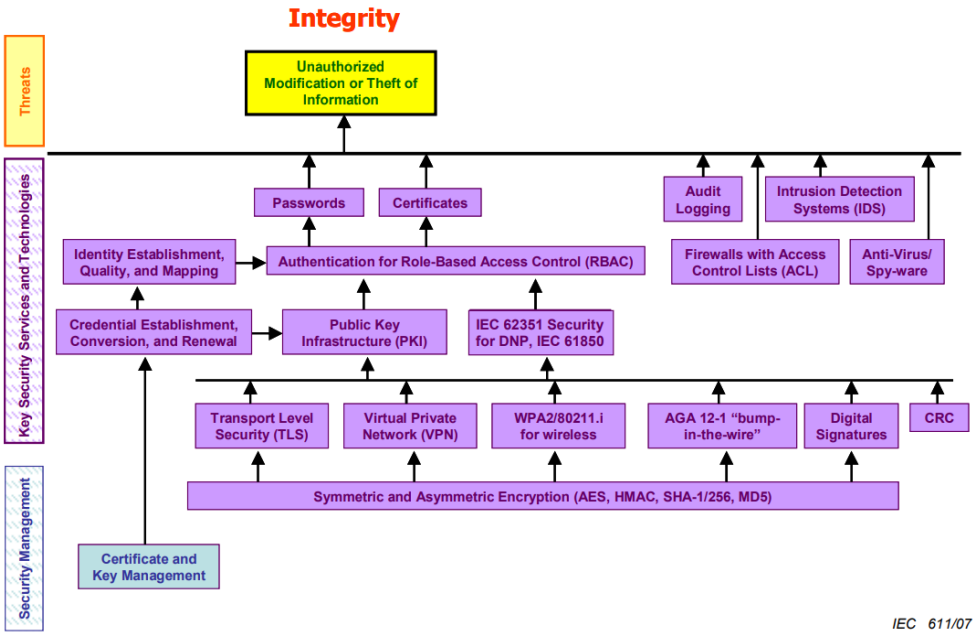


Figure 4: Security measures for integrity, IEC 62351-1 [3].

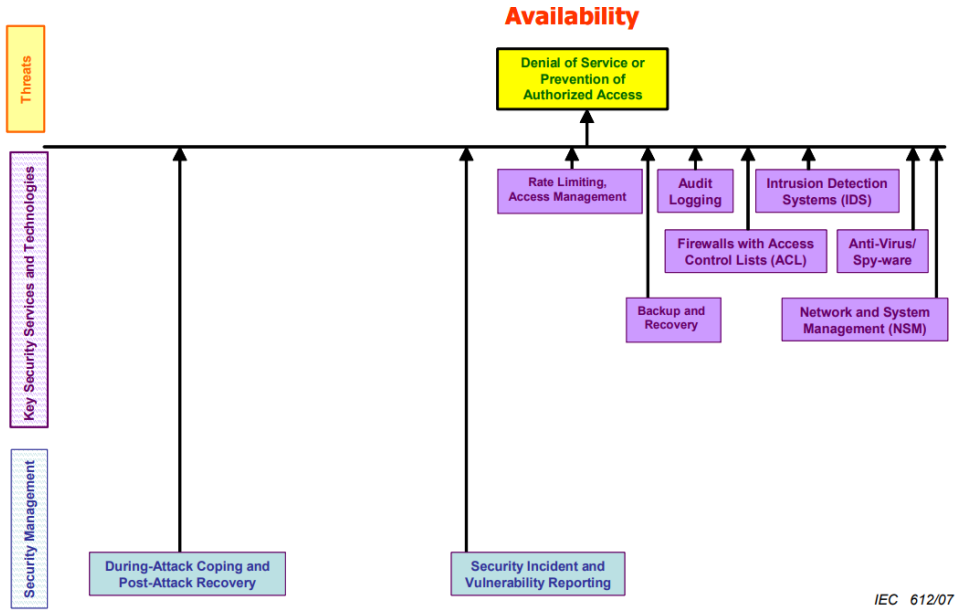


Figure 5: Security measures for availability, IEC 62351-1 [3].

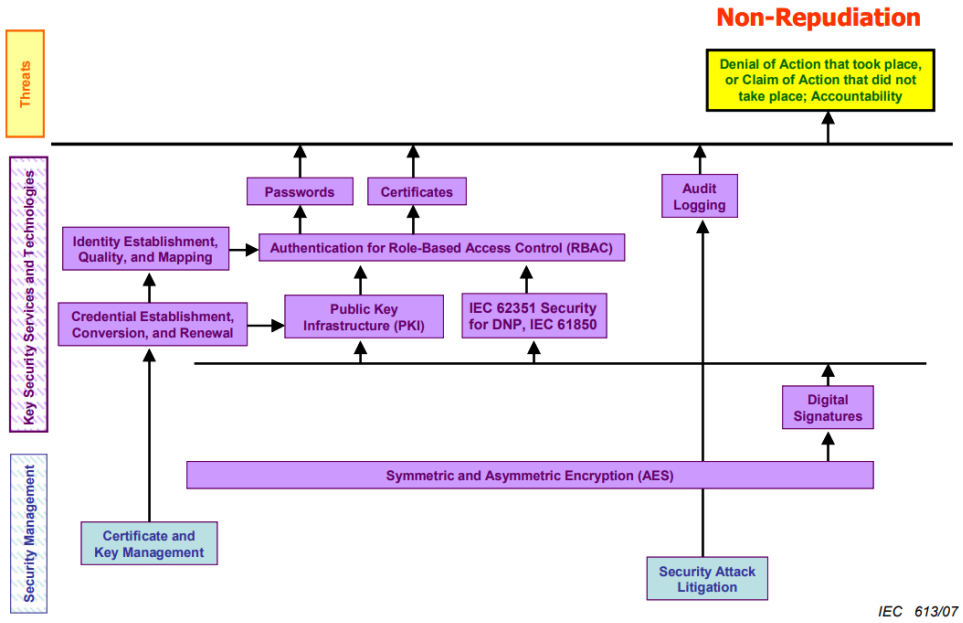


Figure 6: Security measures for non-repudiation, IEC 62351-1 [3].

IEC 62351 emphasizes that not every security measure needs to be implemented for each information security principle to secure the substation communication and data transfers. Careful integration of measures are important to avoid introducing inadvertent problems between the substation equipment. In addition, engineers also need to consider the 3 ms latency requirement (as specified in Section 2.2.2) which means that implementing slow performing security measures, such as encryption methods, might not be doable for all parts of the data transmission chain. Similarly, securing just one information security principle completely is not adequate, as security measures need to be integrated in all principles to achieve end-to-end security.

Part 1 of the security standard then categorizes four focus areas where a substation is particularly vulnerable. Figure 7 illustrates these areas, as well as identifying typical types of attack on each particular area, and which countermeasures that should mitigate potential attacks.

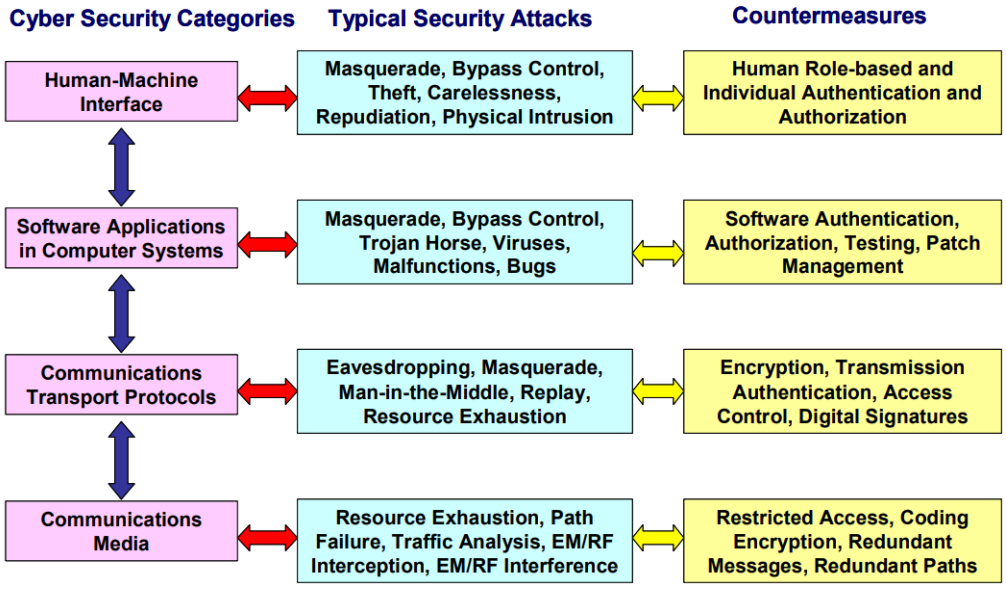


Figure 7: Security categories on a substation, IEC 62351-1 [3].

IEC 62351-2: Glossary of terms

This part of the standard contains a list and brief explanations of the several abbreviations. The glossary used are based on familiar terms within the information security sphere.

IEC 62351-3: Profiles including TCP / IP

Part 3 specifies how the use of TCP / IP transmission protocols provides confidentiality- and integrity protection, and message level authentication for telecontrol protocols and SCADA systems [3]. The scope of this standard is about providing security between devices, or at the very end point of the communication. Part 3 adds protection against Man-in-the-middle attacks, replay attacks and mitigates eavesdropping.

The transmission security is achieved by embracing TLS (or SSL) encryption on the required communication link. Since TLS connections needs to be re-established within some time duration, and the connection between substation devices and end point devices tends to be permanent connections, permanent session keys needs to be considered. This part of the standard specifies how a "permanent" session can be updated seamlessly by utilizing a special mechanism in the X.509 certification exchange.

Part 3 also specifies mandatory *communication profiles*. Communication profiles are pre-determined TLS parameters used for the communication, to allow interoperability. Currently (2018 ed.), only the cipher suite TLS with RSA and SHA-256 hashing is recommended for use. This communication profile applies to IEC 104 and when IP communication is used in IEC 61850.

Although TCP / IP based connection only provides security for OSI layer 4 and lower, and TLS protects OSI layer 5 and above, IEC 62351-3 does not cover application-to-application security (OSI layer 7).

IEC 62351-4: Profiles including MMS and similar payloads

Part 4 specifies communication profiles for transmissions using MMS, at the transport and application layer. This applies to IEC 61850-8-1 [25]. The standard was last revised in 2018 to extend integrity in the TCP and TLS handshake protocols, as well as enhancing the authentication phase.

IEC 62351-5: Security for IEC 60870-5 and derivatives

Part 5 covers security details for serial and network profiles for all parts of IEC 61870-5, but especially aimed at IEC 101 and IEC 104. This standard requires the use of TLS for IP connectivity, and encryption for serial communication. This part aims to protect the principle of confidentiality [3].

IEC 62351-6: Security for IEC 61850

The sixth part of the security standard addresses application security issues for IEC 61850-8-1's GOOSE communication and 61850-9-2's Sampled Values (SV) communication [3]. For applications running these protocols, where the maximum response time is 3 ms, encryption algorithms are not recommended. Instead, the GOOSE or SV applications should transmit information on their own dedicated VLAN's.

If there are special cases where the 3 ms response time requirement is not needed, encryption must be applied. Part 6 provides confidentiality to the system and mitigates replay attacks.

IEC 62351-7: Network and System Management

Part 7 defines abstract Network and System Management (NSM) data object models to monitor the health and conditions for IEDs, RTUs or other important devices in a remote manner [3]. This can be achieved by making use of the Simple Network Management Protocol (SNMP). The NSM data object models provides monitoring for the complementary protocols IEC 61850 and IEC 104. The health of each substation device should be stored in a Management Information Base (MIB). Exactly which solutions of MIB to implement are not specified, but it is expected to utilize one of the existing MIB standards.

This part of the standard protects the information security principle of availability by enhancing the control and monitoring activities.

IEC 62351-8: Role-Based Access Control

Part 8 specifies that Role-Based Access Control (RBAC) must be present in enterprise-wide power systems [3]. RBAC supports a service-oriented or distributed architecture where the overall security is decentralized and all applications are *consumers* of the distributed services. The role of a subject is specified by an "access token", and these access tokens are administered by a federated identity management tool. Each access token should have a defined lifespan, where an authentication process must verify the subject to be issued a renewed access token. Based on the role of the subject, the subject are either permitted or denied access to the requested resource. For each time the subject wants to access a resource, the access token must be verified locally on the substation.

The purpose of the standard is to create a mandatory role hierarchy where individual subjects are assigned, to keep track of all involving actors of the power grid system. Some

pre-defined roles, the use of eXtensible Access Control Markup Language (XACML) to write access policies, and subject-resource permissions are proposed by this part. RBAC policies are stored as XML documents.

Part 8 provides security in terms of authorization, mitigating access from unauthorized personnel.

IEC 62351-9: Key management

Part 9 defines a detailed process of how to manage, create, distribute and revoke Public Key Infrastructure (PKI) certificates and encryption keys to provide protection to information and communication protocols [3]. The standard covers key management methods for asymmetric and symmetric encryption, specified in the companion standards IEC 62351-3 (TLS), IEC 62351-4 (MMS) and IEC 62351-6 (GOOSE and SV) [25]. Asymmetric cryptography are typically used for private keys and issuing of X.509 PKI certificates, whereas symmetric cryptography are most used in session keys between two communicating entities.

Secure storage and distribution of keys increases confidentiality and integrity, as well as acting as a countermeasure to non-repudiation.

IEC 62351-10: Security architecture

Part 10 of the security standard is defined as a technical report that provides guidelines to power system engineers [3]. This part focuses on how to utilize all available standards to securely deploy substation components and secure their interaction.

IEC 62351-11: Security for XML files

Part 11 defines security requirements for exchanging critical XML documents used in IEC 61850 [26]. Furthermore, XML document security involves capabilities like [3]:

1. Header
   - Contains metadata such as date and time of creation.
2. Encapsulation choice
   - Giving the creator of the document a choice of encrypting the file or keeping it in regular plain text format.
3. Access control
   - Determines who is able to access the document, and what their available operations are.
4. Body
   - Contains the actual encapsulated XML document.
5. Signature
   - Digital signature used for authentication and ensuring non-alteration of the document.

IEC 62351-12: Resilience for distributed power systems

Part 12 addresses the information security recommendations in power grid systems to strive for cyber resiliency [3]. Unlike the former parts of the standard, this part does not involve any technical security measures. This part states that a reliable and well-functioning power system relies on a trained operating crew, protective relays and physical perimeter security. The cyber security aspect of substation operation relies on following the best practices for implementation of technical solutions, such as encrypted communication, firewall packet filtration, access controls, etc.

IEC 62351-13: Security guidelines

Part 13 contains guidelines for power grid system developers and engineers to conduct risk assessments, create information security policies, and consider and embed the security requirements from the latter parts of the standard [3]. This part works as a baseline for people outside of the information security field, as there are definitions of what cryptography is, what a wireless- and Internet connection is, what type of security mechanisms can be found on each OSI referencing layer, etc. It is directly aimed at those who are not security experts and acts as a guide to the other technical parts of IEC 62351.

IEC 62351-14: Event logging

Part 14 specifies the importance of event logging, and provides the appropriate details for how to enable this on IED configuration and authentication and authorization processes [26]. This standard helps to avoid system repudiation during an incident by ensuring accountability.

IEC 62351-90-1: Guidelines for handling RBAC

This companion part is an extension of IEC 62351-8 [3]. It provides examples of how XACML can be utilized for access control purposes, since RBAC is a mandatory security requirement. Unlike part 8 that defines seven pre-made standardized roles, part 90-1 defines how custom subject roles can be created. Part 90-1 also addresses special circumstances, such as changing of role during an existing session, and handling synchronous and asynchronous enforcement of RBAC.

These special circumstances only apply when the actual access control is performed locally on an IED, and not as a part of a central authorization solution.

2.3 Access Control Models

This section describes how RBAC and ABAC works, evaluating their pros and cons, as well as briefly touching other access control models.

2.3.1 RBAC

Role-Based Access Control is a security mechanism that provides authorization of users in a system. The purpose of RBAC is to add an intermediate boundary between users and permissions, so that they cannot be accessed directly. By grouping users into different roles, the users within a role have the same authorizations over the resources in the information system [27]. The roles must be instantiated by an administrator in the authorization system *before* assigning the users to a role. The roles in RBAC are usually based on specific job roles and qualifications, organized in a role hierarchy [28]. RBAC is inspired by the Clark-Wilson integrity model, where the separation of duty principle was introduced. The user and group principle has been widely used in Linux operating system.

When a user attempts to access a resource, a user request is created and sent for evaluation by an authorization engine. If the user is belonging to the specific role with permission to the particular resource, the authorization engine grants permission (please refer to the XACML reference model in Figure 9 for more information about the data flow).

Pros and cons

The pros and cons for RBAC is highlighted in the overview below, derived from [3][27][28]:

1. Pros
   - Widely acknowledged.
   - Proposed by IEC standards, e.g. 62351-8 and 62351-90-1.
   - Promotes mutually exclusive roles: a user can have two roles, but cannot use the permissions of both simultaneously.
   - Promotes role inheritance.
   - Provides security advantages over traditional access control models (e.g. MAC and DAC).
2. Cons
   - Roles must be instantiated before new users are added to the system.
   - Low flexibility.
   - Costly and complex to implement.
   - Compromising the user on the top of the role hierarchy grants all / most permissions.
   - Not situational aware of time, location and situation.
   - Not applicable in dynamically changing environments.

- No information flow control.

2.3.2 ABAC

Attribute Based Access Control (ABAC) is also a security mechanism that protects resources (objects) from being accessed by unauthorized users (subjects) [14]. It differs from RBAC in that ABAC provides access based on who the subjects are, rather than what the subjects normally do stated by their job title. ABAC determines which attributes the subjects must have in order to access which resources, and what actions they can perform under which environmental conditions.

Attributes, or *characteristics*, of a subject can for instance be name, age, certification level, security clearance level, subject ID, etc. A protected resource will also have distinct attributes to be evaluated, e.g. device ID, connection type, file path, security clearance level, etc. In addition, ABAC is situational aware and can evaluate the access request based on (dynamically changing) environmental conditions, such as time of day, location, network, etc.

Similar to RBAC, ABAC is expressed in the XACML language. They are conceptually equal. Policy administrators writes access policies and uploads the policy files in the authorization engine. An access request from a subject must be converted into XACML to have the request evaluated by the Policy Decision Point (PDP).

The complete model of which entities are involved and what their purpose are, is found in Section 4.5.

Since RBAC and ABAC are expressed similarly, Coyne et al. have researched if both security models can work in conjunction [27]. ABAC can use role names as attributes, but this would discard the advantages of RBAC. ABAC is attribute-centric, whereas RBAC is role-centric. This implies that even though role names are used as attributes, role inheritance and permissions in RBAC is lost. Moreover, RBAC cannot manage environmental conditions, and therefore it does not make sense to combine the two access control models.

Note that *authentication* and *authorization* are different terms and must not be confused. A prerequisite for authorization mechanisms is that a subject has already been authenticated (identified) by another part of the information system.

Pros and cons

The pros and cons for ABAC is expressed below, derived from [14][27]:

1. Pros
   - Considered as the next generation of access control.
   - Works better for real-time applications.
   - Situational aware.
   - Fine-granular.
   - Suitable in a dynamically changing environment.
   - Convenient to add new users to the system, does not have to be pre-defined prior

to being instantiated.

2. Cons
   - Needs expert personnel to understand and determine which attributes to be selected.
   - Existing research only conceptualizes ABAC and gives no clear indication of how it could be implemented. Existing enterprise solutions are expensive. Please refer to Section 3.1 for more details.
   - Not widely used by organisations, even though the concept has been around for approximately 20 years.

2.3.3 Other access control models

MAC

Mandatory Access Control (MAC) is when a security mechanism in a system is controlling access to an object [29]. The individual users cannot change their access levels in the system, nor can system administrators change the access policy after it has been instantiated. Bell-LaPadula is an access control model enforcing MAC. It is confidentiality oriented. Four security clearances are defined in a hierarchical structure for both subjects (users) and objects (resources): Top secret, secret, confidential and unclassified. Bell-LaPadula has three main rules:

1. The Simple Security Condition (SSC)
2. The Star Property (*-Property)
3. The Strong Star Property

The SSC states that subjects cannot read objects that has a higher security level than themselves, e.g. a subject of *confidential* security clearance cannot read information in objects of *secret* or *top secret* security level. This rule translates to "no read up". Subjects are only allowed read objects that have the same or lower security level as themselves.

The *-Property states that subjects cannot write to objects with a lower security level than themselves, e.g. a subject of *confidential* security clearance cannot write information to objects that are *unclassified*. This rule protects information from being made available to an unauthorized audience, compromising the principle of confidentiality. The *-Property rule translates into "no write down". Subjects are only allowed to write changes to objects that are on the same or a higher security level as themselves.

The Strong *-Property rule applies when a subject and an object have same security clearance level. In this case, the subject has both read and write access to the object, but cannot read objects of a lower security level, nor write up to objects of a higher security level.

When all three rules are satisfied, the system is in a secured state.

The Biba security model is an integrity oriented model that works the exact opposite of the Bell-LaPadula model [29]. They share the same hierarchical structure for subjects and objects. Biba has the following security rules:

1. The Simple Integrity rule

2. The Star Integrity rule
3. The Strong Star Integrity rule

The Simple Integrity rule states "no read down", as subjects only can write changes to the same or a higher security level.

The Star Integrity rule defines "no write up", as subjects are only allowed to write to the same or a lower security level.

The Strong Star Integrity rule works the same way as in Bell-LaPadula. A subject has read and write access to objects on the same security levels, but cannot read and write up or down in the object hierarchy.

A system that satisfies all three rules are considered to be in a safe protection state.

DAC

Discretionary Access Control (DAC) is a security mechanism where individual users assigns the access control policy of the objects they own [29]. The access rights are based on identities in the system. The object owner can grant all rights (read, write, execute, create, delete, etc.), and even grant ownership to other users. DAC is widely used in Linux systems, utilized by the `chmod` and `chowm` commands. The access control policy is stored in an access control matrix. A small example of this is demonstrated by Table 1.

Name/File	`iver_file.xml`	`siv_file.xml`	`andre_file.xml`
Iver	OX	R	-
Siv Hilde	-	OX	RW
André	RWX	RW	RWOX

Table 1: Access control matrix of DAC.

Table symbol explanation:
R: Read, W: Write, X: Execute, O: Own.

Clark-Wilson

As mentioned in Section 2.3.1, the Clark-Wilson model enforces the separation of duty principle. The Clark-Wilson model classifies objects into *unconstrained* data items (UDIs) and *constrained* data items (CDIs) [29]. UDIs can be access directly by the subjects, whereas accessing CDIs consists of an intermediary authentication and authorization process. An integration verification process assesses the access request and evaluates it against an access policy. Only if the subject is authorized, access can be granted to the protected (or constrained) object. The Clark-Wilson model provides confidentiality and integrity. When configured to log all actions, auditability and accountability are also taken care of.

3 Related Work

This chapter contains what knowledge that is already available in the literature, and to what degree it can answer the research questions in Section 1.5 and provide value to this project.

In regards to Role-Based Access Control (RBAC) in power systems, the community have already been conducting some research in this field. Lee et al. [4] identified an interesting problem with IEC 61850 as they point out that the standard only addresses data authentication on the substations, not subject authorization. However, IEC 62351 is an extension of IEC 61850, which is supposed to manage the confidentiality and integrity issues of a remote connection (e.g. authorization of subjects). Yet, the authors highlight that there is still an issue with IEC 62351 because it does not present any demonstrations of how to implement RBAC as a security mechanism. Since substations are already configured in Substation Configuration Language (SLC), and that standard is based on XML, Lee et al. argue that eXtensible Access Control Markup Language (XACML) can be used to write access policies and access requests because it is also based on XML schema. The integration of an XACML client/server model on an SCL configured substation server can be seen in Figure 8.

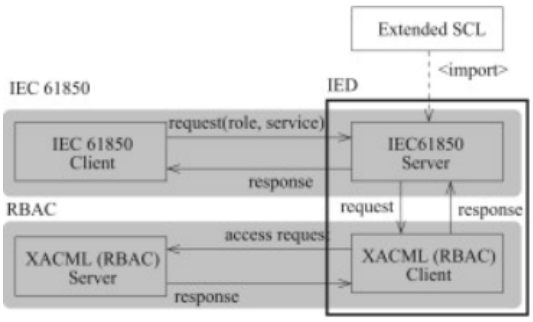


Figure 8: XACML client/server model integrated on SCL server [4].

This research article is a good reference model in terms of the technical implementation of RBAC on substation automation systems. On the other hand, the article does not solve the problem stated in Section 1.3, since a user with a certain role will never have any restrictions of access rights, regardless of the environment. This is because RBAC cannot comprehend environmental conditions, which is only supported in a more granular ABAC system.

The article therefore partially answers research question no. 1 (ref. 1.5). Nevertheless, the work conducted by the researches gives a solid foundation to build further on the security improvements.

Wang et al. [30] suggested a distributed RBAC (DRBAC) methodology in order to solve some identified system load issues. In a traditional RBAC system, both roles and privileges are stored on the same access control server. The authors claim that for each access request, there is a system hiccup due to the processing load on the access control server created by cross-referencing all the numerous roles and privileges. By initially assigning a user to a global role (G-Roles) on a dedicated authentication server, they can map and route the request to the correct intelligent electronic device (IED) where the relevant access policy has been distributed and applied. This ensures that the system load on the access control server for that IED is reduced. The proposed method is promised to be in accordance with the system structure described in IEC 61850.

An immediate concern with this type of access control is the decentralized policy management. Adding a new role or suspending the access rights for a particular user seems problematic, as well as no substations are equipped equally [A]. Additionally, our project rather aims to develop an ABAC system to accommodate the granularity needs of a modern substation and simultaneously ensure a centralized policy management (in the Policy Administration Point (PAP)).

The overall work by Wang et al. lacks completeness in the way that they only propose a conceptualized methodology with no implementation details. Therefore, it briefly touches some of the challenges with RBAC in respect to research question no. 1 in this project (ref. 1.5), but is not relevant at all for the remaining research questions.

The work of Yalcinkaya et al. [13] explain that the majority of ICS lack basic security mechanisms such as authentication and authorization since these systems were not designed with Industry 4.0 in mind. Therefore, ICS have only been secured by perimeter defences like firewalls to accommodate security. Then, RBAC was proposed by several researchers in this field of science, but the authors addresses several concerns with the approach. RBAC causes issues with role administration because it is reasonably difficult to manage, it does not scale very well in larger enterprises, and finally, implementation of fine-grained authorization rules is a complex task.

Their work on an ABAC system gives a solid contribution in this research field since their tested solution seems to eliminate the existing issues with RBAC in ICS. However, their implementation phase is too short and shallow, and only covers the high-leveled aspects. This gives no ease in building further on their concrete work, but to some degree it answers research question no. 3 (ref. 1.5).

On the other hand, this Master thesis will differ from the work of Yalcinkaya et al. because this thesis will focus more on access policy writing. Their work only include one authorization rule and one use case, and does therefore not clearly demonstrate the true benefits of ABAC. This thesis will develop at least three use cases where Statnett needs authorization policies in their substation automation systems (SAS), and combine a policy set of corresponding policies. On the other hand, where our work will look similar, is in the actual representation of the ABAC components. Further clarifications and justifications of the ABAC components that will be used in this project is specified in Section 4.5.

Bhatt et al. [31] present a model for restricted Hierarchical Group ABAC (rHGABAC), with user and object groups organized in a hierarchy. They also present an extension of the model by adding a hierarchy of attributes as well.

This paper is not directly aimed at ICS, but it is interesting how they have described the implementation phase of the complex ABAC system. They also adhere to the NIST reference model and utilize the Policy Machine (PM) framework from NIST [32], which can be helpful resources in this project too. Other parts of their research are fairly formalized and the provided graphs and illustrations are difficult to comprehend.

With respect to this project's research questions (ref. 1.5), the contribution of Bhatt et al. helps to fill in the gaps in regards to research question no. 3.

3.1 Open Problems With ABAC Research

Servos et al. [33] point out a reasonable challenge in the ABAC research field, when they elucidate that ABAC is relatively infancy and the actual implementation is extensive. The authors show that there are barely around 30 ABAC publications yearly (as per 2014). This is a challenge because it implies that there are not many publications written with respect to the industry or substation automation systems. They criticize many publications, NIST's publication included [14], to be too conceptualized and formalized, and proposes no actual way of implementing a solution. Other publications, like Wang et al. [30], propose models that are incomplete or utilizes hybrid models derived from RBAC's role hierarchy.

3.2 Authorization Engines

In the ABAC system, the PDP component is the system entity that evaluates the applicable policy and renders the authorization decision. This section gives an overview of existing authorization engines that can be used as PDP.

OASIS is the developer and maintainer of XACML 3.0 policy language [34]. Since OASIS have not developed an authorization engine themselves, they list various examples of implementations on their website, provided by members of the Technical Committee. The only problem is that XACML version 3.0 was last ratified in 2013, and some of the proposed authorization engines are outdated. Therefore, an updated list of existing authorization engine providers can be found here [35]:

1. Open-source implementations
   - Sun XACML (partially support for version 2.0)
   - Heras AF (supports version 2.0)
   - Balana (partially support for version 3.0)
   - AuthzForce (full support for version 3.0)
   - NIST Policy Machine (full support for version 3.0)
   - WSO2 Identity Server (full support for version 3.0)
2. Commercial implementations
   - Axiomatics Policy Server (full support for version 3.0)

- IMB DataPower (supports version 2.0)
- Oracle Authorization Policy Manager (presumably version 2.0)

4 Research Methodology and Choice of Methods

This chapter gives a description of the methods that has been used in this project, and explains why the chosen methods are appropriate with respect to the research questions.

4.1 Literature Studies

Literature studies was conducted to achieve thorough insight into substation automation systems (SAS), existing access control models and relevant communication protocols such as IEC 60870-5-104, IEC 61850 and IEC 62351. These studies provide the desired knowledge to address the issues identified in research question no. 1 (ref. 1.5).

The literature study of SAS will use two main publications as a foundation, suggested by this project's supervisors, by Padilla [16] and by Knapp et al. [36].
Studies on existing access control models will be based on the text book of Bishop et al. [29] and other peer-reviewed papers to verify academic integrity.
IEC standards will be studied by accessing the repository of standards through NTNU's library [37] and by finding explanatory articles about the standards through Google Scholar search engine.

4.2 Qualitative Interview

In order to capture which parts in the substation automation systems (SAS) where Statnett needs access control and capture the essence of access policies that needs to be enforced, qualitative interview sessions were conducted. In accordance with this project's supervisors, the interviews were arranged with relevant stakeholders from Furuset power station, as this is a substation that is currently evolving into a completely digital station utilizing SAS [38][2].

The interviews were prepared with a number of pre-made structured questions in order to properly identify the use cases for the ABAC system. This contributes to the answer of research question no. 2 (ref. 1.5).

4.3 Use Cases

Use case diagrams will be developed in Unified Modelling Language (UML) [39] to visualize the functionality of the ABAC system. Such diagrams are appropriate because they are easy to understand and depicts the essence of the requirement phase. The precondition for the use cases are a finalized qualitative interview. After knowing the requirements of the ABAC system, the implementation phase can take place (ref. 4.5).

The application of use case diagrams have already been described in the work of Yalcinkaya et al. [13], to demonstrate how a user can request an action on a certain resource. Development of case diagrams will help to answer research question no. 2, in addition to being a dedicated task specified in this project's task description [A].

4.4 Sequence Diagram

A sequence diagram will be developed in UML notation to illustrate the data flow sequences from a user's initial access request to the final access decision made by the ABAC system. Such a diagram is appropriate to develop in order to visualize the interaction between the different ABAC components in the system. Additionally, the sequence diagram contributes to a conceptualized understanding of research question no. 3, because it determines how the access request is flowing through the system.

This method has previously been demonstrated in the existing literature, e.g. by Yalcinkaya et al. [13] and by Lee et al. [4]. Sequence diagrams are often based on the corresponding use case diagrams.

4.5 ABAC System

The ABAC system in this project will build on the baseline derived from OASIS' reference model [5]. Figure 9 illustrates the XACML reference model with all its components and the data flow between the entities.

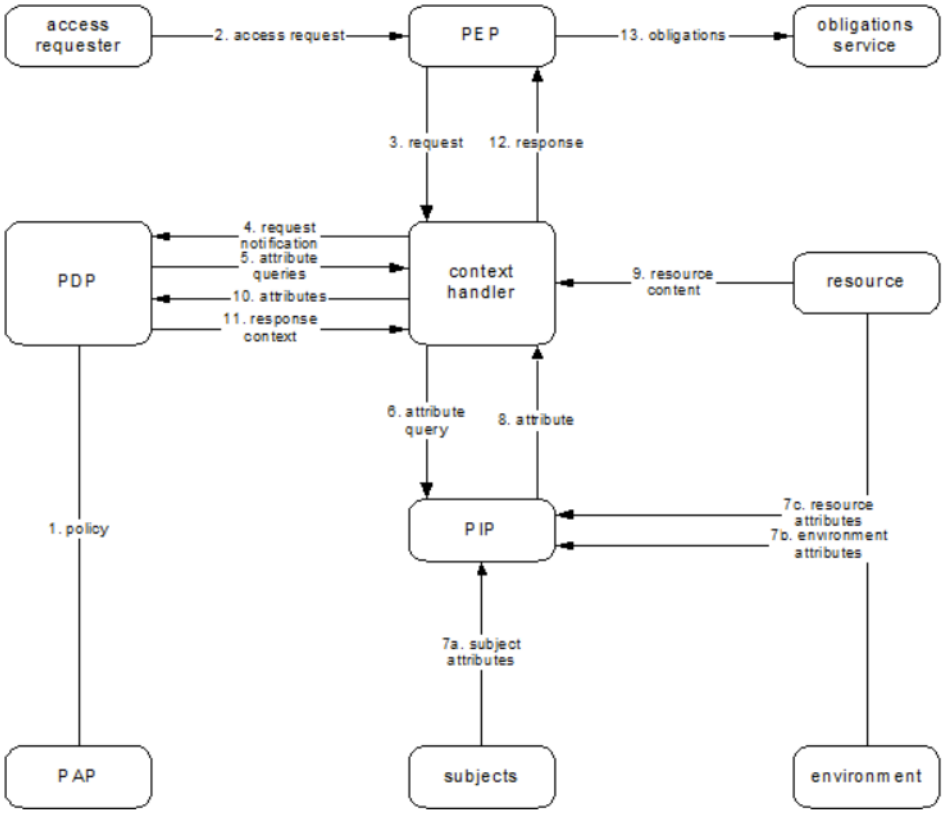


Figure 9: XACML reference model [5].

4.5.1 PEP

The Policy Enforcement Point (PEP) is responsible for being prompted with an access request from a subject and then forward the request to the Policy Decision Point (PDP). The PEP should also convert the subject's access request to an XACML access request (or "context handling" according to Figure 9), since the PDP can only evaluate XACML re-

quests. When the PDP has evaluated the request, it is forwarded back to the PEP again to enforce the actual access control. The PEP is logically protecting a subject from accessing the requested resource. Based on *obligations*, the PEP can perform posterior actions like logging or informing the subject why the access request was denied.

The PEP in this case can be an interface between the remote gateway and the IED, as demonstrated by Lee et al. [4], when they accomplished to configure a IEC 61850- server and client that could forward XACML requests to an XACML- client and server (ref. Figure 8). A custom script located on the XACML client performed the XACML conversion before passing the request to the XACML server.

Another example from the literature, denoted by by Yalcinkaya et al. [13], used SoapUI [40] as an API to forward XACML requests to the PDP. The prerequisite in this case were prepared test cases in Soap format towards the PDP.

In regards to the research questions, this PEP methodology slightly helps to answer research question no. 3 (ref. 1.5). However, the PEP component is not the most crucial part of the ABAC system if the PDP can be fed with requests in an alternative way. Please refer to Section 4.5.2 for the workaround.

4.5.2 PDP

The Policy Decision Point (PDP) is responsible for evaluating the applicable XACML access policy and renders the authorization decision [5]. The PDP decisions can be "Permit", "Deny", "NotApplicable" or "Indeterminate".

The most promising authorization engine in terms of support, overall completeness and usability is the Axiomatics Policy Server [41]. After being informed by Axiomatics' customer service that this authorization engine costs $48.000, it is not appropriate in this project. Therefore, this project will rather use the open-sourced WSO2 IdentityServer as the PDP component [42]. The main reasons for this is that this authorization engine has already been covered by the literature, e.g. in the work of Yalcinkaya et al. [13], and it has the most thorough documentation in terms of installing, running and troubleshooting the service compared to other existing authorization engines (ref. Section 3.2).

The WSO2 IdentityServer fully supports XACML version 3.0 and can be installed on Linux, Windows, Mac, used as a Docker service or configured to run in a cloud environment. The IdentityServer also supports a GUI tool to write simple access policies, but the access policies we need to develop in this project exceeds the complexity of this tool. How access policies will be developed in this project is specified in Section 4.6.

The WSO2 IdentityServer also has a built-in Policy Administration Point (PAP) where the access polices are stored. This simplifies the process of updating, deleting or uploading new policies by the system administrators.

As previously denoted in Section 4.5.1, there is an alternative way to pass access requests to the PDP. Since the IdentityServer can be reached by the API Manager [43], this API can act as the PEP component in the system, which eliminates the need of third-party adaptions.

This PDP part of the methodology provides the desired knowledge in regards to the

technical concerns in research question no. 3, as it propose how the ABAC solution will be built.

4.5.3 PIP

The Policy Information Point (PIP) is the ABAC system component that acts as the source of attribute values [5]. Before the PDP can evaluate the access request from a subject, it must first fetch attributes about the subject itself, attributes about the requested resource, attributes about the desired action and environmental attributes. The relevant attributes must be looked up in the PIP.

In similarity to Yalcinkaya et al. [13], this project will make use of MySQL relation database to store the ABAC attributes [44]. SQL is a standard database language, and database tables can be exported as XML files. This ensures compatibility between the PDP and PIP.

This subsection therefore provides the information needed in order to find out how an ABAC solution can be developed for Statnett, in accordance with research question no. 3 (ref. 1.5).

4.6 ALFA

Access policies uploaded to the PAP, and evaluated by the PDP, expects the policies to be written in XACML. Since XACML is not a human-friendly programming language, Axiomatics have developed the Abbreviated Language For Authorization (ALFA) plug-in module for Visual Studio Code [45]. The module converts ALFA code written in the text editor into XACML, and supports syntax corrections in real-time. This eases the work when uploading the access policy to the PAP.

The ALFA module contributes to the answer of research question no. 3 (ref. 1.5), because the XACML policies are the core logic of the ABAC system. Based on the information that will be gathered in the qualitative interview (ref. 4.2), the appropriate access logic will be applied in the policies.

5 Results

This chapter contains the requirements to the ABAC solution derived from interviews with core stakeholders in Statnett and the results, including the access control use cases and the resulting ABAC solution.

5.1 Requirements

Three rounds of qualitative interviews were held in the period 01.03.2022 to 04.03.2022. The purpose was to capture information about how the existing remote connection worked, how access was technically managed, which resources the key executives needed to access and what operations they performed on the protected resources on a substation.

All participants were asked the same questions. Due to privacy and data protection reasons, the identities of the interview subjects have been concealed. From this point, they will be referred to as "Interview Subject no. (1, 2 or 3)". The complete overview of the interview questions are found in Appendix B.

5.1.1 Interview #1

What is your role in Statnett, and how is it associated with the operation of substations?

This interview was held 01.03.2022. Interview subject no. 1 is a specialist in substation control systems, and is currently involved in an internal Statnett project called "Project digital substation". Their area of responsibility is to maintain, install and patch software on the server where remote connections are accepted. Interview subject no. 1 points at Figure 2 and expresses that this server is located within the substations' main control facility building connected to the station bus (fiber optic LAN on the station level). A central device acts as a proxy and sits between the station bus server and the remote connection, to perform basic authentication. This proxy device is called a Privileged Access Management (PAM) solution. When being let through the PAM solution, an operator will have access to the protected resources on the station bus, e.g. IEDs. The role of Interview subject no. 1 as a specialist in control systems involves trying to establish RBAC on the server behind the PAM solution, in order to strive to be compliant with IEC 62351 part 8. So far, establishing RBAC on the server has been an unsuccessful hassle.

Describe a normal day at a substation. Which tasks are performed?

Interview subject no. 1 explains that the substation monitors and controls the high voltage apparatus in the switchyard, and performs continuous readings of voltage and current levels with Merging Units (MUs) and IEDs. The communication from the IEDs goes via the station bus and by the remote connection to the operating central (SCADA). Protocol conversion happens at the gateway of the substation so that information can be passed with IP based communication to the remote control center, as specified in IEC 104 (ref. Section 2.2.1).

Monitoring the health of the reporting IEDs is also a central daily task that is performed. This information is sent to the remote control center along with the switchyard readings.

Physical activities such as protection of electrical transformers and transmission line maintenance are being done by an on-site operator. By performing physical inspection and monitoring regularly, and having redundant backup equipment, ensures a higher fault tolerance in terms of substation operation.

How does today's remote access solution work in practice? Who is using this solution?

First, the user who wants to access the local substation automation systems must be authenticated by the intermediary PAM solution. Then, privileged access is obtained. This means that the operator is able to access all resources within the station bus, as well as having all available rights. Interview subject no. 1 uses the remote access to maintain the software on the gateway and the server, as well as monitoring and control purposes of the switchyard. When more complex maintenance, installing of patches or reading of event logs needs to be done on IEDs, external vendors can utilize the remote access and perform their tasks. Only the external vendors that have service level agreements with Statnett will be issued a request towards the PAM solution.

Whether or not the PAM session is initiated from internal operators from Statnett or external vendors, the complete session is recorded. This is a control measure to avoid unintentional errors and to quickly identify if the new configuration is faulty. If the latter, they can roll back to the previous configuration. In addition, the remote session is only established within a limited time frame. Then, a new PAM session must be instantiated to continue the work. It is not uncommon that an external vendor have service level agreements with 30 substations. Regardless, the access request must initially be sent by Statnett in order to issue the vendor a PAM session.

Which permissions do you normally need?

Interview subject no. 1 says they only need access to the server connected to the station bus where various applications are running. Of all the eight different applications running on the server, Interview subject no. 1 only needs to access two on normal basis. He needs permissions to write changes to configuration files on the application server.

Interview subject no. 1 adds that the applications on the server are password protected by default passwords. The reasoning behind this is because of convenience: by keeping the default passwords, both Statnett operators and external maintenance crew can access the particular resource. Changing the default passwords will only introduce unwanted complexity. The PAM session is after all recorded.

Are there situations where you need extended rights?

No, there are no situations where Interview subject no. 1 would need extended rights, as they already have all available rights when working through the PAM session. He would only need consultation from external vendors to perform deeper trouble shooting, e.g. acquire special logs from the substation equipment, etc.

What are the minimum rights you must have in order to do your work during a normal operating situation?

Normally, Interview subject no. 1 would only need read and write permissions to inspect the software on the application server. Sometimes, if an IED malfunctions, he would also need to inspect the device to read values and parameters.

Interview subject no. 1 further explains that a local substation operator may also inspect the malfunctioning IED. The operator can read error logs or inspect the configuration through the Human-Machine Interface (HMI). Local changes can also be made through the local HMI.

How would you describe the perfect access control system during a normal situation? And how should it behave during an emergency?

"A system that does not introduce any new errors" is the short answer. If everything works perfectly fine locally, but the authentication and authorization mechanisms makes the remote access unavailable during normal or emergency operations, then access control becomes an obstacle. The perfect access control system should not have too many complex dependencies, as this would interrupt the day to day operation: avoiding different roles for local and remote substation operation, avoiding proprietary vendor implementations that does not integrate with other vendor's equipment or being afraid of doing changes locally.

In an emergency situation, Interview subject no. 1 elaborates that regardless of who is having access, only limited permissions should be allowed. No remote session should have all rights to all resources. Availability is the most important principle for substation operation, therefore this has to be the top priority prior to the security. The perfect access control system should also have a fallback options to revert any unintentional errors made to the substation automation systems.

Let's say a security incident has been detected. It needs to be managed immediately, what would your role be in this situation? What rights would you need? Who else is involved in the incident response?

As specialist in substation control systems, Interview subject no. 1 would be in charge of making the decision when determining whether or not some parts of the automation systems should be shut off. Their role would be system owner of the automation systems and the application server. Interview subject no. 1 assume they would not need any special rights, as external service vendors would connect remotely to the substation and shut that part off, or disconnect it for isolation and troubleshooting purposes.

During an emergency, Interview subject no. 1 as the system owner will be part of the incident response (IR) team, together with KraftCERT and external service vendors.

5.1.2 Interview #2

What is your role in Statnett, and how is it associated with the operation of substations?

The interview of subject no. 2 was held 03.03.2022. This interview subject is a leader in the project "Project digital substation". The role of this subject involves conducting risk analyses and utilizing technology to improve and develop a fully digitized substation. The difference between a conventional and digital substation is that the conventional substation uses analogue tools (e.g. merging units) to perform current and voltage measurements, whereas in a digital substation, only IEDs are employed. Interview subject no. 2 states that all substations operated by Statnett today consists of a hybrid solution of a conventional and digital substation, but the overall goal is to only deploy fully digital substations in the future (ref. Figure 2).

Describe a normal day at a substation. Which tasks are performed?

During a normal day, Interview subject no. 2 works on the development of new IEC 61850 process busses around the substation, assessing who should have physical access to the equipment and enforcing resource control, i.e. ensuring that no one exfiltrates information out from the protected resources (IEDs).

Some of the tasks that are performed on a daily basis, is to change configuration of an IED, download software or files from an external vendor or troubleshoot a component.

How does today's remote access solution work in practice? Who is using this solution?

Interview subject no. 2 states that external vendors are using the remote access solution to test the bay controller on the station. The bay controller is responsible for the communication between the switchyard and the control station (ref. Section 2.1.2). When using the remote access solution, the external vendors are usually updating a particular IED. Interview subject no. 2 elucidates that there are strict rules for accessing the remote solution: first they have to be permitted access through a token-based PAM session issued by Statnett, then it has to be planned what activities that should be performed on the resource.

Which permissions do you normally need?

Since Interview subject no. 2 is a project leader, they do not normally need access to an IED or other equipment on the substation. Therefore, there are no specific set of permissions that Interview subject no. 2 needs, but it is highlighted that those who are involved in the daily substation operation need concrete permissions (ref. Section 5.1.1).

Are there situations where you need extended rights?

No, there are no situations where Interview subject no. 2 needs extended access rights.

What are the minimum rights you must have in order to do your work during a normal operating situation?

Interview subject no. 2 needs access to physical substation components via a remote session to obtain the information needed to improve "Project digital substation". The obtained information is stored in a database for future use, as well as event logging for that component.

How would you describe the perfect access control system during a normal situation? And how should it behave during an emergency?

A perfect access control system would give Interview subject no. 2 access to whichever substation they want through a remote session, having access to the application server (ref. Section 5.1.1), having a database with IP mapping to each physical component for improved control, being able to exfiltrate information from a component when necessary. Default configuration of equipment should be changed to something Statnett has more control of.

During an emergency, Interview subject no. 2 would want to exfiltrate information from multiple regions / security zones simultaneously. Currently, Interview subject no. 2 claims that there are some legislation that prevents them from accessing multiple regions at the same time.

Let's say a security incident has been detected. It needs to be managed immediately, what would your role be in this situation? What rights would you need? Who else is involved in the incident response?

Interview subject no. 2 would not manage the incident directly, but has instead worked to implement preventive routines for such cases. This would involve routines for ensuring that protected files also would be present in a backup database.

During the incident response phase, substation on-site operators and external maintenance crew would be the involved parties, they state.

5.1.3 Interview #3

What is your role in Statnett, and how is it associated with the operation of substations?

Interview subject no. 3 is a leader for network operations on Statnett's substations. Their role is to ensure network connectivity between IEDs on the process- and station bus, as well as providing network access to the remote control center(s).

Describe a normal day at a substation. Which tasks are performed?

During a normal day, they would, for instance, troubleshoot the primary substation installations and investigate why it does not pass information to other components on the substation, e.g. a faulty kilowatt sender. Interview subject no. 3 would also investigate if the reported issue is located on the substation, or if it is a network issue. If it is an error on the station, maintenance crew will be called.

How does today's remote access solution work in practice? Who is using this solution?

The remote access solution is used by the SCADA operating central, as well as internal and external troubleshooting activities. Similar to Interview #1 and #2, Interview subject no. 3 states that external maintenance personnel must have their access request validated by the PAM solution before a remote session is instantiated.

Which permissions do you normally need?

Interview subject no. 3 would need all available rights all the time to perform the required troubleshooting tasks on the network equipment located on the substations. Though, they are only working on one component at a time.

Are there situations where you need extended rights?

No, since all available rights are obtained when accessing the particular substation equipment.

What are the minimum rights you must have in order to do your work during a normal operating situation?

Interview subject no. 3 needs to open and close network ports, change firewall rules on the substation gateway, change configuration on IEDs, or resetting a networking interface.

How would you describe the perfect access control system during a normal situation? And how should it behave during an emergency?

It is stated that the perfect access control system would allow copy and pasting of CLI commands between components, so that there would be no need to re-authorize for each time they are switching from one component to another. In addition, every operator should have personal accounts to ensure accountability and event logging. Interview subject no. 3 stresses the importance of combining IT security with operational uptime.

During an emergency, operation should only be done from a front panel (local HMI), the substation configuration should have a fallback solution, and give the on-site operator permissions to solve problems with extended rights.

Let's say a security incident has been detected. It needs to be managed immediately, what would your role be in this situation? What rights would you need? Who else is involved in the incident response?

Their responsibility would be to limit network access and exposure of a particular substation, to avoid disruption of operation and information disclosure.

Other involved parties would be the Security and Operations Center (SOC), internal specialists on firewalls and external system vendors.

5.2 Use Cases

Based on the obtained requirements from Section 5.1, the following use cases have been developed, as illustrated by Figure 10.

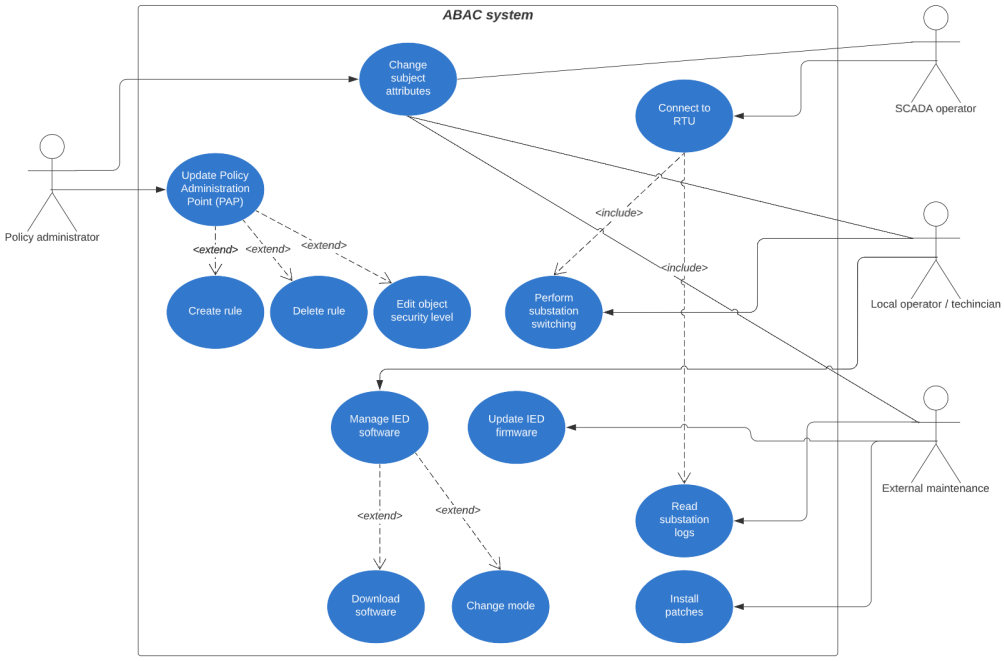


Figure 10: Use Case diagram (author's own figure).

The Use Case diagram consists of four actors: The ABAC policy administrator, the SCADA operator, the local operator and external maintenance crew.

The policy administrator is responsible for maintaining the intermediary access policies between the protected resources and the subjects. This involves creating and deleting access rules when needed, and changing attributes of other subjects and resources in the system.

The SCADA operator can connect to the substation through IEC 104 or other SCADA protocols (ref. Section 2.2.1) and perform remote switching of transmission lines. Additionally, this operator is able to read substation logs and obtain other relevant readings such as health and status of IEDs, as specified in IEC 62351-7 (ref. Section 2.2.4).

Similar to the SCADA operator, the local substation operator is also able to perform substation switching. This is done directly through the local HMI. Via the local HMI, the operator can manage the various IEDs, by changing modes (`run` / `off`), or download appropriate software from the external IED vendors.

External maintenance crew are periodically involved in substation operation. They can for instance update the firmware and install patches on the IEDs, or assist operators in troubleshooting the substation configuration, locally or remotely.

5.2.1 Use Case Selection

The following use cases has been selected for the ABAC solution, as they are considered to be the most important activities where Statnett need access control:

1. Substation switching
2. Updating IED firmware
3. Troubleshooting

5.3 Sequence Diagram

The sequence diagram aims to map which ABAC components that are communicating with each other, and the relative time each component is activated per access request, as seen in Figure 11. The whole purpose of the ABAC system is to evaluate an access request and determine its outcome (`permit` or `deny`). The response to the access request is managed by the `Alternative` condition. Regardless of the decision outcome, the requesting subject will be informed by the authorization system.

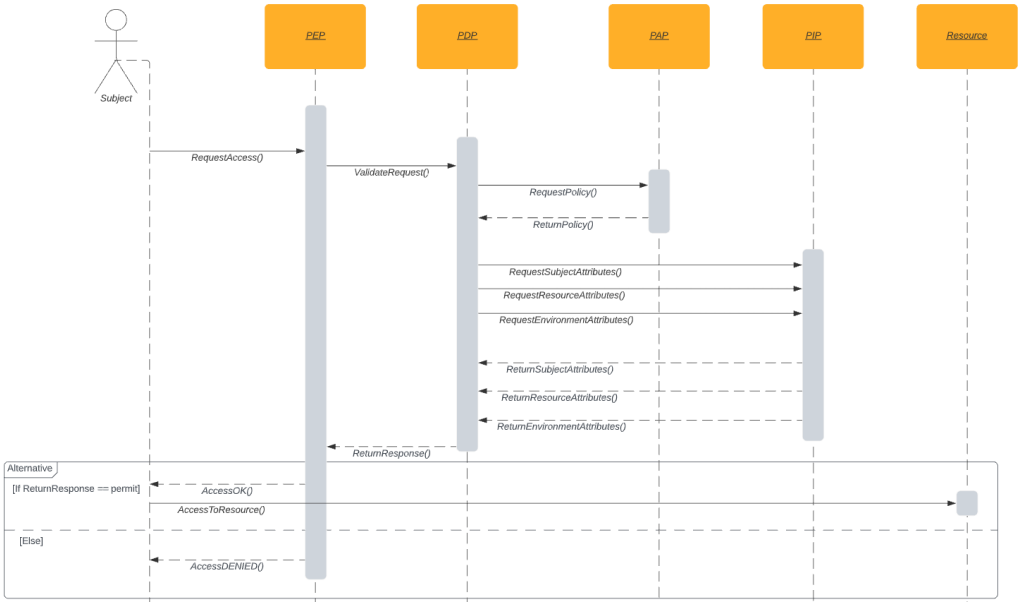


Figure 11: Sequence diagram (author's own figure).

5.4 ABAC Solution

This section is based on the selected use cases from Section 5.2.1. Access policies have been developed in Abbreviated Language For Authorization (ALFA) [45], with respect to Furuset substation in Oslo, Norway [38]. Then, the ALFA access policies have been converted into XACML in order to be accepted by the Policy Decision Point (PDP) in the WSO2 Identity Server [42]. Access requests have been developed in XACML to test and validate the policies.

5.4.1 Use Case 1: Switching

This policy demonstrates how ABAC enforces authorization to perform switching on the substation. The complete access policy is found in Appendix C.

Figure 12 shows an excerpt of a rule that allows for local switching by an operator.

```
/* Rule for local substation switching. */
rule local_Switching {
   target clause Attributes.resourceId == "Transmission_line_1"
   or Attributes.resourceId == "Transmission_line_2"
   or Attributes.resourceId == "Transmission_line_3"
   and Attributes.subjectId == "Alice"
   or Attributes.subjectId == "Bob"
   and Attributes.subjectKeyInfo == "Operator"
   and Attributes.currentTime >= "08:00:00":time
   and Attributes.currentTime <= "16:00:00":time
   and Attributes.situationType == "Normal"
   condition (Attributes.actionId == "Disconnect" || Attributes.actionId == "Connect")
   permit
}
```

Figure 12: Excerpt from the rule `local_Switching` in the policy `Switching.alfa`.

Figure 12 describes that only the *subjects* Alice and Bob are allowed to perform the *actions* connect or disconnect on the *resources* transmission lines at Furuset. In addition, the switching is only allowed between 08:00 and 16:00 during a normal situation, in order to demonstrate that the *environmental* conditions play a role.

The SCADA operator Charlie can also perform switching at this substation, as shown in Figure 13. Charlie can switch at all times during a normal situation or during a maintenance situation, but not during an emergency. This is illustrated by Figure 14, as only Alice is allowed to switch transmission lines during an emergency situation.

```
/* Rule for remote substation switching. */
rule remote_Switching {
   target clause Attributes.resourceId == "Transmission_line_1"
   or Attributes.resourceId == "Transmission_line_2"
   or Attributes.resourceId == "Transmission_line_3"
   and Attributes.subjectId == "Charlie"
   and Attributes.subjectKeyInfo == "SCADA"
   and Attributes.situationType == "Normal"
   or Attributes.situationType == "Maintenance"
   condition (Attributes.actionId == "Disconnect" || Attributes.actionId == "Connect")
   permit
}
```

Figure 13: Excerpt from the rule `remote_Switching` in the policy `Switching.alfa`.

```
/* Rule for local substation switching during an emergency. */
rule emergency_Local_Switching {
   target clause Attributes.resourceId == "Transmission_line_1"
   or Attributes.resourceId == "Transmission_line_2"
   or Attributes.resourceId == "Transmission_line_3"
   and Attributes.subjectId == "Alice"
   and Attributes.subjectKeyInfo == "Operator"
   and Attributes.situationType == "Emergency"
   condition (Attributes.actionId == "Disconnect" || Attributes.actionId == "Connect")
   permit
}
```

Figure 14: Excerpt from the rule `emergency_Local_Switching` in `Switching.alfa`.

Policy validation of Use Case 1

The XACML policy found in Appendix C.1 was uploaded to the WSO2 Identity Server. A manually created XACML request was tested on the policy to check if it worked as intended, as shown in Appendix C.2. The PDP's response to the access request is shown in Figure 15.

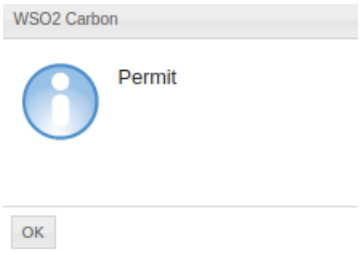


Figure 15: PDP response from XACML access request, Use Case 1.

5.4.2 Use Case 2: Maintenance

In the maintenance policy, it has been defined how three different subjects can perform maintenance tasks on three IEDs. The complete access policy can be seen in Appendix D.

As IED software often has to be updated by an external system vendor, a special rule has been created to allow an external maintenance operator to perform this action remotely, as illustrated by Figure 16.

```
/* Rule for remote updating of IED_3 on a specific date.*/
rule remote_Update_IED_3 {
    target clause Attributes.resourceId == "IED_3"
    and Attributes.subjectId == "Chloe"
    and Attributes.subjectIdQualifier == "ABB"
    and Attributes.situationType == "Maintenance"
    and Attributes.currentTime >= "10:00:00":time
    and Attributes.currentTime <= "14:00:00":time
    and Attributes.currentDate == "01.06.2022":date
    condition (Attributes.actionId == "Update")
    permit
}
```

Figure 16: Excerpt of the rule `remote_Update_IED_3` in the policy `Maintenance.alfa`.

Figure 16 shows that only Chloe from company ABB will be able to update IED_3 on

the date 01.06.2022. Chloe does only have a four hour maintenance window to work with before authorization expires. A pre-requisite for this remote update to happen, is that the system has already been set into "Maintenance" situation type. The access policy differs between the situation types "Normal", "Maintenance" and "Emergency", in which different access rules applies.

Figure 17 shows that the IP address from the accessing subject must be valid and utilize port 2404 according to IEC 104 [20], else the request will be denied. Chloe must therefore use the correct connection to perform updates on IED_3 on the planned maintenance day.

```
/* If remote IP address is invalied, deny access. */
rule deny_Invalid_IP {
condition not(
    ipAddressRegexpMatch(
        "^(10)\\.(10)\\.(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9])\\:([2404])$",
        ipAddressOneAndOnly(Attributes.subjectLocalityIpAddress)))
deny
```

Figure 17: Excerpt of the rule `deny_Invalid_IP` in the policy `Maintenance.alfa`.

According to the access policy (ref. Appendix D), IED_1 and IED_2 can be both updated and patched locally by Mike from Siemens. This means that Mike must be allowed physical access to the substation to perform the updates and patching of the IEDs. When stationed physically on the substation, the ABAC authorization must be enforced as an intermediary step before acquiring direct access to the IEDs. Figure 18 demonstrates the access rules for IED_1 and IED_2, as well as that IED_3 can be updated and patched locally by Grace, but *only* during emergency situations.

```
/* Rule for local updating of IED_1 and IED_2. */
rule local_Update_IED_1_2 {
    target clause Attributes.resourceId == "IED_1"
    or Attributes.resourceId == "IED_2"
    and Attributes.subjectId == "Mike"
    and Attributes.subjectIdQualifier == "Siemens"
    and Attributes.situationType == "Normal"
    or Attributes.situationType == "Maintenance"
    or Attributes.situationType == "Emergency"
    and Attributes.currentTime >= "08:00:00":time
    and Attributes.currentTime <= "16:00:00":time
    condition (Attributes.actionId == "Update" || Attributes.actionId == "Patch")
    permit
}

/* Rule for local updating of IED_3 during emergency. */
rule local_Update_IED_3_emergency {
    target clause Attributes.resourceId == "IED_3"
    and Attributes.subjectId == "Grace"
    and Attributes.situationType == "Emergency"
    condition(Attributes.actionId == "Update" || Attributes.actionId == "Patch")
    permit
}
```

Figure 18: Excerpt of `Maintenance.alfa`.

Policy validation of Use Case 2

The XACML policy found in Appendix D.1 was uploaded in the WSO2 Identity Server, and fed with the access request found in Appendix D.2. Since the test request is about Chloe attempting to perform maintenance on IED_3 *before* the planned date, the PDP's response is shown in Figure 19.

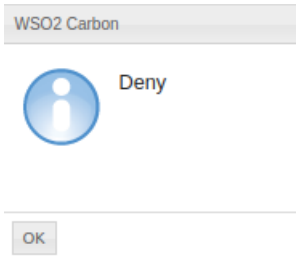


Figure 19: PDP response from XACML access request, Use Case 2.

5.4.3 Use Case 3: Troubleshooting

In the troubleshooting policy, both Statnett and external vendor operators are able to troubleshoot and perform configuration checks on the IEDs. The ABAC policy found in Appendix E demonstrates relevant access rules for the troubleshooting use case. As Statnett operators initially try to perform the troubleshooting themselves, they sometimes need to call for assistance from external vendors. Figure 20 shows how the subject Glenn from Siemens is able to read logs from various IEDs. Since the situation type has to be either "Maintenance" or "Emergency", Glenn cannot access the substation's equipment during a normal situation. In addition, Glenn would only have *read* access during the remote session, so that he can only advise an on-site operator from Statnett to fix the issue.

The same rule from Figure 17 is also present, meaning that only a valid IP address on port 2404 will be accepted.

```
rule remote_External_Troubleshoot {
    target clause Attributes.resourceId == "IED_1.logs"
    or Attributes.resourceId == "IED_2.logs"
    or Attributes.resourceId == "IED_3.logs"
    and Attributes.situationType == "Maintenance"
    or Attributes.situationType == "Emergency"
    and Attributes.subjectId == "Glenn"
    and Attributes.subjectIdQualifier == "Siemens"
    condition (Attributes.actionId == "Read")
    permit
}
```

Figure 20: Excerpt of remote rule in `Troubleshooting.alfa`.

External troubleshooting personnel can also be invited to the substation physically. The access rule in Figure 21 describes how personnel from both Statnett and Siemens can work in conjunction to troubleshoot or check the current configuration on the resources IED_1, IED_2 and IED_3 by investigating their logs. In this rule, they are permitted to not only read logs, but also update and patch the configuration. These actions can be performed during an extended time window compared to normal operating hours, as

well as during a normal situation (if the status of the substation has not officially changed into a "Maintenance" situation yet).

```
rule local_External_Troubleshoot {
    target clause Attributes.resourceId == "IED_1.logs"
    or Attributes.resourceId == "IED_2.logs"
    or Attributes.resourceId == "IED_3.logs"
    and Attributes.situationType == "Normal"
    or Attributes.situationType == "Maintenance"
    and Attributes.subjectIdQualifier == "Statnett"
    or Attributes.subjectIdQualifier == "Siemens"
    and Attributes.currentTime >= "07:00:00":time
    and Attributes.currentTime <= "21:00:00":time
    condition (Attributes.actionId == "Read" || Attributes.actionId == "Update"
    || Attributes.actionId == "Patch")
    permit
}
```

Figure 21: Excerpt of local rule in `Troubleshooting.alfa`.

Policy validation of Use Case 3

Similar to Use Case 1 and 2, the ALFA policy for this use case has been converted into XACML, as seen in Appendix E.1. Then, a manually created XACML access request, as seen in Appendix E.2, was made to test the policy in the WSO2 Identity Server. The PDP's response to the access request is shown in Figure 22.

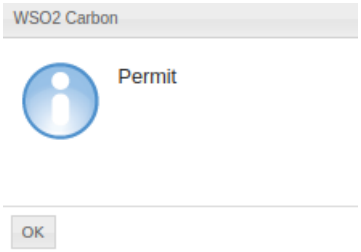


Figure 22: PDP response from XACML access request, Use Case 3.

6 Discussion

This chapter answers the research questions from Section 1.5, discusses the obtained results from Chapter 5 and criticizes the chosen methodology from Chapter 4.

6.1 Research Questions

6.1.1 Why is RBAC not sufficient in power grid systems even though it is a requirement from IEC 62351?

Our research shows that RBAC is not sufficient in power grid systems and industrial control systems (ICS) since role management is an exceedingly complex task for policy administrators. As roles need to be instantiated before the authorization mechanism is deployed as an intermediary service in front of the protected resource, adding new roles and users to the system can not be done afterwards (ref. Section 2.3.1). In addition, the interview sessions in Section 5.1 revealed that Statnett as a national transmission system operator (TSO) deal with multiple tasks and challenges in their daily operations, which implies that new users and permissions has to be assigned and be removed continuously as incidents occurs. This indicates that Statnett need a flexible way to enforce an authorization method on their substations and equipment. RBAC simply cannot provide this profunded flexibility in a dynamically changing environment, nor provide information flow control. As known from Section 2.2.4, event logging is a requirement from IEC 62351-14, but this is impossible to implement with RBAC since accountability and non-repudiation (ref. Figure 6) is lost with ambiguous roles. Similarly, as pointed out by Lee et al. [4] in Section 3, IEC 62351-8 or IEC 62351-90 does not specify how RBAC should be implemented in ICS. By not suggesting a standardized way of implementing the authorization mechanism, fully complying to IEC 62351 remains a problematic issue.

6.1.2 What are the use cases where Statnett need access control?

By interviewing relevant stakeholders in Statnett (ref. Section 5.1), we could establish which activities that needed to be protected by access control, in order to mitigate the typical security attacks described by IEC 62351-1 (ref. Figure 7). Based on the already obtained knowledge from Section 2 and the interview sessions, a Use Case diagram (ref. Section 5.2) was developed to capture the relevant use cases. After considering all use cases, we selected three use cases that seemed the most important to build access policies around, namely switching of high voltage transmission lines, maintenance of IEDs and troubleshooting of substation equipment. Thereafter, a Sequence diagram was developed (ref. Section 5.3) to show the data flow in the access control between the entities described in Section 4.5.

6.1.3 How can we propose an ABAC solution for Statnett's substation automation systems and equipment? How can the solution be generalized to provide value to other TSOs and DSOs?

The research from Section 4.5 specifies how an ABAC solution can be instantiated, based on the XACML referencing model (ref. Figure 9). Access rules have been written in ALFA, then converted into XACML code which is the format that the PDP component accepts, as seen in Appendices C, D and E. After the policies were uploaded to the PDP, manually created XACML requests were tested to verify that the policies worked as intended. The access requests are shown in Appendices C.2, D.2 and E.2. The PDP's responses to each access request are illustrated in Figures 15, 19 and 22.

Even though the ABAC solution from Section 5.4 are based on Statnett's use cases, we can assume that other actors within the power grid industry may find value in the produced results. Statnett's use cases have just been utilized to concretize the ABAC solution in this project, but the results may just as well fit other TSOs and DSOs. In other words, the literature studies from Section 2.2 and the obtained ABAC requirements from Section 5.1 can be generalized to fit whichever TSO or DSO operated substation, presumably with the best fit to another Nordic TSO. This assumption is made because another Nordic TSO may be equally advanced in their adoption of IEC 61850 process bus and digitization of substations as Statnett.

6.2 Discussion of Results

The produced results in Section 5.4 does not fully represent the equipment found on Furuset substation in Oslo. The results have been simplified to demonstrate the benefits of ABAC as an authorization mechanism. In reality, there would be more than just three transmission lines to be switched, more than three IEDs to be managed, and more rules to be applied. The proposed ABAC solution with the fine-grained access policies does indeed exemplify how attributes of *subjects* can be used to access protected *resources*, and what *actions* they can perform under which *environmental* conditions. We have also seen the convenience of how policy administration is done with ALFA authorization language, and that the policies can be tested directly in WSO2 Identity Server by passing a request to the PDP. Having the flexibility of adding and removing subjects and permissions on demand makes ABAC superior compared to RBAC in such a dynamically changing environment. Additionally, our results show that the polices can be situational aware to enforce different rules and permissions in different situations. We can argue that the proposed ABAC solution adds value not only to Statnett and similar TSOs, but also to the research community as a whole, as we have previously pointed out that there are currently no technical report or guide that provides concrete details of how ABAC can be implemented (ref. Section 3.1).

After all, the results from this project indicate that ABAC is an appropriate security mechanism for managing access in power grid substation automation systems (SAS).

6.3 Criticizing the Applied Method

The methods described in Chapter 4 are by no means absolute or perfect. The first point to criticize is that we were not able to give the PEP component (ref. Section 4.5.1) enough attention in our results in Chapter 5. In a complete ABAC system, the access request would be converted from its native format into XACML, then the PEP would pass the request to the PDP for access validation. Since we were not able to properly address this component, the proposed ABAC solution in Section 5.4 is not entirely fulfilled. Fortunately, we were not dependent on the PEP to test the access request towards the PDP, as we were able to test it directly in the WSO2 Identity Server's PDP component. Nevertheless, we have identified two plausible PEP solutions in Section 4.5.1 that can be implemented to fill the gaps in our ABAC solution.

The second aspect to criticize is the absence of the PIP component, as described in Section 4.5.3. Similarly to the PEP component, we cannot state that our ABAC solution is entirely complete, according to the XACML referencing model (ref. Figure 9). The PIP component would be responsible for storing attributes about the subjects, resources and environmental conditions, and the PDP would do a look-up in the PIP to retrieve the necessary attributes upon a subject's access request. Some of the problems we identified in Sections 2.3.2 and 3.1 regarding problems related to ABAC, was that existing solutions were too conceptualized. In this project, we did not find it possible to integrate the MySQL relational database (ref. Section 4.5.3) with the WSO2 Identity Server, even though it initially seemed plausible. Regardless, it should still be possible to use MySQL as a PIP component in an ABAC solution, as the database tables can be exported to XML files, in which the PDP can perform attribute look-ups. Conceivably, it may be more convenient to integrate the PIP component in another authorization engine, or simply invest in an enterprise solution (ref. Section 3.2), to ensure compatibility between components and achieve completeness in the ABAC solution.

7 Conclusion

This research aimed to address the authorization concerns in power grid substation systems and equipment. Based on literature studies of the standards IEC 60870-5-104, IEC 61850 and IEC 62351, and the conducted interviews of core stakeholders in Statnett, we established that the current methods of securing substation systems and equipment was not satisfactory. Our new results indicate that ABAC is an appropriate security mechanism for managing access in SAS. The proposed ABAC solution, with the corresponding access policies, demonstrates how authorization and resource control can be dynamically enforced in critical industrial environments. Statnett's use cases were utilized to concretize the ABAC solution, but the results can be generalized so that other TSOs and DSOs may also find value in this research. In addition, the produced results helps to fill the knowledge gaps in the field of research, as our results also focus on the technical implementations.

7.1 Future Work

In order to fully complete our proposed ABAC solution, as criticized in Section 6.3, future studies should devote research in the following areas:

- Adding the PEP component.
- Adding the PIP component.
- Conduct thorough research on enterprise solutions.
- Integrate the ABAC solution into a physical substation.
  - RBAC integration is already covered by Lee et al. [4], as shown in Figure 8.
- Ratification and updating of the XACML specification scheme by OASIS' Technical Committee. Last revised in 2013 [5].
- Issue a new technical IEC standard that involves ABAC as the next generation of access control and authorization in SAS and ICS.

Bibliography

[1] "Electrical Substation: Equipment, Types, Components & Functions," Mar 2020, [Online; accessed 24. Mar. 2022]. [Online]. Available: https://studyelectrical.com/2019/04/electrical-substation-equipment-types-components-functions.html

[2] R. Løken, Mar 2018, [Online; accessed 28. Jan. 2022]. [Online]. Available: https://www.nek.no/wp-content/uploads/2018/03/03-Statnett-Rannveig-L%C3%B8ken.pdf

[3] IEC:62351, "Power systems management and associated information exchange - data and communications security," International Organization for Standardization, Geneva, CH, Standard, 2007-2020.

[4] B. Lee, D.-K. Kim, H. Yang, and H. Jang, "Role-based access control for substation automation systems using xacml," *Information Systems*, vol. 53, pp. 237–249, 2015. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0306437915000174

[5] "eXtensible Access Control Markup Language (XACML) Version 3.0," 1 2013, [Online; accessed 20. Jan. 2022]. [Online]. Available: http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en.html

[6] "Dette er Statnett," 11 2021, [Online; accessed 17. Jan. 2022]. [Online]. Available: https://www.statnett.no/om-statnett

[7] "Nå er strømkabelen til England ferdigbygd," Jun. 2021, [Online; accessed 30. May 2022]. [Online]. Available: https://www.statnett.no/om-statnett/nyheter-og-pressemeldinger/nyhetsarkiv-2021/na-er-stromkabelen-til-england-ferdigbygd

[8] BBC News, "Ukraine power cut 'was cyber-attack'," *BBC News*, Jan 2017, [Online; accessed 17. Jan. 2022]. [Online]. Available: https://www.bbc.com/news/technology-38573074

[9] "Computing Classification System," Dec 2021, [Online; accessed 1. Feb. 2022]. [Online]. Available: https://dl.acm.org/ccs

[10] K. Stouffer, J. Falco, K. Scarfone *et al.*, "Guide to industrial control systems (ics) security," *NIST special publication*, vol. 800, no. 82, pp. 16–16, 2011.

[11] O. Andreeva, S. Gordeychik, G. Gritsai, O. Kochetova, E. Potseluevskaya, S. I. Sidorov, and A. A. Timorin, "Industrial control systems vulnerabilities statistics," *Kaspersky Lab, Report*, 2016.

[12] "Critical infrastructure and scada/ics cybersecurity vulnerabilities and threats," June 2020, [Online; accessed 17. Jan.

2022]. [Online]. Available: https://www.checkpoint.com/downloads/products/top-10-cybersecurity-vulnerabilities-threat-for-critical-infrastructure-scada-ics.pdf

[13] E. Yalcinkaya, A. Maffei, and M. Onori, "Application of attribute based access control model for industrial control systems," *International Journal of Computer Network and Information Security*, vol. 9, no. 2, pp. 12–21, 2017.

[14] V. C. Hu, D. Ferraiolo, R. Kuhn, A. R. Friedman, A. J. Lang, M. M. Cogdell, A. Schnitzer, K. Sandlin, R. Miller, K. Scarfone *et al.*, "Guide to attribute based access control (abac) definition and considerations (draft)," *NIST special publication*, vol. 800, no. 162, pp. 1–54, 2013.

[15] "The electricity grid - Energifakta Norge," Apr 2019, [Online; accessed 30. Mar. 2022]. [Online]. Available: https://energifaktanorge.no/en/norsk-energiforsyning/kraftnett

[16] E. Padilla, *Substation automation systems: design and implementation*. John Wiley & Sons, 2015.

[17] IEC:61850, "Communication networks and systems for power utility automation," International Organization for Standardization, Geneva, CH, Standard, 2009-2020.

[18] "DS Agile Substation Gateway :: GE Grid Solutions," Apr. 2022, [Online; accessed 23. Apr. 2022]. [Online]. Available: https://www.gegridsolutions.com/multilin/energy/catalog/dsagile_substation_gateway.htm

[19] Inc., "Privileged Access Management Solutions (PAM) Reviews 2022 | Gartner Peer Insights," Apr. 2022, [Online; accessed 28. Apr. 2022]. [Online]. Available: https://www.gartner.com/reviews/market/privileged-access-management

[20] IEC:60870-5-104, "Telecontrol equipment and systems," International Organization for Standardization, Geneva, CH, Standard, 2016.

[21] G. Clarke, D. Reynders, and E. Wright, *Practical modern SCADA protocols: DNP3, 60870.5 and related systems*. Newnes, 2004.

[22] P. Singapore, "IEC 60870-5-104 Protocol," May 2022, [Online; accessed 7. May 2022]. [Online]. Available: https://www.freyrscada.com/iec-60870-5-104.php

[23] "What is an IEC 104 - IEC 60870-5-104? - iGrid Smart Guide," Mar. 2021, [Online; accessed 7. May 2022]. [Online]. Available: https://www.igrid-td.com/smartguide/communicationprotocols/iec-60870-5-104

[24] "Basic understanding of IEC 61850 - What are the key aspects?" Dec. 2021, [Online; accessed 2. May 2022]. [Online]. Available: https://www.sgrwin.com/basic-understanding-iec-61850

[25] S. S. Hussain, T. S. Ustun, and A. Kalam, "A review of iec 62351 security mechanisms for iec 61850 message exchanges," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 9, pp. 5643–5654, 2019.

[26] "IEC 62351 - Cyber Security Series for the Smart Grid - SyC Smart Energy," Jul. 2020, [Online; accessed 8. May 2022]. [Online]. Available: https://syc-se.iec.ch/deliveries/cybersecurity-guidelines/security-standards-and-best-practices/iec-62351

[27] E. Coyne and T. R. Weil, "Abac and rbac: Scalable, flexible, and auditable access management," *IT professional*, vol. 15, no. 3, pp. 14–16, 2013.

[28] R. S. Sandhu, E. J. Coyne, H. L. Feinstein, and C. E. Youman, "Role-based access control models," *Computer*, vol. 29, no. 2, pp. 38–47, 1996.

[29] M. Bishop, E. Sullivan, and M. Ruppel, *Computer Security Art and Science*, 2nd ed. Addison-Wesley, 2019.

[30] B. Wang, S. Zhang, and Z. Zhang, "Drbac based access control method in substation automation system," in *2008 IEEE International Conference on Industrial Technology*. IEEE, 2008, pp. 1–5.

[31] S. Bhatt, F. Patwa, and R. Sandhu, "Abac with group attributes and attribute hierarchies utilizing the policy machine," in *Proceedings of the 2nd ACM Workshop on Attribute-Based Access Control*, 2017, pp. 17–28.

[32] D. F. Ferraiolo, S. I. Gavrila, and W. Jansen, "Policy machine: features, architecture, and specification," *NISTIR 7987 Revision 1*, 2015.

[33] S. L. Servos, Daniel;Osborn, "Current research and open problems in attribute-based access control," *ACM Computing Surveys*, vol. 49, no. 4, p. 1, 2017.

[34] "OASIS eXtensible Access Control Markup Language (XACML) TC | OASIS," Dec 2021, [Online; accessed 13. Feb. 2022]. [Online]. Available: https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml

[35] "Who uses XACML?" Dec 2021, [Online; accessed 25. Jan. 2022]. [Online]. Available: https://stackoverflow.com/questions/2893247/who-uses-xacml

[36] E. D. Knapp and J. Langill, *Industrial Network Security: Securing critical infrastructure networks for smart grid, SCADA, and other Industrial Control Systems*. Syngress, 2014.

[37] NTNU, "Standarder - Kunnskapsbasen - NTNU," Dec 2021, [Online; accessed 18. Jan. 2022]. [Online]. Available: https://i.ntnu.no/wiki/-/wiki/Norsk/Standarder

[38] "Legger frem overordnet plan for sentralnettet i Stor-Oslo," Oct 2018, [Online; accessed 28. Jan. 2022]. [Online]. Available: https://www.statnett.no/vare-prosjekter/region-ost/nettplan-stor-oslo/nyhetsarkiv/legger-frem-overordnet-plan-for-sentralnettet-i-stor-oslo

[39] P. Fettke, "Unified modeling language," in *Encyclopedia of Information Science and Technology, First Edition*. IGI Global, 2005, pp. 2921–2928.

[40] "The World's Most Popular API Testing Tool | SoapUI," Dec 2021, [Online; accessed 16. Feb. 2022]. [Online]. Available: https://www.soapui.org

[41] Axiomatics, Sep 2021, [Online; accessed 16. Feb. 2022]. [Online]. Available: https://www.axiomatics.com/wp-content/uploads/2021/09/axiomatics-policy-server-product-brief-v9-9-2021.pdf

[42] WSO2, “Identity Server - On-Premise and in the Cloud,” Dec 2021, [Online; accessed 20. Feb. 2022]. [Online]. Available: https://wso2.com/identity-server

[43] ——, “WSO2 API Manager Documentation 4.0.0,” Dec 2021, [Online; accessed 20. Feb. 2022]. [Online]. Available: https://apim.docs.wso2.com/en/latest

[44] MySQL, “MySQL :: Download MySQL Community Server,” Dec 2021, [Online; accessed 1. Mar. 2021]. [Online]. Available: https://dev.mysql.com/downloads/mysql

[45] “About this guide - ALFA: Abbreviated Language for Authorization - Documentation,” Nov. 2021, [Online; accessed 20. Jan 2022]. [Online]. Available: https://axiomatics.github.io/alfa-vscode-doc/docs/about/about-this-guide

A Task Description

30. Attribute Based Access Control (ABAC) for Power Grid Substation Systems and Equipment

Contact details:

Siv Hilde Houmb

Phone: 91191632

Email: siv.houmb@statnett.no; siv.houmb@ntnu.no

Thesis title:

Attribute Based Access Control (ABAC) for Power Grid Substation Systems and Equipment

Background:

Statnett is the system operator of the Norwegian power grid and manages more than 11,000 km of high-voltage power lines, 166 substations and 1400 km of subsea and land cables across Norway. Statnett is also responsible for all interconnection abroad such as to Sweden, Finland, Russia, Denmark, Germany, and the Netherlands.

As an owner and operator of critical infrastructure, Statnett is responsible for ensuring the safety and secure operation of the Norwegian power grid. Power grid substation systems plays an essential role in the safe and secure operation of the power grid. Substation systems are comprised of various types of substation equipment and communication networks. Substation equipment includes the gateway to the SCADA system and the circuit breaker in the switch yard, which was manipulated in the 2015 Ukraine power grid attack, and protection devices.

Substation systems, communication protocols and equipment are not built to be cyber resilient and does, in most cases, not have native built-in cybersecurity protection mechanisms. For this reason, substations are protected by perimeter defense measures such as firewalls with strictly managed secure remote access. With the introduction of more IP-based communication and IP-enabled substation equipment, it is important to move state of the art and practice from perimeter defense to a combined model with perimeter defense and built-in cybersecurity protection.

IP-based communication for substations are specified by the IEC 61850 standard, and how to secure IP-based communication and equipment in substation systems is specified in the IEC 62351 standard. IEC 62351 specifies, amongst other things, the use of Public Key Infrastructure (PKI), details on encrypting substation communication, and the use of Role-

Based Access Control (RBAC) for substation systems and equipment. However, RBAC is not optimal for use in a substation as role definitions are implemented differently across substation equipment vendors, and as it does not offer the needed granularity for managing access to substation equipment. For example, if one defines the role "administrator" and gives this role full access, the role "administrator" will have full access no matter the situation in the substation. In cases where there is an emergency situation (power outage, cyber-attack, etc.), or after normal office hours, the permissions should be suspended or reduced. Therefore, there is a need for a more granulated access control model that are also situational aware, such as Attribute-Based Access Control (ABAC).

In this project, you will gain knowledge and understanding of substation systems, communication protocols used in substations and substation equipment, and from this knowledge and understanding you will develop an access control model and prototype for substation systems and equipment based on attribute-based access control (ABAC). The maturity of the model and prototype should be such that the prototype can be used to verify the model (that is, develop 2-3 use cases based on the ABAC model that can be tested and verified using the prototype).

Tasks:

- Task 1: Literature study of substation systems, IEC 104 and IEC 61850 communication protocols and substation equipment.
- Task 2: Literature study on IEC 62351, RBAC and ABAC.
- Task 3: Develop ABAC model for managing access to substation equipment such as gateway and protection devices.
- Task 4: Evaluate and verify ABAC model by means of: (a) develop 2-3 use cases, (b) develop a prototype of the ABAC model, and (c) evaluate use cases using the prototype.
- Result 1: Report from the literature studies.
- Result 2: ABAC model for substation equipment.
- Result 3: ABAC prototype.
- Result 4: Evaluation result.

Reference:

[1] IEC 60870-5-104:2006. Telecontrol equipment and systems – Part 5-104:
[2] Transmission protocols – Network access for IEC 60870-5-101 using standard transport profiles.
[3] IEC 61850-8-1:2011. Communication networks and systems for power utility automation - Part 8-1: Specific communication service mapping (SCSM) - Mappings to MMS (ISO 9506-1 and ISO 9506-2) and to ISO/IEC 8802-3.
[4] IEC 61850-9-2:2011. Communication networks and systems for power utility automation - Part 9-2: Specific communication service mapping (SCSM) - Sampled values over ISO/IEC 8802-3.
[5] IEC 62351-8:2020. Power systems management and associated information exchange - Data and communications security - Part 8: Role-based access control for power system management.

[6] Erkan Yalcinkaya, Antonio Maffei, and Mauro Onori. Application of attribute based access control model for industrial control systems. International Journal of Computer Network and Information Security, 9:12–21, 02 2017.
[7] Other Papers on ABAC.

B Interview Questions

Attributtbasert aksesskontroll (ABAC) for Statnetts substasjoner

1

Bakgrunnsinformasjon

- 11.000 km høyspentledninger
- 1400 km undervanns- og landkabler
- 166 substasjoner
  - Fjernaksess for switching, vedlikehold og systempatching
- IEC 61850
  - Definerer kommunikasjonsflyten mellom komponentene på substasjonene
  - IP-basert
- IEC 62351
  - Definerer hvordan sikre kommunikasjonen med hensyn på IEC 61850
    - TLS-kryptering av data med PKI og X.509 sertifikater, og rollebasert aksesskontroll (RBAC)
- Er RBAC godt nok med tanke på dagens trusselbilde?
  - Hva om rollen «Administrator» blir kompromittert?

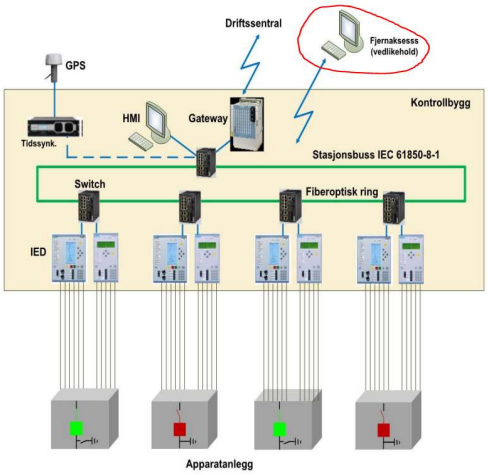
2

Hva oppgaven dreier seg om

- Utforske mulighetene rundt attributtbasert aksesskontroll (ABAC)
  - Økt fleksibilitet og sikkerhet rundt fjernaksess
  - Situasjonsbevisst
- Utvikle et ABAC-system som tilfredsstiller behovene på en digital substasjon
  - Dette intervjuet handlet om å kartlegge behovene for et slikt system

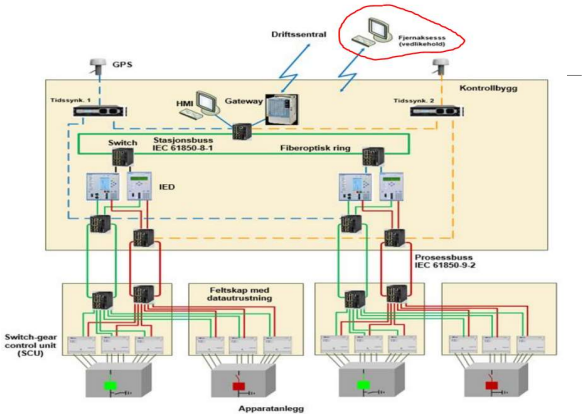
3

Dagens databasert løsning



Kabling til apparatanlegg (HW)

Digital stasjon med prosessbuss



Digital Prosessbuss (61850)

4

Spørsmål til deg (1/8)

- Hvilken rolle har du i Statnett, og hvordan er den tilknyttet driften av substasjoner?
  - Hva er ditt ansvarsområde på en substasjon?

5

2/8

- Kan du beskrive hvordan en vanlig dag ser ut på en substasjon? Hvilke oppgaver utføres?

6

3/8

- Hvordan fungerer dagens fjernaksess-løsning i praksis? Hvem benytter seg av dette?

7

4/8

- Hvilke rettigheter trenger du til vanlig?

8

5/8

- Finnes det situasjoner hvor man trenger utvidede rettigheter?

9

6/8

- Hva er det minste av rettigheter du må ha for å gjøre det du trenger i en normalsituasjon?

10

7/8

- Hvordan ser ditt perfekte aksesskontrollsystem ut for at du skal kunne gjøre din jobb i en normalsituasjon?
  - Hva med en krisesituasjon?

11

Siste spørsmål

- Det har blitt oppdaget en sikkerhetshendelse som må håndteres umiddelbart
  - Hva vil være din rolle i en slik situasjon?
  - Hvilke rettigheter ville du trenge?
  - Hvem andre er involverte i hendelseshåndteringen?

12

C Use Case 1: Switching Policy in ALFA

```
    /* Defining a new environment attribute: */
namespace Attributes {
   import System.*

   attribute situationType {
      id = "situationType"
      type = string
      category = environmentCat
   }
}

/* This policy utilizes the "firstApplicable" rule combining algorithm.
   This means that the rules are ordered. */

namespace Furuset {
   policy Switching {
      apply firstApplicable
      local_Switching
      emergency_Local_Switching
      deny_Remote_Emergency_Switching
      remote_Switching
      deny_Invalid_IP
      default_Deny
   }

   /* Rule for local substation switching. */
   rule local_Switching {
      target clause Attributes.resourceId == "Transmission_line_1"
      or Attributes.resourceId == "Transmission_line_2"
      or Attributes.resourceId == "Transmission_line_3"
      and Attributes.subjectId == "Alice"
      or Attributes.subjectId == "Bob"
      and Attributes.subjectKeyInfo == "Operator"
      and Attributes.currentTime >= "08:00:00":time
      and Attributes.currentTime <= "16:00:00":time
      and Attributes.situationType == "Normal"
      condition (Attributes.actionId == "Disconnect" || Attributes.actionId == "Connect")
      permit
   }

   /* Rule for local substation switching during an emergency. */
   rule emergency_Local_Switching {
      target clause Attributes.resourceId == "Transmission_line_1"
      or Attributes.resourceId == "Transmission_line_2"
      or Attributes.resourceId == "Transmission_line_3"
      and Attributes.subjectId == "Alice"
      and Attributes.subjectKeyInfo == "Operator"
      and Attributes.situationType == "Emergency"
      condition (Attributes.actionId == "Disconnect" || Attributes.actionId == "Connect")
      permit
   }

   /* Remote switching is denied during an emergency. */
   rule deny_Remote_Emergency_Switching {
      target clause Attributes.resourceId == "Transmission_line_1"
      or Attributes.resourceId == "Transmission_line_2"
      or Attributes.resourceId == "Transmission_line_3"
      and Attributes.subjectKeyInfo == "SCADA"
      and Attributes.situationType == "Emergency"
```

```
60      condition (Attributes.actionId == "Disconnect" || Attributes.actionId == "Connect")
61      deny
62    }
63
64    /* Rule for remote substation switching. */
65    rule remote_Switching {
66      target clause Attributes.resourceId == "Transmission_line_1"
67      or Attributes.resourceId == "Transmission_line_2"
68      or Attributes.resourceId == "Transmission_line_3"
69      and Attributes.subjectId == "Charlie"
70      and Attributes.subjectKeyInfo == "SCADA"
71      and Attributes.situationType == "Normal"
72      or Attributes.situationType == "Maintenance"
73      condition (Attributes.actionId == "Disconnect" || Attributes.actionId == "Connect")
74      permit
75    }
76
77    /* If remote IP address is invalied, deny access. */
78    rule deny_Invalid_IP{
79      condition not(
80          ipAddressRegexpMatch(
81              "^(10)\\.(10)\\.(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9])\\:([2404])$",
82              ipAddressOneAndOnly(Attributes.subjectLocalityIpAddress)))
83      deny
84   }
85
86   /* If no rule has been applied yet, return a denied response. */
87    rule default_Deny {
88      deny
89    }
90 }
```

C.1 Use Case 1: Switching Policy in XACML

```
1  <?xml version="1.0" encoding="UTF-8"?><!--This file was generated by the ALFA Plugin for
       Eclipse from Axiomatics AB (http://www.axiomatics.com).--><!--Any modification to
       this file will be lost upon recompilation of the source ALFA file-->
2  <xacml3:Policy xmlns:xacml3="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17" PolicyId="
       http://axiomatics.com/alfa/identifier/Furuset.Switching" RuleCombiningAlgId="urn:
       oasis:names:tc:xacml:1.0:rule-combining-algorithm:first-applicable" Version="1.0">
3      <xacml3:Description/>
4      <xacml3:PolicyDefaults>
5          <xacml3:XPathVersion>http://www.w3.org/TR/1999/REC-xpath-19991116</xacml3:
               XPathVersion>
6      </xacml3:PolicyDefaults>
7      <xacml3:Target/>
8      <xacml3:Rule Effect="Permit" RuleId="Furuset.Switching/Furuset.local_Switching">
9          <xacml3:Description>Rule for local substation switching.</xacml3:Description>
10         <xacml3:Target>
11             <xacml3:AnyOf>
12                 <xacml3:AllOf>
13                     <xacml3:Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-
                           equal">
14                         <xacml3:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#
                               string">Transmission_line_1</xacml3:AttributeValue>
15                         <xacml3:AttributeDesignator AttributeId="urn:oasis:names:tc:xacml
                               :1.0:resource:resource-id" Category="urn:oasis:names:tc:xacml
                               :3.0:attribute-category:resource" DataType="http://www.w3.org
                               /2001/XMLSchema#string" MustBePresent="false"/>
16                     </xacml3:Match>
17                 </xacml3:AllOf>
18                 <xacml3:AllOf>
19                     <xacml3:Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-
                           equal">
```

```
20                    <xacml3:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#
                          string">Transmission_line_2</xacml3:AttributeValue>
21                    <xacml3:AttributeDesignator AttributeId="urn:oasis:names:tc:xacml
                          :1.0:resource:resource-id" Category="urn:oasis:names:tc:xacml
                          :3.0:attribute-category:resource" DataType="http://www.w3.org
                          /2001/XMLSchema#string" MustBePresent="false"/>
22                </xacml3:Match>
23            </xacml3:AllOf>
24            <xacml3:AllOf>
25                <xacml3:Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-
                      equal">
26                    <xacml3:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#
                          string">Transmission_line_3</xacml3:AttributeValue>
27                    <xacml3:AttributeDesignator AttributeId="urn:oasis:names:tc:xacml
                          :1.0:resource:resource-id" Category="urn:oasis:names:tc:xacml
                          :3.0:attribute-category:resource" DataType="http://www.w3.org
                          /2001/XMLSchema#string" MustBePresent="false"/>
28                </xacml3:Match>
29                <xacml3:Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-
                      equal">
30                    <xacml3:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#
                          string">Alice</xacml3:AttributeValue>
31                    <xacml3:AttributeDesignator AttributeId="urn:oasis:names:tc:xacml
                          :1.0:subject:subject-id" Category="urn:oasis:names:tc:xacml:1.0:
                          subject-category:access-subject" DataType="http://www.w3.org
                          /2001/XMLSchema#string" MustBePresent="false"/>
32                </xacml3:Match>
33            </xacml3:AllOf>
34            <xacml3:AllOf>
35                <xacml3:Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-
                      equal">
36                    <xacml3:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#
                          string">Bob</xacml3:AttributeValue>
37                    <xacml3:AttributeDesignator AttributeId="urn:oasis:names:tc:xacml
                          :1.0:subject:subject-id" Category="urn:oasis:names:tc:xacml:1.0:
                          subject-category:access-subject" DataType="http://www.w3.org
                          /2001/XMLSchema#string" MustBePresent="false"/>
38                </xacml3:Match>
39                <xacml3:Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-
                      equal">
40                    <xacml3:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#
                          string">Operator</xacml3:AttributeValue>
41                    <xacml3:AttributeDesignator AttributeId="urn:oasis:names:tc:xacml
                          :1.0:subject:key-info" Category="urn:oasis:names:tc:xacml:1.0:
                          subject-category:access-subject" DataType="http://www.w3.org
                          /2001/XMLSchema#string" MustBePresent="false"/>
42                </xacml3:Match>
43                <xacml3:Match MatchId="urn:oasis:names:tc:xacml:1.0:function:time-less-
                      than-or-equal">
44                    <xacml3:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#
                          time">08:00:00</xacml3:AttributeValue>
45                    <xacml3:AttributeDesignator AttributeId="urn:oasis:names:tc:xacml
                          :1.0:environment:current-time" Category="urn:oasis:names:tc:
                          xacml:3.0:attribute-category:environment" DataType="http://www.
                          w3.org/2001/XMLSchema#time" MustBePresent="false"/>
46                </xacml3:Match>
47                <xacml3:Match MatchId="urn:oasis:names:tc:xacml:1.0:function:time-
                      greater-than-or-equal">
48                    <xacml3:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#
                          time">16:00:00</xacml3:AttributeValue>
49                    <xacml3:AttributeDesignator AttributeId="urn:oasis:names:tc:xacml
                          :1.0:environment:current-time" Category="urn:oasis:names:tc:
                          xacml:3.0:attribute-category:environment" DataType="http://www.
                          w3.org/2001/XMLSchema#time" MustBePresent="false"/>
50                </xacml3:Match>
51                <xacml3:Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-
                      equal">
```

```
52                      <xacml3:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#
                            string">Normal</xacml3:AttributeValue>
53                      <xacml3:AttributeDesignator AttributeId="situationType" Category="
                            urn:oasis:names:tc:xacml:3.0:attribute-category:environment"
                            DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent
                            ="false"/>
54                  </xacml3:Match>
55              </xacml3:AllOf>
56          </xacml3:AnyOf>
57      </xacml3:Target>
58      <xacml3:Condition>
59          <xacml3:Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:or">
60              <xacml3:Apply FunctionId="urn:oasis:names:tc:xacml:3.0:function:any-of-any">
61                  <xacml3:Function FunctionId="urn:oasis:names:tc:xacml:1.0:function:
                        string-equal"/>
62                  <xacml3:AttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:
                        action:action-id" Category="urn:oasis:names:tc:xacml:3.0:attribute-
                        category:action" DataType="http://www.w3.org/2001/XMLSchema#string"
                         MustBePresent="false"/>
63                  <xacml3:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string
                        ">Disconnect</xacml3:AttributeValue>
64              </xacml3:Apply>
65              <xacml3:Apply FunctionId="urn:oasis:names:tc:xacml:3.0:function:any-of-any">
66                  <xacml3:Function FunctionId="urn:oasis:names:tc:xacml:1.0:function:
                        string-equal"/>
67                  <xacml3:AttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:
                        action:action-id" Category="urn:oasis:names:tc:xacml:3.0:attribute-
                        category:action" DataType="http://www.w3.org/2001/XMLSchema#string"
                         MustBePresent="false"/>
68                  <xacml3:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string
                        ">Connect</xacml3:AttributeValue>
69              </xacml3:Apply>
70          </xacml3:Apply>
71      </xacml3:Condition>
72  </xacml3:Rule>
73  <xacml3:Rule Effect="Deny" RuleId="Furuset.Switching/Furuset.
        deny_Remote_Emergency_Switching">
74      <xacml3:Description>Remote switching is denied during an emergency.</xacml3:
            Description>
75      <xacml3:Target>
76          <xacml3:AnyOf>
77              <xacml3:AllOf>
78                  <xacml3:Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-
                        equal">
79                      <xacml3:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#
                            string">Transmission_line_1</xacml3:AttributeValue>
80                      <xacml3:AttributeDesignator AttributeId="urn:oasis:names:tc:xacml
                            :1.0:resource:resource-id" Category="urn:oasis:names:tc:xacml
                            :3.0:attribute-category:resource" DataType="http://www.w3.org
                            /2001/XMLSchema#string" MustBePresent="false"/>
81                  </xacml3:Match>
82              </xacml3:AllOf>
83              <xacml3:AllOf>
84                  <xacml3:Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-
                        equal">
85                      <xacml3:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#
                            string">Transmission_line_2</xacml3:AttributeValue>
86                      <xacml3:AttributeDesignator AttributeId="urn:oasis:names:tc:xacml
                            :1.0:resource:resource-id" Category="urn:oasis:names:tc:xacml
                            :3.0:attribute-category:resource" DataType="http://www.w3.org
                            /2001/XMLSchema#string" MustBePresent="false"/>
87                  </xacml3:Match>
88              </xacml3:AllOf>
89              <xacml3:AllOf>
90                  <xacml3:Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-
                        equal">
91                      <xacml3:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#
```

```
                        string">Transmission_line_3</xacml3:AttributeValue>
92                      <xacml3:AttributeDesignator AttributeId="urn:oasis:names:tc:xacml
                            :1.0:resource:resource-id" Category="urn:oasis:names:tc:xacml
                            :3.0:attribute-category:resource" DataType="http://www.w3.org
                            /2001/XMLSchema#string" MustBePresent="false"/>
93                  </xacml3:Match>
94                  <xacml3:Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-
                        equal">
95                      <xacml3:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#
                            string">SCADA</xacml3:AttributeValue>
96                      <xacml3:AttributeDesignator AttributeId="urn:oasis:names:tc:xacml
                            :1.0:subject:key-info" Category="urn:oasis:names:tc:xacml:1.0:
                            subject-category:access-subject" DataType="http://www.w3.org
                            /2001/XMLSchema#string" MustBePresent="false"/>
97                  </xacml3:Match>
98                  <xacml3:Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-
                        equal">
99                      <xacml3:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#
                            string">Emergency</xacml3:AttributeValue>
100                     <xacml3:AttributeDesignator AttributeId="situationType" Category="
                            urn:oasis:names:tc:xacml:3.0:attribute-category:environment"
                            DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent
                            ="false"/>
101                 </xacml3:Match>
102             </xacml3:AllOf>
103         </xacml3:AnyOf>
104     </xacml3:Target>
105     <xacml3:Condition>
106         <xacml3:Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:or">
107             <xacml3:Apply FunctionId="urn:oasis:names:tc:xacml:3.0:function:any-of-any">
108                 <xacml3:Function FunctionId="urn:oasis:names:tc:xacml:1.0:function:
                        string-equal"/>
109                 <xacml3:AttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:
                        action:action-id" Category="urn:oasis:names:tc:xacml:3.0:attribute-
                        category:action" DataType="http://www.w3.org/2001/XMLSchema#string"
                         MustBePresent="false"/>
110                 <xacml3:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string
                        ">Disconnect</xacml3:AttributeValue>
111             </xacml3:Apply>
112             <xacml3:Apply FunctionId="urn:oasis:names:tc:xacml:3.0:function:any-of-any">
113                 <xacml3:Function FunctionId="urn:oasis:names:tc:xacml:1.0:function:
                        string-equal"/>
114                 <xacml3:AttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:
                        action:action-id" Category="urn:oasis:names:tc:xacml:3.0:attribute-
                        category:action" DataType="http://www.w3.org/2001/XMLSchema#string"
                         MustBePresent="false"/>
115                 <xacml3:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string
                        ">Connect</xacml3:AttributeValue>
116             </xacml3:Apply>
117         </xacml3:Apply>
118     </xacml3:Condition>
119 </xacml3:Rule>
120 <xacml3:Rule Effect="Permit" RuleId="Furuset.Switching/Furuset.remote_Switching">
121     <xacml3:Description>Rule for remote substation switching.</xacml3:Description>
122     <xacml3:Target>
123         <xacml3:AnyOf>
124             <xacml3:AllOf>
125                 <xacml3:Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-
                        equal">
126                     <xacml3:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#
                            string">Transmission_line_1</xacml3:AttributeValue>
127                     <xacml3:AttributeDesignator AttributeId="urn:oasis:names:tc:xacml
                            :1.0:resource:resource-id" Category="urn:oasis:names:tc:xacml
                            :3.0:attribute-category:resource" DataType="http://www.w3.org
                            /2001/XMLSchema#string" MustBePresent="false"/>
128                 </xacml3:Match>
129             </xacml3:AllOf>
```

```
130             <xacml3:AllOf>
131                 <xacml3:Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-
                        equal">
132                     <xacml3:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#
                            string">Transmission_line_2</xacml3:AttributeValue>
133                     <xacml3:AttributeDesignator AttributeId="urn:oasis:names:tc:xacml
                            :1.0:resource:resource-id" Category="urn:oasis:names:tc:xacml
                            :3.0:attribute-category:resource" DataType="http://www.w3.org
                            /2001/XMLSchema#string" MustBePresent="false"/>
134                 </xacml3:Match>
135             </xacml3:AllOf>
136             <xacml3:AllOf>
137                 <xacml3:Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-
                        equal">
138                     <xacml3:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#
                            string">Transmission_line_3</xacml3:AttributeValue>
139                     <xacml3:AttributeDesignator AttributeId="urn:oasis:names:tc:xacml
                            :1.0:resource:resource-id" Category="urn:oasis:names:tc:xacml
                            :3.0:attribute-category:resource" DataType="http://www.w3.org
                            /2001/XMLSchema#string" MustBePresent="false"/>
140                 </xacml3:Match>
141                 <xacml3:Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-
                        equal">
142                     <xacml3:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#
                            string">Charlie</xacml3:AttributeValue>
143                     <xacml3:AttributeDesignator AttributeId="urn:oasis:names:tc:xacml
                            :1.0:subject:subject-id" Category="urn:oasis:names:tc:xacml:1.0:
                            subject-category:access-subject" DataType="http://www.w3.org
                            /2001/XMLSchema#string" MustBePresent="false"/>
144                 </xacml3:Match>
145                 <xacml3:Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-
                        equal">
146                     <xacml3:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#
                            string">SCADA</xacml3:AttributeValue>
147                     <xacml3:AttributeDesignator AttributeId="urn:oasis:names:tc:xacml
                            :1.0:subject:key-info" Category="urn:oasis:names:tc:xacml:1.0:
                            subject-category:access-subject" DataType="http://www.w3.org
                            /2001/XMLSchema#string" MustBePresent="false"/>
148                 </xacml3:Match>
149                 <xacml3:Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-
                        equal">
150                     <xacml3:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#
                            string">Normal</xacml3:AttributeValue>
151                     <xacml3:AttributeDesignator AttributeId="situationType" Category="
                            urn:oasis:names:tc:xacml:3.0:attribute-category:environment"
                            DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent
                            ="false"/>
152                 </xacml3:Match>
153             </xacml3:AllOf>
154             <xacml3:AllOf>
155                 <xacml3:Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-
                        equal">
156                     <xacml3:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#
                            string">Maintenance</xacml3:AttributeValue>
157                     <xacml3:AttributeDesignator AttributeId="situationType" Category="
                            urn:oasis:names:tc:xacml:3.0:attribute-category:environment"
                            DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent
                            ="false"/>
158                 </xacml3:Match>
159             </xacml3:AllOf>
160         </xacml3:AnyOf>
161     </xacml3:Target>
162     <xacml3:Condition>
163         <xacml3:Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:or">
164             <xacml3:Apply FunctionId="urn:oasis:names:tc:xacml:3.0:function:any-of-any">
165                 <xacml3:Function FunctionId="urn:oasis:names:tc:xacml:1.0:function:
                        string-equal"/>
```

```
166                 <xacml3:AttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:
                        action:action-id" Category="urn:oasis:names:tc:xacml:3.0:attribute-
                        category:action" DataType="http://www.w3.org/2001/XMLSchema#string"
                         MustBePresent="false"/>
167                 <xacml3:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string
                        ">Disconnect</xacml3:AttributeValue>
168             </xacml3:Apply>
169             <xacml3:Apply FunctionId="urn:oasis:names:tc:xacml:3.0:function:any-of-any">
170                 <xacml3:Function FunctionId="urn:oasis:names:tc:xacml:1.0:function:
                        string-equal"/>
171                 <xacml3:AttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:
                        action:action-id" Category="urn:oasis:names:tc:xacml:3.0:attribute-
                        category:action" DataType="http://www.w3.org/2001/XMLSchema#string"
                         MustBePresent="false"/>
172                 <xacml3:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string
                        ">Connect</xacml3:AttributeValue>
173             </xacml3:Apply>
174         </xacml3:Apply>
175     </xacml3:Condition>
176 </xacml3:Rule>
177 <xacml3:Rule Effect="Deny" RuleId="Furuset.Switching/Furuset.deny_Invalid_IP">
178     <xacml3:Description>If remote IP address is invalied, deny access.</xacml3:
            Description>
179     <xacml3:Target/>
180     <xacml3:Condition>
181         <xacml3:Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:not">
182             <xacml3:Apply FunctionId="urn:oasis:names:tc:xacml:2.0:function:ipAddress-
                    regexp-match">
183                 <xacml3:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string
                        ">^(10)\.(10)\.(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9])\:([80|443])$</
                        xacml3:AttributeValue>
184                 <xacml3:Apply FunctionId="urn:oasis:names:tc:xacml:2.0:function:
                        ipAddress-one-and-only">
185                     <xacml3:AttributeDesignator AttributeId="urn:oasis:names:tc:xacml
                            :3.0:subject:authn-locality:ip-address" Category="urn:oasis:
                            names:tc:xacml:1.0:subject-category:access-subject" DataType="
                            urn:oasis:names:tc:xacml:2.0:data-type:ipAddress" MustBePresent=
                            "false"/>
186                 </xacml3:Apply>
187             </xacml3:Apply>
188         </xacml3:Apply>
189     </xacml3:Condition>
190 </xacml3:Rule>
191 <xacml3:Rule Effect="Deny" RuleId="Furuset.Switching/Furuset.default_Deny">
192     <xacml3:Description>If no rule has been applied yet, return a denied response.</
            xacml3:Description>
193     <xacml3:Target/>
194 </xacml3:Rule>
195 </xacml3:Policy>
```

C.2 Use Case 1: XACML Test Request

```
<Request xmlns="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17" CombinedDecision="false"
    ReturnPolicyIdList="false">
<Attributes Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource">
<Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id" IncludeInResult
    ="false">
<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Transmission_line_1</
    AttributeValue>
</Attribute>
</Attributes>
<Attributes Category="urn:oasis:names:tc:xacml:3.0:attribute-category:environment">
<Attribute AttributeId="situationType" IncludeInResult="false">
<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Normal</AttributeValue>
</Attribute>
</Attributes>
<Attributes Category="urn:oasis:names:tc:xacml:3.0:attribute-category:environment">
<Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:function:time-equal" IncludeInResult=
    "false">
<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">12:00:00</
    AttributeValue>
</Attribute>
</Attributes>
<Attributes Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject">
<Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id" IncludeInResult="
    false">
<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Alice</AttributeValue>
</Attribute>
</Attributes>
<Attributes Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject">
<Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:subject:key-info" IncludeInResult="
    false">
<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Operator</
    AttributeValue>
</Attribute>
</Attributes>
<Attributes Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action">
<Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id" IncludeInResult="
    false">
<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Disconnect</
    AttributeValue>
</Attribute>
</Attributes>
</Request>
```

D Use Case 2: Maintenance Policy in ALFA

```
namespace Attributes {
    import System.*

    attribute situationType {
        id = "situationType"
        type = string
        category = environmentCat
    }
}

namespace Furuset {
    policy Maintenance {
        apply firstApplicable
        local_Update_IED_1_2
        local_Update_IED_3_emergency
        deny_Invalid_IP
        remote_Update_IED_3
        default_Deny
    }

    /* Rule for local updating of IED_1 and IED_2. */
    rule local_Update_IED_1_2 {
        target clause Attributes.resourceId == "IED_1"
        or Attributes.resourceId == "IED_2"
        and Attributes.subjectId == "Mike"
        and Attributes.subjectIdQualifier == "Siemens"
        and Attributes.situationType == "Normal"
        or Attributes.situationType == "Maintenance"
        or Attributes.situationType == "Emergency"
        and Attributes.currentTime >= "08:00:00":time
        and Attributes.currentTime <= "16:00:00":time
        condition (Attributes.actionId == "Update" || Attributes.actionId == "Patch")
        permit
    }

    /* Rule for local updating of IED_3 during emergency. */
    rule local_Update_IED_3_emergency {
        target clause Attributes.resourceId == "IED_3"
        and Attributes.subjectId == "Grace"
        and Attributes.situationType == "Emergency"
        condition(Attributes.actionId == "Update" || Attributes.actionId == "Patch")
        permit
    }
    /* If remote IP address is invalied, deny access. */
   rule deny_Invalid_IP{
    condition not(
        ipAddressRegexpMatch(
            "^(10)\\.(10)\\.(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9])\\:([2404])$",
            ipAddressOneAndOnly(Attributes.subjectLocalityIpAddress)))
    deny
}

    /* Rule for remote updating of IED_3 on a specific date.*/
    rule remote_Update_IED_3 {
        target clause Attributes.resourceId == "IED_3"
        and Attributes.subjectId == "Chloe"
        and Attributes.subjectIdQualifier == "ABB"
        and Attributes.situationType == "Maintenance"
        and Attributes.currentTime >= "10:00:00":time
```

```
        and Attributes.currentTime <= "14:00:00":time
        and Attributes.currentDate == "01.06.2022":date
        condition (Attributes.actionId == "Update")
        permit
    }

    /* If no rule has been applied yet, return a denied response. */
   rule default_Deny {
    deny
 }

}
```

D.1 Use Case 2: Maintenance Policy in XACML

```
<?xml version="1.0" encoding="UTF-8"?><!--This file was generated by the ALFA Plugin for Eclipse from Axiomatics AB (http://www.axiomatics.com).--><!--Any modification to this file will be lost upon recompilation of the source ALFA file-->
<xacml3:Policy xmlns:xacml3="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17" PolicyId="http://axiomatics.com/alfa/identifier/Furuset.Maintenance" RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:first-applicable" Version="1.0">
    <xacml3:Description/>
    <xacml3:PolicyDefaults>
        <xacml3:XPathVersion>http://www.w3.org/TR/1999/REC-xpath-19991116</xacml3:XPathVersion>
    </xacml3:PolicyDefaults>
    <xacml3:Target/>
    <xacml3:Rule Effect="Permit" RuleId="Furuset.Maintenance/Furuset.local_Update_IED_1_2">
        <xacml3:Description>Rule for local updating of IED_1 and IED_2.</xacml3:Description>
        <xacml3:Target>
            <xacml3:AnyOf>
                <xacml3:AllOf>
                    <xacml3:Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
                        <xacml3:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">IED_1</xacml3:AttributeValue>
                        <xacml3:AttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id" Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource" DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="false"/>
                    </xacml3:Match>
                </xacml3:AllOf>
                <xacml3:AllOf>
                    <xacml3:Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
                        <xacml3:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">IED_2</xacml3:AttributeValue>
                        <xacml3:AttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id" Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource" DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="false"/>
                    </xacml3:Match>
                    <xacml3:Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
                        <xacml3:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Mike</xacml3:AttributeValue>
                        <xacml3:AttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id" Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject" DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="false"/>
                    </xacml3:Match>
                    <xacml3:Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
```

```
28                      <xacml3:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#
                            string">Siemens</xacml3:AttributeValue>
29                      <xacml3:AttributeDesignator AttributeId="urn:oasis:names:tc:xacml
                            :1.0:subject:subject-id-qualifier" Category="urn:oasis:names:tc:
                            xacml:1.0:subject-category:access-subject" DataType="http://www.
                            w3.org/2001/XMLSchema#string" MustBePresent="false"/>
30                  </xacml3:Match>
31                  <xacml3:Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-
                        equal">
32                      <xacml3:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#
                            string">Normal</xacml3:AttributeValue>
33                      <xacml3:AttributeDesignator AttributeId="situationType" Category="
                            urn:oasis:names:tc:xacml:3.0:attribute-category:environment"
                            DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent
                            ="false"/>
34                  </xacml3:Match>
35              </xacml3:AllOf>
36              <xacml3:AllOf>
37                  <xacml3:Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-
                        equal">
38                      <xacml3:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#
                            string">Maintenance</xacml3:AttributeValue>
39                      <xacml3:AttributeDesignator AttributeId="situationType" Category="
                            urn:oasis:names:tc:xacml:3.0:attribute-category:environment"
                            DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent
                            ="false"/>
40                  </xacml3:Match>
41              </xacml3:AllOf>
42              <xacml3:AllOf>
43                  <xacml3:Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-
                        equal">
44                      <xacml3:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#
                            string">Emergency</xacml3:AttributeValue>
45                      <xacml3:AttributeDesignator AttributeId="situationType" Category="
                            urn:oasis:names:tc:xacml:3.0:attribute-category:environment"
                            DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent
                            ="false"/>
46                  </xacml3:Match>
47                  <xacml3:Match MatchId="urn:oasis:names:tc:xacml:1.0:function:time-less-
                        than-or-equal">
48                      <xacml3:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#
                            time">08:00:00</xacml3:AttributeValue>
49                      <xacml3:AttributeDesignator AttributeId="urn:oasis:names:tc:xacml
                            :1.0:environment:current-time" Category="urn:oasis:names:tc:
                            xacml:3.0:attribute-category:environment" DataType="http://www.
                            w3.org/2001/XMLSchema#time" MustBePresent="false"/>
50                  </xacml3:Match>
51                  <xacml3:Match MatchId="urn:oasis:names:tc:xacml:1.0:function:time-
                        greater-than-or-equal">
52                      <xacml3:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#
                            time">16:00:00</xacml3:AttributeValue>
53                      <xacml3:AttributeDesignator AttributeId="urn:oasis:names:tc:xacml
                            :1.0:environment:current-time" Category="urn:oasis:names:tc:
                            xacml:3.0:attribute-category:environment" DataType="http://www.
                            w3.org/2001/XMLSchema#time" MustBePresent="false"/>
54                  </xacml3:Match>
55              </xacml3:AllOf>
56          </xacml3:AnyOf>
57      </xacml3:Target>
58      <xacml3:Condition>
59          <xacml3:Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:or">
60              <xacml3:Apply FunctionId="urn:oasis:names:tc:xacml:3.0:function:any-of-any">
61                  <xacml3:Function FunctionId="urn:oasis:names:tc:xacml:1.0:function:
                        string-equal"/>
62                  <xacml3:AttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:
                        action:action-id" Category="urn:oasis:names:tc:xacml:3.0:attribute-
                        category:action" DataType="http://www.w3.org/2001/XMLSchema#string"
```

```
                        MustBePresent="false"/>
63                  <xacml3:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string
                        ">Update</xacml3:AttributeValue>
64              </xacml3:Apply>
65              <xacml3:Apply FunctionId="urn:oasis:names:tc:xacml:3.0:function:any-of-any">
66                  <xacml3:Function FunctionId="urn:oasis:names:tc:xacml:1.0:function:
                        string-equal"/>
67                  <xacml3:AttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:
                        action:action-id" Category="urn:oasis:names:tc:xacml:3.0:attribute-
                        category:action" DataType="http://www.w3.org/2001/XMLSchema#string"
                         MustBePresent="false"/>
68                  <xacml3:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string
                        ">Patch</xacml3:AttributeValue>
69              </xacml3:Apply>
70          </xacml3:Apply>
71      </xacml3:Condition>
72  </xacml3:Rule>
73  <xacml3:Rule Effect="Permit" RuleId="Furuset.Maintenance/Furuset.
        local_Update_IED_3_emergency">
74      <xacml3:Description>Rule for local updating of IED_3 during emergency.</xacml3:
            Description>
75      <xacml3:Target>
76          <xacml3:AnyOf>
77              <xacml3:AllOf>
78                  <xacml3:Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-
                        equal">
79                      <xacml3:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#
                            string">IED_3</xacml3:AttributeValue>
80                      <xacml3:AttributeDesignator AttributeId="urn:oasis:names:tc:xacml
                            :1.0:resource:resource-id" Category="urn:oasis:names:tc:xacml
                            :3.0:attribute-category:resource" DataType="http://www.w3.org
                            /2001/XMLSchema#string" MustBePresent="false"/>
81                  </xacml3:Match>
82                  <xacml3:Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-
                        equal">
83                      <xacml3:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#
                            string">Grace</xacml3:AttributeValue>
84                      <xacml3:AttributeDesignator AttributeId="urn:oasis:names:tc:xacml
                            :1.0:subject:subject-id" Category="urn:oasis:names:tc:xacml:1.0:
                            subject-category:access-subject" DataType="http://www.w3.org
                            /2001/XMLSchema#string" MustBePresent="false"/>
85                  </xacml3:Match>
86                  <xacml3:Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-
                        equal">
87                      <xacml3:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#
                            string">Emergency</xacml3:AttributeValue>
88                      <xacml3:AttributeDesignator AttributeId="situationType" Category="
                            urn:oasis:names:tc:xacml:3.0:attribute-category:environment"
                            DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent
                            ="false"/>
89                  </xacml3:Match>
90              </xacml3:AllOf>
91          </xacml3:AnyOf>
92      </xacml3:Target>
93      <xacml3:Condition>
94          <xacml3:Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:or">
95              <xacml3:Apply FunctionId="urn:oasis:names:tc:xacml:3.0:function:any-of-any">
96                  <xacml3:Function FunctionId="urn:oasis:names:tc:xacml:1.0:function:
                        string-equal"/>
97                  <xacml3:AttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:
                        action:action-id" Category="urn:oasis:names:tc:xacml:3.0:attribute-
                        category:action" DataType="http://www.w3.org/2001/XMLSchema#string"
                         MustBePresent="false"/>
98                  <xacml3:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string
                        ">Update</xacml3:AttributeValue>
99              </xacml3:Apply>
100             <xacml3:Apply FunctionId="urn:oasis:names:tc:xacml:3.0:function:any-of-any">
```

```
101                 <xacml3:Function FunctionId="urn:oasis:names:tc:xacml:1.0:function:
                        string-equal"/>
102                 <xacml3:AttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:
                        action:action-id" Category="urn:oasis:names:tc:xacml:3.0:attribute-
                        category:action" DataType="http://www.w3.org/2001/XMLSchema#string"
                         MustBePresent="false"/>
103                 <xacml3:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string
                        ">Patch</xacml3:AttributeValue>
104             </xacml3:Apply>
105         </xacml3:Apply>
106     </xacml3:Condition>
107 </xacml3:Rule>
108 <xacml3:Rule Effect="Deny" RuleId="Furuset.Maintenance/Furuset.deny_Invalid_IP">
109     <xacml3:Description>If remote IP address is invalied, deny access.</xacml3:
            Description>
110     <xacml3:Target/>
111     <xacml3:Condition>
112         <xacml3:Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:not">
113             <xacml3:Apply FunctionId="urn:oasis:names:tc:xacml:2.0:function:ipAddress-
                    regexp-match">
114                 <xacml3:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string
                        ">^(10)\.(10)\.(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9])\:([2404])$</
                        xacml3:AttributeValue>
115                 <xacml3:Apply FunctionId="urn:oasis:names:tc:xacml:2.0:function:
                        ipAddress-one-and-only">
116                     <xacml3:AttributeDesignator AttributeId="urn:oasis:names:tc:xacml
                            :3.0:subject:authn-locality:ip-address" Category="urn:oasis:
                            names:tc:xacml:1.0:subject-category:access-subject" DataType="
                            urn:oasis:names:tc:xacml:2.0:data-type:ipAddress" MustBePresent=
                            "false"/>
117                 </xacml3:Apply>
118             </xacml3:Apply>
119         </xacml3:Apply>
120     </xacml3:Condition>
121 </xacml3:Rule>
122 <xacml3:Rule Effect="Permit" RuleId="Furuset.Maintenance/Furuset.remote_Update_IED_3">
123     <xacml3:Description>Rule for remote updating of IED_3 on a specific date.</xacml3:
            Description>
124     <xacml3:Target>
125         <xacml3:AnyOf>
126             <xacml3:AllOf>
127                 <xacml3:Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-
                        equal">
128                     <xacml3:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#
                            string">IED_3</xacml3:AttributeValue>
129                     <xacml3:AttributeDesignator AttributeId="urn:oasis:names:tc:xacml
                            :1.0:resource:resource-id" Category="urn:oasis:names:tc:xacml
                            :3.0:attribute-category:resource" DataType="http://www.w3.org
                            /2001/XMLSchema#string" MustBePresent="false"/>
130                 </xacml3:Match>
131                 <xacml3:Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-
                        equal">
132                     <xacml3:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#
                            string">Chloe</xacml3:AttributeValue>
133                     <xacml3:AttributeDesignator AttributeId="urn:oasis:names:tc:xacml
                            :1.0:subject:subject-id" Category="urn:oasis:names:tc:xacml:1.0:
                            subject-category:access-subject" DataType="http://www.w3.org
                            /2001/XMLSchema#string" MustBePresent="false"/>
134                 </xacml3:Match>
135                 <xacml3:Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-
                        equal">
136                     <xacml3:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#
                            string">ABB</xacml3:AttributeValue>
137                     <xacml3:AttributeDesignator AttributeId="urn:oasis:names:tc:xacml
                            :1.0:subject:subject-id-qualifier" Category="urn:oasis:names:tc:
                            xacml:1.0:subject-category:access-subject" DataType="http://www.
                            w3.org/2001/XMLSchema#string" MustBePresent="false"/>
```

```
138                 </xacml3:Match>
139                 <xacml3:Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-
                        equal">
140                     <xacml3:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#
                            string">Normal</xacml3:AttributeValue>
141                     <xacml3:AttributeDesignator AttributeId="situationType" Category="
                            urn:oasis:names:tc:xacml:3.0:attribute-category:environment"
                            DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent
                            ="false"/>
142                 </xacml3:Match>
143             </xacml3:AllOf>
144             <xacml3:AllOf>
145                 <xacml3:Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-
                        equal">
146                     <xacml3:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#
                            string">Maintenance</xacml3:AttributeValue>
147                     <xacml3:AttributeDesignator AttributeId="situationType" Category="
                            urn:oasis:names:tc:xacml:3.0:attribute-category:environment"
                            DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent
                            ="false"/>
148                 </xacml3:Match>
149                 <xacml3:Match MatchId="urn:oasis:names:tc:xacml:1.0:function:time-less-
                        than-or-equal">
150                     <xacml3:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#
                            time">10:00:00</xacml3:AttributeValue>
151                     <xacml3:AttributeDesignator AttributeId="urn:oasis:names:tc:xacml
                            :1.0:environment:current-time" Category="urn:oasis:names:tc:
                            xacml:3.0:attribute-category:environment" DataType="http://www.
                            w3.org/2001/XMLSchema#time" MustBePresent="false"/>
152                 </xacml3:Match>
153                 <xacml3:Match MatchId="urn:oasis:names:tc:xacml:1.0:function:time-
                        greater-than-or-equal">
154                     <xacml3:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#
                            time">14:00:00</xacml3:AttributeValue>
155                     <xacml3:AttributeDesignator AttributeId="urn:oasis:names:tc:xacml
                            :1.0:environment:current-time" Category="urn:oasis:names:tc:
                            xacml:3.0:attribute-category:environment" DataType="http://www.
                            w3.org/2001/XMLSchema#time" MustBePresent="false"/>
156                 </xacml3:Match>
157                 <xacml3:Match MatchId="urn:oasis:names:tc:xacml:1.0:function:date-equal"
                        >
158                     <xacml3:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#
                            date">01.06.2022</xacml3:AttributeValue>
159                     <xacml3:AttributeDesignator AttributeId="urn:oasis:names:tc:xacml
                            :1.0:environment:current-date" Category="urn:oasis:names:tc:
                            xacml:3.0:attribute-category:environment" DataType="http://www.
                            w3.org/2001/XMLSchema#date" MustBePresent="false"/>
160                 </xacml3:Match>
161             </xacml3:AllOf>
162         </xacml3:AnyOf>
163     </xacml3:Target>
164     <xacml3:Condition>
165         <xacml3:Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:or">
166             <xacml3:Apply FunctionId="urn:oasis:names:tc:xacml:3.0:function:any-of-any">
167                 <xacml3:Function FunctionId="urn:oasis:names:tc:xacml:1.0:function:
                        string-equal"/>
168                 <xacml3:AttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:
                        action:action-id" Category="urn:oasis:names:tc:xacml:3.0:attribute-
                        category:action" DataType="http://www.w3.org/2001/XMLSchema#string"
                         MustBePresent="false"/>
169                 <xacml3:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string
                        ">Update</xacml3:AttributeValue>
170             </xacml3:Apply>
171             <xacml3:Apply FunctionId="urn:oasis:names:tc:xacml:3.0:function:any-of-any">
172                 <xacml3:Function FunctionId="urn:oasis:names:tc:xacml:1.0:function:
                        string-equal"/>
173                 <xacml3:AttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:
```

```
                        action:action-id" Category="urn:oasis:names:tc:xacml:3.0:attribute-
                        category:action" DataType="http://www.w3.org/2001/XMLSchema#string"
                         MustBePresent="false"/>
174                   <xacml3:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string
                        ">Patch</xacml3:AttributeValue>
175                </xacml3:Apply>
176             </xacml3:Apply>
177          </xacml3:Condition>
178       </xacml3:Rule>
179       <xacml3:Rule Effect="Deny" RuleId="Furuset.Maintenance/Furuset.default_Deny">
180          <xacml3:Description>If no rule has been applied yet, return a denied response.</
               xacml3:Description>
181          <xacml3:Target/>
182       </xacml3:Rule>
183    </xacml3:Policy>
```

D.2 Use Case 2: XACML Test Request

```
<Request xmlns="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17" CombinedDecision="false"
    ReturnPolicyIdList="false">
<Attributes Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource">
<Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id" IncludeInResult
    ="false">
<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">IED_3</AttributeValue>
</Attribute>
</Attributes>
<Attributes Category="urn:oasis:names:tc:xacml:3.0:attribute-category:environment">
<Attribute AttributeId="situationType" IncludeInResult="false">
<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Maintenance</
    AttributeValue>
</Attribute>
</Attributes>
<Attributes Category="urn:oasis:names:tc:xacml:3.0:attribute-category:environment">
<Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:environment:current-time"
    IncludeInResult="false">
<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">12:00:00</
    AttributeValue>
</Attribute>
</Attributes>
<Attributes Category="urn:oasis:names:tc:xacml:3.0:attribute-category:environment">
<Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:environment:current-date"
    IncludeInResult="false">
<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">25.05.2022</
    AttributeValue>
</Attribute>
</Attributes>
<Attributes Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject">
<Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id" IncludeInResult="
    false">
<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Chloe</AttributeValue>
</Attribute>
</Attributes>
<Attributes Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject">
<Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id-qualifier"
    IncludeInResult="false">
<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">ABB</AttributeValue>
</Attribute>
</Attributes>
<Attributes Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action">
<Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id" IncludeInResult="
    false">
<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Patch</AttributeValue>
</Attribute>
</Attributes>
</Request>
```

E Use Case 3: Troubleshooting Policy in ALFA

```
namespace Attributes {
    import System.*

    attribute situationType {
       id = "situationType"
       type = string
       category = environmentCat
    }
 }

namespace Furuset {
    policy Troubleshooting {
    apply firstApplicable
    local_External_Troubleshoot
    deny_Invalid_IP
    remote_External_Troubleshoot
    default_Deny
    }

    rule local_External_Troubleshoot {
        target clause Attributes.resourceId == "IED_1.logs"
        or Attributes.resourceId == "IED_2.logs"
        or Attributes.resourceId == "IED_3.logs"
        and Attributes.situationType == "Normal"
        or Attributes.situationType == "Maintenance"
        and Attributes.subjectIdQualifier == "Statnett"
        or Attributes.subjectIdQualifier == "Siemens"
        and Attributes.currentTime >= "07:00:00":time
        and Attributes.currentTime <= "21:00:00":time
        condition (Attributes.actionId == "Read" || Attributes.actionId == "Update"
        || Attributes.actionId == "Patch")
        permit
    }

    /* If remote IP address is invalied, deny access. */
    rule deny_Invalid_IP {
        condition not(
            ipAddressRegexpMatch(
                "^(10)\\.(10)\\.(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9])\\:([2404])$",
                ipAddressOneAndOnly(Attributes.subjectLocalityIpAddress)))
        deny
    }

    rule remote_External_Troubleshoot {
        target clause Attributes.resourceId == "IED_1.logs"
        or Attributes.resourceId == "IED_2.logs"
        or Attributes.resourceId == "IED_3.logs"
        and Attributes.situationType == "Maintenance"
        or Attributes.situationType == "Emergency"
        and Attributes.subjectId == "Glenn"
        and Attributes.subjectIdQualifier == "Siemens"
        condition (Attributes.actionId == "Read")
        permit
    }

    /* If no rule has been applied yet, return a denied response. */
    rule default_Deny {
        deny
    }
```

```
}
```

E.1 Use Case 3: Troubleshooting Policy in XACML

```
<?xml version="1.0" encoding="UTF-8"?><!--This file was generated by the ALFA Plugin for Eclipse from Axiomatics AB (http://www.axiomatics.com).--><!--Any modification to this file will be lost upon recompilation of the source ALFA file-->
<xacml3:Policy xmlns:xacml3="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17" PolicyId="http://axiomatics.com/alfa/identifier/Furuset.Troubleshooting" RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:first-applicable" Version="1.0">
   <xacml3:Description/>
   <xacml3:PolicyDefaults>
      <xacml3:XPathVersion>http://www.w3.org/TR/1999/REC-xpath-19991116</xacml3:XPathVersion>
   </xacml3:PolicyDefaults>
   <xacml3:Target/>
   <xacml3:Rule Effect="Permit" RuleId="Furuset.Troubleshooting/Furuset.local_External_Troubleshoot">
      <xacml3:Description/>
      <xacml3:Target>
         <xacml3:AnyOf>
            <xacml3:AllOf>
               <xacml3:Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
                  <xacml3:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">IED_1.logs</xacml3:AttributeValue>
                  <xacml3:AttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id" Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource" DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="false"/>
               </xacml3:Match>
            </xacml3:AllOf>
            <xacml3:AllOf>
               <xacml3:Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
                  <xacml3:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">IED_2.logs</xacml3:AttributeValue>
                  <xacml3:AttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id" Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource" DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="false"/>
               </xacml3:Match>
            </xacml3:AllOf>
            <xacml3:AllOf>
               <xacml3:Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
                  <xacml3:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">IED_3.logs</xacml3:AttributeValue>
                  <xacml3:AttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id" Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource" DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="false"/>
               </xacml3:Match>
               <xacml3:Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
                  <xacml3:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Normal</xacml3:AttributeValue>
                  <xacml3:AttributeDesignator AttributeId="situationType" Category="urn:oasis:names:tc:xacml:3.0:attribute-category:environment" DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="false"/>
               </xacml3:Match>
            </xacml3:AllOf>
            <xacml3:AllOf>
```

```
35                  <xacml3:Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-
                        equal">
36                      <xacml3:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#
                            string">Maintenance</xacml3:AttributeValue>
37                      <xacml3:AttributeDesignator AttributeId="situationType" Category="
                            urn:oasis:names:tc:xacml:3.0:attribute-category:environment"
                            DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent
                            ="false"/>
38                  </xacml3:Match>
39                  <xacml3:Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-
                        equal">
40                      <xacml3:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#
                            string">Statnett</xacml3:AttributeValue>
41                      <xacml3:AttributeDesignator AttributeId="urn:oasis:names:tc:xacml
                            :1.0:subject:subject-id-qualifier" Category="urn:oasis:names:tc:
                            xacml:1.0:subject-category:access-subject" DataType="http://www.
                            w3.org/2001/XMLSchema#string" MustBePresent="false"/>
42                  </xacml3:Match>
43              </xacml3:AllOf>
44              <xacml3:AllOf>
45                  <xacml3:Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-
                        equal">
46                      <xacml3:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#
                            string">Siemens</xacml3:AttributeValue>
47                      <xacml3:AttributeDesignator AttributeId="urn:oasis:names:tc:xacml
                            :1.0:subject:subject-id-qualifier" Category="urn:oasis:names:tc:
                            xacml:1.0:subject-category:access-subject" DataType="http://www.
                            w3.org/2001/XMLSchema#string" MustBePresent="false"/>
48                  </xacml3:Match>
49                  <xacml3:Match MatchId="urn:oasis:names:tc:xacml:1.0:function:time-less-
                        than-or-equal">
50                      <xacml3:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#
                            time">07:00:00</xacml3:AttributeValue>
51                      <xacml3:AttributeDesignator AttributeId="urn:oasis:names:tc:xacml
                            :1.0:environment:current-time" Category="urn:oasis:names:tc:
                            xacml:3.0:attribute-category:environment" DataType="http://www.
                            w3.org/2001/XMLSchema#time" MustBePresent="false"/>
52                  </xacml3:Match>
53                  <xacml3:Match MatchId="urn:oasis:names:tc:xacml:1.0:function:time-
                        greater-than-or-equal">
54                      <xacml3:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#
                            time">21:00:00</xacml3:AttributeValue>
55                      <xacml3:AttributeDesignator AttributeId="urn:oasis:names:tc:xacml
                            :1.0:environment:current-time" Category="urn:oasis:names:tc:
                            xacml:3.0:attribute-category:environment" DataType="http://www.
                            w3.org/2001/XMLSchema#time" MustBePresent="false"/>
56                  </xacml3:Match>
57              </xacml3:AllOf>
58          </xacml3:AnyOf>
59      </xacml3:Target>
60      <xacml3:Condition>
61          <xacml3:Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:or">
62              <xacml3:Apply FunctionId="urn:oasis:names:tc:xacml:3.0:function:any-of-any">
63                  <xacml3:Function FunctionId="urn:oasis:names:tc:xacml:1.0:function:
                        string-equal"/>
64                  <xacml3:AttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:
                        action:action-id" Category="urn:oasis:names:tc:xacml:3.0:attribute-
                        category:action" DataType="http://www.w3.org/2001/XMLSchema#string"
                         MustBePresent="false"/>
65                  <xacml3:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string
                        ">Read</xacml3:AttributeValue>
66              </xacml3:Apply>
67              <xacml3:Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:or">
68                  <xacml3:Apply FunctionId="urn:oasis:names:tc:xacml:3.0:function:any-of-
                        any">
69                      <xacml3:Function FunctionId="urn:oasis:names:tc:xacml:1.0:function:
                            string-equal"/>
```

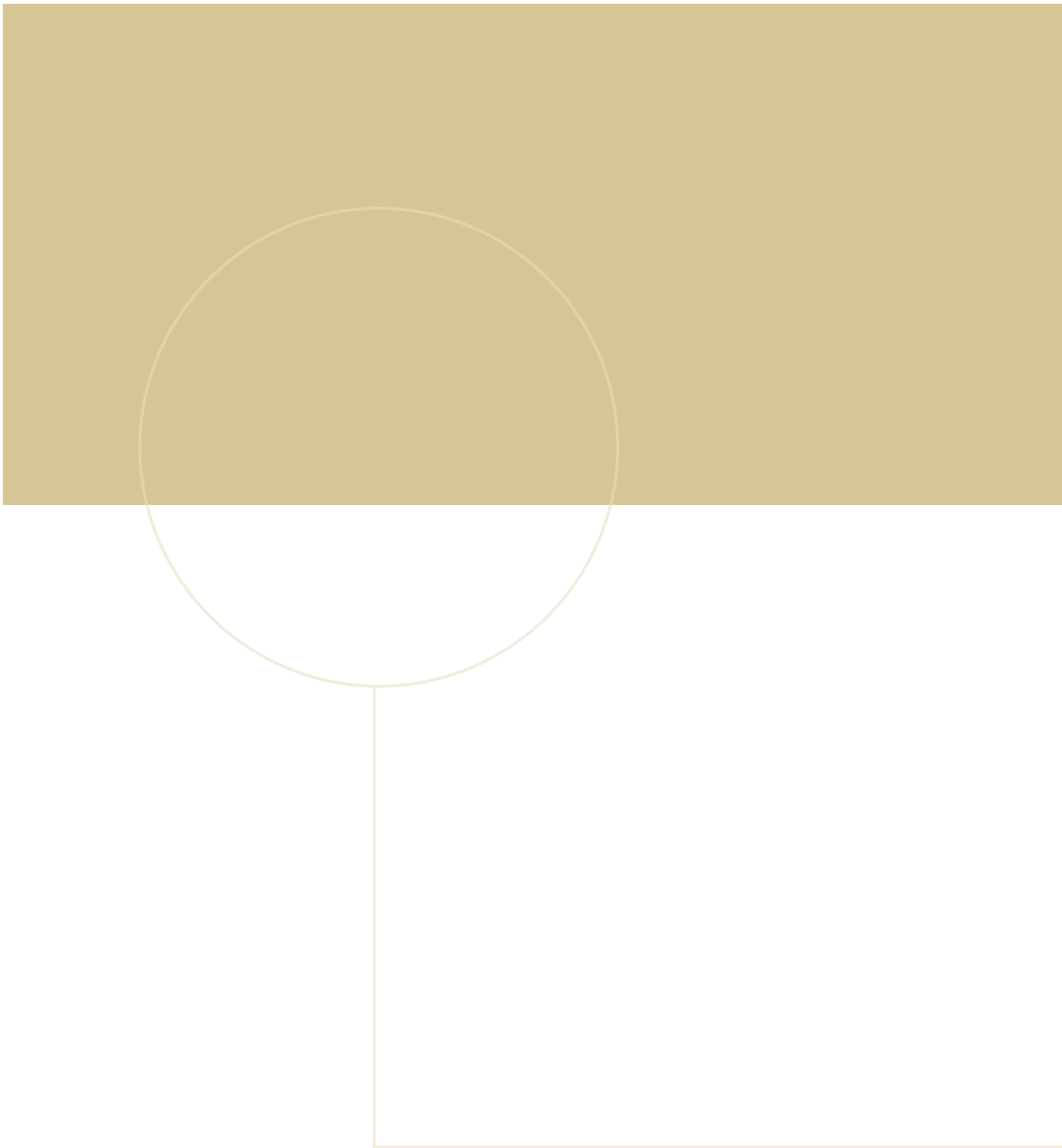
```
70                      <xacml3:AttributeDesignator AttributeId="urn:oasis:names:tc:xacml
                            :1.0:action:action-id" Category="urn:oasis:names:tc:xacml:3.0:
                            attribute-category:action" DataType="http://www.w3.org/2001/
                            XMLSchema#string" MustBePresent="false"/>
71                      <xacml3:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#
                            string">Update</xacml3:AttributeValue>
72                  </xacml3:Apply>
73                  <xacml3:Apply FunctionId="urn:oasis:names:tc:xacml:3.0:function:any-of-
                        any">
74                      <xacml3:Function FunctionId="urn:oasis:names:tc:xacml:1.0:function:
                            string-equal"/>
75                      <xacml3:AttributeDesignator AttributeId="urn:oasis:names:tc:xacml
                            :1.0:action:action-id" Category="urn:oasis:names:tc:xacml:3.0:
                            attribute-category:action" DataType="http://www.w3.org/2001/
                            XMLSchema#string" MustBePresent="false"/>
76                      <xacml3:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#
                            string">Patch</xacml3:AttributeValue>
77                  </xacml3:Apply>
78              </xacml3:Apply>
79          </xacml3:Apply>
80      </xacml3:Condition>
81  </xacml3:Rule>
82  <xacml3:Rule Effect="Deny" RuleId="Furuset.Troubleshooting/Furuset.deny_Invalid_IP">
83      <xacml3:Description>If remote IP address is invalied, deny access.</xacml3:
            Description>
84      <xacml3:Target/>
85      <xacml3:Condition>
86          <xacml3:Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:not">
87              <xacml3:Apply FunctionId="urn:oasis:names:tc:xacml:2.0:function:ipAddress-
                    regexp-match">
88                  <xacml3:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string
                        ">^(10)\.(10)\.(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9])\:([2404])$</
                        xacml3:AttributeValue>
89                  <xacml3:Apply FunctionId="urn:oasis:names:tc:xacml:2.0:function:
                        ipAddress-one-and-only">
90                      <xacml3:AttributeDesignator AttributeId="urn:oasis:names:tc:xacml
                            :3.0:subject:authn-locality:ip-address" Category="urn:oasis:
                            names:tc:xacml:1.0:subject-category:access-subject" DataType="
                            urn:oasis:names:tc:xacml:2.0:data-type:ipAddress" MustBePresent=
                            "false"/>
91                  </xacml3:Apply>
92              </xacml3:Apply>
93          </xacml3:Apply>
94      </xacml3:Condition>
95  </xacml3:Rule>
96  <xacml3:Rule Effect="Permit" RuleId="Furuset.Troubleshooting/Furuset.
        remote_External_Troubleshoot">
97      <xacml3:Description/>
98      <xacml3:Target>
99          <xacml3:AnyOf>
100             <xacml3:AllOf>
101                 <xacml3:Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-
                        equal">
102                     <xacml3:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#
                            string">IED_1.logs</xacml3:AttributeValue>
103                     <xacml3:AttributeDesignator AttributeId="urn:oasis:names:tc:xacml
                            :1.0:resource:resource-id" Category="urn:oasis:names:tc:xacml
                            :3.0:attribute-category:resource" DataType="http://www.w3.org
                            /2001/XMLSchema#string" MustBePresent="false"/>
104                 </xacml3:Match>
105             </xacml3:AllOf>
106             <xacml3:AllOf>
107                 <xacml3:Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-
                        equal">
108                     <xacml3:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#
                            string">IED_2.logs</xacml3:AttributeValue>
109                     <xacml3:AttributeDesignator AttributeId="urn:oasis:names:tc:xacml
```

```
                        :1.0:resource:resource-id" Category="urn:oasis:names:tc:xacml
                        :3.0:attribute-category:resource" DataType="http://www.w3.org
                        /2001/XMLSchema#string" MustBePresent="false"/>
110                 </xacml3:Match>
111             </xacml3:AllOf>
112             <xacml3:AllOf>
113                 <xacml3:Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-
                        equal">
114                     <xacml3:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#
                            string">IED_3.logs</xacml3:AttributeValue>
115                     <xacml3:AttributeDesignator AttributeId="urn:oasis:names:tc:xacml
                            :1.0:resource:resource-id" Category="urn:oasis:names:tc:xacml
                            :3.0:attribute-category:resource" DataType="http://www.w3.org
                            /2001/XMLSchema#string" MustBePresent="false"/>
116                 </xacml3:Match>
117                 <xacml3:Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-
                        equal">
118                     <xacml3:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#
                            string">Normal</xacml3:AttributeValue>
119                     <xacml3:AttributeDesignator AttributeId="situationType" Category="
                            urn:oasis:names:tc:xacml:3.0:attribute-category:environment"
                            DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent
                            ="false"/>
120                 </xacml3:Match>
121             </xacml3:AllOf>
122             <xacml3:AllOf>
123                 <xacml3:Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-
                        equal">
124                     <xacml3:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#
                            string">Maintenance</xacml3:AttributeValue>
125                     <xacml3:AttributeDesignator AttributeId="situationType" Category="
                            urn:oasis:names:tc:xacml:3.0:attribute-category:environment"
                            DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent
                            ="false"/>
126                 </xacml3:Match>
127             </xacml3:AllOf>
128             <xacml3:AllOf>
129                 <xacml3:Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-
                        equal">
130                     <xacml3:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#
                            string">Emergency</xacml3:AttributeValue>
131                     <xacml3:AttributeDesignator AttributeId="situationType" Category="
                            urn:oasis:names:tc:xacml:3.0:attribute-category:environment"
                            DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent
                            ="false"/>
132                 </xacml3:Match>
133                 <xacml3:Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-
                        equal">
134                     <xacml3:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#
                            string">Glenn</xacml3:AttributeValue>
135                     <xacml3:AttributeDesignator AttributeId="urn:oasis:names:tc:xacml
                            :1.0:subject:subject-id" Category="urn:oasis:names:tc:xacml:1.0:
                            subject-category:access-subject" DataType="http://www.w3.org
                            /2001/XMLSchema#string" MustBePresent="false"/>
136                 </xacml3:Match>
137                 <xacml3:Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-
                        equal">
138                     <xacml3:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#
                            string">Siemens</xacml3:AttributeValue>
139                     <xacml3:AttributeDesignator AttributeId="urn:oasis:names:tc:xacml
                            :1.0:subject:subject-id-qualifier" Category="urn:oasis:names:tc:
                            xacml:1.0:subject-category:access-subject" DataType="http://www.
                            w3.org/2001/XMLSchema#string" MustBePresent="false"/>
140                 </xacml3:Match>
141             </xacml3:AllOf>
142         </xacml3:AnyOf>
143     </xacml3:Target>
```

```
        <xacml3:Condition>
            <xacml3:Apply FunctionId="urn:oasis:names:tc:xacml:3.0:function:any-of-any">
                <xacml3:Function FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-
                    equal"/>
                <xacml3:AttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:action
                    :action-id" Category="urn:oasis:names:tc:xacml:3.0:attribute-category:
                    action" DataType="http://www.w3.org/2001/XMLSchema#string"
                    MustBePresent="false"/>
                <xacml3:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                    Read</xacml3:AttributeValue>
            </xacml3:Apply>
        </xacml3:Condition>
    </xacml3:Rule>
    <xacml3:Rule Effect="Deny" RuleId="Furuset.Troubleshooting/Furuset.default_Deny">
        <xacml3:Description>If no rule has been applied yet, return a denied response.</
            xacml3:Description>
        <xacml3:Target/>
    </xacml3:Rule>
</xacml3:Policy>
```

E.2 Use Case 3: XACML Test Request

```
<Request xmlns="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17" CombinedDecision="false"
    ReturnPolicyIdList="false">
<Attributes Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource">
<Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id" IncludeInResult
    ="false">
<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">IED_2.logs</
    AttributeValue>
</Attribute>
</Attributes>
<Attributes Category="urn:oasis:names:tc:xacml:3.0:attribute-category:environment">
<Attribute AttributeId="situationType" IncludeInResult="false">
<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Maintenance</
    AttributeValue>
</Attribute>
</Attributes>
<Attributes Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject">
<Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id" IncludeInResult="
    false">
<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Glenn</AttributeValue>
</Attribute>
</Attributes>
<Attributes Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject">
<Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id-qualifier"
    IncludeInResult="false">
<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Siemens</AttributeValue
    >
</Attribute>
</Attributes>
<Attributes Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action">
<Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id" IncludeInResult="
    false">
<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Read</AttributeValue>
</Attribute>
</Attributes>
</Request>
```



NTNU

Norwegian University of
Science and Technology