A Generic Role Based Access Control Model for Wind Power Systems

Anand Nagarajan and Christian Damsgaard Jensen†
Technical University of Denmark
Kgs. Lyngby, Denmark
†*Christian.Jensen@imm.dtu.dk*

Abstract

The electrical power infrastructure is facing a transition from a largely centralised distribution infrastructure with a few large power plants to an increasingly distributed infrastructure that must incorporate privately owned and operated power generation units based on fuel cells or sustainable energy sources, such as wind turbines, solar energy or wave energy. This introduces important new security challenges that are not adequately addressed by existing approaches to security in the electrical power distribution infrastructure.

In this paper we examine some of the security challenges that may arise in the emerging energy distribution infrastructure. In particular, we examine the security problems that arise in the area of wind power communication infrastructures based on the IEC 61400-25 and IEC 62351 standards. These standards define ways of representing elements of the wind power infrastructure in a software domain in a manufacturer independent manner as well as establishing secure communication and authenticating the other parties in electrical power infrastructures, but they do not address the problem of access control. We therefore propose a generic model for access control in wind power systems, which is based on the widely used role-based access control model. The proposed model is tested using a prototype designed in conformance with the standards that are in use in modern wind power infrastructure and the results are presented to determine the overhead in communication caused while adhering to the proposed access model.

1 Introduction

Dwindling fossil energy reserves and an increased focus on clean energy have lead to an increased use of wind power as a source of energy. This has resulted in an increase in the size and scale of the wind power infrastructure from earlier wind power generator consisting of a single wind turbine to large wind power plants with more than a hundred wind turbines which can generate several hundreds of megawatts [7]. The distributed location of wind power systems and the sheer size of the total wind power infrastructure encompassing several of these wind power plants make it difficult to control and monitor them by manual means as was initially done when wind power systems emerged. This has resulted in the need for control and monitoring of these components remotely, preferably over the Internet, along with standards to facilitate the control and monitoring of these systems.

Exposing wind power systems to the Internet has made them vulnerable to attacks from various malicious forces from the external world who strive to disrupt the network, usually for financial reasons. Standardization makes it much easier to launch attacks as knowledge about data structures and communication frameworks used in the industry are no longer secret as was normally the case in earlier wind power systems, where each manufacturer had their own data structures and their own proprietary communication protocols that where often considered trade secrets. In order to mitigate attacks from different external entities, the Internal Energy Commission (IEC) had introduced the IEC 62351 standards defining security measures for the protection of the communication infrastructure used to control and monitor these wind power plant and the individual components remotely over the Internet. However,

Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, volume: 1, number: 4, pp. 35-49

the standard does not offer a complete mitigation of these threats since the standard does not address the issue of access control. In the absence of an access control policy, an entity can claim more privileges than it is entitled to which can be disastrous. Regulating the access to the different components of a wind power infrastructure is therefore crucial to minimize the impact of attacks and also to ensure a secure and accountable operation of wind power systems. The purpose of this paper is to describe an access control model that can supplement the IEC 62351 standards which facilitate security of the wind power systems along with presenting suggestions to improve the security of the IEC 62351 standard. The three main contributions of this paper are to:

1. Provide a brief overview of the standards that define the operation and security of wind power systems;
2. identify the access control requirements that must be enforced by a secure electrical power infrastructure;
3. present a general role-based access control (RBAC) based framework for a wind power control infrastructure.

The rest of this paper is organized in the following way: we start, in Section 2, by a brief presentation of the architecture of modern wind power infrastructures. This is followed, in Section 3, by a brief overview of the the evolution of the wind power infrastructure in the past couple of decades and security standards that are emerging to address new threats to the critical electrical power infrastructure. Section 4 examines the assets, threats and resources in wind power infrastructures and identify some of the most important security requirements. The access control model that we have developed to address the specific security requirements relating to access control in wind power systems is presented in Section 5 and the simple prototype that we developed is presented in Section 6. Finally, in Section 7, we conclude by presenting a brief review on the goals of this paper and the interoperability of the proposed access control model with the existing standards without adding significant overhead while serving the security purpose.

2 Modern Wind Power Infrastructure

Modern wind power systems are complex architectures spread over hundreds of kilometres and are normally composed of several grids that generate electricity. The fundamental component, which is responsible for generating electricity, is a wind turbine. Several wind turbines are typically located in a single area to form a wind farm. A power grid normally includes several such wind farms. Theoretically the total amount of energy generated by the wind power system architecture is the sum of the energy produced by each individual turbine present in that network. Power Generation is monitored and regulated through a common communication infrastructure that conveys the control commands to the respective turbines and farms.

Thus, the modern Infrastructure for wind power systems comprises both the physical electrical power generation components and the communication infrastructure used to monitor and control those components. The physical infrastructure consists primarily of the machinery that is responsible for generating electricity from the wind, i.e., the wind turbines. The communication component of the infrastructure consists of the protocols and instructions that are used to control and monitor the physical infrastructure in order to regulate the amount of energy produced. Regulation plays an important role in compensating the discrepancy in the generated power, thus allowing the producer to meet his contractual obligations, as well as ensure that the amount of generated power is not too high to cause an outage. The generation of electrical power is controlled by a hierarchy of agencies that control power generation at national,

regional and local levels. Every wind farm is associated with a wind farm controller that manages and controls the individual wind turbines in the wind farm. Generated power is regulated at grid level by identifying the grid that is producing surplus or less energy. Having identified the grid the focus is next on identifying the individual wind farms that cause this erratic behaviour and then once the malfunctioning wind farms are identified, the individual wind turbines responsible for wind farms to exhibit the anomaly are identified. Appropriate action is then taken by passing control instructions to reduce the amount of generated power in case excess power is being generated. In case of a shortfall, the deficit is compensated by increasing the output from other wind turbines or other wind d farms or adjoining grid depending on the magnitude of the deficit and the ability of these farms to produce energy. A smaller deficit would mean that the deficit can be compensated locally within the same farm or with the adjoining wind farms while a larger one would result in the need for a number of wind farms or grids to increase their production accordingly. In addition to the regulation of power, monitoring is also used for statistical reasons such as billing, reporting, and logging.

3 Evolution and Standardisation in Wind Power Systems

In the following, we present a brief overview of the evolution of wind power systems for electrical power generation during the past 40 years and the standards that are emerging to address the increasingly important role of wind power in the global electrical power generation infrastructure.

3.1 Evolution of Wind Power Systems

Initially Wind Power Systems were local energy resources that catered to users within a short distance from their location. This resulted in distributed energy generation, where a relatively small independent unit is constructed close to the area where power is consumed in order to reduce transmission losses. Proximity of the power generation system and the need for the system to cater only to users within a specific location – with isolation from outside its region of infrastructure – meant that the operator was free to use proprietary or customized standards in the design and implementation of the wind power system. However, growing demands for renewable energy and the subsidies that establishment of wind power plants has received from governments and environmental agencies coupled with the lucrative profits to be earned saw the entry of major players into the wind energy market. This has led to the establishment of wind power plants distributed over large geographical areas that are not necessarily close to each other but which are owned and operated by a single electrical power company which controls and monitors the operation of individual wind turbines. The geographical distribution of the wind turbines and wind farms over large areas increased the need for automation and communication.

The existence of multiple operators, where each operator has their own distinct communication and implementation methodologies, introduces the following problems:

- Use of non-standardized custom protocols by operators hinders inter-operability between different operators in a power grid since customized protocols must be developed to interact with each foreign operator; this does not scale well with the increasing growth of players in the wind energy market

- The presence of multiple operators provides a possibility for a customer to change from one operator to another. However, the tight coupling between a vendor and his customer means that a customer who wishes to change from one vendor to another has to make several changes to his software infrastructure.

3.2 Standards in Wind Power Systems

The ideal solution to the issues identified above is that all vendors use the same modelling of the wind power plants, so that customers can choose vendor from a business related perspective rather than letting the modelling of the wind power plants be the key decision factor.

In order to facilitate the monitoring and control of wind power plants in a manufacturer, operator agnostic manner, the IEC 61400-25 [5] standards were developed. This standard defines every element of the wind power infrastructure, along with their attributes, and represents the individual elements in the software domain. In order to prevent naming collisions, as well as to identify each element uniquely in the wind power domain, the standard provides a hierarchical naming scheme for information about the individual components (more about that in Section 4). By carefully defining attributes, the standard also aims to provide information about components without conflicting with the commercial interests of the manufactures. An outcome of adoption of the standards was that it facilitates exchange of information between wind power plant components in a manufacturer independent environment and the standard addresses vendors (manufacturers, suppliers), operators, owners, planners and designers of wind power plants as well as system integrators and utility companies operating in the wind energy market in a seamless fashion. Additionally, the IEC also developed the IEC 62351 standard [6] to promote secure communication between components in a wind power system.

4 Security Requirements

Automation and control of wind power systems have meant that the security of the infrastructure is not only based on the security of the physical infrastructure but also that of the communication infrastructure.

As mentioned above, the early days of the wind power industry was dominated by wind power systems that were locally owned and operated. Consequently this meant that the communication infrastructure was still primitive and had the following features:

- The communication was point to point and the control instruction to the components of the power system was relayed through wires that were directly connected to the components control infrastructure from the command centre.
- Prior to the development of the standards mentioned in the previous section, wind power producers had their own proprietary protocols to monitor communications. These protocols did not attach much importance to security, because communication lines were considered physically secure and details of the protocol implementation were hidden from the outside world.

In short, the communication was secure as long as the link had not been physically compromised and the proprietary details had not been revealed.

In the current scenario, however, where implementation details are well known and communication is no longer restricted to secure point-to-point connections, many of the security benefits offered by the earlier arrangement are no longer valid.

Hence it becomes clear that Security can no longer be neglected as was the case earlier. In order to secure the communication infrastructure, the International Energy commission came out the with the IEC 62351 [6] standards. Although the IEC 62351 provides measures to ensure the security of the communication infrastructure and the authentication of entities, the standard does not provide means to enforce authorisation rights in detail.

In order to understand the importance of authorisation, we present below the results of a simple risk analysis in the domain of interest, where we identify resources along with the threats associated with these resources.

4.1 Assets

Assets in the wind power domain can be classified into the following categories:

Generated Power The primary asset in a wind power system is the generated electrical power. The amount of power generated is regulated by the contractual obligations between the producer and the regulating agencies. From a software perspective, attackers (discussed in the ensuing section) can cause a violation of the contract by making the software controlled components behave erratically, causing an outage (excess production of power) or causing a partial or a complete disruption of the generated power.

As an example, an attacker could block a rotor, by issuing a command to block the rotor or to change its angle in an adverse manner to disrupt the working of the rotor.

Information about components and logs Information about the attributes of a component (such as the manufacturer of turbine) is also an important asset in a wind power system from a commercial perspective. In order to understand the utility of this asset, let us review the composition of a typical wind farm. As described in Section 2, a wind farm consists of several wind turbines, where each wind turbine is made up of a several individual components, such as the rotor, the yaw motor etc. Each wind turbine in the farm typically have components that are produced by competing manufacturers. As an example, a wind farm can have x number of turbines whose rotor is manufactured by company X and y number of turbines whose rotors are manufactured by a competitor Y. It is also possible that a third company Z is responsible for the maintenance of all the rotors in the wind farm. A unique aspect of the wind power industry is that the manufactures of the components enter into an privacy agreement with the buyers of the component (the wind turbine owner in our case) who must guarantee that their identity and the number of components sold is not revealed to their competitors, so that market poaching by such competitors can be prevented. One possible solution would be that components do not provide information about their manufacturers. However, this solution is not acceptable since the manufacturer has to be contacted in the case of warranty related claims and the manufacturer may wish to keep track of the performance of produced components in order to obtain feedback that is essential to improve the existing design or help in the design of new components. Under such circumstances information that could reveal the identity of the manufacturer has to be safeguarded from competitors who could potentially use these information to engage in market poaching.

Information contained in logs is also an important asset that has to be protected from adversaries. In a typical wind turbine, the logs record information about the operational parameters as well as the measurements recorded. Adversaries might wish to affect the working of the system by modifying the operational parameters (such as modifying the event timing information in logs to prevent components from changing their values, such as direction, at the time specified in the logs).

Reputation of the Producer The reputation of the producer is a less tangible asset but its security significance comes into play in the case a producer has to honour its commitment to manufacturers of a wind power component that their identity would not be revealed to its competitors, and also if the producer has to honour his commitment of producing the agreed amount of power.

4.2 Attackers

Assets listed in the above section are exposed to attack from various attackers. These attackers can be classified as:

Enthusiasts They consist of individuals or small loosely knit teams who want to disrupt the generation of power for their personal pleasure. Their goal is to break the security system, and in many cases the motivating factor is the fame associated with breaking the system. This group is characterized by having limited financial resources and expensive equipment needed to carry out attacks is not available to them. This community, however, has a wealth of technical knowledge and time that they can use to disrupt the working of one or more wind power components.

Professional Hackers They are essentially criminal entities who break into the assets at the behest of a competitor or for their own ulterior motives like extorting money from owners of wind power plants by threatening an attack on the infrastructure that may disrupt the generation of power. This group of attackers is characterized by a desire for financial gain. This group of attackers has access to greater technical resources than enthusiasts. Professional hackers disrupting power and holding companies to ransom have gained notoriety over the past few years.

On August 14th 2003 large parts of the Northeastern and Midwestern United States and Ontario, Canada, suffered a power blackout as a consequence of power outage caused supposedly due to a hacker [3]. The blackout affected an estimated 10 million people in the Canadian province of Ontario and 45 million people in eight U.S. states. This incident is not an isolated case and there have been several reports of hackers extorting companies of millions of dollars. According to Allan Paller, director of the SANS Institute, an organisation that hosts a crisis centre for hacked companies, describes cyber-extortion as the biggest untold story of the cyber-crime industry. Paller further states that "Hundreds of millions of dollars have been extorted, and possibly more. It's difficult to know, because they pay to keep it a secret."[4].

Competing companies This is probably the smallest group of attackers which consist of competing manufacturers who wish to damage the revenue stream of a competitor by using unfair business practises to increase their sales at the cost of a competitor. This category has almost limitless resources and can employ means like spying or employing professional hackers to obtain the information of interest. In addition they can obtain nearly all the necessary information via bribery, extortion or other means.

Insiders Knowledgeable insiders who have turned malicious are also quite a small group of attackers which includes disgruntled employees and spies.

Terrorists The growing relevance and prominence of wind power system makes them prone to attack by terrorists to disrupt the power generation. Typical Scenarios may include a terrorist bypassing the authentication mechanism of Internet controlled wind power components, and in a majority of the organisations where the control instructions are taken over the analog means like the telephone, masquerading (pretending to be someone whom they are not) to issue malicious control instructions to disrupt the functioning of the wind power plants to disrupt power generation that could have far reaching consequences.

While not exhaustive, we believe that these categories presented above cover the vast majority of significant types of attackers and it is to protect against them that we have designed our solution.

5 Access Control in Wind Power Systems

Having identified the need for an access control mechanism, we now proceed to identify the actors in the infrastructure so as to arrive at a correct access control model.

5.1 Actors in Wind power Systems

Wind power systems have different actors and stake holders. As it is the actors who are actively operating the system, we limit our analysis to identifying the actors that are commonly found in wind power systems. These actors are described below:

Transmission System Operator (TSO) The TSO is an unbiased organisation which is normally owned by the state. The purpose of the TSO is to regulate and balance the power market and to guarantee the security of the energy supply. The TSO also defines and upholds the market rules, which the power market participants must comply with when producing, trading and purchasing power. This is done to ensure a fair and free market. The TSO will, based on market information sent from a number of approved Balance Responsible Entities, balance the grid to prevent shortages of power.

Distribution System Operators (DSO) Each DSO has been approved by the TSO to control and maintain a portion of the distribution grid. They control the operation of wind farms or individual wind power plants under their domain to an amount of wind energy consistent with the required power and meteorological conditions by coordinating with the dispatch responsible entity and maintenance and operational centre for each individual zones that the portion under control has been further sub divided to.

Balance Responsible Entity (BRE) A BRE can be a power producing or trading company with special obligations toward the TSO. The BRE must supply the TSO through the DSO with information about production, consumption and trade for the upcoming 24-hour period. The TSO will then use this information to balance the market. The Balance Responsible Entity is also called the Dispatch Responsible Authority.

Wind Farm Controller (WFC) A wind farm is a collection of wind turbines which the WFC operates as a whole to obtain a consistent amount of wind power. The WFC reports to the maintenance and control operating centre of the Balance Responsible Entity.

Technical personnel for various components They include personnel who manage and repair the components of a wind power system. For example: Rotor service personnel should be allowed to monitor the state of the rotor and its service logs and to repair or replace the rotor when it is necessary.

all of these actors may have access to monitor and modify the settings for different parts of the wind power systems. In many cases, this includes remote access using the wind power system's *Supervisory Control and Data Acquisition (SCADA) system.* SCADA systems are used extensively to perform monitoring and acquire data from individual wind turbines. Control instructions to SCADA systems are given by wind farm controllers in response to the data obtained by individual wind turbines and instructions received from other entities, such as the WFC. SCADA systems then relay these instructions to the individual wind turbines.

The transient nature of the technical personnel who are typically given access to the repair and modification of the system – a task that may necessitate the need to look at different components without certainty about which components will be accessed, makes it difficult to use the mandatory access control framework, where privileges are usually hard coded. The Discretionary Access Control model is not a good candidate either since there is no way to provide fine grained control. Hence Role Based Access Control model offers the best fit to our problem domain owing to the fact that the number of roles is limited compared to the number of users and these roles can be extended easily to define new roles if needed.

5.2 Roles in Wind Power Systems

Based on the functionality and span of control associated with the actors identified in the previous section, we have identified the two classes of roles: Static Roles and Dynamic Roles. These classes of roles are described in greater details in the following.

5.2.1 Static Roles

The static roles are long term roles that correspond to the actors that are defined by legislation or regulation authorities. These can be divided into:

Regulator Roles These roles correspond to actors: BRE, TSO and the DSO. These actors maintain a long term association with the server. Currently the actors in this role can only read the values of all wind power components.

Control Roles These roles correspond to the wind farm controllers who can modify all values of the wind power components. Like the Regulators, these roles also maintain a long term association with the server. The regulators control the attributes of the individual components through the control entities.

The Regulator and control roles could be thought of as sharing a hierarchical relationship with the Control role having all the read privileges as the regulator along with its own write access roles.

5.2.2 Dynamic Roles

The dynamic roles are defined by the market and the practical considerations involved in operating a wind power infrastructure. These roles can be further divided into two main classes:

Operative Roles These Roles correspond to the technical personnel who carry out maintenance and repair of components. In order to prevent business poaching or to protect the interests of manufacturers, privileges to access attributes should be given on a case by case basis. For example: A wind Turbine is usually made up of components that do not belong to the same manufacturer. A Turbine may have some gear boxes manufactured by a company X and some by a company Y. The Turbine could be maintained by either company X or Y or a third company Z. The maintenance personel who belongs to company X should not know the manufacturer of gear boxes not manufactured by his company for business reasons.

Another essential feature of these roles is that these actors have a short term association with the server that is time bound when the actors are created (i.e., for an amount out of time a service personnel is allowed to undertake his maintenance work) and the privileges associated with actors role should be revoked at the end of duration. Another important facet associated with actors belonging to this role is that their privileges to resources are not clearly defined. This is because many a times a rotor maintenance person might need access to other components that influence the behaviour of the rotor. From a security and business perspective, privileges associated with operative roles must be carefully allocated in order to ensure that security of the system and the business obligations are not violated.

A means to enforce the privileges associated with the role would be the use of attribute certificates that could be self-signed by the administrator. An attribute certificate, which is defined in RFC 3281 [2], is similar to an X.509 identity certificate [1] except that it stores the mapping between a user and his assigned permissions. Attribute Certificates will have to be signed by an authority called as the source of authority (SOA). The SOA can either be a local signing authority or a

trusted third party. In our system, it is proposed that that the SOA be a local authority (the owner of the individual wind turbine). This is mainly due to the fact that getting a certificate signed commercially can be a costly affair. Moreover in a wind mill a finite and a limited number of components exist and these components are within the same domain and hence this justifies the use of self signed attribute certificates. The use of attribute certificates can be beneficial in case there arises a future need for the clients to directly interact with the components, with the role of server being only to authenticate the client and handing it the attribute certificate to enable the client interact with the component directly.

Manufacturer Roles These roles correspond to those actors who have manufactured the component. These roles also maintain a long association with the server. These actors enjoy an unlimited access to read the names of the components they have manufactured. However to access other attributes, they would have to be allocated privileges under the operative role.

Needless to say , the identified roles may be further sub classified as being dynamic and static roles with the Regulators , the Controllers having static privileges and the operative and manufacturer roles having dynamic privileges.

5.3 Resources in the Wind Power Domain

The resources include Wind Turbine Components Sub Component covered under this section include the rotor, transmission, generator, converter, nacelle, yaw system, tower and alarm system. These elements are represented in the software domain as classes according to the IEC 61400-25 series. Other components include the electrical power components and the meteorological components, however, but these components are not of importance to us because they are not represented in the software domain.

5.4 Assigning permissions to actors

Actors like the DSO and TSO are government owned entities and can virtually obtain information about all wind power components while a gearbox operator of a particular company should not have access to the name of a gear box that does not belong to him. The essence of assigning permissions to roles is to ensure that an entity does not obtain more privileges than it is legitimately entitled to. The resources that have been identified in our frame work have a number of attributes as defined in the IEC 61400-25 series. The names of the manufacturers of these components can only be seen by the owner and the wind farm controller and are hidden from the rest of the entities.

These attributes along with the valid permissions assigned to each of the actors are summarized in the thesis work[3]. For reasons of clarity and brevity, we consider only three of the classes of components specified in the IEC 61400-25 standards, and present a description of the roles along with the threats that are possible when these permissions are violated. The permissions are divided into read- and write access and identifies the type of role that should have that particular access right.

5.4.1 Physical Device Class

The physical device class defined in the IEC 61400-25 standard posses several attributes and operations. In the table below, we list only a subset of these attributes and operations along with the privilege associated with roles on these attributes. As described above, the attribute Phoneme describing the vendor name can only be read by an entity having manufacturer role and not any other entity thus providing protection from competitors who might engage in market poaching. The operation attribute pwrUp that is used to signal an increase in the amount of generated power can only be issued by entities having the

control roles and in case of entities possessing the dynamic roles only when the privilege to issue the pwrUp is assigned to them. Other entities corresponding to the Regulator role can only read the current Power Level and cannot modify the same.

Attribute Class		Permission		Threat Mitigated
Attribute	Description	write access	read access	
Phoneme	Name of vendor		Manufacturer	Market poaching
pwrUP	Increase power generation	Control roles, Dynamic roles (authorized operative roles)	Regulator(s), Control roles, Dynamic roles (authorized operative roles)	Power outage

Table 1: Assigning permission to roles for the physical device class

5.4.2 General Turbine Class

The wind turbine general information class defined in the IEC 61400-25 standard defines the statistical as well as the operational data of wind turbine along with operations to alter the operational data of the turbine. In the table presented below, we have presented a subset of these attributes to demonstrate the relevance of the access control model.

One of the important attributes of the wind turbine class is the AvlTmRs attribute that denotes the duration of time during which the turbine is available to participate in the generation of energy. Uncontrolled access to this attribute enables malicious entities to modify this attribute to a very low value that may result in a power deficit.

Another important attribute of any power generation network is the power factor. The power factor is defined theoretically as the ratio of active power divided by the sum total of the active power and the reactive power. A high power factor is at all time preferable and reduces energy consumption in the network and consequently the cost.

In relation to the active, reactive power and the powerfactor, the wind turbine class makes it feasible to disrupt the system by misusing commands, such as the active energy demand (DmdCh), the reactive enegery demand (DmdCh), prioritzation of the reactive energy over the active energy (VarRefPri) and the set points for the active and the reactive powers in order to optimize the power factor. A malicious entity with an uncontrolled access to these attributes can alter the attributes in a way that increases the powerfactor beyond or reduces it below the optimum value which can result in an economic impact, such as increased operational cost, which may in turn have an effect on the operating margin of the suppliers, or result in imbalances in the amount of active energy produced where an excess can cause an outage while a lower level can result in a shortage.

In the table below, we present the permissions that may be assigned to the entities that regulate these attributes along with a brief description of the threats mitagated by regulating these permissions. The table shows that almost all classes of roles are currently granted read access to all attributes, while control roles and dynamic roles that have been delegated authority by the WFC are granted write access to the attributes. These dynamic privileges are often short lived and assigned in an ad-hoc manner, i.e., when the privilege is needed to perform an assigned duty, so we have only listed the high level class of roles in the table. It is, however, important to note that the dynamic roles that have been granted write access to the AvlTmRs may be different from the dynamic roles that have been granted write access to the VarRefPri attribute.

Attribute Class		Permission		Threat Mitigated
Attribute	Description	write access	read access	
AVITRMS	Turbine availability time	Control roles, Dynamic roles (authorized operative roles)	Regulator(s), Control roles, Dynamic roles (authorized operative roles)	Can be altered to shut down the turbine
Dmdwh	Active energy demand	Control roles Dynamic roles (authorized operative roles)	Regulator(s), Control roles, Dynamic roles (authorized operative roles)	Can be altered to cause imbalance in energy production
DmdCh	Reactive energy demand	Control roles Dynamic roles (authorized operative roles)	Regulator(s) Control roles, Dynamic roles (authorized operative roles)	Can be altered to cause imbalance in energy production
SetTurOp	Wind turbine operation command	Control roles Dynamic roles (authorized operative roles)	Regulator(s), Control roles, Dynamic roles (authorized operative roles)	Can be altered to cause imbalance in energy production
VarOvw	Wind power reactive priority over active command	Control roles Dynamic roles (authorized operative roles)	Regulator(s), Control roles, Dynamic roles (authorized operative roles)	Can be altered to cause imbalance in energy production
VarRefPri	Wind turbine reactive set point priority command	Control roles Dynamic roles (authorized operative roles)	Regulator(s), Control roles, Dynamic roles (authorized operative roles)	Can be altered to cause imbalance in energy production
DmdW	Turbine active power generation set point	Control roles, Dynamic roles (authorized operative roles)	Regulator(s), Control roles, Dynamic roles (authorized operative roles)	Can be altered to cause imbalance in energy production
DmdVar	Turbine reactive power generation set point	Control roles Dynamic roles (authorized operative roles)	Regulator(s), Control roles, Dynamic roles (authorized operative roles)	Can be altered to cause imbalance in energy production
DmdPF	Turbine power factor set point	Control roles, Dynamic roles (authorized operative roles)	Regulator(s) Control roles, Dynamic roles (authorized operative roles)	Can be altered to cause imbalance in energy production

Table 2: Permissions of actors to the attributes of wind power general turbine class

5.4.3 Wind Turbine Transformer Class

The wind turbine transformer information class comprises the data that represent the wind turbine transformer information. In Table 3 below, we have presented a subset of these attributes to discuss the relevance of an access control model.

Attribute Class		Permission		Threat Mitigated
Attribute	Description	write access	read access	
AtvGriSw	Activation Command to main grid switch	Control roles, Dynamic roles (operative roles roles)	Control roles, Dynamic roles (operative roles roles)	Can cause Malfunction

Table 3: Permissions for the wind turbine transformer information class

An important attribute of the wind turbine transformer is the AtvGriSw attribute which controls access to the grid switch that can be used to connect or disconnect the wind turbine to the grid. This attribute is purely operational in nature, so it is only personnel with control roles or operative roles (ad-hoc personel with permissions assigned although this is rare) that have access to this attribute.

Unauthorised access to this attribute can result in an entire grid being turned off, causing an an energy deficit, so access to this attribute must be controlled; Table 3 illustrates the access control mechanism defined for this attribute.

5.4.4 Summary

The role based access control model presented in this paper distinguish between static and dynamic roles. The examples assigning prvileges to the different components of a wind power system, presented in this section, illustrates how the model works at the general level.

Table 1 shows the physical device class, where only the manufacurer of a component may access the name, while the regulation of power may be written by the Control roles and read by Regulator roles, Control roles and the dynamic roles to whom the WFC has delegated authority.

The general turbine class, illustrated in Table 2 illustrates a more complex access control scenario. It is important to note that the WFC may delegate different privileges to different operative roles in an ad-hoc manner, so despite the fact that the rows look very similar in Table 2, they may be very different in the actual enforcement of the access control model.

The attributes in the wind turbine transformer information class relate directly to the operation of the individual wind turbine, so only the Control role and the dynamic roles to whom the WFC has delegated authority are able to access the attributes.

6 Prototype

Having identified the conceptual access control model, we now proceed to describe the software implementation of the prototype.

In accordance with the IEC standard's recommendation for a client-server architecture to implement the virtual power plant model, our system will also have client server architecture. The proposed system has a Server that will provide a regulated interface through which external actors can monitor and control the components of the wind power plant. All requests for information and control commands to the individual components will be sent through the server. The Server then performs authentication and

access control to ensure that the requests and commands are legitimate and are issued only by an authorized entity. In case the request is found to be legitimate the request is forwarded on to the appropriate component. The response from the component is then forwarded to the requesting entity after suitably modifying the response to be in tune with the access privileges of the requester. Modules to perform authentication and access control are developed as separate components, so that the server can delegate authentication and access control to these components. This facilitates loose coupling and also prevents the overloading of the server module. Another advantage of this approach is that no changes are needed to the individual classes since authorization is not handled by these individual components.

The individual components only constitute a request response relationship with the server and will gladly send all the details to the server. The Access control module performs the task of selectively screening the response so that the requesting client gets access only to those data that it is entitled to. The overall system design is as illustrated below:

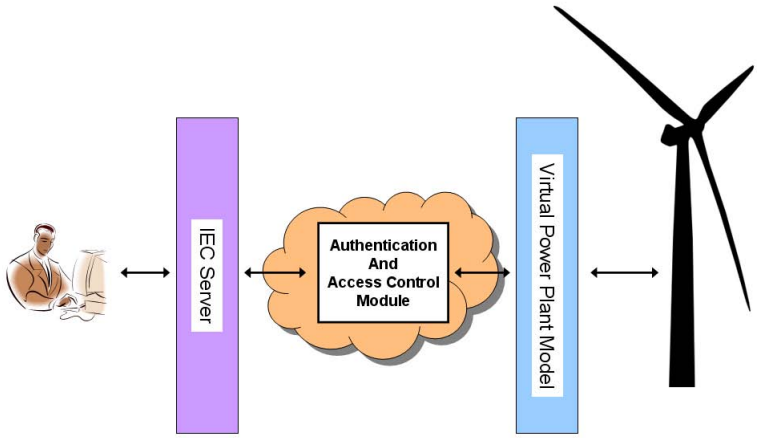

Figure 1: Overall prototype design

The access control module is located and managed at the wind farm controller in case the virtual power plant model has a wind farm. In case the virtual power plant model has no wind farm, then the access control module is present at the individual wind turbine. Needless to say, Access to the database or the list that is accessed by the access control module should be password protected and it is fair to assume that the alternate mechanisms exist to ensure defined rules are not circumvented in any way by a malicious administrator. A possible solution would be to enforce a secret sharing mechanism which ensures that at least an administrator and another competent authority must exercise their rights together to define new permissions or to modify existing permissions assigned to a role.

The implemented solution was validated by testing the system both manually and using automatic testing. An interesting observation being that the addition of the authorization module did not add to significant overhead to the execution time. This is quite understandable as the solution is software implemented and the data base is usually stored locally and data base reads and writes are not that time intensive.

6.1 Performance Evaluation

The overhead of introducing these two modules were simulated by measuring the time taken to receive a typical response with and without the addition of these two modules. The test results are as summarized

below :

	Time for 100 tests (seconds)
with authorization module	6.0
without authorization module	5.6

Table 4: Performance of the prototype access control mechanism

As indicated by the above test results carried out on a Intel Core 2 Duo, 4 Ghz Ram configuration, with the access data base, it becomes clear that the addition of these two modules have not contributed to significant overhead.

7 Conclusions

The main objective of this paper has been to design an access control framework for use in the Internet controlled wind power plants based on the IEC 61400 and the IEC 62351 standards. The need for an access control framework arise because the IEC 62351 standards does not address the issue of enforcing access control in detail. The importance of access control in wind power systems increases because standardization means that intricate details of the system, such as algorithms used, representation of elements of a wind power system in the software domain, become known to all, thus increasing the probability of a successful attack against the system which will result in disruption. Another important issue that necessitates access control is to protect the interests of manufacturers of components who want their names to remain hidden from other manufacturers to prevent market poaching. The access control model was devised after conducting an in-depth analysis of the relevant standards and extensive communication with representatives for both power regulators and electricity companies. This analysis has identified actors, the resources and the associated threats from attackers as well as the motivation for the attackers to attack these resources. The design of the access control mechanism using role based access control is intended to provide us with a flexible and easily extensible approach, because the number of distinct roles is normally much smaller than the number of individual entities. This means that mapping individual entities to a role and assigning permissions to roles makes it easier to manage the permissions associated with each resource. Our analysis of existing wind power systems, however, indicates that ad-hoc delegation of access rights from the wind farm controller to different dynamic roles is very common – this is partly indicated in Table 2. We believe that this can be largely attributed to the current scale and immaturity of the wind power industry, where commands and authorisations are simply communicated over the phone between a relatively small number of agents. We conjecture, however, that the continued development in wind power systems will soon result in systems that will be unmanageable with the current approach and that the advantages of our RBAC based modelling approach will become apparent.

We have presented a simple prototype of our model, where a proxy server mediates all interaction between agents and components of an existing wind power infrastructure. The permissions associated with each role can be stored either as access control certificates or as simple access control entries in an access protected database at the server end. The solution is also scalable since no modifications are required at the software of the individual component and a performance testing has revealed that addition of the authorization module does not cause a significant overhead

Based on the analysis presented above and the results of our testing, we conclude that the proposed solution is suitable for specifying and enforcing an efficient access control policy for Internet controlled

wind power plants based on the IEC 62351 and the IEC 61400 standards. The generic nature of the access control model developed also means that the model can be used even if new standards or changes to existing standards take place in the future.

References

[1] X.509 : Information technology – open systems interconnection – the directory: Public-key and attribute certificate frameworks, 2008.

[2] S. Farrell and R. Housley. An internet attribute certificate profile for authorization. RFC 3281, The Internet Engineering Task Force (IETF), April 2002.

[3] Anand Nagrajan. Enhancing the security of internet control wind power communication infrastructure based on iec 62531. Master's thesis, Department of Informatics and Mathematical Modelling, Technical University of Denmark, 2009.

[4] Kelly O'Connell. Cia report: Cyber extortionists attacked foreign power grid, disrupting delivery. *Internet Business Law Service*, January 23, 2008.

[5] The International Energy Commision. *IEC 61400-25 – Communications for monitoring and control of wind power plants*.

[6] The International Energy Commision. *IEC 62351 – Power systems management and associated information exchange – Data and communications security*.

[7] Whitelee Windfarm Visitor Centre. About the wind farm. `http://whiteleewindfarm.co.uk/about_windfarm`, *visited 2 April 2010*.

Anand Nagarajan holds a Bachelors degree in computer science and engineering from MS Ramaiah Institute of Technology, one of the most prestigious universities in the Silcon Valley of India (Bangalore) and a Masters degree specializing in Data Security and Mobile Computing from the Technical University of Denmark. His primary interests are security and applications of cryptography to solve issues that have a tangible impact on people's lives. Besides programming and research, his interests include travelling and hiking.

Christian Damsgaard Jensen holds an M.Sc. in computer science from the University of Copenhagen (Denmark), an M.A. (jure officii) from Trinity College Dublin (Ireland) and a Ph.D. in computer science from Universite Joseph Fourier (Grenoble, France). He is an associate professor at the Department of Informatics and Mathematical Modellling at the Technical University of Denmark, where he teaches and conducts research in the area of security in open distributed systems. For the past 10 years, he has focused on trust-based methods and technologies to secure collaboration among entities in open distributed system. This work addresses all 3 As in AAA: Authentication technologies and entity recognition; Access control policies and mechanisms; and Accountability through reputation and recommendation systems.