ARTICLE/PHOTOCOPY

Thursday, March 19, 2009

ILLiad TN: 299704

Call #: TK7885 .I49 2007

Location: b

ILL Number: 52152778

___ Not On Shelf

___ Not Found As Cited

___ Other (Please list reason):

Borrower: TXJ

Ariel: 129.115.122.243

Lending String: *RCE,IXA,IXA,COF,COD

Patron: Sandhu, Ravi

Journal Title: Innovative algorithms and techniques in automation, industrial electronics and telecommunications /

Volume: Issue:
Month/Year: 2007 Pages: 329-335

Article Author:

Article Title: ; PLS copy chapter on pages given. Thanks

Imprint: Dordrecht ; Springer, 2007.

Odyssey: 129.115.117.96

Charge
Maxcost: 30.00IFM

Shipping Address:
21272000123190
Univ Texas-San Antonio TEX:62-SAT
Library, ILL
6900 North Loop 1604 West
San Antonio, TX 78249-0671

Fax: 210-458-4571

This document has been supplied to you from:
Rice University Library (OCLC: RCE)
ILL Dept., MS-240
6100 Main St.
Houston, TX 77005
713-348-2284 / 713-348-4117 (Fax)
ill@rice.edu
Thank You for Using Interlibrary Lending!

RBAC Model for SCADA

Munir Majdalawieh[1], Francesco Parisi-Presicce[2],Ravi Sandhu[3]

[1] American University of Sharjah, mmajdalawieh@aus.com,
[2] George Mason University, fparisi@ise.gmu.edu
[3] George Mason University and NSD Security, sandhu@gmu.edu

Abstract - This paper focuses on recommending the usage of the Role-Based Access Control (RBAC) model to define the users' security roles, permissions, authorization, and role hierarchy to access the SCADA system. Achieving the desired level of authorization and access control will involve integrating the security system with SCADA operations and building role based access control capabilities in the application level.

Keywords: DNP3, DNPSec, SCADA, RBAC

1.0 Introduction

The Supervisory Control and Data Acquisition (SCADA) systems and the communication network they operate in are moving from proprietary and legacy environment to more open standard, modern microprocessor, and networking technologies. These systems have evolved over the years from totally centralized mainframe systems to distributed systems built with Commercial Off-The-Shelf (COTS) hardware and custom software. Figure 1.0 illustrates the components of SCADA systems. The availability of reliable communications between the SCADA components and the advanced functionality of the software used to manage the hardware systems are the major factors in the renovation and the growth in these systems.

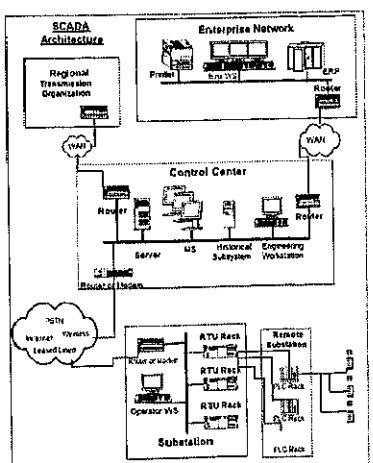

Figure 1.0: SCADA Components

Traditionally, network and security community in the utilities industries have focused virtually most of their attention on the "enterprise network", generally ignoring the other part of the network associated with the supervisory control and data acquisition systems in the belief that SCADA resides physically on a separate, standalone network [16]. Combining this assumption with the adoption and the deployment of these new technologies is creating a vulnerable environment for sophisticated terrorist, malicious attacks, cyber assaults, and inside assaults to target and break into the SCADA information systems. As a result, the fundamental principles of security (confidentiality, integrity, and availability) is compromised and the results will create unsafe conditions, which could lead to loss of the critical infrastructure assets, loss of lives, and loss of consumer confidence.

In October 1997, the security of the energy industries became a major focus, when the United States President's Commission on Critical Infrastructure Protection highlighted the risk of successful cyber attacks on the SCADA systems used in these industries as part of the critical infrastructures assets, stating that "the widespread and increasing use of SCADA systems for control of energy systems provides increasing ability to cause serious damage and disruption by cyber means." In February 2003, the United States President provided additional attention to these systems and highlighted concern about "the threat of organized cyber attacks capable of causing debilitating disruption to our Nation's critical infrastructures, economy, or national security," noting that "disruption of these systems can have significant consequences for public health and safety" and the protection of control systems has become "a national priority." [20]

This created more urgent need for the SCADA decision makers to take corrective actions to tighten up their security components and protect their assets from such attacks by the use of new security measures. These security measures start by developing a comprehensive security policy to cover all the elements of security infrastructure, and work with the vendors to apply more strict security capabilities in their systems and applications. In addition, the public sector needs to take a practical initiative to partner with the private sector to help in promoting the security's best practices that have been implemented successfully in its infrastructure. This partnership requires some incentives for the private sector to allocate resources and budget to deal with these issues.

T. Sobh et al. (eds.), Innovative Algorithms and Techniques in Automation, Industrial Electronics and Telecommunications, 329–335.

This paper focuses on the access control aspect of the security policy. Our approach is built on the Role-Based Access Control (RBAC) model to define the users' security roles, permissions, authorization, and role hierarchy to access the SCADA system. Achieving the desired level of authorization and access control will involve integrating the security system with SCADA operations and building role based access control capabilities in the application level throughout the entire life-cycle of the development of these applications. Enforcement of access control decisions at the time of assigning roles to users and during a real time operation will prevent malicious commands from reaching the field instruments and thus prevent harm.

RBAC provides great flexibility in the way administrators assign permissions to roles and roles to users. Users have access to the permissions that are associated with roles and users are made members of appropriate roles. Users can be assigned to a role based on their job description and function and easily can be reassigned from one role or another or removed altogether from the system without modifying the underlying access control structure. Role can be granted new permission when necessary, and permission can be removed from role as needed.

Identifying the data types used in SCADA system, the function codes used to communicate between the SCADA objects, and the users who access the SCADA system and defining their roles and responsibilities are the first steps in developing such a policy. In the following subsections we examine each of these elements and their characteristics to motivate our approach.

2.0 Access control security policy

In general, the security policy goal is to protect the organization assets and to ensure that mechanisms are established to protect the assets' confidentiality, integrity, and availability. There are many elements that are part of an enterprise-wide security policy. Few other papers provide high level framework and guidance for SCADA enterprise security policy [10] [21] [22], but very little has been done in providing models for all the elements of the security policy.

SCADA access control security policy starts by identifying critical and important resources, then determining who can access these resources, and knowing exactly what kind of access is provided. The roles within SCADA organization need to be defined and the type of access to these critical resources, activities, and operations need to be detailed.

This paper focuses on the access control security policies within the SCADA resources, mainly in and between the control center (CC), the Substation (SS), and the Remote Substation (RS). The interaction between CC, the Enterprise Network (EN) and the Regional Transmission Organization (RTO, e.g. electric power industry), is out of the scope of this paper. It is not practical to propose one approach for the entire utilities. Our approach is general since each organization using the SCADA system needs to adjust our model to fit its own specific roles and operations.

RBAC is a framework to help in articulating access control policies. One of the main design principles of the RBAC model is to minimize the potential for inside security violations by providing greater control over users' access to applications, information, and resources. Another design principle of the RBAC model is to allow administrators to assign access control to users based on their function in the organization. RBAC accomplishes this by introducing a new element called role. Roles can be granted new permissions as new functions and actions are incorporated, and permissions can be revoked from roles as needed.

A general RBAC model was defined by Sandhu [15] and a reference model is shown in Figure 2.0a [8]. The core RBAC elements are users, roles, objects, permissions, and operations. A user has access to an object based on his/her assigned role which is defined based on his function in the organization. The object is concerned with the user's role and not the user. Permissions are defined based on job authority and responsibilities within a job function. Operations on an object are invoked based on the permissions.

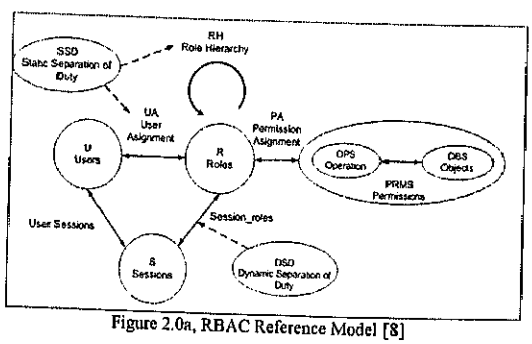

Figure 2.0a, RBAC Reference Model [8]

In RBAC, the administrator uses the role to manage permissions and assignments. For example, a utility company using a SCADA system may create a role called "Senior Operator" that has the permissions to access specific function codes and specific objects that he/she needs to conduct to carry his/her day-to-day job. When a senior operator is hired, he/she is assigned the "Senior Operator" role and directly has all required permissions to do his job.

Section 2.1 introduces the objects of a SCADA system. Section 2.2 describes the first three elements of RBAC: users, roles, and operations on objects. Section 2.3 describes our recommendation for a SCADA role hierarchy. Section 2.4 describes our approach for the permitted operations on objects and functions for the predefined roles

in SCADA systems. Section 2.5 highlights the policy rules in RBAC for SCADA systems.

2.1 SCADA Objects

Objects in SCADA are composed of sets of resources that contain or receive information. Figure 2.1a highlights the objects in SCADA. The Control Center's main function is to monitor and control remote equipment. The control may be automatic, or initiated by operator commands. The CC initiates all communications, gathers and stores data, sends control commands, and interfaces with remote devices directly or through the substations; it provides the infrastructure to the operators to handle these functions. The Historical Server (HS) logs real-time data in the database and is configured for a predefined set of remote devices and equipments. This data is used by the corporate office to conduct business analysis, auditing, and provide reporting.

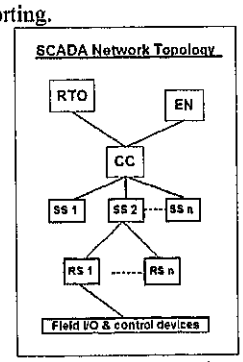

Figure 2.1a, SCADA Objects

The SubStation initiates communication with the Remote Substations or the field devices and works as the middle man between the Control Center and the field devices.

The Remote Substation gathers information from its remote devices, like valves, meters, alarms and pumps and reports it back to the CC or the SS based on the setup and the pre-defined flow of data. The CC or the SS scans IEDs or the IEDs report back data to the Master Station or to the SubStation.

Figure 2.1b [4] depicts some of the inputs and the outputs from and to the three main SCADA components, CC, SS, and RS.

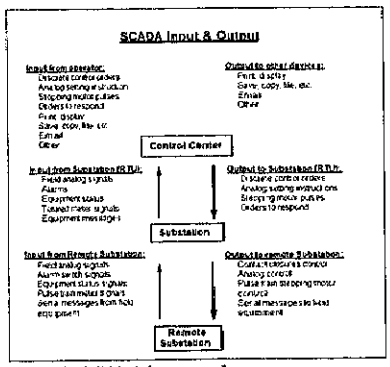

Figure 2.1b, SCADA inputs and outputs per component

The SCADA objects listed above, in addition to the operations and the functions permitted on these objects, need to be listed as part of RBAC permissions in the SCADA application level and in turn to be assigned to roles.

2.2 Users, Roles and Operations

The SCADA internal and external roles need to be identified and the type of access each of these roles requires for the SCADA system should be outlined. The external role is defined as any external user accessing the SCADA system. Access should be allowed only to the HS) database and not to any other data in the SCADA system. The flow of this data should be from the SCADA system to the corporate enterprise network. We call this role an External User (EU) Role and the permission type need to be restricted and assigned by the SCADA System Administrator (SA) and the organization should decide what type of security controls should be put in place to enforce such policy.

Several internal roles need to be defined. In a SCADA environment, we find a Manager (MR), a Supervisor (SU), a Senior Operator (SO), a Junior Operator (JO), an Instrument Technician (IT), and an Engineer (EG) role. The permissions to access SCADA objects for these users should be restricted to the role of each user. SCADA applications provide the infrastructure for the CC to communicate with the rest of the SCADA objects. The SCADA Operator initiates the communications with these objects. For example, CC through the MS sends requests (commands) to SS and RS and receives data from SS, RS, and the field devices. It receives requests from EU to access HS.

The policy for the interaction of CC with SS and RS should be centered around the input, the output, and control functions between these identities. CC receives deferent types of data from SS. For example, CC could receive field analog data, alarms, equipment status, totaled meters signals, and equipment messages. A "Junior Operator" (JO) could have permission to poll and view such data.

Also, CC controls field instruments by executing some operational commands. As a result, MS could send discrete control orders, analog setting instructions, stepping motor pulses, and orders to SS to respond. A Supervisor (SU) could have permission to conduct such functions. In Figure 2.2a, we show the different users, roles, and operations [4] in the SCADA systems.

A utility company using the SCADA system may create the roles and functions we identified in Figure 2.1a. When a user is hired, he/she is assigned the role based on his/her job description and in turn he/she will be carrying his/her job function based on the permissions assigned to his/her role. For example, when the company hires an "Instrument Technician", the administrator will assign the "Instrument Technician" role to the user. Based on the pre-assigned permission to this role, the user will be able to carry the following operations: view any screen, tune controllers, analyze all alarm reports, and conduct simple configuration. When the user leaves the company, he will be removed from the position of "Instrument Technician" role and no longer has the permission to access the system.

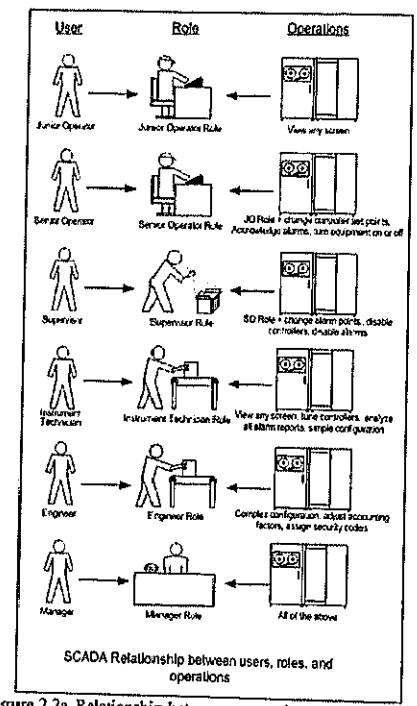

Figure 2.2a, Relationship between users, roles, and operations in SCADA

A user can be assigned to one or many roles, and a role can be assigned to one or many users. In our model we assume that we have a single administrator who assigns users to roles and roles to users. For example, the supervisor is assigned a junior operator, senior operator, and supervisor roles. The supervisor needs all of these roles to conduct his job.

2.3 Role Hierarchy

The Role Hierarchy reflects the organizational structure based on job's authorities and responsibilities. In some organizations, one role can include the tasks and permissions that are associated with another role. In such case, RBAC role hierarchy provides an efficient way to avoid specifying common tasks. Tasks and roles depend on organizational policies. When tasks overlap, you can establish hierarchies of roles.

The President's Critical Infrastructure Protection Board, and the Department of Energy, has developed 21 steps to help a utility organization improve the security of its SCADA system [19]. Step number 12 defines the importance of taking an action to "Clearly define cyber security roles, responsibilities, and authorities for managers, system administrators, and users." To address this issue we recommend a role hierarchy structure for a SCADA organization as described in Figure 3.3a. For example, the "Supervisor" role overlaps with the "Senior Operator" role. SU will have authority to carry the tasks of SO, which is established by assigning SO role to SV.

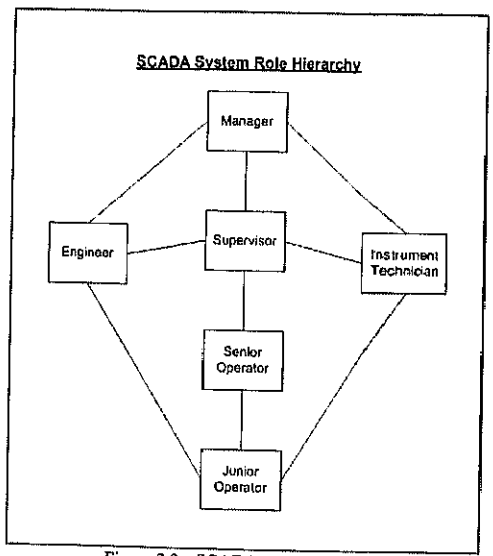

Figure 2.3a, SCADA Role Hierarchy

2.4 Roles and Permissions at the Application Level

Sandhu [13] indicated that the nature of permissions and operations mediated by RBAC depends on the nature of the system in which RBAC is embedded. The authorization decisions associated with the operations are based on factors that can be known only to the application. Similarly, the request (commands) and reply (status/data) control operations must be programmed as part of the SCADA application access control. Vendors should provide functionalities for application programmers to effectively build such application programs that provide abstract application-level operations and to protect them by means of RBAC capabilities. The use of role-based con-

trols at the application level will enable enforcement of policies that closely conform to the intentions of stakeholders, while causing minimal interference with legitimate operator actions.

SCADA abstract application operations and permissions are centered around the system objects and the interface objects. In section 3.1 we discussed the system objects which are composed of CC, SS, RS, and IEDs.

The interface objects are presented by the system communication protocols. There are several protocols that are supported in the SCADA communications architecture. For the purpose of this paper we will use the DNP3 protocol [6] [9]. The DNP3 or Distributed Network Protocol version 3.3 (DNP3) is a telecommunication standard protocol that defines communications between MS, SS, RS, and IEDs. In the Master/Slave architecture, the master communicates with the slaves using the application layer message function.

The DNP frame format is limited to 292 bytes. One important structure of the frame fields is the frame control byte. The control byte is used to communicate the function codes (commands) from the master-to-slave (request) and the slave-to-master (reply). The request commands need to be carefully examined and assigned to the right role and the roles be assigned the right permissions based on the function code of such command. Such assignment should occur at the application user level. The application should have some mechanisms to verify that the user has permission to use such code function when a user attempts to perform an operation on an object. At the same time, mechanisms should be implemented at the slave side to verify that the command code function is coming from a trusted source.

The request and response function codes specified in the frame control byte are described in the DNP3 specifications [6]. The function code identifies the purpose of the message and indicates what function is required to be performed. For example, the Freeze Functions type could be assigned to the "Supervisor" role and excluded from the "Junior" role. At the time of operation the SCADA application should provide mechanisms to allow the Supervisor to execute (request) such function on a specific object and deny the "Junior Operator" access to such functions. As an example, table 2.1a shows the freeze request function codes.

Table 2.1a: Freeze Request Function Codes

Code	Function	Description
7	Immediate Freeze	Copy the specified objects to a freeze buffer and respond with status of the operation.
8	Immediate Freeze – No Ack	Copy the specified objects to a freeze buffer; do not respond with a message.
9	Freeze and clear	Copy the specified objects to a freeze buffer, then clear the objects; respond with the status of the operation.
10	Freeze and clear – No Ack	Copy the specified objects to a freeze buffer, then clear the objects; do not respond with a message.
11	Freeze with time	Copy the specified objects to a freeze buffer at the specified time and intervals; respond with status.
12	Freeze with time – No Ack	Copy the specified objects to a freeze buffer at the specified time and intervals; do not respond with a message.

In RBAC, a session relates one user to possibly one or more roles. A user establishes a session during which he or she activates some subset of roles that he / she is a member of. The permissions available to the user are the union of permissions from all roles activated in that session. Each session is associated with a single user. Permissions are assigned and granted to roles in order to access the object. The permission for a specific role could be restricted to access specific objects, which in turn deny the user with such role to send and receive information from such object. In addition the permission for the same role could be restricted to access specific function codes, which in turn deny the user with such role to access other function codes.

A user assigned to a role is authorized to perform an operation on the object only if the operation is a member of the set of permitted functions for that object (See Figure 2.4a). As such, the operations for an object need to be defined and the object access types need to be identified and permissions need to be authorized to perform a function on an object at the SCADA application level. For example, a user assigned to the "Senior Operator" role must be able to view screens, send control signals to controllers, and receive and acknowledge alarm alerts. Thus, the "Senior Operator" has permission to read information displayed on the Human Machine Interface, send (request) control signals (ON/OFF) to the controllers attached to the Substations and the Remote Substations, and receive (reply) and acknowledge alarm alerts from the controllers attached to the Substations and the Remote Substations. On other hand, the "Senior Operator" does not have permission to send (request) signals (ON/OFF) to change alarm points, to send signals (ON/OFF) to disable controllers, or to send signals (ON/OFF) to disable alarms attached to the Substations or to the Remote Substations. These operations need to be mapped by the SCADA application and allocated specific function codes that can carry such operations.

Associating permissions with function codes and objects has the potential to create a level of difficulty to the policy to be understood and developed without further knowledge about the SCADA application and its protocols. Since the function codes and the objects (by name and address) are predefined, the SCADA application vendors need to provide some tools to help the SCADA administrators to associate roles with permissions and vise versa. Such tools will help also to provide the mechanisms to associate objects and function codes with permissions.

Also, there is a need in using application specific factors in authorization decisions. The sophisticated access control policies in SCADA systems are due to the major

effect these systems have on the service to the public and the liability requirements imposed by state and federal legislation. Ideally, authorization decisions in the SCADA systems should be based on the following factors: the size of operations, subject affiliation (EN, RTO), subject role, subject location, access time, and relationship between the subject and the SCADA objects whose data are to be accessed.

By introducing role based access control on the application level, authorization decisions and objects access types for SCADA systems and the affiliation with other subjects are two important topics for future work.

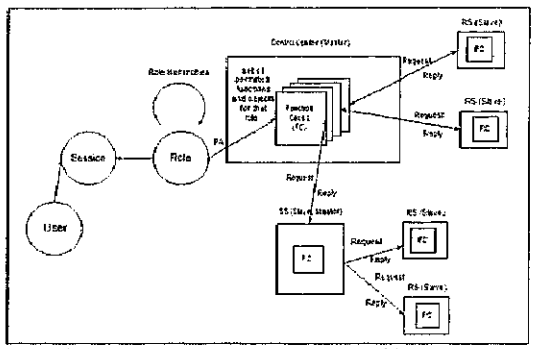

Figure 2.4a, SCADA System Topology: Multiple Master

3.5 Policy Rules in the RBAC model

The main purpose of a policy is to be sure that the resources are protected and information is transmitted in secure and appropriate manner. In addition, all users who access the system are using appropriate permissions based on their roles to conduct specific tasks and operations in a secure and control manner. RBAC supports several security principles and policies that can be implemented as a set of rules to be used in defining and enforcing access control policy for a SCADA system. Some of these are: the role authorization, the enforcement of least privilege for administrators and users, the dynamic separation of duties, and the cardinality property.

These policies can be enforced at the time operations are authorized for a role, at the time users are assigned a role, at the time of role activation, or when a user attempts to perform an operation on an object. The SCADA vendors can design and build such policies in their applications and provide some mechanisms to implement such policies in the SCADA systems. For example, a Senior Operator can be constrained to change controller set points but not to change alarm points. This is possible because of the RBAC capability to associate the operations with the roles. The decision to grant or deny an SO from changing the controller set points or changing the alarm point could be enforced at the time when SO attempts to perform such operation or at the time such SO assigned to a role.

In the role authorization policy, a user can never have an active role that is not authorized for that user. To perform an operation on an object controlled under RBAC, a user must be active in some role. Before the user can be active in a role, that user must first have been authorized as a member of the role by an administrator. In Figure 2.2a we described the major roles in the SCADA systems and the operations associated with each role. For example, the administrator assigns an "Engineer" role to a new employee whose job function is to carry complex configuration operations. When this user accesses the SCADA system, the granting or denying access to this operation will take place at the time the user is assigned to the role and will be in effect when the user uses the system.

The enforcement of the least privilege principle is based on allocating the minimum amount of permissions in a role to access an object. In the same principle, the user is assigned to a role that allows him/her to perform only what's required for that role. In addition no single role is given more permission than the same role for another user. As discussed earlier, the norm in SCADA environment is to trust the users when they are inside the control station center. With RBAC, users are authorized to access objects based on pre-assigned permissions and pre-defined operations. These permissions and operations should be at a minimum to allow the user to conduct his/her day-to-day job and be responsible for such actions.

The Dynamic Separation of Duty (DSD) rule provides the capability to address potential conflicts of interest issues at the time a user's membership is authorized for a role. However, in some organizations it is permissible for a user to be a member of two roles which do not constitute a conflict of interest when acted independently, but introduce policy concerns when allowed to be acted in simultaneously. DSD places constraints on the users that can be assigned to a set of roles, thereby reducing the number of potential permissions that can be made available to a user. The objective behind DSD is to allow more flexibility in operations. DSD places constraints on the simultaneous activation of roles. So for example, a SCADA "Senior Operator" can be authorized for both the acknowledgement of alarms and the change of the alarm points, but can dynamically assume only one of these roles at the same time. This could happen when a "Senior Operator" is covering for a "Supervisor" Role.

Some roles can only be occupied by a certain number of employees at any given time. This policy is enforced by the cardinality property. For example, consider the role of a Manager. Although other employees may act in that role, only one employee may assume the responsibilities of a Manger at a certain time. A user can become a new member of a role as long as the number of members allowed for the role is not exceeded.

An important design principle of RBAC model is the administrative capabilities it supports. In other access control models, the administrative process is very complex and requires a specific capability and knowledge. In

RBAC, users become members of roles based on their functions and responsibilities in the organization. Users are not granted permission to perform operations based on individual basis, but operations are associated with roles, and users are associated with roles. Under RBAC, new operations can be added to a role and operations could be removed from a role. All of this could happen without affecting the assignment of a user to a role.

Another administrative advantage of RBAC is that administrators control access at an abstraction level. This is established by introducing the "role" principle. Users are assigned to roles based on their job function and responsibility. After creating the RBAC framework, the administrator's actions will be limited to granting and revoking users into and out of roles. Therefore, RBAC simplifies the administrator role and makes it very efficient.

4 Conclusion

SCADA systems were not designed with security capabilities in mind. The SCADA vendors can build such capabilities by utilizing the RBAC functions with a minimum time and cost and without a major impact on the systems components. RBAC strong administration capabilities can help simplifying the process of security management in SCADA systems.

In this paper we developed a security access control framework using RBAC for the SCADA systems. We described the capabilities of RBAC in providing abstract application level operations such as request (send) and reply (receive) signals (ON/OFF) from and to the Control Center, the SubStation, and the Remote Substation. A security model to verify the authorization at the time of operations on the system objects using the DNP3 could be a topic worth more investigation.

In addition, the external users (EN, RTO) accessing the SCADA systems could be a topic worth of further investigation. Moreover, the flow of data between the major SCADA objects could be another topic for research in the contents of access control policy.

References

1. Gail-Joon Ahn and Ravi Sandhu, "Role-Based Authorization Constraints Specification"
2. John Barkley, Anthony Cinotta (NIST), "Managing Role/Permission Relationships Using Object Access Types"
3. L. Beaver, D.R. Gallup, W. D. NeuMann, and M.D. Torgerson., "Key Management for SCADA" http://www.sandia.gov/scada/documents/013252.pdf
4. Stuart Boyer 2004, "SCADA, Spervisor Control and Data Acquisition, 3rd edition"
5. Brian Broyles and Frank Kling, "Is there anything new under the SCADA sun?" http://www.rigzone.com/insight/insight.asp?i_id=32
6. DNP User Group, http://www.dnp.org
7. DF Ferraiolo, "Role-Based Access Control (RBAC): Features and Motivations", 11th Annual Computer Security Applications Proceedings, December 1995
8. David Ferraiolo, Ravi Sandhu, Serban Gavrila, D. Richard Kuhn, and Ramaswamy Chandramouli, "Proposed NIST Standard for Role-Based Access Control"
9. Munir Majdalawieh, Francesco Parisi-Presicce and Duminda Wijesekera, DNPSec: A Security framework for DNP3 in SCADA Systems, in International Joint Conference on Computer Information and Systems Sciences and Engineering, Bridgeport, CT. December 10-20, 2005.
10. NERC, Version, June 14, 2002. Security Guidance for the Electricity Sector: Cyber – Access Controls.
11. Jaehong Park and Ravi Sandhu , "The UCONABC Usage Control Model"
12. The Register, "Hacker jailed for revenge sewage attacks" http://www.theregister.co.uk/2001/10/31/hacker_jailed_for_revenge_sewage
13. Ravi Sandhu, "Issues in RBAC", http://www.list.gmu.edu/workshop/issue.pdf
14. Ravi Sandhu, Venkata Bhamidipati, and Qamar Munawer, "The ARBAC97 Model for Role-Based Administration of Roles."
15. Ravi Sandhu, Edward J. Coyne, Hal Feinstein, and Charles Youman, "Role-Based Access Control Models"
16. Riptech, Inc. January 2001 "Understanding SCADA System Security Vulnerabilities", http://www.iwar.org.uk/rerources/utilities/SCADAWhitepaperfinal1.pdf
17. Sandia National Laboratories, The Center for SCADA Security, SCADA Brief History http://www.sandia.gov/scada/history.htm
18. Joe St Sauver, Ph.D. University of Oregon. SCADA Security, http://darkwing.uoregon.edu/~joe/scada/
19. U.S. Department of Energy, "21 Steps to Improve the Cyber Security of SCADA Networks," http://www.ea.doe.gov/pdfs/21stepsbooklet.pdf
20. U.S. General Accounting Office, "Critical Infrastructure Protection: Challenges and Efforts to Secure Control Systems" http://www.gao.gov/new.items/d04354.pdf
21. William F. Young, Jason E. Stamp, and John D. Dillinger. "Communication Vulnerabilities and Mitigation in Wind Power SCADA Systems"
22. Bill Young and Mark Rumsey . "Communication Vulnerabilities and Mitigations in Wind Power Supervisory Control and Data Acquisition."