Intelligent Security System for HMI in SCADA Applications

Rajesh Singla and Arun Khosla

***Abstract*—Supervisory control and data acquisition (SCADA) systems are vital components of most nations' critical infrastructures. They control pipelines, water and transportation systems, utilities, refineries, chemical plants, and a wide variety of manufacturing operations. SCADA provides managing the real-time data on production operations, implements more efficient control paradigms, improves plant and personnel safety, and reduces costs of operation. These benefits are made possible by the use of standard hardware and software in SCADA systems combined with improved communication protocols and increased connectivity to outside networks, including the Internet. However, these benefits are acquired at the price of increased vulnerability to attacks or erroneous actions from a variety of external and internal sources.**

This paper focuses on suggesting a user security on the basis of roles assigned to multi users with the help of password and biometrics with iris recognition security. Recommending a role based hierarchy to allow users access system according to their capabilities in the particular application.

***Index Terms*—SCADA, HMI, RSView32, RSLogix500, user security, panelbuilder32, IRIS.**

I. Introduction

SCADA is the technology that enables a user to collect data from one or more distant facilities and or send limited control instructions to those facilities[1]. SCADA stands for Supervisory Control and Data Acquisition. As the name indicates, it is not a full control system, but rather focuses on the supervisory level. As such, it is a purely software package that is positioned on top of hardware to which it is interfaced, in general via Programmable Logic Controllers (PLCs), or other commercial hardware modules. SCADA systems are used not only in most industrial processes: e.g. steel making, power generation (conventional and nuclear) and distribution, chemistry, but also in some experimental facilities such as nuclear fusion. The size of such plants ranges from a few 1000 to several 10 thousands input/output (I/O) channels. However, SCADA systems evolve rapidly and are now penetrating the market of plants with a number of I/O channels of several 100K. SCADA systems used to run on DOS, VMS and UNIX, in recent years all SCADA vendors have moved to NT[2]. The processing power of SCADA has increased dramatically. They are more capable of complex tasks than ever before and have closely followed the overall trends in computer architectures. Current technology SCADA systems like current technology computer networks are most often architected in a distributed model. While individual components perform complex tasks, data are shared between components in order to optimize the overall process that is under SCADA control. The greatest benefit of current technology SCADA is its ability to integrate directly with back-end business systems. It is the integration of SCADA into the business system that causes the greatest concern. By integrating the SCADA system into the business systems of the enterprise, you are inadvertently increasing the risks within the SCADA system by adding those of the enterprise network and often those of the public Internet as well. Which is increased the threat of exposure further. Some of the main security threats to SCADA systems are as follows:

Malware – SCADA systems are potentially vulnerable to viruses, worms, trojans and spyware. For the purposes of this characterization I define the malware threat as an undirected attack that has no "interest" in SCADA systems. It could impact the system by corrupting data, slowing the system which will delay action taken to control I/O.

Insider – The dissatisfied worker who knows the system can be one of the largest threats. The insider may be motivated to damage or disrupt the SCADA system or the utility's physical system. An insider may also attempt to illicitly gain higher privileges for convenience sake. Bored or inquisitive Operators may unknowingly create problems which can bring down the system. The lack of authentication and authorization are regarded as the typical high-level weaknesses in SCADA.[3]

Hacker – Here the individual is an outsider who may be interested in intruding or controlling a system. Attackers break into networks for the thrill of the challenge or for bragging rights in the attacker community.

Terrorist – This is the threat that distinguishes critical infrastructure systems from most IT systems. A terrorist is likely to want to either disable the SCADA system to disrupt monitoring and control capability, take control of the SCADA system to feed false values to the operators or to use the control system to degrade service or possibly damage the physical critical infrastructure system.

The vendors in the SCADA world are working on securing their products. They are aware of the market value and competitive advantage of secure products. SCADA systems should be consistent with and integrated with existing IT security experience, programs, and practices, but must be tailored to the specific requirements and characteristics of SCADA system technologies and environments. Organizations should review and update their security plans and programs regularly to reflect changes in

Manuscript received May 10, 2012; revised June 28, 2012.

R. Singla is with the Instrumentation and Control Engineering Department, National Institute of Technology, Jalandhar, PIN 144011 INDIA (e-mail: rksingla1975@gmail.com).

A. Khosla is with the Electronics and Communication Engineering Department, National Institute of Technology, Jalandhar, PIN 144011 INDIA (e-mail: khoslaak@nitj.ac.in).

technologies, operations, standards, and regulations, as well as the security needs of specific facilities.

So there is a need of such a secure SCADA system in the industries. We have designed a SCADA System for controlling and monitoring of temperature and level of three tank system. After that we are suggesting a role based access model to different users for different operating parts of the system. This model is useful to prevent users from certain parts of the system and secure the SCADA commands, graphic display, OLE objects and tags. This paper is helpful to secure the SCADA project manager and prevents users from going outside of the project privileges for that code to access the SCADA features allowed by that code. This paper gives a hierarchy of user to secure the system and allowing each user to access a different set of features. Biometrics with iris recognition is also used in this system to secure top level of hierarchy model.

II. Experimental System

A. *Hardware:*

Hardware is setup of three tank system as shown in Fig. 1. In this system there are two experiments to control the temperature and level of the control tank by manipulating inflow from the hot tank and Cold tank using control valves. System's main requirement is continuous output from the control tank.

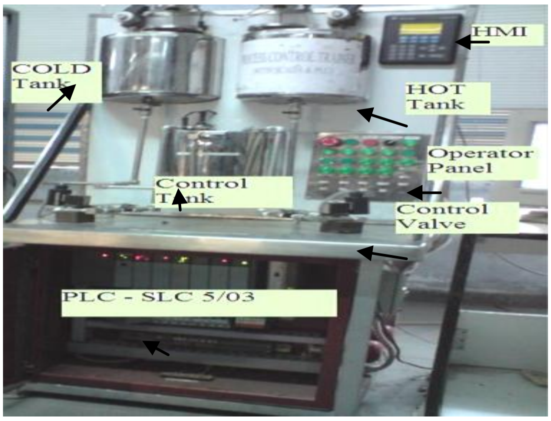


Fig. 1. Hardware setup

This system has two experiments which are as follows:

- In temperature control when temperature of control tank is low inflow from hot tank is started while when temperature is high inflow from cold tank is started. If temp of fluid goes high then we have heat exchanger which will cool down the fluid.
- In level control of the control tank we increase or stop the inflow from the cold tank to control tank according to the required level.

To control it manually we have HMI (PV300) which is used to give set point and selecting experiment. SCADA window has graphics or operator panel where the present status of different valves, level and pump is shown using different indicators. It also has start, stop and emergency stop buttons.

B. *Software:*

In this system three software are used, PLC software RSlogix500 (by Rockwell), SCADA RSview32 (by Rockwell) and Panelbuilder32.

RSView32 [4] is an integrated, scalable, component-based HMI for monitoring and controlling automated machines and processes. Designed for Microsoft Windows NT and Windows 95/98, RSView32 integrates Microsoft Visual Basic for Applications (VBA), which allows you to customize and extend its core functionality. It is both an OPC client and server which provide you added flexibility for peer-to -peer networking and the ability to implement a control system that easily and reliably interfaces control products from multiple vendors. RSView32 offers:

- Rich graphics and animation tools.
- Customizable alarm monitoring.
- Activity, alarm, and data logging with ODBC database support.
- Historical and real-time trending on the same graphic display.
- Event detection that can trigger automated responses.
- Project-level and system-level security features.
- DDE and OPC communications.

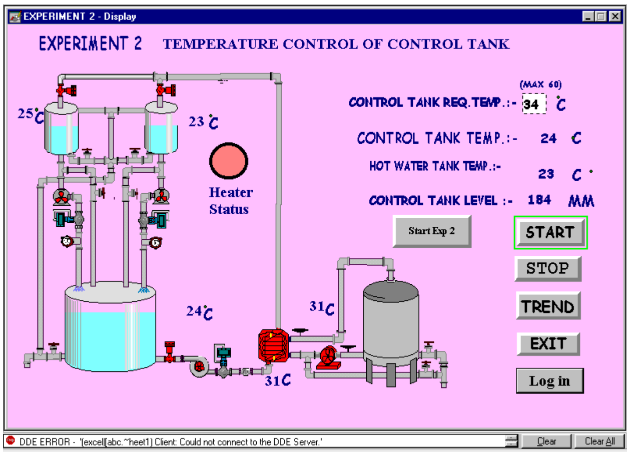
RSLogix500 [5] was the first PLC programming software to offer unbeatable productivity with an industry-leading user interface. RSLogix 500 comes in two editions a Standard edition that provides basic ladder logic editing functions, and a Professional edition that provides additional functions to expand your automation solutions and make editing ladder logic simple.

1) Microsoft Visual Basic for Applications support.
2) Custom Graphical Monitor.
3) Editing project databases using Microsoft.
4) Logic Trace.

Panelbuilder32 [6] software supports the entire family of Panel View Standard terminals, allowing for easy conversion and reuse of existing applications. Configure screens quickly and easily using standard tools, objects, graphics, and imported bitmaps. Other time-saving advantages include cut/copy/paste and tag import/export capabilities in and between Panel View applications. In addition, multiple applications can be open at the same time.

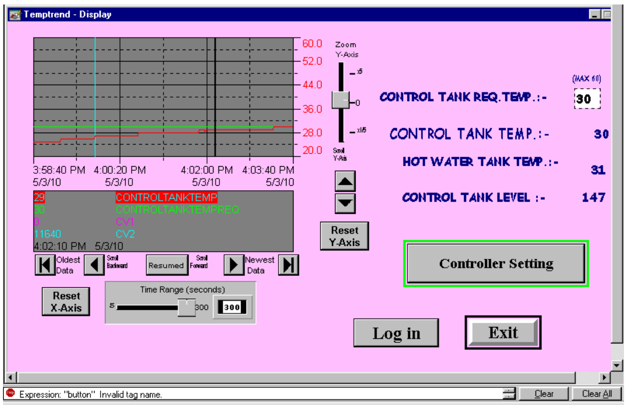
A SCADA window is designed for above hardware for controlling and monitoring the system. In this window there are controlling switches, switches start exp2, and start and stop which are used to start or stop the process .Numeric input is used to give required temperature or level of the control tank as shown in Fig. 2. Trend button is to see the trend how the temperature or level varying of the control tank as shown in Fig. 3.

This research paper also provides secure access to the system. Login button is used to login as different user at any time. Graphics shows the present temperature of three tanks, heat exchanger inlet and outlet temperature and status of various pumps and solenoid valves. Heater status is also in the graphics as the heater starts it start blinking. User can also define the alarms for the level, temperature, heater, solenoid valves which is shown in alarm window where a user can acknowledge them and take a corrective action according to their role and access granted to them. For proper controlling of the system we also provided user to change the controller setting to get best response from the system.


EXPERIMENT 2 - Display
EXPERIMENT 2 TEMPERATURE CONTROL OF CONTROL TANK
(MAX 60)
CONTROL TANK REQ.TEMP.:- 34 C
CONTROL TANK TEMP.:- 24 C
HOT WATER TANK TEMP.:- 23 C
CONTROL TANK LEVEL :- 184 MM
25 C
23 C
Heater Status
24 C
31 C
31 C
Start Exp 2
START
STOP
TREND
EXIT
Log in
Clear
Clear All

DDE ERROR - 'excel|abc.~heet1} Client: Could not connect to the DDE Server.'

Fig. 2. Controlling and monitoring window



Expression: "button" Invalid tag name.

Fig. 3. Trend and controller setting window.

The complete setup has PLC, SCADA and HMI as shown in the figure 4. Hardware system can be treated as the plant and the SCADA window can be taken as the control room for a large system having input outputs in the range of thousand located at large distance.

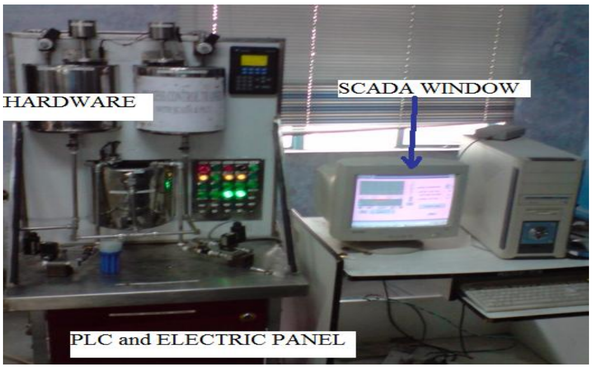


Fig. 4. Experimental Setup

III. Security

This paper proposed a hierarchy for the users according to their roles to secure the system. SCADA access control security policy is used 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 system need to be defined and the type of access to these critical resources, activities, and operations need to be detailed [7]. The SCADA internal and external roles 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. Main focus of this paper is on the security from the internal user so several internal roles needed to be defined. In SCADA environment for our application different roles found like a Manger, a Supervisor, Senior operator, Junior operator, Instrument technician, and Engineer role.

The permissions to access SCADA objects for these users should be restricted to the role of each user. Hierarchy we have suggested is shown in table-1. Users access restricted in the system so that they can access only those resources which they can handle according to their role and knowledge without affecting system perfectly.

TABLE I: HIERARCHY FOR USER ACCORDING TO THEIR ROLE[7]

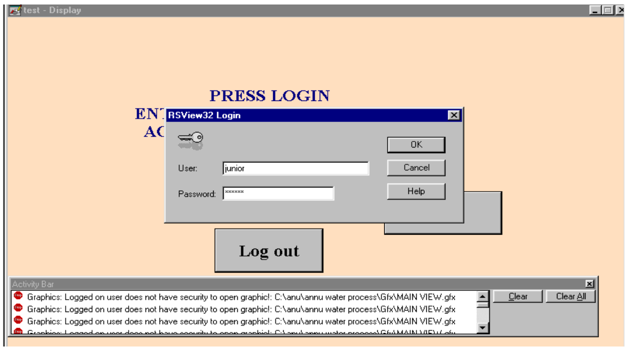
USER	*Role*	*Security type*	*Operations*
Junior Operator	Junior operator role	Password	Monitor any screen
Senior Operator	Senior operator role	Password	JO Role, can start or stop the system, Acknowledge alarm
Supervisor	Supervisor role	Password	SO Role, disable alarm, can change set points.
Instrument technician	Technician role	Password	Can change graphics, see alarm logs, change security codes
Engineer	Engineer role	Password	Configure graphics, Controller setting, Security codes
Manager	Manager	Password & Biometric(iris)	All of the above

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. To implement this hierarchy system codes are used to prevent users from accessing certain parts of the system. Each code allows users with security privileges for that code to access the SCADA features allowed by that code. Users can be assigned combinations of security codes, allowing each user to access a different set of features. Three types of system of codes are used to secure our system which is as follows:

Command Security: In this type of security the system checks the security codes of commands and macros no matter they are issued from:

- Macros
- Object Display, and Global keys
- Command line
- Button objects
- Object configured with touch animation
- Alarm identification field in the database.

In this system security is given to the startup config. database, account and acknowledges all commands according to the requirement of our system.



test - Display

PRESS LOGIN

EN AC

RSView32 Login

User: junior

Password: ******

Activity Bar

Graphics: Logged on user does not have security to open graphic!: C:\anu\annu water process\Gfx\MAIN VIEW.gfx
Graphics: Logged on user does not have security to open graphic!: C:\anu\annu water process\Gfx\MAIN VIEW.gfx
Graphics: Logged on user does not have security to open graphic!: C:\anu\annu water process\Gfx\MAIN VIEW.gfx

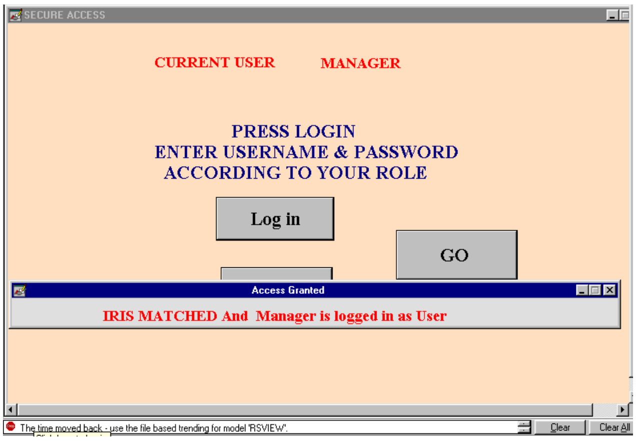
Fig. 5. Password login window.

Graphic display security: Security is assigned to a graphic display in the Graphic Display editor. Engineer can assign security while he or she are creating a graphic display, or can assign it later. In this system junior operator not allowed to see the trend window as there is no need for him to monitor that.

Tag security: In this part of security we give security to Tags so that a user is restricted write access to a tag. A user cannot change the tags value like the set points, controller tuning parameters etc.

In this system password security used for our initial level and for highest level of manager biometrics security used to secure the activity logging, data logging and alarms database. Before accessing the system user has to give his username and password which is given to him according to his role as shown in Fig 5. After logging in as an authorized user then he can use the system according to his role.

For manager level we have used biometrics recognition with iris as security to login the user. When the iris of the user is going to match then only user can access the system. When the iris gets matched window will give a message “IRIS matched and Manager is logged in as user” as shown in Fig 6.



SECURE ACCESS

CURRENT USER MANAGER

PRESS LOGIN
ENTER USERNAME & PASSWORD
ACCORDING TO YOUR ROLE

Access Granted

IRIS MATCHED And Manager is logged in as User

The time moved back - use the file based trending for model 'RSVIEW'.

Fig. 6. Login window accessing using IRIS matching.

Biometrics with iris recognition as security can also be provided as security at other level according to the need of the system.

IV. Biometrics as Security

There are different ways to secure the critical systems. Traditional approaches such as ID cards, password & user name neither satisfactory nor reliable enough in many security areas like process industries. These methods are not very secure. Token, PIN number & password may be shared or stolen [8]. So, modern security requires more secure and more reliable identity authentication technology. Biometrics is used as a suitable solution of higher security. It is a technique of verifying person’s identity from physical or behavioral characteristics. Biometrics includes fingerprint, facial features, retina, iris, voice, gait, hand geometry & palm prints. Among the various traits iris recognition attached a lot of attentions due its greater speed, simplicity and accuracy compared to other biometrics. The iris is the colored ring on the human eye between the pupil and the white sclera as shown in Fig. 7. Lots of physical biometrics can be found in the colored rings of the tissues like corona, filaments, flecks, pits, radial furrows and striations. It has been found that every iris is unique means even a person left and right eye iris patterns are never same and is stable throughout the human life. Most of the biometrics has 13 to 60 distinct characteristics but iris have 266 unique features. So these factors make iris an ideal tool for identification.

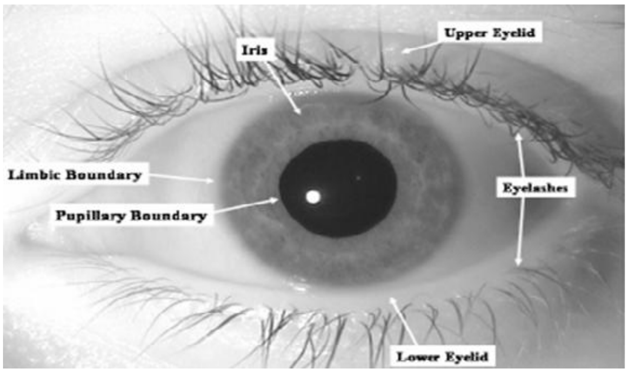


Fig.7. Eye image.

Iris recognition process includes eye image database, pre-processing stage, feature extraction stage and matching stages.

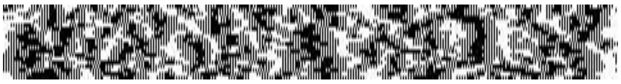


Fig. 8. Iris template

With the help of pre-processing and feature extraction stage we get an iris template. This template is used for matching. Here matching done with hamming distance method. With the hamming distance method a decision can be made that the two templates generated from same or not and particular user could be allowed to access the system secured.

V. Results

SCADA software has been used for monitoring the present process system. Level and temperature of the control tank are monitored and controlled using SCADA system and to secure the system resources according to the roles assigned to the users proposed hierarchy is implemented .If somebody wants to particular feature he should be allowed by administrator to access that feature. These features are secured by the different system of codes and to access these codes user have to login by the username or iris recognition assigned by the administrator. User can access the particular feature only if he is logged in as user who has permission to access that feature of SCADA. In this system at initial levels of hierarchy password is used while for the top most level biometrics with iris recognition is used to secure the system. Biometrics security can also be used at other level which depends on the need of the system.

VI. Conclusion

As SCADA systems progressed from stand-alone architectures using proprietary hardware, software, and protocols to interconnected elements comprising PCs, Windows, and standard protocols, they also became more vulnerable to attacks. This paper highlighted some of the threats and vulnerabilities that the SCADA system face and gives an approach to provide security to a multiuser system.

It gives a hierarchy system to implement security to restrict unauthorised user to access resources of the SCADA system. The unauthorised access is restricted using one of the most common method password secured access and Iris secured access. As this paper demonstrates other method of biometrics further can also be used to secure systems like fingerprint and facial features. Biometrics is attractive because they base authentication on a physical characteristic of the individual attempting to access relevant components of a SCADA system.

Currently, biometrics is promising, but is not completely reliable. Depending on the characteristic being examined, there might be a high number of false rejections or false acceptances throughput problems, human factor issues, and possible compromises of the system. However, the technology is progressing and biometrics should become a viable option for controlling SCADA system access.

References

[1] SCADA: *Supervisory Control And Data Acquistion* by Stuart A.Bover, Published by ISA The instrumentation Systems and Automation Society; 3rd edition.

[2] WHAT IS SCADA? "International Conference on Accelerator and Large Experimental Physics Control Systems," 1999, Triests, Italy, A. Daneels, CERN, Geneva, Switzerland, W.Salter, CERN, Geneva, Switzerland.

[3] *Techno Security's Guide to Securing* SCADA A Comprehensive Handbook On Protecting The Critical Infrastructure, Jack Wiles, Tedclaypoole.

[4] Listen think solve, product profile RSView32, publication VW32-PP002B-EN-PAugust 2007.

[5] Listen think solve RS logix500, Getting results guide, publication LG 500-GR002C-ENP-January 2007.

[6] Allen Bradley panelbilder32 software, getting results Publication 2711-GR003D-EN-P - June 2009.

[7] M. Manjdalawieh, F. Parisi-Presicce, and R. Sandhu, "RBAC Model for SCADA," *Innovative Algorithms and Techniques in Automation, Industrial Electronics and Telecommunications*, 329-335, 2007 Springer.

[8] D. Lauber, "Biometrics: A Brief Overview," SANS Institute 2003 Qichuan Tian, Xirong Liu, Ziliang Li, and Lingsheng Li" Imperfect iris information for identity recognition" *IEEE*.

R. Singla was born in Punjab, India in 1975. He obtained B.E Degree from Thapar University in 1997, M.Tech degree from IIT -Roorkee in 2006. Currently he is pursuing Ph.D degree from National Institute of Technology Jalandhar, Punjab, India. His area of interest is Brain Computer Interface, Rehabilitation Engineering, and Process Control.

He is working as an Assistant Professor in National Institute of Technology Jalandhar, India since 1998.

Dr. A. khosla was born in Punjab, India . He received the BE degree from Thapar University, India, M. Tech from NIT Kurukshetra, and Ph.D. degree from Kurukshetra University, India. His research areas include Artificial Intelligence, Bio Medical instrumentation.

He is working as an Associate Prof. in the department of Electronics and Communication Engineering, NIT Jalandhar. He is also Head of the department since 2010.