Wireless Sensor Network, 2010, 2, 520-527
doi:10.4236/wsn.2010.27064 Published Online July 2010 (http://www.SciRP.org/journal/wsn)

Developing a Multi-Layer Strategy for Securing Control Systems of Oil Refineries

Musaria K. Mahmood[1], Fawzi M. Al-Naima[2]
[1]*Department of Electrical Engineering, College of Engineering, Tikrit University, Tikrit, Iraq*
[2]*Department of Computer Engineering, College of Engineering, Nahrain University, Baghdad, Iraq*
E-mail: *Musariaoja@yahoo.com, fawzi.alnaima@ieee.org*
Received May 12, 2010; *revised May* 21, 2010; *accepted May* 27, 2010

Abstract

The energy industry and in particular the Oil Refineries are extremely important elements in Iraq's infrastructure. A terrorist attack on one oil refinery will have a catastrophic impact on oil production and the whole economy. It can also cause serious damage to the environment and even losses of human lives. The security of information systems and industrial control systems such as Supervisory Control and Data Acquisition (SCADA) systems and Distributed Control System (DCS) used in the oil industry is a major part of infrastructure protection strategy. This paper describes an attempt to use several security procedures to design a secure, robust system for the SCADA and DCS systems currently in use in the North Oil Refinery in the city of Baiji located in northern Iraq.

Keywords: DCS, SCADA, Security, Encryption, Internet, Public Key, DMZ, Data Security

1. Introduction

The increased use of computer network in control systems and the use of internet as communication backbone have brought benefits in communication and for the process control in general. The ability to share information, making decision concerning production stoking and distribution has been greatly improved [1]. New information technologies have recently been introduced for control system based on open standards like Visual Basic, Java, Open Database Connectivity (ODBC), Ethernet communication and finally the use of internet based control system. Internet or web based control system uses some internet protocols in the application layer to monitor and control plants at a distance. Older control systems were based on closed protocols implemented by vendors of SCADA, DCS, and Programmable Logic Controller (PLC) systems. However, the new common technology and the use of internet introduced many challenges in the area of security, such as cyber threats [2].

The North Oil Refinery in Baiji is a large industrial complex located on various sites scattered around the city of Baiji, north of Baghdad. This complex comprises four basic big refineries: 1) Salah Aldine-1, 2) Salah Aldine-2, 3) North, and 4) Chemical Products. All these refineries are functioning under the same direction and are technically sported by unified sections. Each refinery unit has many DCS systems controlling several chemical processes. These processes are independent of each other and are situated at different geographical locations. Each DCS acts as standalone control system with its private communication network and local control room (LCR).

DCS systems in operation are based on new information technology (IT) with open standards such as TCP/IP protocols using fiber optic Ethernet for data transmission between field and LCR. The refineries direction begins a new project to connect all DCS systems to a Central Control Room (CCR) via intranet. Local server of each DCS will be connected to system server located at the CCR. System server will be connected to the Internet as part of web based control system of the refineries.

Multi-layered security system is suggested for Baiji Oil Refineries. This strategy of security will be based on the "ring of defense" around each local network of each DCS and also around the overall corporate intranet (which will be similar to SCADA system) [2].

The suggested security system can also be used for other SCADA systems in general like those used in Electrical Power Plants, Water Purification and many other Oil Industries.

2. Networking DCS's

The model to be adopted in this work is to consider each

DCS system as a node or "station" of a global SCADA system in the perspective of grouping all LCR of all DCS's of the North Refineries in the CCR. CCR will be the central control of the overall SCADA system. Each DCS will keep its local server, local database, and local LCR, and will be connected to the CCR via appropriate communication links.

The connection of local servers to the system server (or web server) of SCADA system located at the CCR is made via corporate intranet as depicted in **Figure 1**. Communication links between LCR sites and CCR can be accomplished by fiber optics, coaxial cable or wireless links regarding several factors related to topology, geography, and required bandwidth. Reliability, availability and redundancy are major factors for the design of network topology. System database and all local databases use the same standard SQL database. The system database is located near the system server at the interface zone between corporate intranet and the internet. This location is chosen at the border of the system to minimize the risk of unauthorized intruder. The topology definition and the reliability of the communication network are not a part of this work.

3. Security Strategy

The similarity of the new SCADA system and the ordinary IT system leads to the adoption of the same security approach used in computer communication network. The principal of networks separation into "rusted network" and "non-trusted network" fit perfectly for securing SCADA systems [3]. The ring of defense (multi-layer security system) will be implemented using various techniques, which are cited as the principal countermeasure for securing SCADA [4]. The goal of such model will be the repetition of countermeasures to enhance the global system security as shown in **Figure 2**.

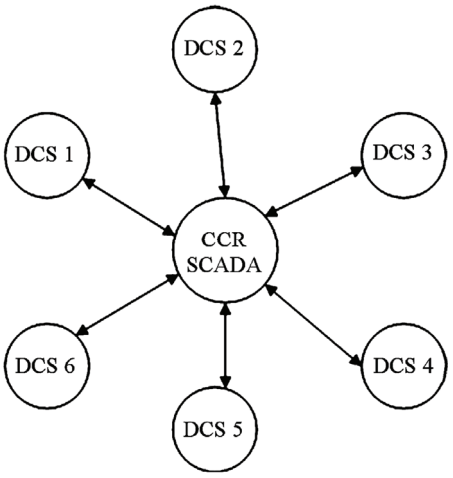

Figure 1. Networking DCS's.

Each layer will acts against one or more of possible security challenges. There exist many cyber threats facing control systems as cited in **Table 1** [5]. Each security layer will be part of the defense on depth against threats.

The possible attack will be considered from the external non trusted network (the Internet) in the direction of the internal trusted network (the corporate intranet).

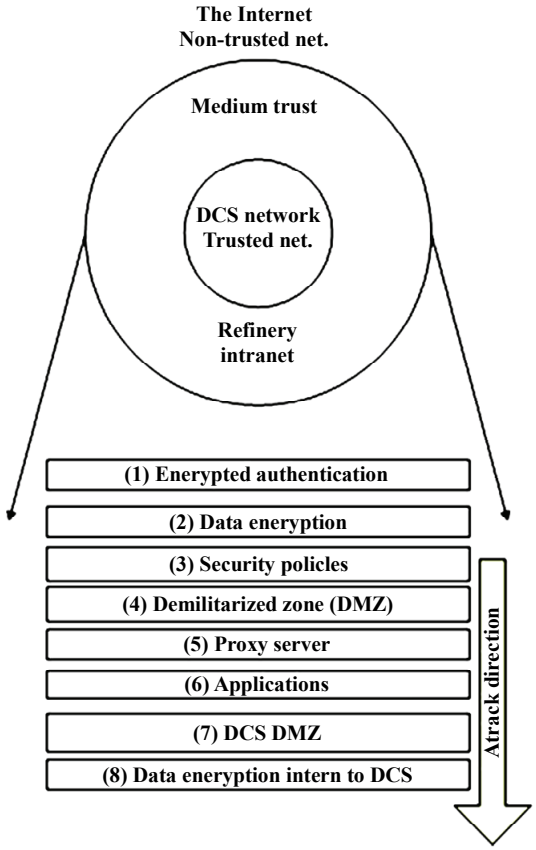

Figure 2. Ring of defense.

Table 1. Correlation of security threats and properties.

Properties	Cyber threats	Importance
Message confidentiality	Eavesdropping	Low
	Traffic analysis	Low
Message integrity	Message modification	High
	False message injection	High
Message freshness	Message replay	High
Availability	Denial-of-service	Middle
	Malicious codes	Middle
Source authentication	Masquerade	High
	Unauthorized access	Middle

The compatibility of countermeasures like encryption standards, firewall, antivirus, intrusion detection techniques will be accomplished by the use of standardized techniques. Each DCS system can be isolated immediately from the SCADA network and then be controlled locally if needed. The connection or the disabling of connection of one DCS can be made locally or from the CCR by some fixed authorization protocol. The connection of DCS system to the CCR server and then to the internet will be subject to several layers of security defense rings as illustrated in **Figure 3**. Between each DCS system and the corporate intranet network a demilitarized zone (DMZ) is used where the local server and database of DCS reside. The global SCADA system is connected to the internet via another DMZ. To login from browser to the SCADA intranet an original process of encrypted authentication and digital signature is implemented.

3.1. Encrypted Authentication

It is the first security stage for an external client. An original authentication process is developed based on asymmetric key encryption algorithm as shown in **Figure 4**. The RSA algorithm is used to encrypt the password two times for the implementation of authentication and the secrecy of password [3,6].

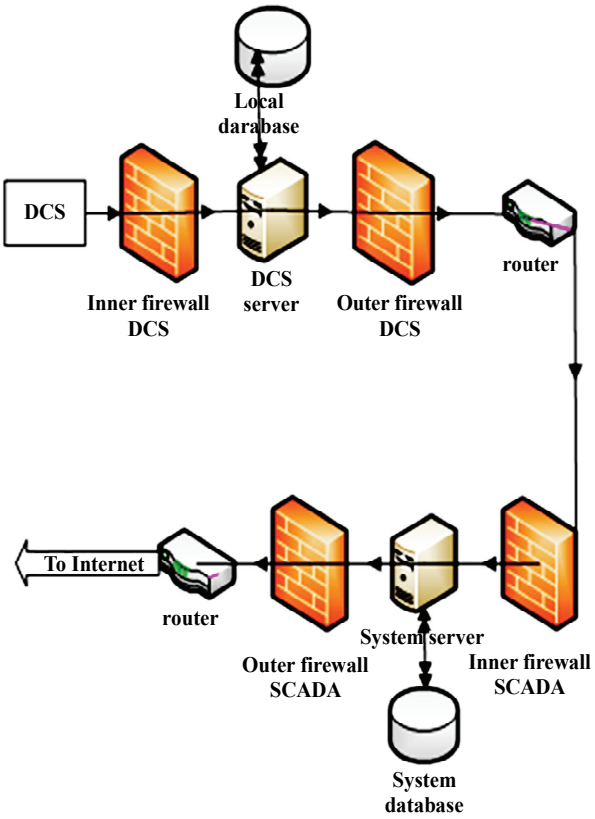

Figure 3. Security layers from DCS to internet.

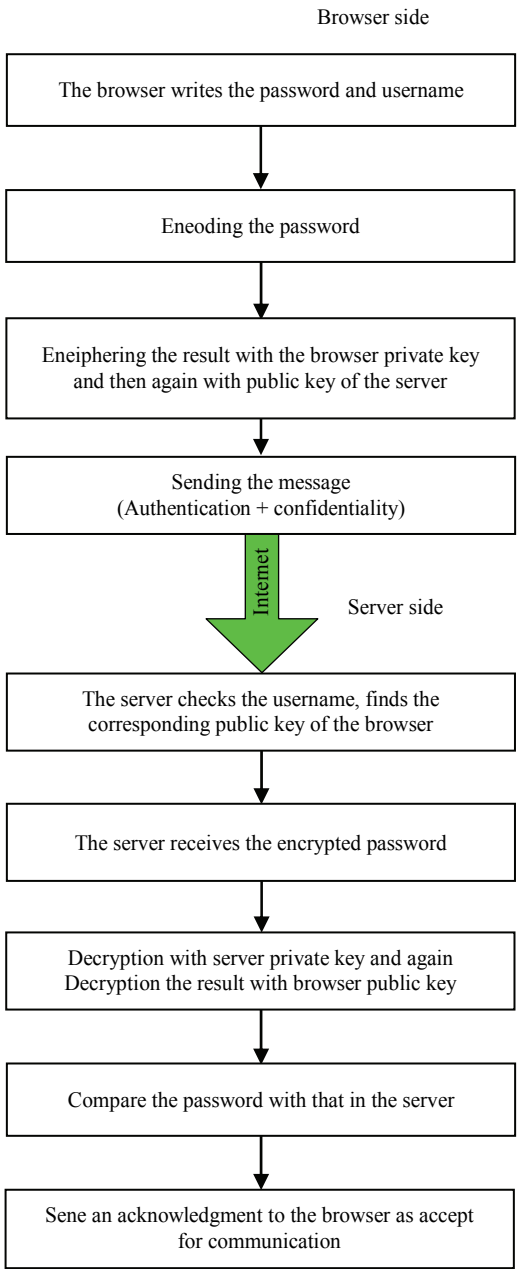

Figure 4. Authentication process.

The implementation of public key algorithm was made with two key groups (e_1,d_1), and (e_2,d_2), where e_1 is the public key of the first key group, d_1 is the private of browser (personal private key), e_2 is the second public key, and d_2 is the private key of server.

The method of defining these keys, and the encryption algorithm is as follows:

Choose two large prime numbers (p and q), let:

$$n = p \times q \tag{1}$$

The function $\beta(n)$ is the number of numbers less than (n) with no factors in common with (n).

Choose an integer number e, ($e < n$) relatively prime to $\beta(n)$. Find second integer (d) such that

$\{e \times d \bmod \beta(n) = 1\}$

Then, the Public Key = (e, n)

The Private Key = (d, n)

The encryption function of RSA for a plain text (M) is (C) such that:

$$C = M^{d} \bmod n \quad (2)$$

Then, the recovered plain text (M) is:

$$M = C^{e} \bmod n \quad (3)$$

If (e) is used instead of (d) for the encryption of equation (2), then (d) will be used for the decryption in Equation (3).

The password will be encoded using ASCII code or other encoding system. Each byte will be encrypted two times: the first with (d_1) and the second with (e_2) This will ensure both secrecy and authentication of the password. At the server side, the reverse process is executed. The received cipher password will be first decrypted using (d_2) and then (e_1) in order to get the original plain text password.

The result will be compared to usernames table in the server. If matching is achieved then the server will open a communication channel and begin responding to browser requests.

3.2. Data Encryption

To protect SCADA system already connected to the internet and its data from unauthorized accesses many algorithms for data protection exist. In this work two encryption algorithms are used to encrypt data.

1) *Encryption*-1(*security layer* 2): This encryption algorithm used to encrypt data over the Internet. We propose to use the Secure And Fast Encryption Routine (SAFER+), which is one of the known symmetric key algorithms that accomplishes requirements for real time data encryption. The SAFER+ was designed by James Messey for Cylink Corporation in 1998 as the new algorithm of SAFER family (safer-64, safer-128...) [7]. It was one of the candidates of the Advanced Encryption Standard (AES) chosen for its good hardware-software tradeoff orientation, simplicity, high throughput compared to other algorithms, and low memory requirement [8], [9]. Also, this algorithm brought attention recently by the use in as security measure in Bluetooth and wireless communication [10,11].

A detailed analysis of maximum bit rate for one DCS proves that SAFER+ fits well for the encryption of data over Internet to get the required real data transmission. SAFER+ is published with three options, 128 bits, 192, bits and, 256 bits key lengths. All three options are used to encrypt 16-byte plaintext. The plaintext block then passes through R rounds of encryption where R is determined by the key length chosen for encryption in the following manner:

- If key length = 128 bits then R = 8 rounds.
- If key length = 192 bits then R = 12 rounds.
- If key length = 256 bits then R = 16 rounds.

Our choice was the adoption of SAFER+ with 128 bits key length as other key lengths were found with certain key weaknesses [12]. Also, by increasing key length more computation time is needed related to rounds number which will affect the assumption of real data transmission in control system.

This algorithm will be implemented as hardware in the server side and portable software in the client side. If there is wireless link between two sites interior to the corporate intranet, SAFER+ must be used with hardware encryption decryption processes. SAFER+ algorithm is divided into three blocks: the key scheduling, encryption process, and decryption process. Programming is accomplished using Turbo Pascal.

2) *Encryption*-2 (*security layer* 8): This algorithm is used to encrypt data over the network of one DCS. This algorithm is not a part of this work but we can use the American Gas Association (AGA) standard which is proven to be a good choice for data over DCS network when dealing with protocols such as MODBUS or DNP3 [13]. In this work we found that securing data over the DCS network has no significant impact to enhance the security of overall system because all DCS system are well physically protected in isolated areas and we take care about data security when data circulate outside DCS network by other countermeasures. This encryption procedure is mentioned here merely for other case studies with other compromises and challenges related to other situations.

3.3. SAFER+ Encryption/Decryption

Giving the 16-byte key (128 bits), SAFER+ begin by calculating a set of 17 keys each with same length 16 bytes. The calculation uses sample arithmetic and logic functions like bit rotation, bit-by-bit exclusive-or of bytes, modulo 256 addition of bytes, and selection byte process.

The 17 sets of keys are used in the encryption rounds. Two keys are used for each round. Round (i) uses key K_{2i-1} and K_{2i}. At the end of 8 rounds key K_{17} is used for the output operation which is the output transformation. The output transformation uses bit-by-bit exclusive-or of bytes and modulo 256 byte addition as shown in **Figure 5**. At the reception the reverse process is used for decrypting the cipher text. Beginning by the input transformation, Key K_{17} is used. The input transformation uses same functions of the output transformation but with modulo 256 subtraction of bytes instead of addition of bytes. Each encryption round (i) begin by the bit-by-bit Xor of bytes, and modulo 256 addition of bytes for the

key K_{2i-1} to the input 16-byte of the round **Figure 6**. The 16-bytes result are then fed to a layer of nonlinear function. The value x of byte j is converted to 45^x mod 257 for j = 1, 4, 5, 8, 9, 12, 13, and 16 (with the convention that when x = 128, then 45^{128} mod 257 = 256 is represented by a 0). The value x of byte j is converted to $\log_{45}(x)$ for j = 2, 3, 6, 7, 10, 11, 14, and 15 (with convention that when x = 0, then $\log_{45}0$ = 128). The output of the nonlinear layer is then subject to same addition and Xor operation similar to the first block with key K_{2i}. At the end of round (i), a block of matrix multiplication is used. The 16 bytes are multiplied by matrix T in mod 256 arithmetic. T is a 16 × 16 predefined matrix.

The operations in the decryption round are simply conducted in reverse order to the operations from the encryption round.

The first operation in the decryption round (i), is to post multiply the 16-byte round input by matrix T^{-1}, which is the modulo 256 inverse of T to give the 16-byte result (S). The first round sub key $K_{16-2i+2}$, is then "subtracted" from (S) in the manner that the round sub key bytes 1, 4, 5, 8, 9, 12, 13, and 16 are subtracted modulo 256 from the corresponding bytes of (S), while round sub key bytes 2, 3, 6, 7, 10, 11, 14, and 15 are added bit-by-bit modulo 2 to the corresponding bytes of (S). The 16-byte result is then processed nonlinearly in the manner that the value x of byte j is converted to $\log_{45}(x)$ for bytes j = 1, 4, 5, 8, 9, 12, 13, and 16 (with the convention that when x = 0, $\log_{45}0$ = 128). For j = 2, 3, 6, 7, 10, 11, 14, and 15, the value x is converted to 45^x mod 257 (with the convention that when x = 128, 45^{128} mod 257 = 256 round sub key $K_{16-2i+1}$, is then "subtracted" from the 16-byte result in the manner that the round sub key bytes 1, 4, 5, 8, 9, 12, 13, and 16 are added bit-by-bit modulo 2 to the corresponding input bytes. Sub key bytes 2, 3, 6, 7, 10, 11, 14, and 15 are subtracted modulo 256 from the corresponding input bytes to produce the 16-byte output of the round.

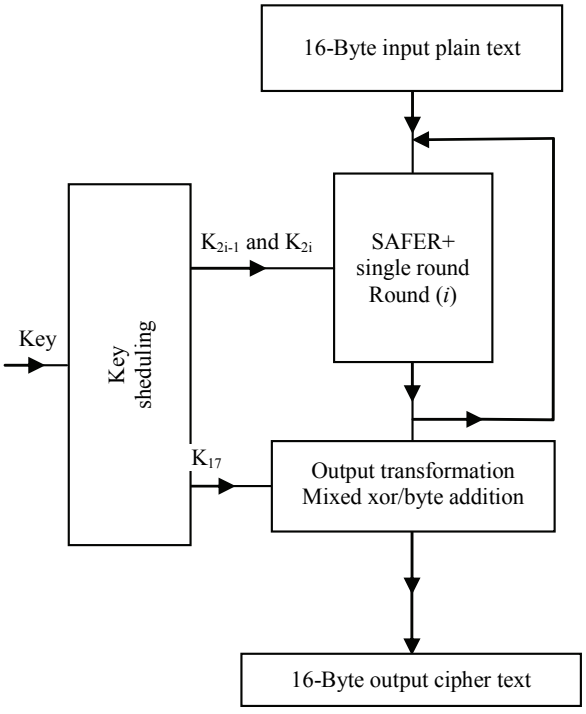

Figure 5. SAFER+ encryption process.

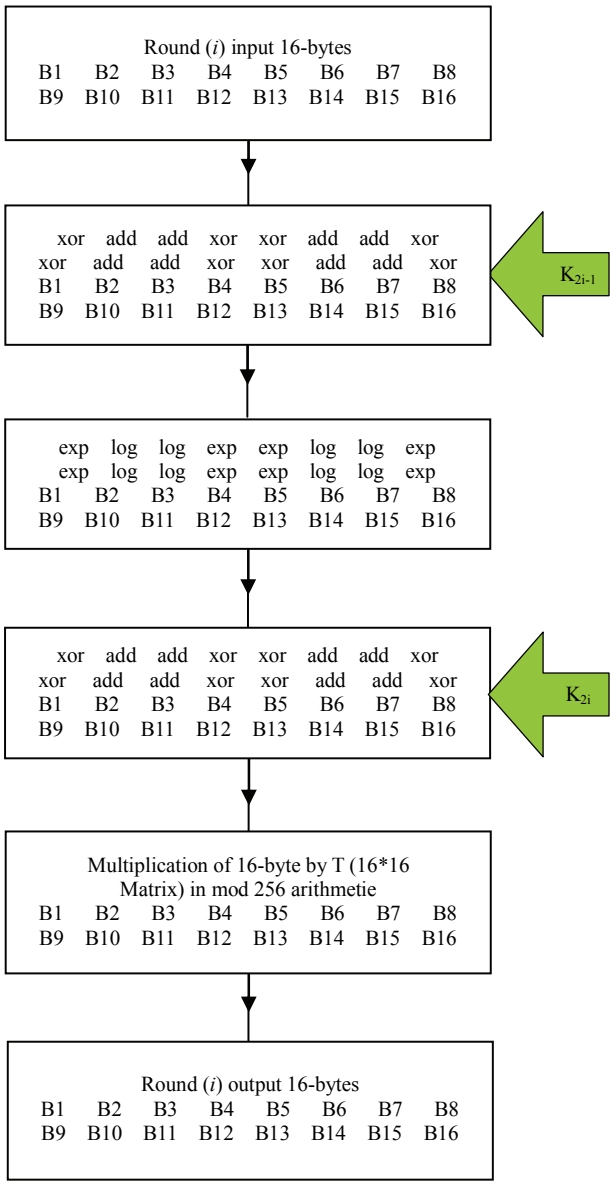

Figure 6. Encryption round (*i*).

3.4. Demilitarized Zone (DMZ)

DMZ is a good technique for securing communication network based on the principal of "networks separation strategy", between trusted network (like DCS LAN) and

another network with less level of trust [1,3]. In the DMZ the server and database reside in safe place, see **Figure 3**. Proxy server and application action like antivirus are also deployed in the DMZ. In this work a double protection is found by the use of two DMZs. The first is as a security interface between SCADA system and the external non-trusted Internet (security layer 4), while the second is between the DCS trusted network and the less trusted corporate intranet for SCADA (security layer 7). DMZ is a zone between an inner firewall and an outer firewall. This firewall, properly configured, can protect passwords, IP addresses, and files. Firewall acts as a filter that permits the data to enter from certain ports and blocks others. At the DMZ output a router is used as border router to route information to correct destination.

3.5. Security Policies

Security policies must be fixed by the security committee of the enterprise. Correct procedure of effective policies can reduce violation of security rules. Training personnel at the vocation of security can increase the defense in depth strategy. Developing documentation and well defining the access authorization will be a very active point. The choice of password must be as random as possible with at least ten characters, including symbols and numbers.

In this work all the required information of the group of DCS in the North Oil Refinery will be available in the system server in the master DMZ (between corporate network and the internet).

4. Simulation Results

RSA and SAFER+ encryption algorithms are implemented in Turbo Pascal language. As example to show how the encrypted authentication will be calculated. Let the password be chosen as the random word 'playmyaudio'. Encoding this password with simple code from 01 for (a) to 26 for (z), will give:

$$M = 16, 12, 1, 25, 13, 25, 1, 21, 4, 9, 15.$$

C will be composed by the same number of 11 bytes. Consider for our example the following values for the keys are taken:

$$e_1 = 13,\ d_1 = 53,\ e_2 = 37,\ d_2 = 17,\ n = 77$$

Using equation (2) twice with browser private key d_1 and then with server public key e_2 the cipher text will be:

$$(16^{53} \bmod 77)^{37} \bmod 77 = 60$$

$$(12^{53} \bmod 77)^{37} \bmod 77 = 45$$

For the same for other bytes, we have:

$$C = 60, 45, 1, 58, 13, 58, 1, 21, 37, 53, 15.$$

At the server, the received cipher text will be converted back to the original password using Equation (3) twice:

$$(60^{13} \bmod 77)^{17} \bmod 77 = 16$$

$$(45^{13} \bmod 77)^{17} \bmod 77 = 12$$

So on for other bytes to get the original password:

$$M = 16, 12, 1, 25, 13, 25, 1, 21, 4, 9, 15.$$

The use of double RSA encryption procedure will gives both authentication and secrecy.

SAFER+ algorithm uses matrix to represent the 17-sub keys (17 × 16 matrix).given the secrete key (K_1) as series of 16 bytes, the 16 other keys, each of 16 bytes will be generated. The calculation of each round is made using iterative process and many preprogrammed procedure (for Xor, Exp, log..).

As an example for the encryption/decryption process, let the 16 byte user selected input key (secrete key) be: 41, 35, 190, 132, 225, 108, 214, 174, 82, 144, 73, 241, 241, 187, 233, 235.

After the execution of key schedule procedure of **Figure 7**, for 128 bit key we have the (17 × 16) matrix which represents the 17 sub keys each of length 16 bytes (128 bits). Each key is represented by a row, where row (1) represents K_1 (the secrete key), to row (17) which represents K_{17}, this will give the matrix (K) shown in **Figure 8**. The resulting 17 sub keys and the plain text are used to generate the cipher text as presented in **Figure 5**.

The plain text block input (16 byte plain text) = 179, 166, 219, 60, 135, 12, 62, 153, 36, 94, 13, 28, 6, 183, 71, 222.

The resulting cipher text will be = 224, 31, 182, 10, 12, 255, 84, 70, 127, 13, 89, 249, 9, 57, 165, 220.

The predefined bias matrix (B) is given as (16 × 16) matrix as input to generate sub key matrix [7]. This procedure will be used to encrypt input data by block of 16 bytes at a time. The schedule procedure will be executed next time when the secrete key is changed to find the new matrix (K).

5. Conclusions

The use of open standard improves the control operations by improving the possibility of interconnecting many systems from different vendors together without restrictions in term of standards. Action for the security of SCADA system must be up to date regarding the continued advances in information technology. Care must be taken for the use of latest version of antivirus, and intrusion detection programs. Symmetric encryption algorithms can be used to encrypt data over internet for SCADA system if the required bit rate is accomplished. SAFER+ algorithm can accomplish the real data transmission requirement. Using SAFER+ give us the possibility to encrypt data by software or hardware implementations.

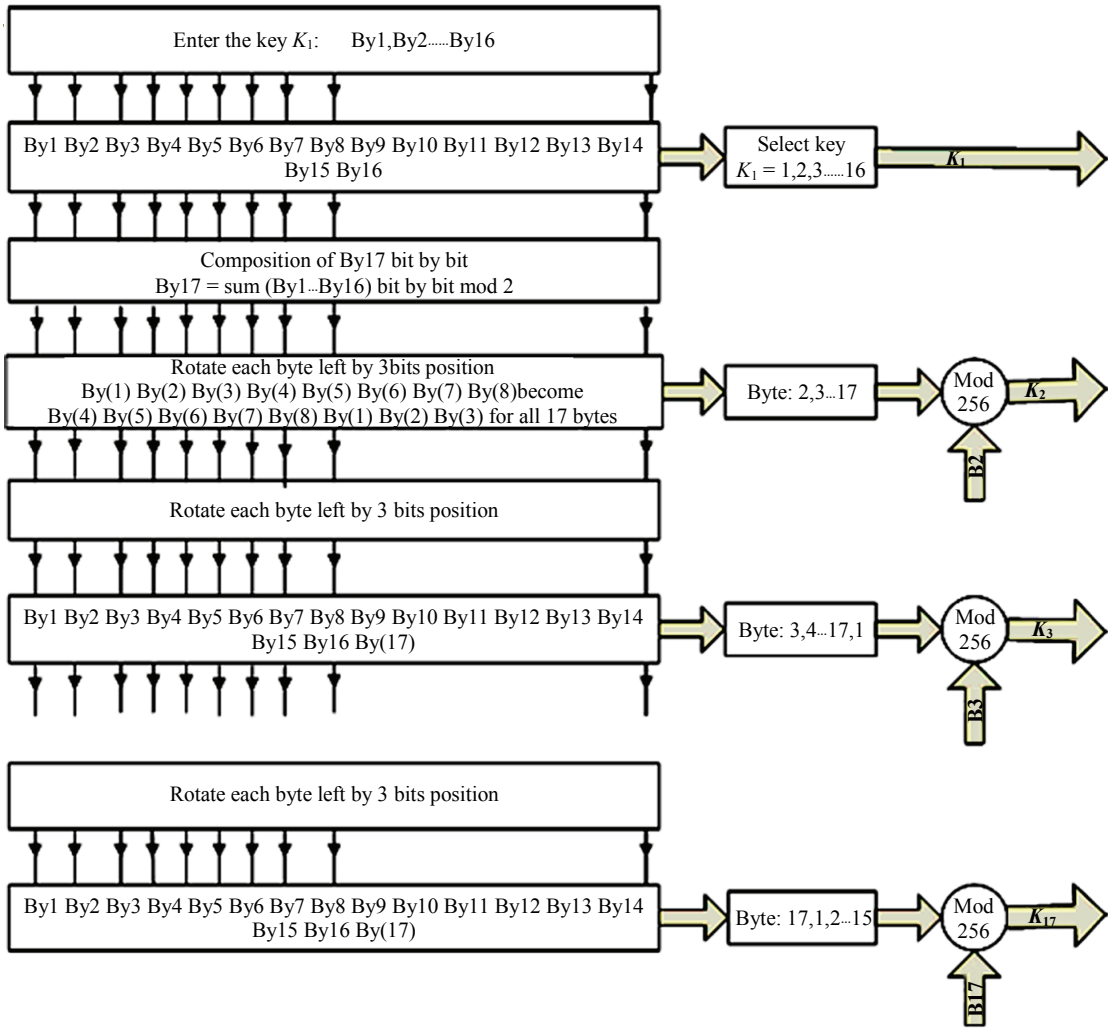

Figure 7. Sub keys generation process.

$$K = \begin{bmatrix}
41 & 35 & 190 & 132 & 225 & 108 & 214 & 174 & 82 & 144 & 73 & 241 & 241 & 187 & 233 & 135 \\
95 & 140 & 213 & 201 & 6 & 109 & 133 & 156 & 73 & 129 & 66 & 88 & 55 & 119 & 11 & 35 \\
155 & 204 & 34 & 225 & 28 & 64 & 236 & 49 & 74 & 22 & 114 & 92 & 224 & 214 & 2 & 135 \\
147 & 134 & 176 & 54 & 199 & 141 & 87 & 219 & 38 & 162 & 98 & 167 & 109 & 138 & 186 & 230 \\
123 & 29 & 255 & 9 & 250 & 122 & 240 & 218 & 65 & 124 & 92 & 57 & 59 & 43 & 149 & 127 \\
96 & 204 & 15 & 93 & 122 & 189 & 245 & 243 & 244 & 52 & 219 & 76 & 177 & 210 & 163 & 209 \\
56 & 190 & 201 & 32 & 12 & 248 & 157 & 109 & 168 & 81 & 214 & 221 & 102 & 105 & 53 & 81 \\
15 & 26 & 46 & 250 & 110 & 124 & 137 & 222 & 74 & 13 & 5 & 12 & 134 & 18 & 149 & 185 \\
207 & 61 & 251 & 224 & 179 & 66 & 183 & 96 & 253 & 60 & 37 & 78 & 211 & 15 & 222 & 9 \\
68 & 215 & 94 & 56 & 94 & 49 & 35 & 230 & 120 & 133 & 111 & 195 & 97 & 68 & 203 & 173 \\
78 & 156 & 190 & 181 & 130 & 222 & 6 & 159 & 38 & 59 & 53 & 238 & 123 & 180 & 138 & 107 \\
221 & 238 & 152 & 211 & 241 & 232 & 248 & 255 & 101 & 167 & 37 & 36 & 134 & 238 & 244 & 243 \\
55 & 111 & 165 & 66 & 105 & 237 & 214 & 179 & 86 & 233 & 14 & 214 & 53 & 115 & 165 & 201 \\
34 & 65 & 73 & 224 & 185 & 205 & 107 & 140 & 123 & 117 & 55 & 254 & 4 & 179 & 82 & 236 \\
212 & 162 & 91 & 17 & 41 & 175 & 56 & 251 & 163 & 238 & 13 & 249 & 50 & 54 & 180 & 74 \\
51 & 1 & 59 & 215 & 18 & 174 & 202 & 253 & 151 & 91 & 101 & 89 & 167 & 98 & 148 & 104 \\
127 & 111 & 186 & 111 & 62 & 132 & 35 & 230 & 184 & 23 & 199 & 252 & 186 & 75 & 227 & 149
\end{bmatrix}$$

Figure 8. Sub key matrix (*K*).

The use of computer network protection can be very useful in SCADA like DMZ, and network segmentation from the trust point of view. Layered strategy is a good method to secure SCADA, DCS and control systems in general. The use of different layered actions against cyber threats makes the defense in depth active. Authentication is one of most used and active countermeasure for security in control systems. The use of RSA public key algorithm for encrypt password will ensure security and authenticity.

6. References

[1] R. L. Krutz, "Securing SCADA Systems," Wesley Publishing, Inc., Indianapolis, 2006.

[2] J. Pollet, "Developing a Solid SCADA Security Strategy," *Proceedings of the Second ISA/IEEE Sensors for Industry Conference*, Houston, November 2002, pp. 148-156.

[3] M. Bishop, "Introduction to Computer Security," Addison-Wesley, Boston, 2005.

[4] J. Nordlander, "What is Special about SCADA System Cyber Security," Master Dissertation, Royal Institute of Technology, Sweden, 2009.

[5] H. Lim, S. Hong, M. S. Choi, S. J. Lee, T. W. Kim, S. W. Lee and B. N. Ha, "Security Protocols Against Cyber Attacks in the Distribution Automation System," *IEEE Transactions on Power Delivery*, Vol. 25, No. 1, 2010, pp. 448-455.

[6] T. Davis, "RSA Encryption," October 2003. http://www.geometer.org/mathcircles

[7] J. Messy, H. Kh and K. Kuregian, "Nomination of SAFER+ as a Candidate Algorithm for the AES," 1998. http://csrc.nist.gov/archive/aes/round1

[8] A. Schubert and W. Anheier, "Efficient VLSI Implementation of Modern Symmetric Block Ciphers," 6*th IEEE International Conference on Electronics, Circuit and Systems*, Pafos, Vol. 2, September 1999, pp. 757-760.

[9] S. Mukherjee, D. Ganguly and S. Naskar, "A New Generation Cryptographic Technique," *International Journal of Computer Theory and Engineering*, Vol. 1, No. 3, August 2009, pp. 284-287.

[10] I. S. Ashour, "Online Data and Voice Encryption System Based on FPGA," 24*th National Radio Science Conference*, Cairo, National Republican Senatorial Committee, 2007, pp. 1-7.

[11] D. Sharmila and R. Neelaveni, "Performance Analysis of SAFER+ and Triple DES Security Algorithms for Bluetooth Security System," *International Journal of Computer Science and Network Security*, Vol. 9, No. 2, 2009, pp. 74-87.

[12] J. Kelsey, B. Schneier and D. Wagner, "Key Schedule Weaknesses in SAFER+," *Second Advanced Encryption Standard Candidate Conference*, Rome, 1999, pp. 155-167.

[13] A. West, "Securing DNP3 and Modbus with AGA12-2J," *IEEE Power and Energy Society General Meeting*: *Conversion and Delivery of Electrical Energy in the* 21*st Century*, Pittsburgh, 20-24 July 2008, pp. 1-4.

