A Risk-Assessment Model for Cyber Attacks on Information Systems

Sandip Patel, Ph.D.
Email: Sandip.Patel@morgan.edu

Jigish Zaveri, Ph.D.
E-mail: Jigish.Zaveri@morgan.edu

Department of Information Science & Systems, Morgan State University, Baltimore, MD 21251

***Abstract* –Industrial process-plants are an integral part of a nation's economy and critical infrastructure. The information systems used by automated industrial plants are enticing targets of cyber attacks. However, the financial damages resulting from these cyber attacks are difficult to estimate since the resultant losses are not as tangible as physical losses. In this paper, we propose a mathematical model for determining the financial losses resulting from cyber attacks on a computer-based information system used in industrial plants.**

Limited work has been published to systematically explore the types of possible cyber attacks and their financial impact on the process. The primary objective of this research is to propose a risk-assessment model to assess the impact of cyber attacks on a plant that runs fully or partially by control systems such as supervisory control and data acquisition (SCADA). Managers could use the model for cost/benefit analysis of security software and hardware acquisition. We also illustrate this model's use on a SCADA system using a case. The proposed model could be applied to different industries and organizations with minor modifications to reflect the specifics of that industry or organization.

***Index Terms*–Cyber attacks, computer security, risk assessment, control systems, information systems.**

I. INTRODUCTION

The industrial process-plants are an essential part of a nation's critical infrastructure sector. The industrial processes in such plants include chemical or mechanical steps to manufacture chemicals and/or other products. An industrial plant functions using control systems, which are electronic, software-based systems that monitor and control the functions and processes of the plants. America's economic vitality, national security, and way of life depend on the production and dissemination of chemicals and chemical byproducts [1]. However, these control-system-based plants are vulnerable to damages due to natural as well as malicious attacks on the control systems. Cyber attacks on industrial plants can have a devastating impact on the nation's economy. Only limited research has been published to systematically analyze the financial losses resulting from cyber attacks. The quantification of losses is a complex task since there is a wide category of losses, with each category different in probability and nature. In this research, we propose a mathematical model for calculating the financial losses resulting from cyber attacks on a control system used in industrial plants. The control systems are a part of organizational information system. We consider short-term financial losses resulting from only real-time cyber attacks that result in incapacitating some or all of the plant operations. After proposing the model, we demonstrate its utility with a case study of a chemical engineering plant.

The proposed model is comprehensive and could be applied to a wide spectrum of industries and organizations to estimate financial damages from the cyber attacks. Managers could use the model for cost/benefit analysis of security hardware and security software they plan to buy. Using the proposed model, managers could justify the resource allocation or spending money to protect an information system. Third, the model could also be used by the insurance companies for risk analysis and management. The model could provide such companies with financial estimates on the losses resulting from different types of cyber attacks. We illustrate this model's use on a Supervisory Control and Data Acquisition (SCADA) system. To demonstrate the utility of the model, the method is applied to a case study on a chemical engineering plant located at the University of Louisville, Kentucky.

The process of implementing security includes the phases of risk assessment, policy determination, security-enhancement implementation, user training, and auditing [2, 3, 4]. The goals of risk management are to identify, measure, control, and minimize the losses associated with uncertain events or risks. Risk assessment includes tasks such as analyzing assets, identifying vulnerabilities and potential risks due to threats, finding risk-reducing measures, and making decisions related to the acceptance, avoidance, or transfer of risk. Risk management also includes determining risk-reducing measures and budgeting, implementing, maintaining, and having priorities assigned to the measures. In section II, we provide background on risk management and SCADA security. Section II presents a detailed discussion on the research methodologies utilized to construct the proposed model. In section IV, we describe a comprehensive real-

doi:10.4304/jcp.5.3.352-359

world case study that applies the model to a chemical engineering plant. Section V contains conclusions followed by the directions for future research.

II. Background and Related Work

A. Risk Management

In the post 9/11 era, risk management has been a contemporary issue affecting all organizations private and public alike. For example, a recent report [5] indicates that the Pentagon spent more than $100 million in the last six months responding to and repairing damage from cyber attacks and other computer network problems. The money was spent on labor, computer technology and contractors hired to clean up after both external probes and internal mistakes. Additionally, Air Force General Kevin Chilton, the head of U.S. Strategic Command, acknowledged the need for the military to improve tracking the costs associated with cyber attacks.

Risk assessment [6, 7] is usually the first, the toughest, and the most error-prone step in the risk management process. Risk or revenue loss is assessed by estimating two quantities, namely, the magnitude of the potential loss L, and the probability p that the loss will occur. The risk or revenue loss R is calculated as follows [8].

$$R_i = L_i p(L_i)$$
$$R_{total} = \sum_i L_i p(L_i)$$

Obtaining both, L, and p, accurately is difficult for each risk-prone occurrence *i* because of uncertainties in the measurements. For example, the accuracy of L and p depends upon the ability of risk experts, economists, managers, and engineers to estimate the impact of events. These personnel also need to accurately estimate the impacts on the events of different probabilities. To make the calculation more challenging, risk management involves multiple metrics because of the interrelationship between these two quantities. That is, a risk-prone event with a high probability and small potential loss requires to be treated differently than the case of a risk-prone event with a low probability but a large potential loss. To help account for this interrelationship, the loss exceedance probability (EP) curves [9] are sometimes used. The EP curves depict the loss L versus the probability p(L) that losses will exceed L. Using the probabilistic risk analysis, the set of events that could produce a given dollar loss amount L are combined and the resulting probability of this loss are determined. In addition to the magnitude of losses in terms of a dollar figure, the EP curves incorporate the uncertainty in the probability of an event occurring within 5% and 95% confidence interval curves. Based on these estimate curves, the mean exceedance probability curve is constructed.

Cyber Security Prediction Models [10] provide the users with a vehicle for testing hypotheses about how to respond to a cyber attack before it occurs, using risk, vulnerabilities, time between attacks, and intrusion (numbers and durations) concepts. This testing is done by reasoning about the elements of predictive models and their relationships, which are needed to mirror objects and events in the real world of cyberspace. The models provide definitions, equations, plots, and analyses to answer the "what if" questions concerning potentials attacks.

B. SCADA Networks

Supervisory control and data acquisition (SCADA) networks are complex control and monitoring systems used by infrastructure services. A SCADA system is a common process automation system, which is used for gathering data from sensors and instruments located remotely and displaying this data at a central site for either control or monitoring purposes. SCADA networks are used to perform vital functions for industrial measurement and control systems and are commonly used by utility and infrastructure companies such as electric power generation, transmission, and distribution; oil and gas refining and pipelines; chemical production and processing; and manufacturing [11, 12]. SCADA networks control field devices remotely and automatically. SCADA networks control and monitor a variety of remote field-devices such as electric circuit breakers, gas and water pumps, valves, relays, sensors, track switches, and traffic signals automatically. According to ARC Advisory Group [13], the worldwide market for SCADA systems for the electric power industry alone was $1.7 billion in 2006 and is expected to grow to $3 billion in 2013. The European SCADA-systems market revenues were $1.2 billion in 2007.

As shown in Figure 1 [11, 14] using the Internet, today's SCADA systems enable monitoring from various points including over the Internet.

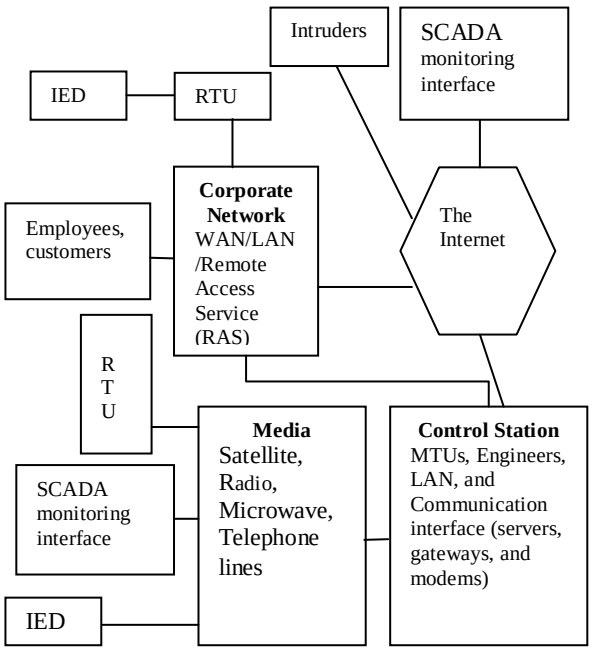

Figure 1. Modern SCADA Architecture [11, 14]

SCADA architecture consists of one of more master terminal units (MTUs) that are used by engineers in a control station to monitor and control a large number of remote terminal units (RTUs) located in the field or an

industrial plant. An MTU is a general-purpose computer, running SCADA utility programs and RTUs are generally small dedicated-devices designed for harsh field or industrial environments. One or more SCADA MTUs retrieve real-time analog and status data from RTUs, store, and analyze these data. MTUs automatically send control commands to the RTUs or enable the engineers to do so manually.

C. Distributed Control Systems

In recent years, SCADA networks, implemented as a part of distributed control systems (DCS) [15, 16, 17, 18, 19], have also enjoyed an increase in popularity within process control industries for monitoring and control. Today, many SCADA systems are included as a part of distributed control systems. DCS are used in industrial applications to monitor and control distributed equipment with remote human intervention. A DCS solution does not require operator intervention for its normal operation, but with the line between SCADA and DCS disappearing, systems claiming to offer DCS may actually permit operator interaction via a SCADA system [20].

The architecture of a DCS involves either a direct connection to physical equipment such as switches, pumps and valves or a connection via a secondary system such as a SCADA system. A DCS integrates programmable logic controllers (PLCs) and process controllers into an interactive system that enables a DCS to manage the whole process as a complete system. The measurement and actuation devices are connected to a local controller. All the local controllers are connected to one another via communication links such as the controller area network or a field bus. According to a survey by market research firm Datamonitor [16], global revenues from sales of control systems were $10.3 billion in 2000 that grew to $12.4 billion in 2006 and are predicted to grow to $13.9 billion in 2009. This continuous rise in popularity is fueled by the advancements in network technologies such as the wireless technology and wide use of TCP/IP protocol, which is used for Internet technology. Implementing these networks is also becoming simpler because of amount of equipment available to install the networks. Thirdly, the increased need to monitor the industrial production facilities, such as a chemical plant, remotely and as automatically as possible has increased the value of SCADA.

D. SCADA Security

The use of SCADA systems has become popular since the 1960's as a need arose to more efficiently monitor and control the state of remote equipment [21]. SCADA networks were initially designed with little attention to security. SCADA networks traditionally used dedicated telephone lines to send control messages to the field devices from the control station and get the status of the field equipment. Initially, SCADA systems were designed to be isolated from other systems with an emphasis on software stability that did not change very often and allowed limited access to users. With advances in computer technology and telecommunications, modern SCADA networks have been increasingly integrated with corporate networks and the Internet. This is done to increase the accessibility and subsequently enhance the efficiency and effectiveness of SCADA networks. However, this integration has made them far more vulnerable to unauthorized cyber attacks putting the national infrastructures at risk [22] and potential targets of attacks by cyber terrorists and hackers. By sending a false control message from the Internet, an unauthorized intruder, for example, can hamper operations of electric-power stations or chemical process-control systems [12]. The evolved, modern control system with open interconnectivity requires rigorous risk management.

As SCADA integrates more and more standard devices that use widely available communication protocols, an adversary will more easily have the ability to disrupt a vastly increased area by manipulating data streams emanating from a component of the system and do so while never leaving the comfort and privacy of home [23]. Threats against SCADA networks have raised significant government concerns, since terrorists have threatened to attack several SCADA networks [24] and successfully launched near-disastrous attacks. For example, in January 2003, a worm attack on a computer network at Ohio's Davis-Besse nuclear power plant disabled a safety monitoring system for nearly five hours [25]. The infamous Maroochy water SCADA breach in Australia [26] plagued the wastewater treatment system for two months and leaked hundreds of thousands of gallons of putrid sludge into parks, rivers, and private properties as a result of which marine life died, the creek water turned black, and left an unbearable stench in the surrounding areas. Unauthorized software was installed and a computer was damaged at a California canal system to divert water from the Sacramento River by an unauthorized person [27].

The cyber communication-attacks are the general cyber attacks that can be launched against both the MTU and RTU. The attacks against the master are specific attacks that can be launched against the MTU. The attacks against the slave are the specific attacks that can be launched against a RTU. Table 1 lists and gives a detailed description of both types of attacks. In this research, we consider losses from only real-time attacks that result in incapacitating parts or all of the plant operations. Losses such as proprietary-information loss that includes stealing business and trade secrets are not considered. For example, a company could lose its trade secrets to its competitors if such information is compromised.

There are direct and indirect losses associated with information-system breaches. For example, the direct or primary losses from an attack on a SCADA-controlled power plant would include the loss of power generation. The indirect or secondary losses would include social instability caused during the blackouts and the economic losses incurred by businesses of the affected regions. If a chemical plant is attacked, the indirect losses would be both the short and long-term environmental effects.

To keep the focus on active attacks, in this paper, we have limited the scope of the paper to the operational attacks that can cause real-time or short-term losses. If other type of losses are also considered, managers can justify spending more money on security enhancements. When we consider such losses, the benefits of the proposed research become more important.

Additionally, the attacks such as eavesdropping (unauthorized interception of information in transit through the use of methods other than wiretapping), traffic analysis (intercepting and examining messages to deduce information from patterns in communication), and man-in-the-middle (gaining information by sniffing or tapping a line between two unsuspecting parties) are excluded in this research since they are passive forms of attacks which do not directly impact SCADA security. We are assuming no damage to human-life is caused by any of these attacks. Due to the built-in redundancy, a system may have small direct or tangible-loss value when the attack affects a small percent of the system. However, as the impact of the attack increases linearly, the amount of indirect or intangible loss could increase non-linearly. The total loss value increase at much higher rate that could even be exponential [28, 29, 30, 31].

In well-engineered systems, fail-safe provisions could prevent some catastrophic consequences of unauthorized intrusions. However, a successful attack launched by the intrusions could still result in economic impacts. For example, by an attack that would halt a chemical plant or damage its products and equipment badly. Additionally, in a SCADA system with a very large number of variables, there are limitations as to how many conditions these engineering safeguards can prevent. A well-designed attack can possibly find a way to damage public health and safety by circumventing the engineering safeguards.

III. Research Methodology

In this research, we first present various types of revenue-losses that can occur due to cyber attacks. We treat these losses as functions of (a) the type of cyber attacks and, (b) other losses whose financial values can be estimated by plant managers in consultation with plant operators, engineers, supervisors, and foremen. We have provided a list of the most probable cyber-attacks and their description in Table 1.

Figure 2 depicts the proposed model. At the core of this model is a set of revenue-loss functions used for calculating the total loss. These functions derive their values from the probabilities of different attack types and manager's financial estimates of the losses that make up a related revenue loss. For example, the revenue loss function $R_{control\text{-}loss}$ takes probability for control-loss as one of its input and manager's estimates of revenues for the normal and manual plant operations as its other input. As shown in Figure 2, there are five revenue loss functions and there are seven attack types with different probability of causing damage. The attack-type probabilities are used to calculate relative damage done by an attack. For example, based on our research and literature review [8, 32, 33, 34, 35, 36, 37], a control-message modification attack is much less likely to cause product damage (5% probability) whereas the same attack is much more likely to cause equipment damage (50% probability).

Table 1. Attack Descriptions

Type of Attacks (A_{type})	Description
Replay	Capture a message and resend it at a later point one or more times.
Spoofing	Pretend to be an MTU or RTU.
Denial of Service	Send a very large number of spurious messages so that RTU is unable to fulfill a valid request.
Control message modification	Capture a request, modify some of its parameters and send it to RTU.
Write to MTU	Add or modify files on MTU.
RTU- response alteration	Capture a response, modify some of its parameters and send it to MTU.
Write to RTU	Add or modify values on RTU.

The default values for the attack types are shown in Table 2. For example, a denial-of-service attack, is much more likely to cause loss of control and monitoring capabilities; hence, it is given a relative weight of 0.5 as compared to other attacks such as the RTU-response-alteration, which usually do not result in losing the control and monitoring capabilities. An attack can cause different types of losses with different probabilities. Hence, each row in Table 2 adds up to 1.

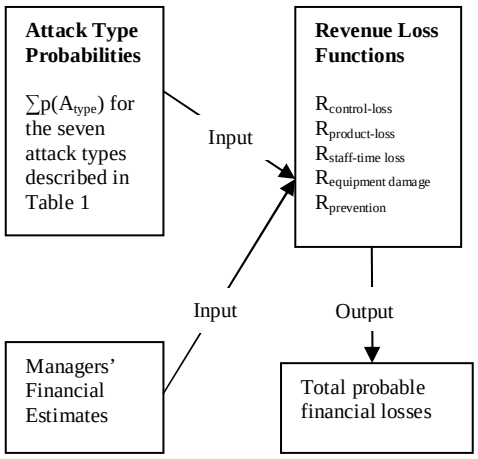

Figure 2. Proposed Model with its Inputs and the Output

Damages caused by different attacks are not mutually exclusive. For example, loss of control caused by the replay attack does not exclude the loss of control cause by the spoofing attack. Therefore, the loss of control caused by replay attack adds a separate risk from that of the spoofing attack. Hence, the total of probabilities for each column does not add to 1. The model for the risk assessment allows managers to modify or update probabilities based on historical data and after consultations with plant operators, engineers, supervisors, and foremen. Specifically, if an organization has installed a security system, managers are able to decide which attacks are less likely to cause a particular type of damage

by updating the values for the probabilities shown in Table 2. Table 2 lists suggested values based on a detailed literature review and our research experience on SCADA cyber-attacks [8, 12, 32, 33, 34, 35, 36, 37].

A cyber attack on an information system can result in various types of losses (damages). The following section lists the attack types and the revenue-loss function associated with each loss. The revenue-loss functions are the functions that determine the values for the financial loss resulting from different types of attacks.

Table 2. Default Values of Probabilities for Attack Types

A_{type}	Probability				
	Control-loss	**Product-Loss**	**Staff-Time Loss**	**Equip Damage**	**Prevention**
Replay	0.20	0.40	0.20	0.10	0.10
Spoofing	0.20	0.20	0.20	0.20	0.20
Denial of Service	0.50	0.10	0.25	0.05	0.10
Control message modificat.	0.15	0.05	0.10	0.50	0.20
Write to MTU	0.10	0.05	0.05	0.30	0.50
RTU-response alteration	0.30	0.10	0.10	0.40	0.10
Write to RTU	0.30	0.20	0.20	0.20	0.10

The relevant attack-scenarios are determined, together with their probabilities of occurrence. We use quartile points for calculating the number of machines attacked: 25% machines down, 50% machines down, 75% machines down, and 100% machines down. A manager inputs these values after reviewing data such as financial records, previous failure logs, existing security measure, and other pertinent databases. Additionally, a manager should also consult with plant operators, engineers, supervisors and foremen to gain a better understanding of the plant operations and use this knowledge to estimate these values on potential financial losses. These values are also used as input values to the revenue loss functions in the proposed model.

A. Control and Monitoring Loss

The loss of control or view is the financial damage caused while trying to run the process without SCADA control. When a SCADA system is attacked, the intruder may hamper plant operations by disabling the monitoring and control operations. For example, some operations in a chemical plant that required constant monitoring by engineers may no longer be performed because of an attack. However, several operations may be possible if they do not require an engineer's monitoring and control.

This loss is treated as a function of revenues per day for the normal plant operation (R_{normal}), the revenues per day if the plant were to run manually without SCADA (R_{manual}), and the type of cyber attack (A_{type}). R_{manual} accounts for various costs associated with running the plant manually, which includes the cost of extra operator(s) who are trying to run the process manually and reduction in production. Restarting the plant (that is, bringing it to normalcy) is also included in this cost.

As discussed earlier in section II, SCADA enables monitoring of several remote devices. Most of the time a MTU makes decisions based on a large number of parameter values obtained from many inter-related activities. When SCADA is attacked, these decisions have to be made manually by engineers. Since any missing parameter value could lead to more damages, we are assuming that even if only one of the SCADA controlled computer is attacked, the SCADA controlled process is disabled.

Other assumptions include that a plant is down for one day. This assumption is modified from the reference [35] who assumes that the duration of SCADA-power-plant blackout is for the duration of 8 hours. Another assumption is that the components of SCADA system and the production system fail independently so that the attack-type probabilities do not have an effect on the number of machines that are down.

$$R_{control\text{-}loss} = (R_{normal} - R_{manual}) * (\sum p(A_{type}) \text{ for control-loss})$$

In the above function, $\sum p(A_{type})$ *for control-loss* is summation of probabilities of all types of attacks that could lead to control loss. The default values of such probabilities are listed in Table 2.

B. Material Loss

Loss of material is the damage caused by bad product quality because the products in the process chain could not be used; or the material in stock became worthless because the raw materials were not used before their expiration dates. For example, raw material in a food-and-beverage plant would be wasted if the material stayed unused for several days. Material cleanup cost is also included in this calculation. This loss is treated as a function of number of vulnerable machines. The revenue loss is $R_{\%\ machines\ down}$ at a given percentile point if vulnerable machines are down.

$R_{product\text{-}loss}$ is estimated by calculating the average of four quartile points. The quartile points are 25% machines down, 50% machines down, 75% machines down, and all of the machines down. The corresponding revenue losses at these points are $R_{25\%}$, $R_{50\%}$, $R_{75\%}$, and $R_{100\%}$.

$$R_{product\text{-}loss} = ((R_{25\%} + R_{50\%} + R_{75\%} + R_{100\%}) /4) * (\sum p(A_{type}) \text{ for product loss})$$

C. Staff-time Loss

Loss of staff time is the revenue loss resulting from idle personnel. For example, a company must continue paying their full-time employees irrespective of whether the plant is operating or not. This value is calculated by multiplying the number of operators, their idle hours, and their hourly pay rate. This loss is represented as follows:

L = (Time taken to fix machines) * (Number of idle operators) * (hourly pay rate)

The quartile points are 25% machines down, 50% machines down, 75% machines down, and all machines

down. The corresponding losses at these points are $L_{25\%}$, $L_{50\%}$, $L_{75\%}$, and $L_{100\%}$.

$R_{\text{staff-time loss}} = ((L_{25\%} + L_{50\%} + L_{75\%} + L_{100\%}) /4) * (\sum p(A_{\text{type}})$ for staff-time loss)

D. Equipment Damage

The equipment damage or loss is the amount of damage done to the process equipment. For example, an adversary may be successful in damaging a turbine by sending unexpectedly high dynamic load for a long period. This loss is treated as a function of total cost of SCADA-operated machines that could be permanently damaged and total cost of SCADA-operated machines that could be temporarily damaged.

Cost of purchasing new equipment: Since not all equipment needs to be replaced, we take each piece of equipment that can be damaged and its cost. Therefore, the average loss, $L_{\text{equipment replace}}$, will be:

$L_{\text{equipment replace}}$ = (Total equipment cost)/(number of equipment)

Cost of fixing the temporary damages can be estimated by the managers. The managers may need to look at historical data and use statistical analysis to accurately estimate these values.

This loss value $L_{\text{equipment fix}}$ is given by the following formula:

$L_{\text{equipment fix}}$ = (total cost to fix equipment from the past records) / (total number of problems in the past records)

$R_{\text{equipment damage}} = (L_{\text{equipment replace}} + L_{\text{equipment fix}}) * (\sum p(A_{\text{type}})$ for equipment damage)

E. Prevention Costs

Cost of preventing intrusion includes fixing the software problems and updating and replacing any hardware. For example, to prevent an attack similar to the one that caused damage, a company may need to upgrade to computer hardware or equipment that are resistant to such attacks. If software was attacked, it might need to be upgraded, replaced, or reinstalled. This cost of updating or replacing necessary software and hardware is treated as a function of protecting the damaged machines from similar attacks in the future.

This cost can be calculated from the average cost of similar repair and upgrades in the past as follows:

$R_{\text{prevention}} = (L_{\text{prevention}}) * (\sum p(A_{\text{type}})$ for prevention)

IV. An Example of Risk Assessment

In this section, we illustrate the use of the proposed model on a SCADA DCS system that is used to monitor and control a chemical plant. This case study illustrates how the proposed methodology is used for a SCADA system test bed that is implemented at the University of Louisville, Kentucky, USA. As show in Figure 2, the proposed model uses attack types, manager's financial input and damage probabilities to estimate the corresponding probable financial losses. The attack types and the revenue loss functions have been illustrated in the previous section. We consider a case [8] to illustrate the financial losses that a manager would input to estimate the probable total financial loss due to these attacks. We first describe the experimental test bed and then provide the financial estimates for this plant.

The main objective of Intelligent Systems Research and Chemical Engineering Laboratories at the University of Louisville is to evaluate operation of a SCADA system under carefully monitored and safe operating conditions. This example [8] considers operating a 14 foot, 50 liter, 6–tray binary distillation column currently used by the students to study laboratory operations. Collection of data, as well as control of the distillation process, is carried out using actual SCADA hardware and software. The distillation process, from start up to shut down is monitored and controlled by a computer-based SCADA control system, specifically iFIX™ software from GE-Fanuc. Remote monitoring and control [38] were achieved over the Internet where the laboratory personal computers are connected to the distillation column. Other computers connect to the personal computer through the web server to access a page that provides a Human-machine interface (HMI), gets data values from the server and updates the values of control variables by sending them back to the server. In this SCADA system the laboratory personal computer serves as an RTU, another personal computer with a browser serves as an MTU, and the university local area network provides the network connection between the RTU and the MTU. The schematic diagram for the distillation column and its control system is shown in Figure 3 [39]. The digital-to-analog converter (DAC) and Analog-to-Digital Converter (ADC) are used to send and receive signals from the RTU computer to the distillation column and back.

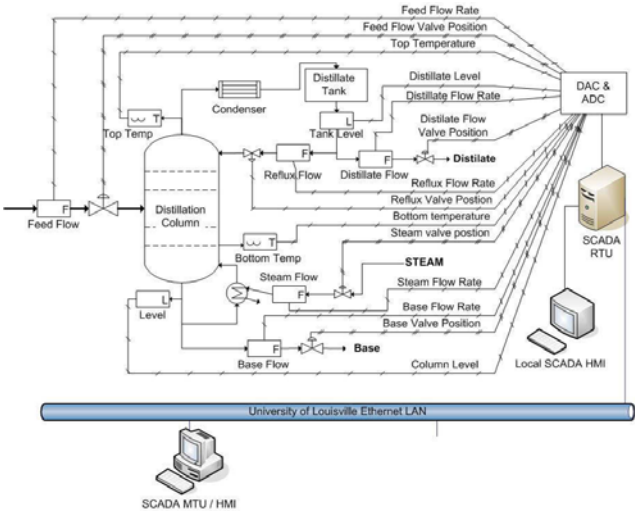

Figure 3: Schematic Diagram of Distillation Column and SCADA-based Controller [39]

The values of estimated probable losses and revenues described in the previous section are as follows:

1. Revenues per day for the normal plant operation (R_{normal}). For the case study, the estimated daily revenue is $100,000.

2. Revenues per day if the plant were to run manually without SCADA R_{manual}. For the proposed case, we assume that half of the plant can be run manually. Hence, the estimated R_{manual} is $50,000.

3. Revenues if various percent of machines were down. That is, $R_{25\%}$, $R_{50\%}$, $R_{75\%}$, and $R_{100\%}$. The reason that we had suggested four failure percent was that the proposed model takes into account possibility of non-linear distribution of the damages. However, for simplicity, we are assuming linear distribution for this case, which gives the estimated damages to be $12,500, $25,000, $37,500, and $50,000 respectively for $R_{25\%}$, $R_{50\%}$, $R_{75\%}$, and $R_{100\%}$. However, a manager can use a non-linear function for their plant operations for the losses.

4. To calculate L, staff time loss, which includes $L_{25\%}$, $L_{50\%}$, $L_{75\%}$, and $L_{100\%}$, the following inputs are needed from the managers: the average time to fix one machine, total number of machines, total number of operators, and average operator's salary. The case [8] lists an average of $35 per hour per operator. The number of operators varies from 1 to 5 depending on the type of the attack and the number of hours to fix the problem varies from 40 to 120 depending on the type of the attack. Using these values, we estimate $2,625, $5,250, $7875, and $10,500 for the average losses $L_{25\%}$, $L_{50\%}$, $L_{75\%}$, and $L_{100\%}$ respectively.

5. Cost of replacing and fixing equipment, which are: $L_{equipment\ replace}$ and $L_{equipment\ fix}$. For the case [8], these values are estimated to be $100,000 and $25,000 respectively.

6. Cost of updating and replacing software and hardware, which is, $L_{prevention}$. This cost is estimated to be $50,000.

Using the above values, we calculate the following revenue loss values:

For example, the values for Control Loss were calculated using the following formulae:

$$R_{control\text{-}loss} = (R_{normal} - R_{manual}) * (\sum p(A_{type}) \text{ for control-loss})$$

Control and Monitoring Loss = ($100,000-$50,000) * (0.2 +0.2+0.5+0.15+0.1+0.3+0.3) = $87,500

Similarly, Material Loss, Staff-time Loss, Equipment Damage, and Prevention Costs are calculated to be $75,625, $7,219, 218,750, and $65,000 respectively using the software that we have created to automate the estimation process. The total estimated revenue loss from all cyber attacks is $454,094. This dollar figure gives an estimate to managers about the average yearly revenue loss. As discussed earlier, this figure can also help insurance companies to estimate the premiums for insuring such information systems.

V. Conclusion

Risk management has been a challenge faced by almost all organizations in the post 9/11 years. However, few methods have been proposed that could estimate financial losses resulting from various cyber attacks on organizational information systems. In this article, we have presented a method that could be used by many different organizations to perform risk assessment of their control systems and also facilitate cost-benefit analysis to justify software and hardware acquisition. This model can also be used by insurance companies to perform risk assessment and estimate premiums to insure the client company's assets.

We have presented a list of possible attack types and probabilities for different types of damages the attacks can cause. We provided revenue loss functions for these attacks, which use these damage probabilities and the corresponding revenue losses. Each of the revenue losses is obtained mathematically from simple and easy-to-obtain financial data. The proposed model provides company managers and insurance companies a valuable tool to estimate their financial damages. We also presented an example of SCADA-based chemical plant to illustrate the use of the proposed method.

In this research, we have considered only active attacks and the immediate resultant financial losses. To extend the model to other losses, future research could consider passive attacks such as eavesdropping, traffic analysis and others that can result in proprietary information loss, loss of competitive advantage, and other losses.

Acknowledgement

This research is supported in part by funds from the Morgan State University Office of Faculty Professional Development under a Title III grant from the U.S. Department of Education.

References

[1] CSIA (2009). Cyber Security Industry Alliance, http://www.csialliance.org/issues/chemicalplantsecurity/index.html, Accessed on March 20, 2009.

[2] Broder, J. R., (2006). *Risk Analysis and the Security Survey*, 3rd Ed., Butterworth-Heinemann, Massachusetts.

[3] Cruz, M. (2004). *Operational Risk Modelling and Analysis: Theory and Practice*, Risk Books, London, UK.

[4] Krause, M. and Tipton, H. F. (1999). *Handbook of Information Security Management*, Auerbach, Washington, D.C.

[5] CBS News (2009). "Pentagon Bill to Fix Cyber Attacks: $100M," On-line Article, April 7, http://www.cbsnews.com/stories/2009/04/07/tech/main4926071.shtml?tag=topHome;topStories, Accessed on April 14, 2009.

[6] Biswas, G., Debelak, K. A., and Kawamura, K. (1989). "Applications of qualitative modeling to knowledge-based risk assessment studies," 1989, *Proceedings of the 2nd international conference on Industrial and engineering applications of artificial intelligence and expert systems* - Tullahoma, Tennessee, ACM, 92 – 101.

[7] Mkpong-Ruffin, I., Umphress, D., Hamilton, J., and Gilbert, J. (2007). "Quantitative Software Security Risk Assessment Model," *Proceedings of the 2007 ACM workshop on Quality of protection*, Alexandria, Virginia, October, 31-32.

[8] Patel, S. C., Graham, J. H., and Ralston, P. S. (2008). "Quantitatively assessing the vulnerability of critical information systems: A new method for evaluating security enhancements," *International Journal of Information Management*, 28(6), 483-491.

[9] Kunreuther, H. (2001). "Mitigation and Financial Risk Management for Natural Hazards," *The Geneva Papers on Risk and Insurance*, 26(2), 276-295.
[10] Schneidewind, N. F. (2005). "Cyber Security Prediction Models", *The R & M Engineering Journal*, 25(4), American Society for Quality, December.
[11] Patel, S.C. (2006). *Secure Internet-Based Communication Protocol for SCADA Systems*. Ph.D. Dissertation, J.B. Speed School of Engineering, University of Louisville, Louisville, Kentucky.
[12] IEEE (2007). IEEE Power Engineering Society**, "**IEEE Recommended Practice for Network Communication in Electric Power Substations," 1-93.
[13] ARC (2009). Advisory Group, Market Study, "SCADA Systems for Electric Power Worldwide Outlook." *http://www.arcweb.com/Research/Studies/Pages/SCADA-Power.aspx*, Accessed on April 14, 2009.
[14] Patel, S., Bhatt, G., and Graham, J., (2009). "Improving the Cyber Security of SCADA Communication Networks," *Communications of the ACM*, 52(7), 139-142.
[15] Basile, F., Chiacchio, P., and Grosso , D. D. (2009). "A Two-stage Modeling Architecture for Distributed Control of Real-time Industrial Systems: Application of UML and Petri Net," *Computer Standards and Interfaces*, 31(3), 528-538.
[16] Geer, D. (2006). "Security of Critical Control Systems Sparks Concern," *IEEE Computer*, 39(1), 20-23.
[17] Mahalik, N. C., Lee, S. K. (2003). "Design and Development of System Level Software Tool for DCS Simulation," *Advances in Engineering Software*, 34(7) 451-465.
[18] Rubio, A., and Ors, R. (2003). "A Comparative Analysis of the Reliability of Simple and Two-level Checkpointing Techniques in Two Different Distributed Industrial Control System Architectures," *Systems Analysis Modeling Simulation*, 43(7), 945 – 957.
[19] Mahalik, N. C., Lee, S. K. (2002). "A Study on Production Line Automation with LonWorks™ Control Networks," *Computer Standards and Interfaces*, 24(1), 21-27.
[20] Encyclopedia (2009). Distributed Control System, *http://www.nationmaster.com/encyclopedia/Distributed-Control-System*, Accessed on April 14, 2009.
[21] Sandia (2009). "The Center for SCADA Security." Sandia National Laboratories, *http://www.sandia.gov/scada/history.htm*, Accessed on April 14, 2009.
[22] Byres, E. (2004). "The Myths and Facts Behind Cyber Security Risks for Industrial Control Systems," *BCIT News*, News Release, October 04.
[23] Beaver, C., Gallup, D., Neumann, W. and Torgerson, M. (2002). "Key Management for SCADA," *Technical Report*, March, Sandia National Laboratories, Albuquerque, New Mexico.
[24] Dacey, R. (2003). "Critical Infrastructure Protection: Challenges in Securing Control Systems", *Report GAO-04-140T*, United States General Accounting Office, October.
[25] Poulsen, K. (2003). "Slammer Worm Crashed Ohio Nuke Plant Net", *The Register*, *http://www.theregister.co.uk/2003/08/20/slammer_worm_crashed_ohio_nuke*, Accessed on April 14, 2009.
[26] Gellman, B. (2002). "U.S. Fears Al Qaeda Cyber Attacks," *Washington Post*, Wednesday, June 26.
[27] McMillan, R. (2007). "Insider charged with hacking California canal system," *Computer World*, November 29.
[28] Finne, T., (2002). "A Conceptual Framework for Information Security Management", *Computer Security*, 17(4), 303-307.
[29] Meadows, C., (2001). "A Cost-based Framework for Analysis of Denial of Service in Networks," *Journal of Computer Security*, 9(1/2), 143-164.
[30] Hoo, K. S. (2000). "How Much Security is Enough: A Risk Management Approach to Computer Security", Ph.D. Dissertation, Stanford University, Stanford, California.
[31] Buzzard, K., (1999). "Computer security-What Should you Spend your Money on", *Computer Security*, 18(4), 322-334.
[32] Hua, J., Patel, S., and Zaveri, J. (2009). "Securing Business Information Systems from Cyber-Attacks," *Journal of Digital Business*," 3(1, 2), 2009, 35-53.
[33] Karanja, E., Zaveri, J, and Patel, S. (2007). "The Role of Access Control and Authentication in Information System Security," *Proceedings of the 38th Annual Meeting of the Decision Sciences Institute*, Phoenix, AZ, November 17-20, 2281-2286.
[34] Patel, S. C., Graham, J. H., and Ralston, P. S. (2006). "Security Enhancement for SCADA Communication Protocols Using Augmented Vulnerability Trees," *Proceedings of the 19th International Conference on Computer Applications in Industry and Engineering*, Las Vegas, Nevada, November 13-15, 244-251.
[35] Hamoud, G., Chen, R. L., and Bradley, I. (2003). "Risk Assessment of Power Systems SCADA," *IEEE Power Engineering Society General Meeting*, 13-17 July, Vol. 2, 758-764.
[36] Ghajar, R. and Billington, R. (1985). "Evaluation of the Marginal Outage Costs in Interconnected and Composite Power Systems," *IEEE Transactions on Power Systems*, 10(2), 753-759.
[37] Billington, R. and Allan, R. N. (1983). *Reliability Evaluation of Engineering Systems: Concepts and Techniques*, Springer, New York.
[38] Tantalean-Carrasco, R. Z. (2003). *Internet-Based Expert System for Monitoring and Control of Chemical Processes*. Ph.D. Dissertation, University of Louisville, Louisville, Kentucky.
[39] Patel S. C., Hieb, J. L., and Graham, J. (2009). "Secure Internet-Based SCADA For Monitoring and Control of Industrial Processes," *International Journal of Computers and Their Applications*, in press.

Sandip C. Patel is an Assistant Professor in the Department of Information Science and Systems, Earl Graves School of Business and Management at Morgan State University. He received his Ph.D. from the University of Louisville and Master of Science from Georgia Institute of Technology. He has over ten years of industry experience. Dr. Patel has worked as a consultant with IBM and as a systems analyst and engineer at AT&T. He has also established and operated a computer consulting company. Dr. Patel is on the editorial board for six journals.

Jigish Zaveri is an Associate Professor in the Department of Information Science and Systems, Earl Graves School of Business and Management at Morgan State University. He received the Ph.D. (MIS) and M.S. degrees from University of Kentucky. Dr. Zaveri has numerous research publications that have appeared in *Decision Science*, *IEEE Transactions on Systems, Man, and Cybernetics*, *Decision Support Systems*, and others. He has written several book chapters and has more than 45 research presentations and articles presented at major conferences. He has worked on numerous projects for several agencies including the Department of Homeland Security, the National Transportation Center, the National Security Agency, and others.