Abstract

Supervisory Control and Data Acquisition (SCADA) for water distribution systems monitor and control pipes transporting water from pump stations or reservoirs to various places within the distribution area. SCADA systems are regularly implemented in water resource industries to improve maintenance, operation, reliable and secure water supply to customers. The SCADA system consists of a master system that communicates with the Remote Terminal Units (RTU) to gather data and check the values for the optimum functioning of the water distribution system. The SCADA system checks various parameters like the pressure, temperature, density of the water inside the pipe. Security of SCADA system is extremely important for the proper transportation of the water to various locations through pipes. This project first identifies the factors that affect the security of SCADA systems, evaluates the security using a goal oriented technique, namely the NFR Approach, and validates security using simulation.

Chapter 1

Introduction

Water distribution and management has always been a problem or challenge for many countries (even well developed countries). Poor infrastructure or inefficient management of water supply result in inconvenience and unsatisfied customers due to insufficient supply of water to different places across the state at right time, increased cost of supply, etc. So, in order to overcome problems caused due to poor infrastructure of water supply system, we need to design or introduce improvements to an existing system architecture that operate on real time data communicated from remote places to central or main control center. For this purpose SCADA systems are used; SCADA stands for supervisory control and data acquisition system and SCADA systems are built and installed to monitor and control processes in areas such as water distribution, waste water treatment, oil refineries, gas pipelines, etc. SCADA systems are regularly implemented in water resource industries to improve maintenance, operation and reliable water supply to customers. SCADA system consists of various sub systems like human machine interface (HMI), remote terminal units (RTU), supervisory control system and communication infrastructure. HMI is a user interface that presents the processed data to the operation personnel who then analyses data and controls the process based on these values. A supervisory control system collects the data and sends commands to the process. RTUs are connected to sensors in the process and finally the connection between supervisory system and RTUs is made using the communication infrastructure.

SCADA security is crucial as ever today with cyber attacks and physical security. Physical security relates to access control, intrusion detection etc. evaluation of SCADA security will allow its stakeholders to determine the safety of the system. The techniques used for evaluating SCADA security are discussed below.

1. Nessus [21] is a remote security scanner which performs security checks against a target SCADA system, detecting vulnerable services running on the scanned hosts and provides a warning level recommended fix for each possible vulnerability. But, Nessus may be not detect all vulnerabilities; therefore it is only a starting point for assessing the system.

2. Ethereal [21] is a widely used network protocol analyzer that monitors communications between the individual SCADA system components. But, Ethereal can’t detect other security threats.

3. Attention to requirements is crucial for quality. Much of the system quality is expressed in as non-functional requirements also called as quality attributes. The NFR Approach [16] makes the relationships between quality requirements and intended decisions explicit. The NFR Approach evaluates the security that not only results in a score but also gives us the justifications for it.

NFR approach is used to evaluate security of three different water pipeline SCADA systems.

Chapter 2

SCADA system

This chapter briefly describes the SCADA system and its application in water distribution.

2.1 What is a SCADA system?

SCADA stands for Supervisory Control and Data Acquisition. It is an industrial control system used to control and monitor a process .It consists of the following subsystems [8]

- ❖ Human machine interface (HMI)
- ❖ Supervisory control system
- ❖ Communication infrastructure
- ❖ Remote terminal units(RTUs)

- **Human machine interface** is a user interface that presents the processed data to the operation personnel. He then analyses data and controls the process based on these values.
- **Supervisory control system** collects the data and sends commands to the process
- **Communication infrastructure** is used to build the connection between the supervisory control system and remote terminal units.
- **Remote terminal units (RTUs)** are small computerized units deployed in the field at specific locations to gather reports from sensors within the process.

2.2 How does SCADA system work?

A SCADA system performs four functions: [13]

- Data acquisition
- Networked data communication
- Data presentation
- Control

These functions are performed by four kinds of SCADA components:

1. Sensors (either digital or analog) and control relays that directly interface with the managed system.
2. Remote telemetry units (RTUs). These are small computerized units deployed in the field at specific sites and locations. RTUs serve as local collection points for gathering reports from sensors and delivering commands to control relays.
3. SCADA master units. These are larger computer consoles that serve as the central processor for the SCADA system. Master units provide a human interface to the system and automatically regulate the managed system in response to sensor inputs.
4. The communications network that connects the SCADA master unit to the RTUs in the field.

2.3 SCADA system for Water pipeline:

SCADA communication network is spread throughout the water distribution system. Workstations, which are typically PC-based and located in a control room and allow operators to view the entire process and perform, control actions. Within the plant, process controllers or programmable logic controllers (PLC's) supervise unit processes, such as chemical treatment and filters. A local area network (LAN), such as Ethernet, links the controllers to the workstations as well as to one another. Remote terminal units (RTU's) are used at remote sites and usually exist in vulnerable areas, such as pump stations, storage tanks, valve vaults and treatment facilities. The RTU's communicate on a wide area network that is typified by the radio system .Traditionally a dial-up or leased telephone line system; the wide area network is now more often being implemented with wireless communication. In the old days, getting an elevated tank or pump station on the network meant contracting for leased telephone lines. Long runs are very expensive and installation not necessarily very timely. Today, the only problem is deciding among all the wireless options. Even if you need a new RTU, today's equipment is cost effective, uses open architectures, and is available through numerous systems suppliers, who can reliably interface it to your existing system.

Water is distributed from the pump station to various places through pipes. Since water supplied to long distances, a single system cannot monitor the entire distribution process right from the reservoir, pump station and final destination. Hence we need various devices such as field instruments, Programmable logic units and PRV's (pressure regulation valves) are connected to RTUs and master station monitors all the RTU's. Generally at peak time's pressure of water increases and this result in pipe bursts and maintenance costs increases. So, PRV's are installed at critical points to ensure that pressure is maintained constant even at peak times. RTU's are used to maintain pump station efficiency, minimize leaks in pipe and provides reliable water supply with customer satisfaction. RTUs present in pump stations calculate the volume of pumped water, monitor peak power drawn by the pump during its activation, monitor average energy supplied to that pump and compare these values and set values to the bench mark and send signal to the master station.

Since there are many RTUs located at different places and they communicate with the master station, exchange of data takes place. The RTUs sends data from various remote places to the central master station. Supervisory control and data acquisition (SCADA) is a system that allows an operator to monitor and control processes that are distributed among various remote sites. SCADA systems allow remote sites to communicate with a control facility and provide the necessary data to control processes. Field instruments like RTUs, sensors and actuators are directly interfaced to the remote sites like pump stations and reservoir as shown in Figure 1. They generate analog and digital signals that will be monitored by the remote station. The central monitoring station (CMS) refers to the location of the master or host computer. Several computer workstations may be configured on the CMS, if necessary. SCADA master station analyzes and compares those values to the bench mark values and sends a message to particular RTU if there are any changes to be made. Then the RTU takes the required action. So, finally SCADA system linked with these monitoring devices will eliminate or reduce the need for manned patrols and cut down the maintenance costs.

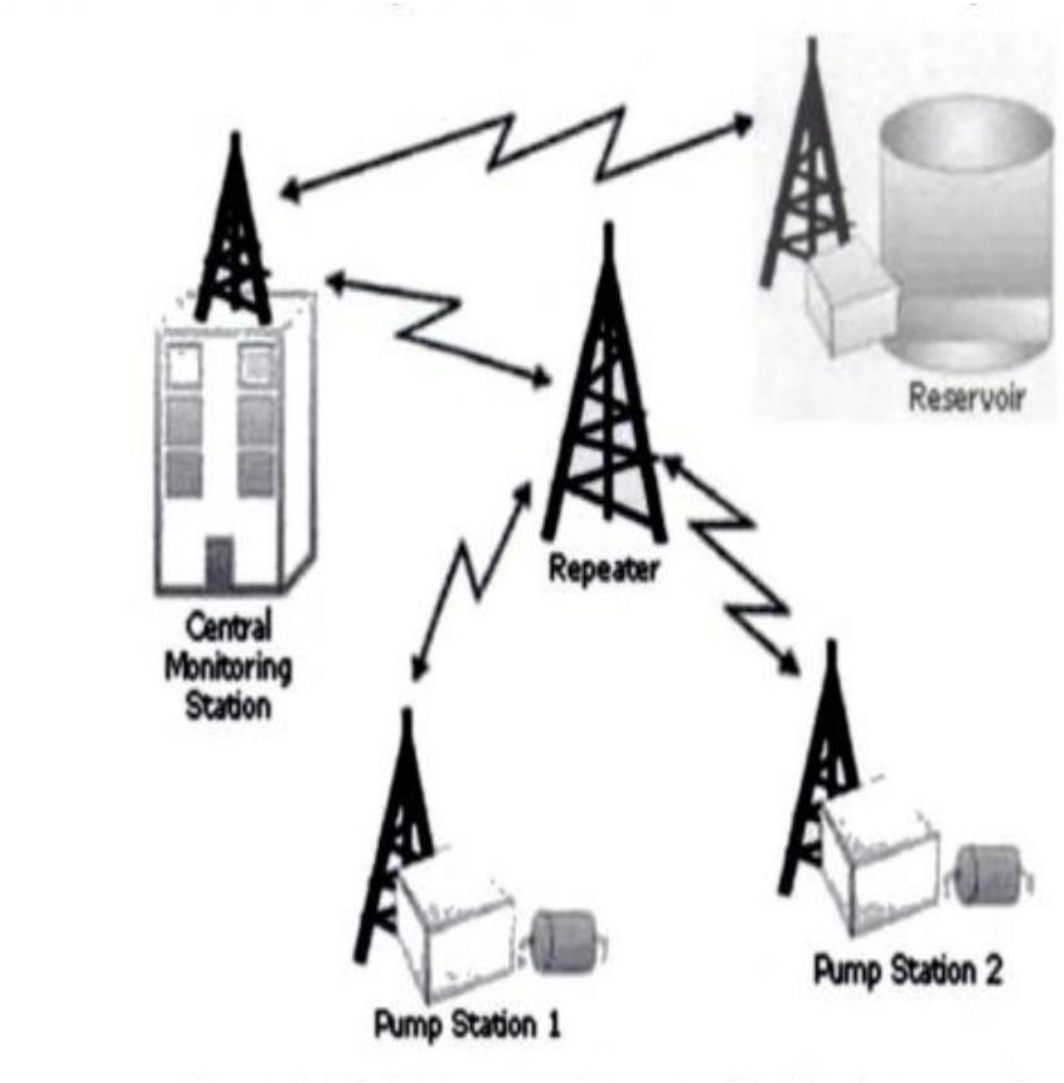


Figure 1: SCADA system for water pipeline network [14]

Chapter 3

Security of water pipeline SCADA systems

3.1 Factors that affect the security of SCADA

The factors affecting the security in Water Pipeline SCADA systems (WPSS) can be broadly classified into

1. Physical Security

2. Network Security

3. Data Security

1. Physical Security:

Physical security is a part of SCADA system's comprehensive control and open strategy Physical Security means the security of the remote assets and the security of the water itself. Remote assets like RTUs and pumps are very vulnerable to be stolen or destroyed due to vandalism.

The water security infers the quality of the water should be maintained. Water can be mixed with harmful chemicals and agents as a deliberate attempt to impure. It continuously monitors and logs water quality parameters such as pH, turbidity, chlorine level and dissolved oxygen to quickly detect equipment malfunction, contamination or raw sewage spillage.

2. Network Security:

It refers to the security and monitoring of all available connections to the system, including local access to enterprise networks, remote access via modems and wireless radios and the internet, Intrusion detection system (IDS) are the first line of defense. Implementing Network based [a packet monitor] and host based IDSs which look at system logs for malicious or suspicious application activity in real time.

3. Data Security:

Data security refers to adopt security in data transmission and information storage. There will be hackers and eavesdroppers who breach the data and cause integrity and availability issues. Security against such activities is taken care in data security. Implementing security in communication protocol and message encryption is possible but not the only solutions.

Chapter 4

NFR Approach

4.1 What is NFR approach?

NFR approach is a goal oriented approach and the goal here is to achieve security. NFR approach is based on the NFR framework and views security as a non-functional requirement (NFR) to be achieved by SCADA system and employs a goal-directed graph called Softgoal interdependency graph (SIG) that treats security to be a goal to be achieved by any SCADA system. The SIG decomposes security into its constituent factors. The features of the SCADA system are then taken into account when determining the contributions made by the SCADA system to the security factors.

The contributions determine the extent to which feature satisfy a factor and are of four types; strongly positive, positive, negative, strongly negative. The well-defined propagation rules of the NFR Approach help to propagate the contributions up the SIG to finally obtain the qualitative score for security.

4.2 NFR approach for evaluating security of WPSS

NFR approach is a goal-oriented approach and views security as non-functional requirement (NFR). In order to apply NFR approach a structure called Softgoal Interdependency Graph as mentioned above is developed. This SIG is used to evaluate security. The SIG is developed using the four steps: [16]

1. Decomposition of the factors that affect WPSS security into an AND-OR-EQUAL graph: two factors (also referred to as softgoals) are related by an AND relation if both the factors are important to satisfy the parent factor; two factors are related by an OR relation if either of the factors is important to satisfy the parent factor; a factor is related to another by EQUAL relation if the child factor is important to satisfy the parent. Generally, factors are named using the convention Type [Topic1, Topic2,…] where Type is the factor and Topic is the field of application of Type; Topic is optional.
2. Determine the various features for each WPSS – could be the graphical interfaces, graphing algorithms, multi-user ability; we refer to these as the WPSS features.
3. Determine the extent to which the WPSS features affect the leaf security factors identified in the first step by calculating the contributions the WPSS features make to the security factors; the contributions can be one of four types: strongly positive or MAKE, positive or HELP, negative or HURT, and strongly negative or BREAK.
4. Capture the justifications for the contributions in step 3 so that a historical record of rationale for contribution changes is maintained.

The ontology used for SIG is given in Figure 2.

After getting the SIG done, the propagation rules of the NFR Framework are applied to propagate the contributions in step 3 above to the top of the SIG. The propagation rules of the NFR framework are: [16]

R1. If all the contributions received by a leaf security factor are TYPE then that leaf security factor is considered TYPE-satisfied.

R2.If a leaf security factor receives at least one HELP contribution then that leaf security factor is HELP-satisfied.

R3.If a leaf security factor receives at least one HURT contribution then that leaf security factor is HURT-satisfied.

R4.If a leaf security factor receives at least one BREAK contribution then that leaf security factor is BREAK-satisfied.

R5.If R2, R3, and R4 apply, then the tie is broken in the order R4, R3, and then R2.

R6.If a leaf security factor does not receive a contribution then it is considered MAKE-satisfied if it is involved in an AND or EQUAL relations, and BREAK-satisfied if it is involved in an OR relation.

R7.In the case of AND-related factors, if all child factors are TYPE-satisfied then the parent security factor is TYPE-satisfied.

R8.In the case of AND-related factors, if even one of the child factors is TYPE-satisfied then the parent security factor is TYPE-satisfied; the priority decreasing in the order: BREAK > HURT > HELP > MAKE.

R9.In the case of OR-related factors, if all child factors are TYPE-satisfied then the parent security factor is TYPE-satisfied.

R10.In the case of OR-related factors, if even one of the child factors is TYPE-satisfied then the parent security factor is TYPE-satisfied; the priority decreasing in the order: MAKE > HELP > HURT > BREAK

R11.In the case of EQUAL-related factors (only one child) the parent is TYPE-satisfied if the child is TYPE-satisfied.

In order to evaluate security of each WPSS the following actions are iteratively performed for each system:

1. Step 3 of SIG development – determines the extent to which the WPSS satisfies the security factors,
2. Step 4 of SIG development – captures the reasons for contributions in Step 3, and
3. Application of propagation rules R1 through R5 to evaluate security of the system.

The result of this evaluation is that security score for each tool will be qualitatively categorized into one of MAKE, HELP, HURT, or BREAK, with their ranking being:

MAKE > HELP > HURT > BREAK.

This determination of security score will help us conclude the security of the system as follows: [16]

C1.If the root security factor (the factor at the top of the SIG) is MAKE-satisfied, then that system provides excellent security.

C2.If the root security factor (the factor at the top of the SIG) is HELP-satisfied, then that system provides good security.

C3.If the root security factor (the factor at the top of the SIG) is HURT-satisfied, then that system provides poor security.

C4.If the root security factor (the factor at the top of the SIG) is BREAK-satisfied, then that system is not secured.

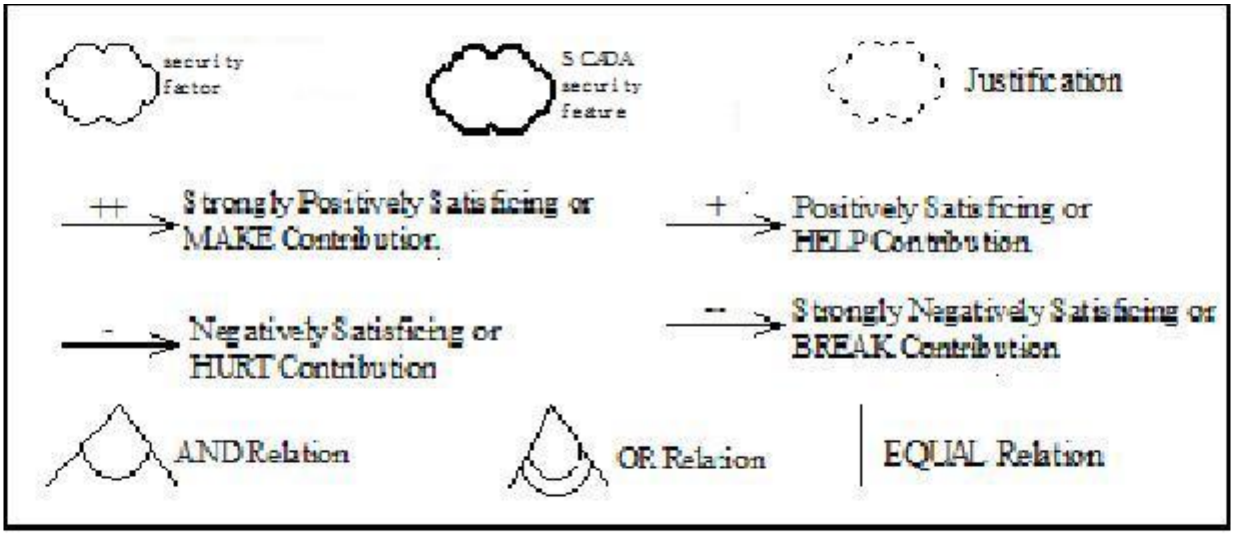

security factor
SCADA security feature
Justification
++
Strongly Positively Satisficing or MAKE Contribution
+
Positively Satisficing or HELP Contribution
-
Negatively Satisficing or HURT Contribution
--
Strongly Negatively Satisficing or BREAK Contribution
AND Relation
OR Relation
EQUAL Relation

Figure 2: Ontology for Softgoal Interdependency Graph [16]

Chapter 5

Application of the NFR approach for Evaluation of security of WPSS

This chapter primarily focuses on the outstanding security implementations in three different SCADA systems and evaluates them using NFR approach. It also discusses the improvements techniques if any to the corresponding systems. The following steps are followed along this approach. This chapter uses symbols, terms and definitions from previous chapters. The conclusion has design level security improvement techniques and acts as the preface for the following chapter by discussing the topic chosen to simulate a SCADA system.

5.1Madison Water Utility, Madison, Wisconsin:

Vendor: Long watch

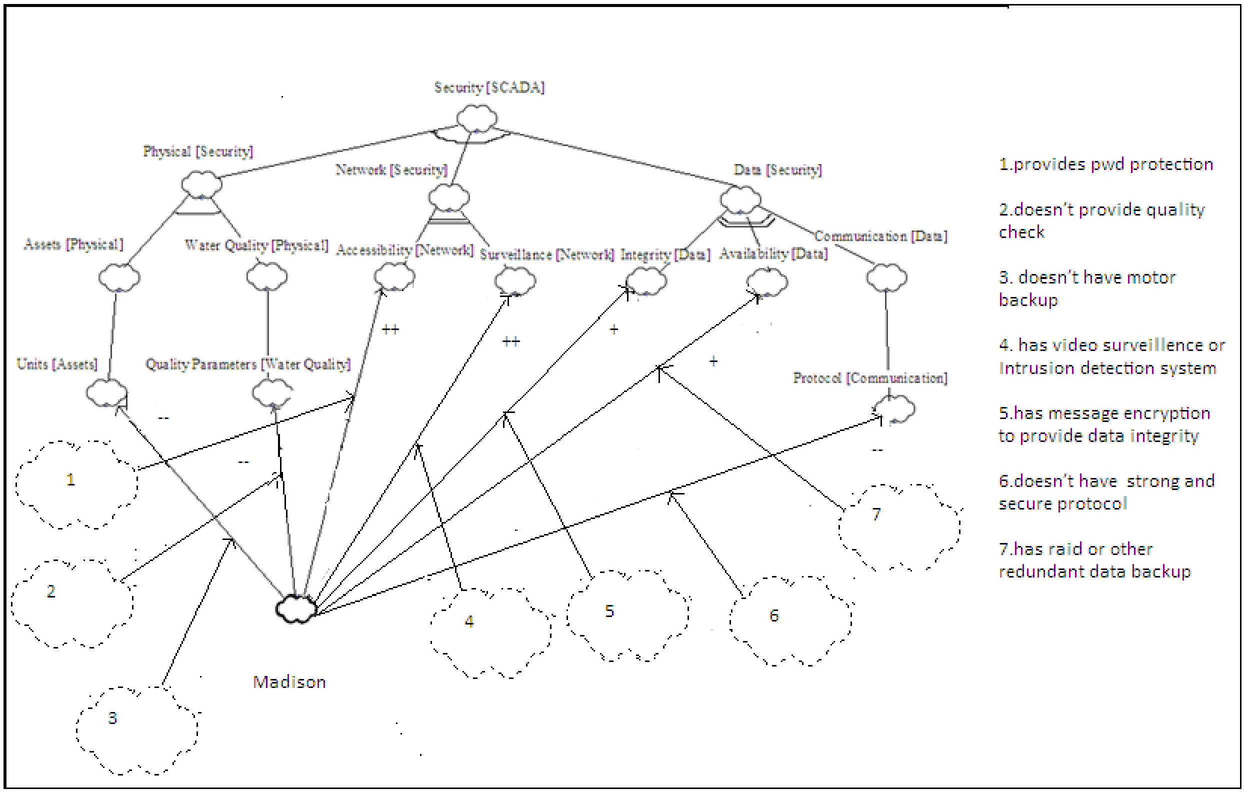
After 9/11 the United States quickly acknowledged vulnerabilities at airports, borders, and food supply and water supply systems [17]. Soon after, the government required vulnerability assessments (VAs) for all municipalities - with large cities required to go first. In 2002, Madison Water Utility (MWU) in Madison, Wisconsin, underwent its VA and saw a need for video cameras at many locations, including 32 remote sites.

MWU replaced its dialup telephone system with MDS iNet 900 radios in 2002 and 2003[17]. The system was installed with the intention to use it for the SCADA system, a door access system, and for video surveillance. This will provide operators with information about system operations, records, logs real-time data, and will allow operators to view video and monitor system status.

The system uses 64 AXIS cameras at 32 remote locations connected to local Longwatch hardware and software. A typical site video hardware [17] setup includes one to four video cameras at each site connected to a Longwatch Video Engine. The Video Engine records high-resolution video 24 hours a day, seven days a week and stores it up to 30 days. It simultaneously sends Live Video and Event Clips to the Video Control Center (VCC) at the central office control center. The Video Engine also monitors door switches and motion sensors and other detection devices that indicate the presence of an intruder to create an alarm condition.

The Video Engine is configured so that if any alarm is triggered, it will retrieve previous footage and transmit the archived video and live video as a "video clip" to the VCC, using the existing radio system. MWU continues to fine tune and adjust the system to minimize false alarms. Issues with car lights and lightning may require adjusting or modifying triggers at some locations. Multiple frequent false alarms tend to desensitize pump operators and lessen the impact of the system.

The NFR for security adaptability is shown in the Figure 3.



1.provides pwd protection

2.doesn't provide quality check

3. doesn't have motor backup

4. has video surveillence or Intrusion detection system

5.has message encryption to provide data integrity

6.doesn't have strong and secure protocol

7.has raid or other redundant data backup

Figure 3: SIG for MWU

Application of NFR approach for Evaluation of security in Madison Water Utility:

1.Application of R1:

The leaf security factor units[Assets] is BREAK satisficed

The leaf security factor Quality Parameters[Water Quality] is BREAK satisficed

The leaf security factor Protocol[Communication] is BREAK satisficed

The leaf security factor accessibility[Network] is MAKE satisficed

The leaf security factor surveillence [Network] is MAKE satisficed

The leaf security factor integrity[Data] is HELP satisficed

The leaf security factor availability [Data] is HELP satisficed

2. By R11 Security factor Assets is BREAK satisficed

3. By R11 security factor Water Quality is BREAK satisficed

4.By R7 security factor Physical Security is BREAK Satisficed

5.By R9 security factor Network Security is MAKE satisficed

6.By R11 security factor communication is BREAK satisficed

7.By R9 security factor Data is HELP satisficed

8.By R8 Security is BREAK satisficed

9.BY C4 Madison Water System is not secured.

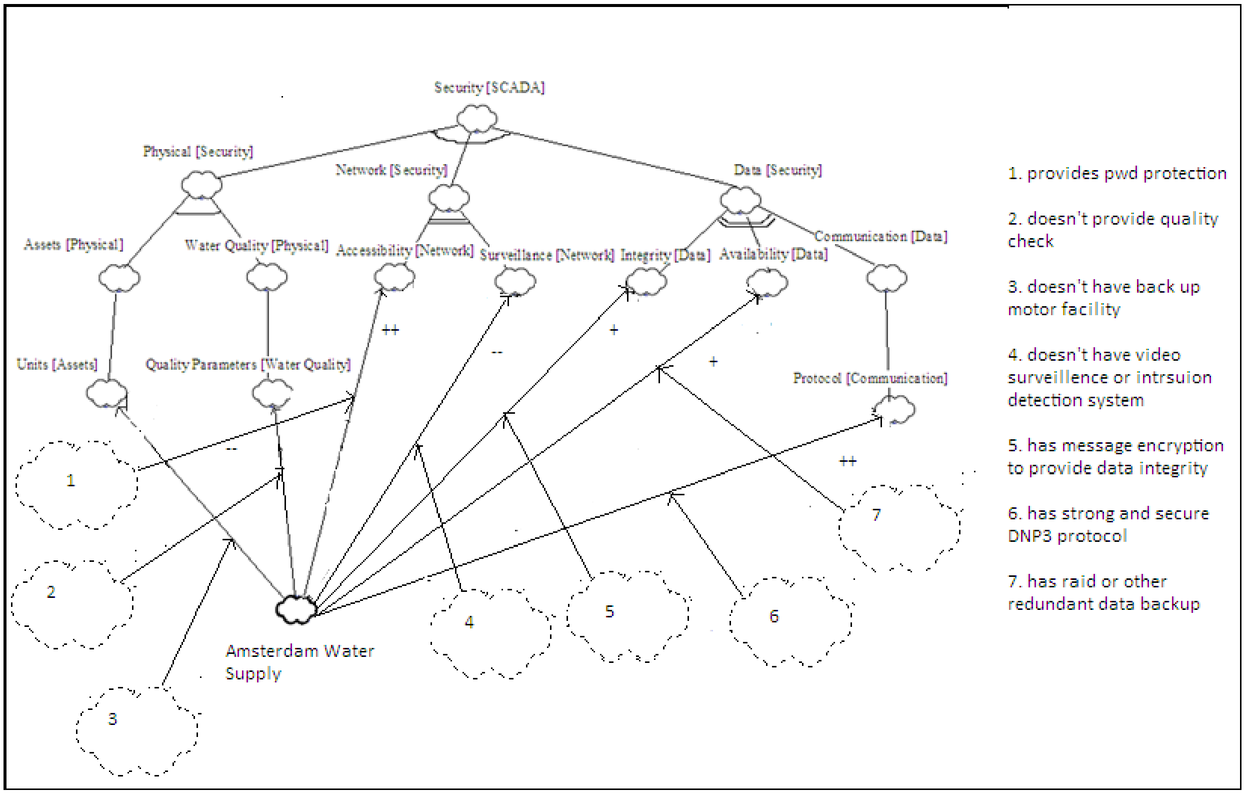
Improvements:

No doubt the video surveillance enhances the intrusion detection system a lot more security can be incorporated by adding few other things like a key less entry system using a card reader. Every authorized person has an electronic card which has access credentials. Each time the card is swiped the user information and the time of access is logged and recorded.

The only concern in having these feature at all remote locations is cost. This will seriously affect the cost of the system. Another improvement is to have a backup motor.

5.2Amsterdam Water Supply, Amsterdam, Netherlands

The SCADA systems are built using public or proprietary communication protocols which are used for communicating between an MTU and one or more RTUs. Amsterdam Water Supply (AWS) has adopted security in communication protocol. The SCADA protocols provide transmission specifications to interconnect substation computers, RTUs, IEDs, and the master station. SCADA security is enhanced by using an open source implementation OpenSSL of Secure Sockets Layer (SSL) / Transport Layer Security (TLS) protocols. SSL/TLS secures communication channels for any reliable communication over TCP/IP and has been in use for about a decade providing virtual private network for the Internet users. The SIG for AWS can be seen as in Figure 4.



1. provides pwd protection

2. doesn't provide quality check

3. doesn't have back up motor facility

4. doesn't have video surveillence or intrsuion detection system

5. has message encryption to provide data integrity

6. has strong and secure DNP3 protocol

7. has raid or other redundant data backup

Figure 4: SIG for AWS

Application of NFR approach for evaluation of security in Amsterdam Water System

1.Application of R1:

The leaf security factor units[Assets] is BREAK satisficed

The leaf security factor Quality Parameters[Water Quality] is BREAK satisficed

The leaf security factor Protocol[Communication] is MAKE satisficed

The leaf security factor accessibility[Network] is MAKE satisficed

The leaf security factor surveillence [Network] is BREAK satisficed

The leaf security factor integrity[Data] is HELP satisficed

The leaf security factor availability [Data] is HELP satisficed

2. By R11 Security factor Assets is BREAK satisficed

3. By R11 security factor Water Quality is BREAK satisficed

4.By R7 security factor Physical Security is BREAK Satisficed

5.By R9 security factor Network Security is MAKE satisficed

6.By R11 security factor communication is MAKE satisficed

7.By R9 security factor Data is MAKE satisficed

8.By R8 Security is BREAK satisficed

9.BY c4 Amsterdam Waster Supply System is not secured.

The security of AWS can be improved by having a backup motor and by proving systematic water quality checks.

5.3Carson city Water Distribution, Nevada:

Vendor: Sage Inc.

Carson City Water Distribution (CWD) SCADA system has security in the following areas: Physical Security[19]: It relates to access control, intrusion detection and perimeter control which is tied to existing SCADA system to offer an effective monitoring and response system. It has a keyless entry device such as a card reader connected serially to a PLC/RTU, which allows site access to automatically log with time and date in the controller as well as the central site.

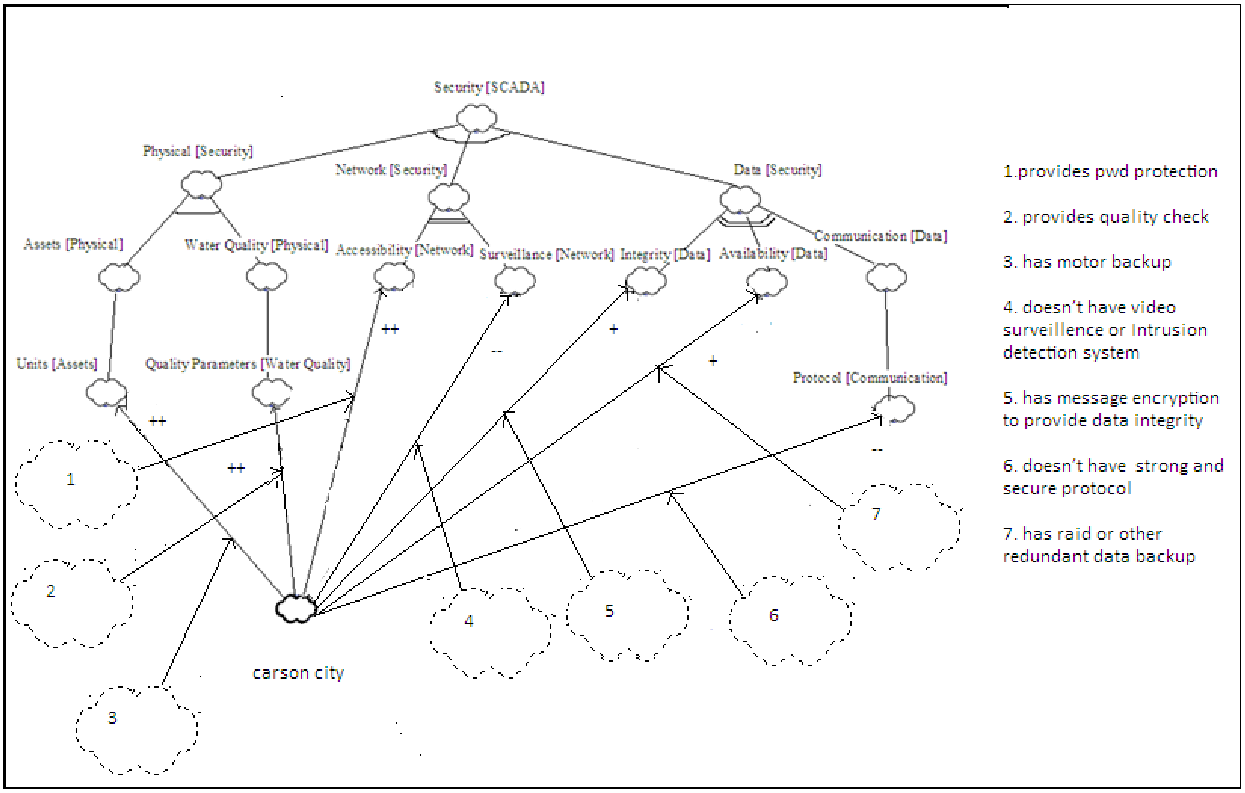
It has a motion or intrusion detector which is connected to the PLC/RTU digital input board providing instant alarm notification and logging at the central site. Intrusion sensors [19] are deployed at access doors, ladders and man holes alarm records are correlated with operational information to get a precise picture of the situation. Furthermore due to widespread use of high bandwidth Wide Area Networks, inexpensive IP based web cameras are utilized to provide video frames from remote locations over wireless networks such as Ethernet spread spectrum radios or WI-FI technologies or by using conventional wire based networks such as fiber optic and high speed leased lines.

Physical security is also a part of SCADA system's comprehensive control and open strategy. If a site has been breached, SCADA system automatically performs safe shutdown of the remote assets to isolate the problem and to limit widespread service disruption or communication. It also has advance warning and response system against biological and chemical threats such as release of harmful chemicals and agents. It continuously monitors and logs water quality parameters such as pH, turbidity, chlorine level and dissolved oxygen to quickly detect equipment malfunction, contamination or raw sewage spillage.

Network Security:

It identifies all available connections to the system, including local access to enterprise networks, remote access via modems and wireless radios and the internet, Intrusion detection system (IDS) are the first line of defense. It has two types of IDSs. Network based [a packet monitor] and host based which looks at system logs for malicious or suspicious application activity in real time. Firewalls are configured properly which provide protection against intrusion at the point of entry. It has remote access service which is call back mode, allows legitimate users to access SCADA systems from off-site locations. Antivirus software is deployed and regularly updated on the network to protect the system from virus threats, spyware and keystroke loggers. All the above mentioned tools are augmented by strict password practices.

The SIG of security NFR is shown in Figure 5:



1.provides pwd protection

2. provides quality check

3. has motor backup

4. doesn't have video surveillence or Intrusion detection system

5. has message encryption to provide data integrity

6. doesn't have strong and secure protocol

7. has raid or other redundant data backup

Figure 5: SIG for CWD

Application of NFR approach for evaluation of security in Carson City Water Distribution

1.Application of R1:

The leaf security factor units[Assets] is MAKE satisficed

The leaf security factor Quality Parameters[Water Quality] is MAKE satisficed

The leaf security factor Protocol[Communication] is BREAK satisficed

The leaf security factor accessibility[Network] is MAKE satisficed

The leaf security factor surveillence [Network] is BREAK satisficed

The leaf security factor integrity[Data] is HELP satisficed

The leaf security factor availability [Data] is HELP satisficed

2. By R11 Security factor Assets is MAKE satisficed

3. By R11 security factor Water Quality is MAKE satisficed

4.By R7 security factor Physical Security is MAKE Satisficed

5.By R9 security factor Network Security is MAKE satisficed

6.By R11 security factor communication is BREAK satisficed

7.By R9 security factor Data is HELP satisficed

8.By R8 Security is HELP satisficed

9.BY c2 Carson City Water Distribution is well secured.

The combined SIG for all the three SCADA systems can be depicted as below in Figure 6.

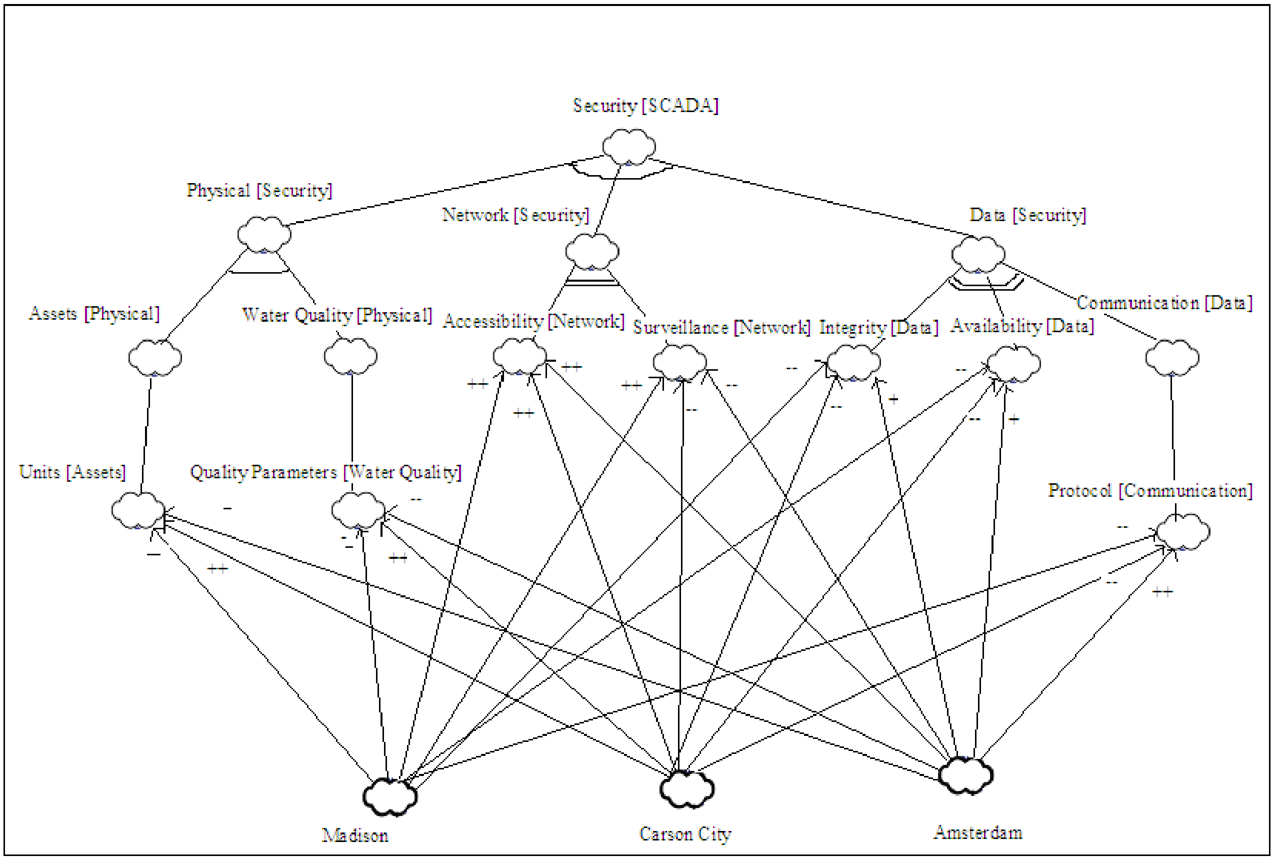


Figure 6: SIG for evaluating security of three WPSS

The bottom portion of the above figure has three SCADA Systems. At the top is Security NFR. It is decomposed into physical, network and Data sub NFRs. They are in turn decomposed in to various other NFRs. The links between the NFRs show the association between the NFRs like parent –child relationship. The arcs at the angle of the links show either 'AND' conjunction or the 'OR' conjunction of the NFRs. The extent to which the systems support the NFRs is given by the symbols like '++'.

Table 1: shows how the respective SCADA system contributes to the NFR Softgoal:

Security/SCADA system	Madison	Carson City	Amsterdam
Units [Assets]	BREAKS	MAKES	BREAKS
Quality Parameters [Water Quality]	BREAKS	MAKES	HURTS
Accessibility [Network]	MAKES	MAKES	MAKES
Surveillance [Network]	MAKES	BREAKS	BREAKS
Integrity [Data]	HELPS	HELPS	HELPS
Availability [Data]	HURTS	HELPS	HELPS
Protocol[Data]	BREAKS	BREAKS	MAKES

Table 1: Justifications for the Contributions in the SIG of Figure 6.

Legend for the Table 1:

Units [Assets]:

The Carson City Water System MAKES this NFR soft goal whereas the Madison and Amsterdam water systems BREAK it. This can be achieved in these systems by having the facility to properly secure the remote stations and have the breached pumps shut down to isolate the problem.

Quality Parameters [Water Quality]:

MWS and AWS both of them BREAK this NFR, but Carson City MAKES it. The reason is that the Carson City checks for the quality parameters of water on regular basis of time and location.

The same can be introduced into the other systems to MAKE this softgoal.

Accessibility [Network]:

All the three Water Systems MAKE this Softgoal as they all have user authentication and authorization which allow only those users with sufficient credentials to look into the system.

Surveillance [Network]:

Madison Water System has video surveillance in its remote locations which supports it to MAKE this Softgoal. This can be made possible in other two systems by having proper video surveillance and intrusion detection systems at their remote locations.

Integrity [Data]:

All the three systems HELP this soft goal as they properly check for the wholesomeness of the data which is being transferred.

Availability [Data]:

Madison Water System HURTS this NFR as it does not have any facility for data availability if the information is lost. It can be achieved by redundancy of data and proper storage. Redundant Array of Independent Disks (RAID) is one possible solution.

Protocol [Data]: Only Amsterdam Water System MAKES this goal because it implements protocol security strongly. Madison and Carson City both do not have protocol security. This can be achieved by secure protocols such as DNP3 and having SSL/TCP security and Message encryption during transfers.

Based on the above SIG and Justification table once can design the SCADA system to have the features he/she needs. One has lot of ways to decompose the NFR and design the application based on the contribution.

Security/SCADA system	Madison	Carson City	Amsterdam
Units [Assets]	BREAKS by user	MAKES by user	BREAKS by user
Quality Parameters [Water Quality]	BREAKS by user	MAKES by user	HURTS by user
Accessibility [Network]	MAKES by user	MAKES by user	MAKES by user
Surveillance [Network]	MAKES by user	BREAKS by user	BREAKS by user
Integrity [Data]	HELPS by user	HELPS by user	HELPS by user
Availability [Data]	HURTS by user	HELPS by user	HELPS by user
Protocol[Data]	BREAKS by user	BREAKS by user	MAKES by user
Physical [Security]	BREAKs by 97	MAKES by R7	BREAKS byR7
Network[Security]	BREAKS by R9	MAKES by R9	MAKES byR11
Data[Security]	BREAKS by R9	HELPS by R9	MAKES byR9
Security[Scada]	BREAKS by C4	HELPS by C2	BREAKS by C4

Table 2: Application of propagation rules to the SIG of Figure 6.

Next chapter simulates a SCADA system. The scenario here chosen is pump failure scenario. In this case the system shuts down the pump to isolate the problem and starts a backup for the smoother operation.

Chapter 6

Simulation of WPSS

In the pipeline industry, SCADA systems are used to collect data from pipeline sensors in real time and display these data to humans who monitor the data from remote sites and remotely operate pipeline control equipment. For most of the existing simulators, the main emphasis is on the leak detection scenarios and how the simulators would handle those leaks. Therefore we developed Water Pipeline SCADA Simulator (WPSS). WPSS is multithreaded and employs message passing between threads in Java.

Description of the system:

Figure 7 shows the Class diagram for the WPSS. We have a thread named Pressure Sensor. The assumption is that the inside temperature of the water pipeline will be constant. Some other classes are also being used like RemoteThermalProcessor, RemoteThermalCommunicator, SuperProcesor, SuperCommunicator & Glide. For some specific scenarios we have used Backing classes. Figure 8 shows the Sequence diagram. The SensorProcessor class initiates the thread PressureSensor. This thread senses the pressure of the water flowing in the pipe and sends them to RemoteThermalProcessor. RemoteThermalProcessir class sends the above values collected to RemoteThermalCommunicator which in turn sends the values to SuperCommunicator. And then the SuperCommunicator class sends to SuperProcessor which writes the value to a text file and checks these values. If the values are in range then it sends a message “Safe” to RemoteThermalProcessor. If the values doesn’t fall in the range and is low then it sends an

“Increase” message to RemoteThermalProcessor. When RemoteThermalProcessor class receives this message from SuperProcessor then it starts the Glide.

When the SuperProcessor sends this message to RemoteThermalProcessor class, it follows the below path:

SuperProcessor to SuperCommunicator

SuperCommunicator to RemoteThermalCommunicator

RemoteThermalCommunicator to RemoteThermalProcessor

When the RemoteThermalProcessor sends this message to SuperProcessor class, it follows the below path:

RemoteThermalProcessor to RemoteThermalCommunicator

RemoteThermalCommunicator to SuperCommunicator

SuperCommunicator to SuperProcessor

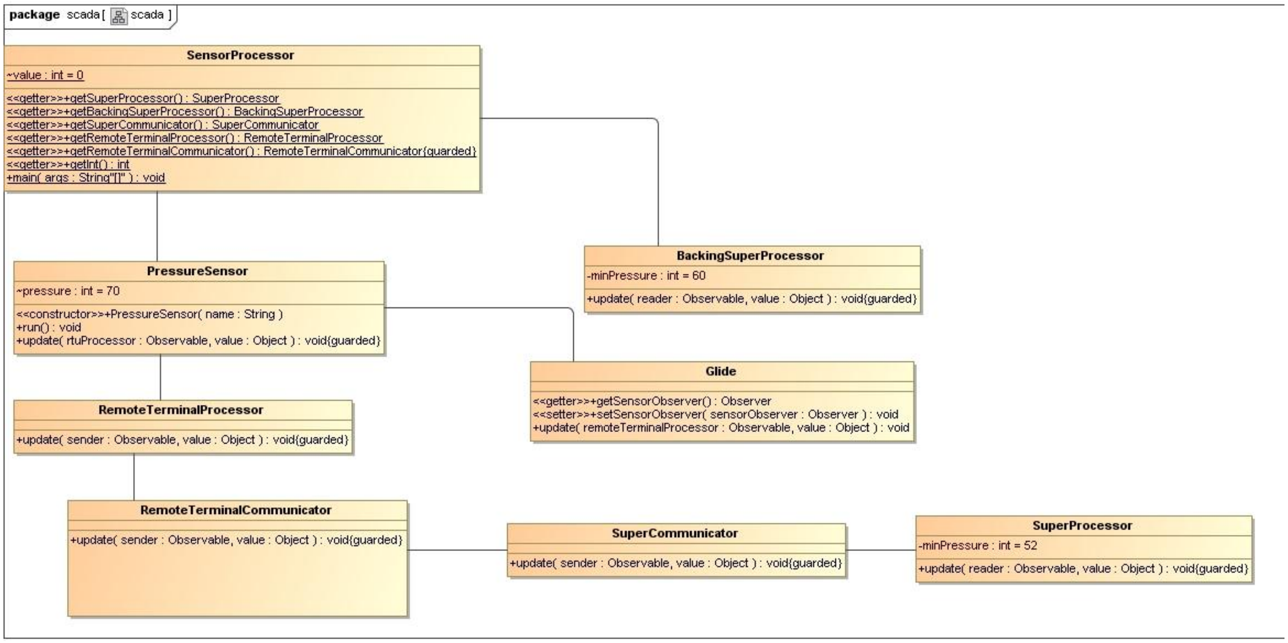

package scada[scada]
SensorProcessor
~value : int = 0
<<getter>>+getSuperProcessor() : SuperProcessor
<<getter>>+getBackingSuperProcessor() : BackingSuperProcessor
<<getter>>+getSuperCommunicator() : SuperCommunicator
<<getter>>+getRemoteTerminalProcessor() : RemoteTerminalProcessor
<<getter>>+getRemoteTerminalCommunicator() : RemoteTerminalCommunicator{guarded}
<<getter>>+getInt() : int
+main(args : String"[]") : void
BackingSuperProcessor
-minPressure : int = 60
+update(reader : Observable, value : Object) : void{guarded}
PressureSensor
~pressure : int = 70
<<constructor>>+PressureSensor(name : String)
+run() : void
+update(rtuProcessor : Observable, value : Object) : void{guarded}
Glide
<<getter>>+getSensorObserver() : Observer
<<setter>>+setSensorObserver(sensorObserver : Observer) : void
+update(remoteTerminalProcessor : Observable, value : Object) : void
RemoteTerminalProcessor
+update(sender : Observable, value : Object) : void{guarded}
RemoteTerminalCommunicator
+update(sender : Observable, value : Object) : void{guarded}
SuperCommunicator
+update(sender : Observable, value : Object) : void{guarded}
SuperProcessor
-minPressure : int = 52
+update(reader : Observable, value : Object) : void{guarded}

Figure 7: Class diagram for WPSS

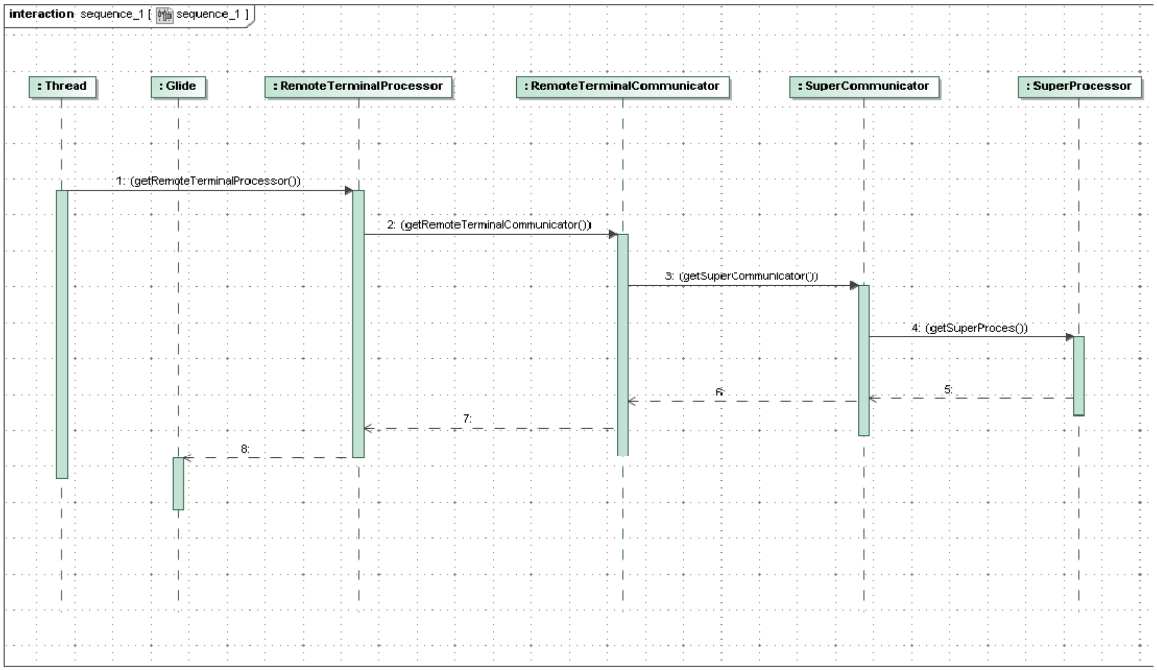

interaction sequence_1 [sequence_1]
: Thread
: Glide
: RemoteTerminalProcessor
: RemoteTerminalCommunicator
: SuperCommunicator
: SuperProcessor
1: (getRemoteTerminalProcessor())
2: (getRemoteTerminalCommunicator())
3: (getSuperCommunicator())
4: (getSuperProces())
5:
6:
7:
8:

Figure 8: Sequence diagram for WPSS

Details of the sequence diagram:

1. PressureSensor thread senses the pressure inside the pipeline and sends the values to the RemoteThermalProcessor class.

2. RemoteThermalProcessor class checks for where the message came from. If the message is from the PressureSensor thread, it sends the pressure value to the RemoteThermalCommunicator class.

3. RemoteThermalCommunicator class checks for where the message came from. If the message is from the RemoteThermalProcessor class, it sends the pressure value to the SuperCommunicator class.

4. The SuperCommunicator class checks for where the message came from. If the message is from the RemoteThermalCommunicator class, it sends the pressure value to the SuperProcessor class.

5. The SuperProcessor class stores these values in a file and checks if the pressure values are in range. If they are in range it sends a “Safe” message to the SuperCommunicator class. If the pressure value is low, it sends an “Increase” message to the SuperCommunicator class.

6. The SuperCommunicator class checks for where the message came from. If the message came from the SuperProcessor class, it sends the same message to the RemoteThermalCommunicator class.

7. The RemoteThermalCommunicator class checks for where the message came from. If the message is from the SuperCommunicator class, it sends the same message to the RemoteThermalProcessor class.

8. The RemoteThermalProcessor class checks for where the message came from. If the message is from the RemoteThermalCommunicator class, it checks for if the message is “Safe” or “Increase”. If the message is “Increase” it sends a message to the Glide class asking it to activate.

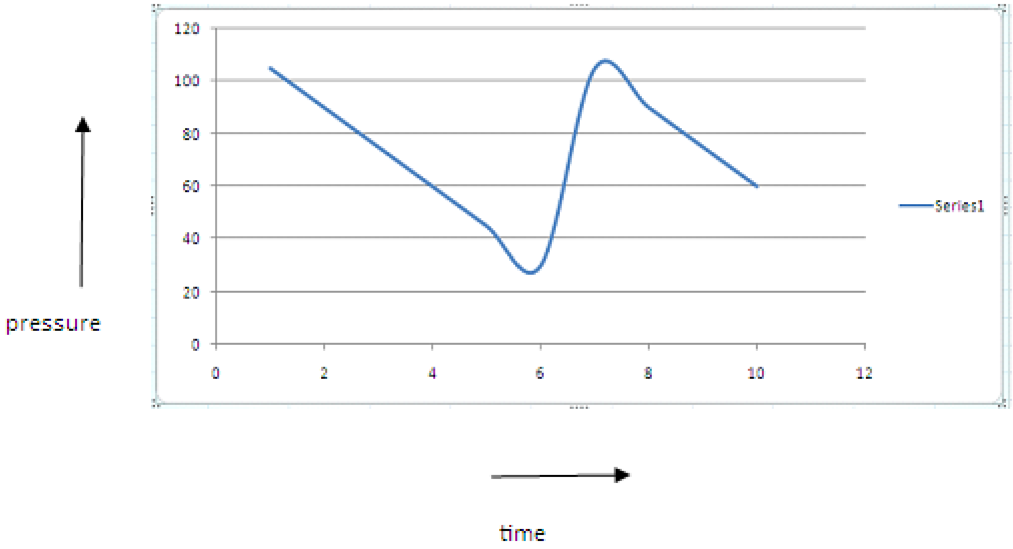


Figure 9: Output graph with backup glide.

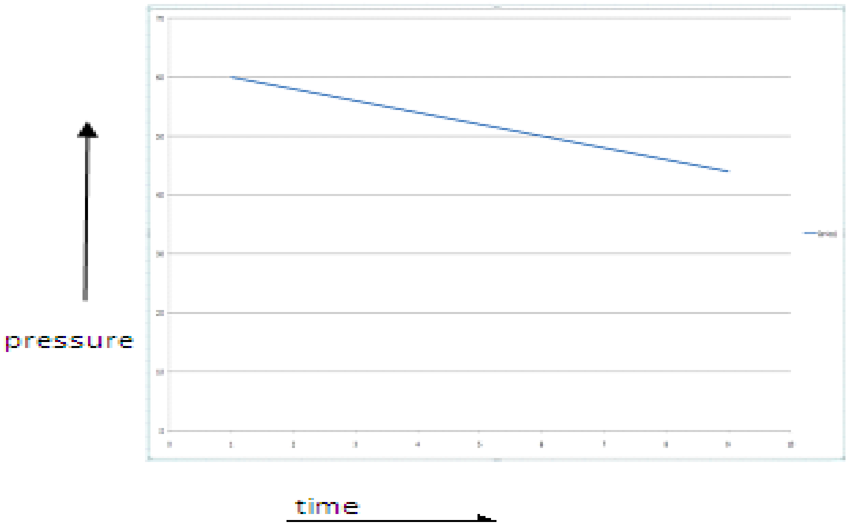


Figure 10: Output graph without backup glide.

Chapter 7

Conclusion and Future Work

In this project we discuss what is SCADA and the factors that affect its security. Later the security has taken as an NFR that has to be achieved by SCADA system. Softgoal Interdependency Graph (SIG) is developed to evaluate the security of SCADA system. Based on this evaluation, the security of the SCADA system is directly inferred. We applied the NFR approach to three different water pipeline SCADA systems namely, Madison Water Utility (MWU), Amsterdam Water Supply (AWS) and Carson city Water Distribution (CWD).

The advantages of NFR approach is historical record maintenance in the form of graphs which is very easy to recollect past decisions from graphs.

As computer systems are more integrated, the distinction between security and safety is beginning to disappear and therefore both security and safety need to be evaluated together. Another possibility is quantitative evaluation and simulating more number of scenarios for better results.

Chapter 8

Bibliography

1. http://www.onsitewater.com/ow_0703_scada.html

2. http://www.elettra.trieste.it/ICALEPCS99/proceedings/papers/mc1i01.pdf

3. http://www.cse-semaphore.com/pdf/whitepaper_scada.pdf

4. Reliable and Secure Data Communications for SCADA Systems, DanEhrenreich, CIGRE 2005 Conference Cuernavaca, Mexico.

5. Ezell, B., Risks of Cyber Attack to Supervisory Control and Data Acquisition for Water Supply, Masters of Science (Systems Engineering) Thesis, School of Engineering and Applied Science, University of Virginia, May1998.

6. Water security: the role of SCADA system by Kevin Finnan

7. www.toodoc.com/**GIS**-for-**water-distribution-system**-pdf.html

8. en.wikipedia.org/wiki/SCADA

9. Replacing the London water supply SCADA system. Water engineering and management March 2003, Neil Parker, B.Sc.

10. SCADA systems security by Arjun Venkatraman

11. http://www.riptech.com/industry/energy.html

12. http://www.gisdevelopment.net/proceedings/gita/2000/os/os010pf.htm

13. Do You Know These Key SCADA Concepts? SCADA Tutorial: A Quick, Easy, Comprehensive Guide.

14. Security of water supply systems: from source to tap by Jaroslav Pollert, Bozidar Dedus.

15. Software Architecture Adaptability: An NFR Approach by Nary Subramanian and Lawrence Chung, international conference on software engineering, 52-61, 2001.

16. Evaluation of Information Visualization Tools Using the NFR Approach by Puspha Kumar, Nary Subramanian and Kang Zhang, Springer-verlag, pages: 44-55, 2008.

17.http://www.automatedbuildings.com/news/mar09/articles/longwatch/090220025009longwatch.htm.

18. http://www.cs.louisville.edu/facilities/ISLab/tech%20papers/ISRL-04-01.pdf

19. SCADA, security and automation newsletter. A publication of sage designs, Inc.volume 15, issue 2. Fall/winter 2005.

20. http://ijikm.org/Volume3/IJIKMv3p073-086Hentea361.pdf

21. Permann, May Robin, and Kenneth Rohde. “Cyber Assessment Methods.” InTech 1 Nov. 2005.