SCADA SYSTEM SECURITY IN POWER SYSTEM PROTECTION

A graduate project submitted in partial fulfillment of the requirements for the degree of Masters of Science in Electrical Engineering.

By
PRAMOD ESWAR THADAKALURU

May 2013
The graduate project of Pramod Eswar Thadakaluru is approved by:

________________________________________  ____________________________
Dr. Hang, Xiyi  ____________________________

________________________________________  ____________________________
Dr. Mallard, Benjamin F  ____________________________

________________________________________  ____________________________
Dr. Osorno, Ignacio B, Chair  ____________________________

California State University, Northridge
ACKNOWLEDGEMENT

I would like to thank my professor, committee chair Dr. Bruno Osorno for being my advisor and guide. I am grateful to him for his continuous support and invaluable inputs he has given me to proceed ahead in my project. This work would not have been possible without his support and encouragement. I would also like to thank him for showing me some examples that related to my project.

Besides, I would like to thank the Department of Electrical and Computer Engineering for providing me with a good environment and facilities to complete this project. It gave me an opportunity to participate and learn about the software My SQL and OPNET. In addition, I would like to thank my professor in providing valuable information as guidance to my project.
# TABLE OF CONTENTS

Signature Page............................................................................................................. ii  
ACKNOWLEDGEMENT.............................................................................................. iii  
List Of Tables........................................................................................................... v  
List Of figures:.......................................................................................................... vi  
ABSTRACT................................................................................................................ vii  

1. SCADA SYSTEM................................................................................................... 1  
   1.1Introduction:..................................................................................................... 1  
   1.2 Components of SCADA:.................................................................................. 2  
      1.2.1 Remote terminal unit (RTU):...................................................................... 2  
      1.2.3 Master Terminal Unit (MTU).................................................................... 2  
   1.3 Principle of Operation:..................................................................................... 4  
   1.4 Advantages and Disadvantages:...................................................................... 5  

2. SCADA SECURITY.................................................................................................. 6  
   2.1 Introduction:..................................................................................................... 6  
   2.2 Vulnerable effects:.......................................................................................... 7  
   2.3 PROTOCOLS:.................................................................................................. 9  
      2.3.1 DNP3 Protocol:.......................................................................................... 9  
      2.3.2 IEC (International Electro-technical Commission):................................. 10  

3. ATTACKS ON SCADA SYSTEMS......................................................................... 12  
   3.1 DDOS Attack:.................................................................................................. 12  
   3.2 OPL ARCHITECTURE:..................................................................................... 13  
   3.3 Test Bed Development:................................................................................... 14  

4. RESULTS................................................................................................................ 17  
CONCLUSION:.......................................................................................................... 22  
Reference:.............................................................................................................. 23  
APPENDIX – A.......................................................................................................... 24
List of Tables

Table 2.2 Vulnerable effects ................................................................. 8
Table 4.1 IEEE 9–bus system power flow data ..................................... 18
List of Figures:

Fig 1.1 Remote Terminal Unit Block Diagram .................................................. 2
Fig 1.3 Block Diagram of SCADA System ......................................................... 4
Fig 3.2 Overlay Protection Layer (OPL) Architecture ..................................... 13
Fig 3.3 Power Cyber Test-Bed Architecture .................................................... 15
Fig 4.1 Test bed Architecture of SCADA Security System ............................ 17
Fig 4.2 Power flow in IEEE 9-Bus system ...................................................... 18
Fig 4.3 Warning Message in My SQL server .................................................. 19
Fig 4.3 Network Diagram in OPNET ............................................................... 20
Fig 4.4 Traffic received in OPNET ................................................................. 20
Fig 4.5 Response Time in OPNET ................................................................. 21
ABSTRACT

SCADA SYSTEM SECURITY IN POWER SYSTEM PROTECTION

By
Pramod Eswar Thadakaluru
Master Of Science in Electrical Engineering

Supervisory Control And Data Acquisition (SCADA) is a system, which controls and monitors the paired device data. This paper discusses the basic concepts of SCADA and their components. It also discusses the need for security in SCADA system and different vulnerable effects caused due to complexity of the system and different methods to reduce those effects. One of such effect on SCADA system is Distributed Denial Of Service (DDOS) attack, which may cause the black out of the whole system. This paper discusses the two methods OPL architecture and Test-Bed Development to reduce the DDOS attack on SCADA system.
1. SCADA SYSTEM

1.1 Introduction:

Power system includes generation, transmission and distribution. Identification of fault and steps to compensate the faults are the major concerns in power systems. Fault identification is a very difficult task in transmission and distribution systems. With this in mind SCADA application is introduced in 19th century. It stands for Supervisory Control And Data Acquisition. As the name itself indicates that it supervises controls and monitors the data as required. SCADA is not a technology but it’s an application, any system that controls and monitors the data is given as SCADA application. With the introduction of this application it becomes easy in most of the sectors like power, water, transport etc. to control and monitor the data.

Consider a small area with a substation feeding 40 houses. Major concern is to have a continuous power supply without any interruption. If any fault occurs at some point of this area identification and steps to reduce the fault takes lot of time. If this is case for a small area, consider a distribution system with different networks inters connected to it, then identification of fault is fairly an impossible task. Considering this as primary reason substation automation is introduced. If the entire substation is automated then identification of fault is easy which reduce the interruption duration and the reliability of that system increases. So for automation of any system SCADA is one of the applications.

SCADA means controlling and monitoring the data. It has three main components

1. Master Terminal Unit (MTU)
2. Remote Terminal Unit (RTU)
3. Communication Network
1.2 Components of SCADA:

1.2.1 Remote terminal unit (RTU):

Remote terminal unit are usually located in remote areas, which communicate with different IED’s (Intelligent Electronic Devices) such as protective relays, circuit breakers.

![RTU Block Diagram]

With the advancement in microprocessor-based relays RTU’s are inbuilt in IED’s, which can directly communicate with the master station. So Remote Terminal Unit is a microprocessor based device, which collects all the date and communicate with the master terminal unit. RTU’s has digital/analog input and output with light emitting diode (LED) indication.

1.2.3 Master Terminal Unit (MTU)

It is also called as “SCADA MASTER” or “CONTROL STATION”, to which different RTU’s are connected. This will have an alarm indication, which indicates the fault location and alerts the user to take necessary decisions. Its main function is

- Gathering data, storing information, communicating, sending information
- It analyses the data collected from RTU and takes necessary action.
1.2.4 Communication Network

RTU’s, which are located in remote areas, are connected to MTU’s by different communication channels such as radio, cable, fiber optics, and WAN, different communication protocols. The use of communication channel depends on

- Distance between RTU and MTU
- Hardware/Software used in RTU and MTU
- Number of RTU’s connected to MTU

The data from the RTU’s should be transmitted to MTU’s and vice versa through communication channels. This process should be fast enough and should not have any noise or interruptions in between so different communication protocols are introduced. Use of these protocols makes the system more reliable. In recent times IEC 61850 communication protocols are used substation automation.
1.3 Principle of Operation:

In general, different physical equipment’s such as numerical relays, circuit breakers, C.T’s, P.T’s (which are called as IED’s) are connected to a remote terminal unit (RTU), which receives, or send the data in digital/analog form. This remote terminal unit analyses the data received from different IED’s according to the algorithm given to it and communicates with the master terminal unit. If any fault occurs on IED’s remote terminal unit senses the type of fault and point of fault occurred and communicates with the master terminal unit. MTU has an alarm indication, which alerts the user to communicate with that particular IED on which fault has occurred through MTU and RTU and he can make necessary changes to clear the fault. So by using SCADA application a user in the control room can be able to clear a fault, which occurred in a remote area.
1.4 Advantages and Disadvantages:

Advantages:

• It helps the system to have continuous operation without any interruption.
• System is more efficient with less manpower.
• It provides faster response in any emergency conditions
• It improves customer service and maintenance.
• It increases the reliability of the system.

Disadvantages:

• Communication between different computers makes the system more complicated.
• Capital investment is more.
• As most of the SCADA systems use Internet as their communication medium there are chances to hack the system.
2. SCADA SECURITY

2.1 Introduction:

From the previous chapter we came to know that SCADA system controls and monitors the data. Since the data is transferred and monitored and controlled SCADA security is at most concern in automation. Most of the data is monitored and controlled from two or more different places in which media of communication in most of the cases is Internet. As Internet plays a very important role in communication there are chances for hackers to hack the data and modify it. So the security of the SCADA system is very important to have a reliable network.

With the increase of SCADA systems in industrial, water, power systems application the network topology of the system became more complicated. Due to the network complication it becomes unsafe, which may result in causing threats and vulnerable effects on the system. The word vulnerable is different from the threats, for example a vulnerability would be a hole in the fence where as a threat would be the person who wants to get through the fence. SCADA systems are converged into IT systems to improve the communication between RTU’s and HMI, which has lead to different vulnerable effects. As Internet serves open source to all the users, necessary steps are taken prevent the SCADA systems from cyber attacks. Lack of proper security in any of the SCADA component may lead to massive destruction on the network.

Since the SCADA systems are widely used in different sectors there are more possible threats, which may occur to the system. Most of the threats are from terrorist groups hackers, company insiders who hack the data and modify them accordingly. So if we can try to prevent the SCADA systems from most of the vulnerable effects and threats we can a secure SCADA system.
### 2.2 Vulnerable effects:

Vulnerability of the system occurs due to poor maintenance, miss-configurations etc.

<table>
<thead>
<tr>
<th>Vulnerability</th>
<th>Description</th>
</tr>
</thead>
</table>
| 1 Password setting    | • Unauthorized persons can use if there are no password setting  
                          • Sending and receiving of passwords without proper encrypting and decrypting  
                          • Lack of password strength                                                                                                                |
| 2 Backup power        | • Lack of backup power may cause some of the components IEDs to shunt down and cause unsafe conditions when general power loss occurs              |
| 3 Testing             | • Without proper testing and initial checks may cause system failure                                                                           |
| 4 Network             | • Lack of proper firewall may cause unnecessary data to pass between networks which may include attackers and malware spread between networks |
| 5 Attack              | • ICS software could be vulnerable to DoS attacks, resulting in the prevention of authorized access to a system resources or delaying system operations and functions |
| 6 Password guessing   | Poorly chosen passwords can easily be guessed by humans or computer algorithms to gain unauthorized access which include:  
                          • Passwords that are short, simple or otherwise do not meet typical strength requirements. Password strength also depends on the specific Internet Connection Capability (ICS) capability to handle more stringent passwords. |
<table>
<thead>
<tr>
<th></th>
<th>OS and application security patches are implemented without exhaustive testing</th>
<th>• OS and application security patched deployed without testing could compromise normal operation of the ICS. Documented procedures should be developed for testing new security patches.</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>Insiders</td>
<td>• Insider’s threats are due to lack of proper security measures in the companies. Most of them are caused accidentally which has highest possible occurrence.</td>
</tr>
</tbody>
</table>

Table 2.2: Vulnerable Effects
2.3 PROTOCOLS:

SCADA systems are developed to collect data from long distances using different communication systems providing high level of reliability and operability. From the past 30 years development is SCADA system concept is carried on with the advancement of communication technologies and media. SCADA security directly relates to have a secure communication link. If a system is having a dial-up line with a secret phone number it can be easily trapped by using a war dialer program which weakens the whole system security. So to have secure communication standard SCADA protocols are introduced to communicate between Master Terminal Unit (MTU) and one or more Remote Terminal Units (RTU). The most common protocols used are

- DNP3 (Distributed Network Protocol version 3.0)
- IEC (International Electro technical Commission)

2.3.1 DNP3 Protocol:

DNP3 protocol is a set of protocols used to communicate between SCADA components. It is widely used in electrical industries. DNP3 protocol is from DNP user group, which is based on early work of IEC that resulted in IEC 60870-5 protocols for SCADA. Both these protocols are IEEE standards.

DNP3 is designed to have a secure communication in SCADA system so to meet the requirements it uses the TCP/IP Ethernet (The protocol used to communicate over the internet), Fiber Optics System. DNP3 communication is divided into two layers in the first layer it collects all the data and separates them accordingly and it undergoes error check and it priorities. In the second layer it address the
### 2.3.2 IEC (International Electro-technical Commission):

IEC (International Electro-technical Commission), which is a non-profit, non-governmental organization, has proposed standardized communication protocols for substation automation to achieve some advantages, which are listed as follows:

1. To facilitate the interoperability. i.e., to make the communication possible between the automation devices which are from different vendors.
2. To decrease the time taken to re-configure the new automation device which is replacing the faulty one.

**Standard Protocols:**

Available standard protocols from IEC exclusively for substation automation are:

1. IEC-60870-5
   1. IEC-60870-5-101
   2. IEC-60870-5-104

2. IEC-61850

IEC-60870-5 series is proposed when the communication hardware is not so developed. It cannot communicate in a fast way. Considering the available technology at that time, they have prepared the standards. Now many new technologies have came, which can make the communication possible at very high speeds. IEC-61850 is the latest standardized protocol, which is designed considering these high-speed technologies.

**IEC-61850:**

IEC-61850 is the latest standardized protocol for substation automation, which is getting attention from all over the world. The IEC Technical Committee 57 (TC57) associated with “Power Systems Management and Associated Information Exchange” issues it. Compared to the other standard protocols, this protocol is best suited for the present technologies in the hardware used for communication.

IEC-61850 ensures the following features as per requirement:
➢ This protocol standard is totally based on the existing IEEE/IEC/ISO/OSI standards of communication.

➢ This protocol supports self-descriptive devices and is open.

➢ This protocol allows adding a new functionality.

➢ This standard is based on the data objects corresponding to the needs of the electric power industry.

➢ The syntax and semantics used for communication is based on the common data objects corresponding to the power system network.
3. ATTACKS ON SCADA SYSTEMS

3.1 DDOS Attack:

The RTU’s, which are located in remote areas, communicate with MTU and exchange data thought Internet as a major source. Since the media to communicate is internet there are chances to have different vulnerable effects and different cyber attacks on the system. Effects of attacks on SCADA systems are

- Switching of the power supply
- Information theft
- Inefficient running of the system
- Destruction of power plant, which may be due to overloading.

Distributed Denial of Service attack (DDOS attack) is one of the major kinds of threat to SCADA systems. DDOS attack is an attempt by a single person or a group of persons to hack the system and cause deny of service to the customers. DDOS attacks the IP address of the data, which is transferred through the Internet. As Internet is the major source of communication in SCADA system there are chances for the hacker to make a black out of the whole system.

The person who is hosting the DDOS attack is a hacker. The attacker before hosting a DDOS attack will go through the victim’s resources. Resources may be bandwidth of the network, computing power, data structure of the system etc. by organizing these resources he will create a network. To create an attack on this network he will identifies the vulnerable sites or hosts on the network. Vulnerable hosts are those, which are not having proper security. The hacker tries to gain access to this vulnerable hosts and tries to install new program to get access of the whole system and to create an attack.

If the hacker is successful in gaining the access to the network he can exploit the following cases

- Obtain access to SCADA Master Control Station
- Obtain access to Remote Terminal Unit (RTU)
- Sending incorrect data to RTU’s
- Disconnecting the communication between SCADA Master Terminal Unit and RTU’s
- Modifying RTU control settings
- Shutting down the MTU’s and RTU’s

3.2 OPL ARCHITECTURE:

Overlay Protection layer (OPL) network architecture is a type of approach to prevent from DDOS attack. This is an intermediate network in the communication channel. OPL network consists of different nodes, which communicate with each other only on confirmed sites i.e. a data must be authenticated through the OPL architecture before the data is allowed to forward to the destination. Set of these nodes knows and some of these nodes are unknown which are called as green nodes.

Fig 3.2 Overlay Protection Architecture [8]
The main goal of the OPL architecture is to distinguish between authorized and unauthorized use of the network. For this to happen firewall functionality should be designed to allow only authentication data and to drop unauthenticated data. For this functionality of the firewall specific protocols are used to allow only authenticated data.

3.3 Test Bed Development:

Determining the vulnerabilities of a SCADA system in real time is a complicated process because of the complex hardware and software interactions that must be considered. Developing a simple system that captures the complexity of the whole system is called Test Bed. Various companies and universities have developed different Test Beds for SCADA systems.

- Cyber Physical Test Bed was developed by IOWA State University by using ISEAGE project, real time digital simulation (RTDS) and DIgSILIENT power factory software for non real time analysis.
- Sandia National Laboratories developed a Virtual Control System Environment (VCSE) by utilizing OPNET, Power World simulator and by using centralized model/simulation management tool such as Umbra to provide control over various components.
- Virtual Power System Test Bed (VPST) was developed at University of Illinois, which utilizes Power World, and Illinois developed Real Time Immersive (RINSE) network integration.
- The Test Bed for Analyzing Security Of SCADA control system (TASSCS) has been developed by University of Arizona by utilizing OPNET and Power World simulators and by using Modbus R Sim software.
- SCADA Sim Test Bed has been developed at Royal Melbourne Institute of Technology (RMIT) University to study the network performance under cyber attack by using common SCADA protocols.
Fig 3.3 Power Cyber Test-Bed Architecture [7]

- Real time Digital Simulation (RTDS)
- Autonomic Software Protection System (ASPS)
- Real Time Immersive Network Simulation Environment for Network Security Exercise (RINSE)
- All the above are different types of Simulations used in different Test-Bed development
Power Cyber Test Bed Architecture is divided into different layers Physical system, Simulator, Substation, Cyber Communication, and Control Center. In this Test Bed 9-bus system is considered as a physical system and real time digital simulator is used to collect all the simulated data from the 9-bus system. DNP3 protocol is used to communicate between control center and different RTU’s. An independently developed Internet-Scale Event and Attack Generation Environment (ISEAGE) is used to create different scenarios of cyber attack and simulation procedures are conducted accordingly. To have secure communication different firewall protection are used.

Consider this Test-Bed is configured to create a DDOS attack scenario through Internet by using HTTP server. Power flow data from the 9-bus system is entered into real time digital simulator. From this, data is transferred to relays and to different RTU’s by using DNP3 and IEC-61850 protocol. Data from the RTU’s is transferred to HMI through Internet by using HTTP server, which is the source for the attacker to hack the data and can make black out of whole system. So ISEAGE is configured to block the data, which is transferring to HTTP server to prevent from DDOS attack. Test-Beds are configured to study different scenarios and their effects on the system.
4. RESULTS

➢ To explain the SCADA system security Test-Bed architecture is designed by using IEEE 9 bus system and securing the bus data by using MySQL server and by OPNET simulation tool cyber attack scenarios can be studied.

Fig 4.1 Test bed Architecture of SCADA Security System
Power flow of an IEEE 9 bus system by using POWER WORLD Simulator is as shown in fig

![Power flow diagram]

Fig 4.2 Power Flow of IEEE 9 bus system

Data from the Power flow is entered into the My SQL server by using code (Appendix-A).

<table>
<thead>
<tr>
<th>Number</th>
<th>Name</th>
<th>Nom Volt Kv</th>
<th>Pu Volt</th>
<th>Volt Kv</th>
<th>Angle( Deg)</th>
<th>Load MW</th>
<th>Load Mvar</th>
<th>Gen MW</th>
<th>Gen Mvar</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Slack</td>
<td>16.5</td>
<td>1</td>
<td>16.5</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td>118.6</td>
</tr>
<tr>
<td>2</td>
<td>Generator</td>
<td>18</td>
<td>1</td>
<td>18</td>
<td>0.76</td>
<td></td>
<td></td>
<td></td>
<td>100</td>
</tr>
<tr>
<td>3</td>
<td>Generator</td>
<td>13.8</td>
<td>1</td>
<td>13.8</td>
<td>1.59</td>
<td></td>
<td></td>
<td></td>
<td>100</td>
</tr>
<tr>
<td>4</td>
<td>230</td>
<td>0.975</td>
<td>21</td>
<td>224.2</td>
<td>-4.02</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Load</td>
<td>230</td>
<td>0.955</td>
<td>219.8</td>
<td>-6.38</td>
<td>90</td>
<td>30</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>230</td>
<td>0.990</td>
<td>36</td>
<td>227.7</td>
<td>-1.8</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Load</td>
<td>230</td>
<td>0.969</td>
<td>227.8</td>
<td>-4.87</td>
<td>100</td>
<td>35</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>230</td>
<td>0.983</td>
<td>87</td>
<td>226.2</td>
<td>-2.89</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>Load</td>
<td>230</td>
<td>0.941</td>
<td>216.4</td>
<td>-7.76</td>
<td>125</td>
<td>50</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 4.1 IEEE 9 Bus system Data
After entering the data trigger is created to the data to notify if any unauthorized person is trying to change the data.

To test the trigger code try to change bus number 2 Generator MW to 0

We can see a message as shown in fig

Not allowed
Msg 3609, Level 16, State 1, Line 1
The transaction ended in the trigger. The batch has been aborted.

Data from the My SQL server is sent through Internet to HMI.

When transferring the data through Internet Test-Bed tool OPNET simulator is used. OPNET is a student demonstration tool so we can’t input the data from My SQL into OPNET.

So I have designed networks in OPNET by considering three scenarios one with no firewall protection, one with firewall protection and third scenario is if any attacker is trying to hack the data by using HTTP server, that data can be blocked by using OPNET.

By using these three scenarios data transformed and response-time of the network is obtained.
From the Fig 4.5 we can see the traffic received in three scenarios. Third scenario is to block the HTTP server; we can see the traffic received in third scenario is zero.
From the Fig 4.6 we can see that the network with firewall have lower response time than the network with no firewall due to the presence of proxy processing server.
CONCLUSION:

This paper presents the basic concepts of SCADA system and its components. It also discussed the different vulnerable effects caused due to complexity of the SCADA system and its security issues. By using the standard protocols security of the system is increased. Securing of the system is further studied by considering the DDOS attack on the SCADA system and by using OPL architecture and by Test Bed Development DDOS attack can be prevented. Considering DDOS attack on the system Test-Bed is developed by using IEEE-9 bus system, My SQL server software, and by using student version OPNET simulation tool. Power flow of IEEE-9 bus system data is secured by creating trigger alert to the data using My SQL server software. Since the student version of OPNET is used as a demonstration tool I cant input the My SQL server data into OPNET. So I have considered three scenarios one with no firewall protection, with firewall protection, and third scenario is to block the HTTP server if any hacker is trying to hack the data from this server. So by this we can conclude that the power flow data can be sent securely by using My SQL server and by OPNET simulation tool.
Reference:


APPENDIX –A

- My SQL code for creating tables and creating trigger to the data in the tables

--------Creating table

create table power_MY
(  
  Number int,
  Name nVARCHAR(max),
  STATUS nVARCHAR(max),
  Nominal_voltage decimal(18,2),
  PU_Voltage decimal(18,2),
  voltage_kv decimal(18,2),
  Angle_Deg decimal(18,2),
  Load_MW decimal(18,2),
  Load_Mvar decimal(18,2),
  Generator_MW decimal(18,2),
  GEnerator_Mvar decimal(18,2),
);

--------Inserting Values

insert into power_MY values(1,'Slack','Closed',16.5,1,16.5,0,0,0,118.61,47.20);

insert into power_MY values(2,'Generator','closed',18.0,1.0,18.0,0.76,0,0,100,28.99);

insert into power_MY values(3,'Generator','Closed',13.80,1.0,13.80,1.59,0,0,100,19.42);

insert into power_MY values(4,'Bus','Closed',230.00,0.97521,224.298,-4.02,0,0,0,0);
insert into power_MY values(5,'Load','Closed',230.0,0.95583,219.841,-6.38,90.00,30.00,0,0);

insert into power_MY values(6,'Bus','Closed',230.0,0.99036,227.782,-1.80,0,0,0,0);

insert into power_MY values(7,'Load','Closed',230.0,0.96902,227.874,-4.87,100.00,35.00,0,0);

insert into power_MY values(8,'Bus','Closed',230.0,0.98387,226.289,-2.89,0,0,0,0);

insert into power_MY values(9,'Load','Closed',230.0,0.94116,216.466,-7.76,125.00,50.00,0,0);

select * from power_MY;

--------Creating Trigger

create trigger Dont_Enter
on dbo.power_MY
after insert
  as
  begin
    print('Not Allowed')
    rollback transaction
  end
  go

--------Creating Update Trigger

create trigger Dont_update1
on dbo.power_MY
after insert
  as
  begin
print ('Not Allowed')
rollback transaction
end
go

---------Testing

insert into power_MY values(2,'Generator','Closed',18.0,1.0,18.0,0.76,0,0,0,0,0);
select *from power_MY