Operation Arctic Breeze: Simulation of Industrial Control Systems With Rapid SCADA

Mentor Lt Agee - Interns: Spencer Scamman, Ashley Yu, Thomas Brigham, Zachary Werle, Alicia Unterreiner, Timothy Reidy, Katelyn Atkinson

Background

Industrial Control Systems (ICS): A catch-all term for the various systems used to control and automate industrial projects. An example of industrial control systems is SCADA.

Supervisory Control and Data Acquisition (SCADA): Software used to control and automate industrial systems. The goal of our project is to create a simulation of a SCADA environment. This can be used to model and study various real-world systems.

MODBUS TCP: Message protocol developed by Modicon now Schneider Electric. The programmable logic controller acts as the server and the devices are the clients. Communication between devices is connected over port 502.

Simulations

SCADAsim: An open-source Python based simulator for SCADA systems. It uses Modbus TCP/RTU for the communication protocol. Abandoned because it had several bugs that made it difficult to use.

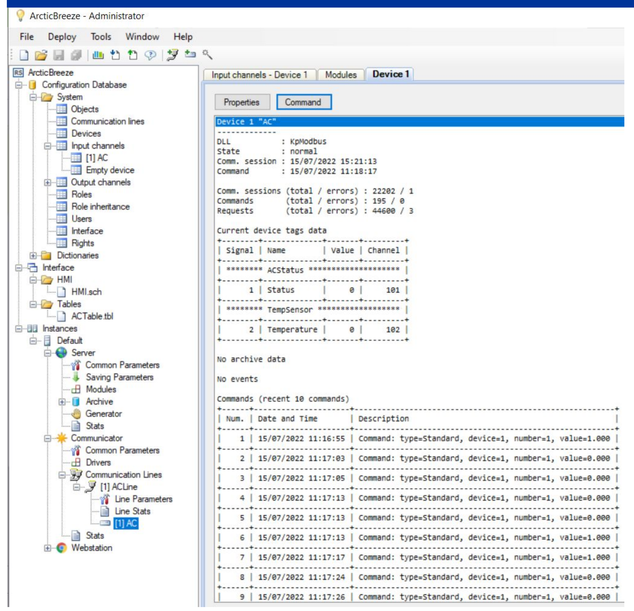
OMNeT++ & Scilab/Xcos: We were going to create our own ICS simulator by integrating OMNeT++ and Scilab/Xcos. OMNeT++ is an open-source network simulator while Xcos in Scilab is an open-source control system modeling simulator. The plan was based on TRUST-SCADA from UC Berkeley. Abandoned because Rapid SCADA proved superior.

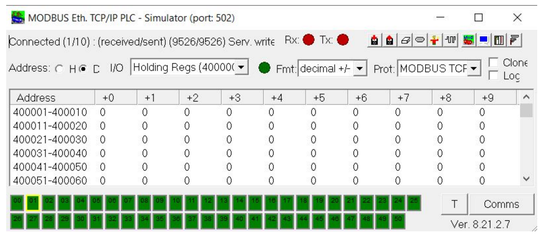
ASTORIA: An open-source toolset for simulating attacks on a smart grid network. Abandoned because developers did not update the project which left it incompatible with present-day computer systems.

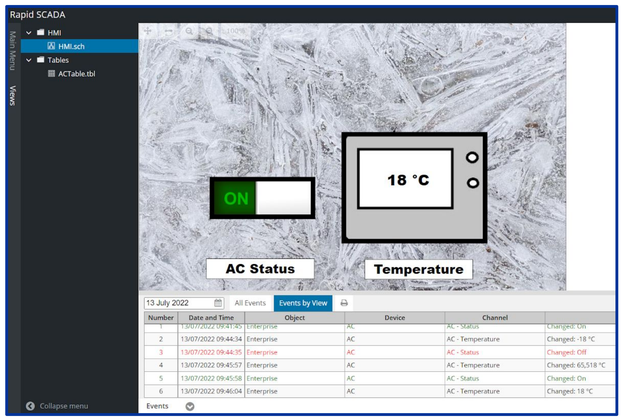
Rapid SCADA: An open-source platform for creating human machine interfaces and control systems. In large scale implementations, Rapid SCADA can create custom SCADA set ups.

ModRSsim2: An open source programmable logic controller that acts as the client. The simulator supports MODBUS TCP and all four types of MODBUS data.

Rapid SCADA and ModRSsim2








```
dim status
dim temp

status=GetRegisterValue(3,1)
if status<0 then
SetRegisterValue 3, 0, -1
else
SetRegisterValue 3, 0, 0
end if

status=GetRegisterValue(0,0)
if status=1 then
temp=GetRegisterValue(3,1) - 1
SetRegisterValue 3, 1, temp
else
temp=GetRegisterValue(3,1) + 1
SetRegisterValue 3, 1, temp
end if
```

Overview:
Rapid SCADA is simulating a freezer with an AC that will turn on when the temperature has reached 0℃ and turn off when the temperature has reached -16℃. The scheme is the visual representation of the operators workspace. The tables below shows the changes to and current state of each element in the device. MdRSsim2 simulates the programmable logic controller and shows the registers of a station.

MODBUS Device Interaction:
Using ModRSsim2, we can initialize our Modbus devices on the local computer as well as change the values of the registers/coils of our devices. The PLC is simply started and the local machine begins transmitting and receiving via the Modbus TCP protocol.

Automatic Control Module:
We purchased and employed the use of the Automatic Control Module in order to send automatic commands to the slave based on certain system conditions. Automatic commands to turn the AC on and off were deployed when the temperature fell below or above acceptable range.

Scheme:
The scheme is the visual representation of the operators workspace. The scheme is made up of textual and graphic elements that can change according to commands sent. The switch turns on and off to indicate the power status of the AC. The thermostat shows the current temperature in celsius of the freezer. The scheme along with the record of events can be viewed on the webstation application. The table view show the states of the AC and the thermostat.

Conclusions

Rapid SCADA and ModRSsim2 work effectively together to simulate an industrial control system environment. Both simulators are well documented allowing it to be quickly picked up by users. Both simulators allows for scaling of large projects. The use of additional plug-ins and modules in Rapid SCADA and the ability to code simulation scripts for ModRSsim2 allows expandability and catering to specific ICS.

Limitations

Rapid SCADA has a limitation in that it does not run on Linux due to incompatibility with GUI elements, particularly Mono Windows Forms is not supported by Rapid SCADA in Linux. MacOS is also not supported. Additionally, the formulas for calculating output values in the devices are only displayed in the Webstation. The simulator also requires purchase of extra modules, such as the Automatic Control Module. Additionally, we found either latency in Rapid SCADA software or the lag-time in the transfer of data prevented simultaneous change between the ModRSsim2 registers and the Rapid SCADA display. Rapid SCADA may be modified to support a server other than the localhost, while ModRSsim2 only supports localhost as the slave and needs a Modbus master simulator tp change the host.

Future Applications

With enough time and effort the models could become the equivalent of real-world industrial control systems. This could be taken even further and be used to test the security features of a ICS in the event of a cyber-attack. Instead of having to assume what would happen in the event of an attack, researchers and security experts can accurately test installed security features.

Acknowledgements Special Thanks to the VICEROY program.