Østfold University College

Simulated operative process: Monitoring of tank level

Pre project report

Marcus Lund Berthinussen

24.03.20

Bachelor's program in electrical engineering

Faculty of engineering

Østfold University College

Table of Contents

Høgskolen i Østfold

Project information

Project information	
Project title	Simulated operative process: Monitoring of tank level
Project number	B20E11
Starting date	10.03.20
End date	10.06.20
Client	Université d'Orleans IUT de l'Indre Châteauroux Issoudun
Supervisor	Manuel Avila Université d'Orleans IUT de l'Indre Châteauroux Issoudun manuel.avila@univ-orleans.fr +33 6 85 92 19 34

Contractor	
	Marcus Lund Berthinussen Tel: +47 40201095 E-post: marcus_inbox@outlook.com Born: 13. January 1995 Contact Person Student at: Østfold University College Program: Bachelor's degree in electrical engineering (Electrical Power)

Problem definition and background

In 2010 the uncovering of the Stuxnet-attack shocked the whole world. The complex computer worm was used as a weapon causing havoc on the Iranian uranium enrichment facility in Natanz. By targeting the PLC's that control the electromechanical components in the facility, it was able to destroy several centrifuges by causing them to burn themselves out. (McAfee, n.d.)

The malware was using undiscovered weaknesses in windows software to spread from USB-sticks to various Microsoft computers. Once the malware was on the computer it searched for a specific Siemens PLC software. From the PLC it was able to manipulate the speed of the centrifuges, periodically spinning the centrifuges too fast while manipulating the feedback so that the operators believed everything was fine. This made the virus practically invisible. (The New Jersey Cybersecurity and Communications Integration Cell, 2017)

This first of its kind attack paved the way for a wave of similarly functioning malwares often referred to as "sons of Stuxnet". Some of these include Duqu, Flame, Havex, BlackEnergy, Industroyer, Triton and most recently in 2018, an unnamed malware also attacking Iran. The threat from these kinds of attacks is severe. They can be used to target critical infrastructure such as, powerplants as seen in Iran, they can be used to hit the electrical grids, water treatment facilities, military equipment and more. (McAfee, n.d.) As a matter of fact, Duqu has been observed in energy facilities in eight different countries and both Industroyer and BlackEnergy has been reported to cause power outages in Ukraine. Blackenergy left 1,4 million people without power. (Piggin, 2016)

Since the Stuxnet-attack, the frequency of cyber-attacks has increased. The integration of IT and OT systems has facilitated the problem, making industries more vulnerable to cyber-attacks, both large and small. (Piggin, 2016) One of the most common motivations for cyber-attacks is extorsion and one in four power companies globally has been victim of this. (McAfee, n.d.) Ransomware is a good example of this.

In response to cyber threats such as these, Exera created the cyber security of industrial systems commission in 2013, CT CSI for short. Exera is an association for companies/industries involved in measurement, regulation/control and automation technology. The main purpose of the commission is to monitor the evolution of the legislative and regulatory environment in France, as well as sharing rules of good practice and knowledge of the cybersecurity market. (Commission technique « Cybersécurité des systèmes industriels » Exera, 2020)

To increase awareness among its members and complement efforts undertaken by other security actors, the commission is arranging a hacking tournament. Through discovering security

vulnerabilities, the tournament will hopefully contribute to improvements of the equipment from the participating members as well as asses the role of the hardware and software from other suppliers.

A series of objectives for the hackers are defined which relates to the security concerns of the members. Each participant defines and installs an OT-loop which conforms to the standards of Exera. Each OT-loop has its own access and its own equipment, including supervision console, automation/PLC, sensors, actuators and process station simulating an industrial process.

As seen on the figure below, the architecture for the tournament allows direct access to the OT-loop or access via a router which represents a bridge between the IT and OT network. The first scenario is where attackers have direct access to the IT-network. The second scenario is with an additional difficulty, where the attackers have penetrated the company's IT-network, but still must cross from the IT-to OT network. The attackers in the tournament are selected professional security experts and will try their best to break through the security or discover any vulnerability.

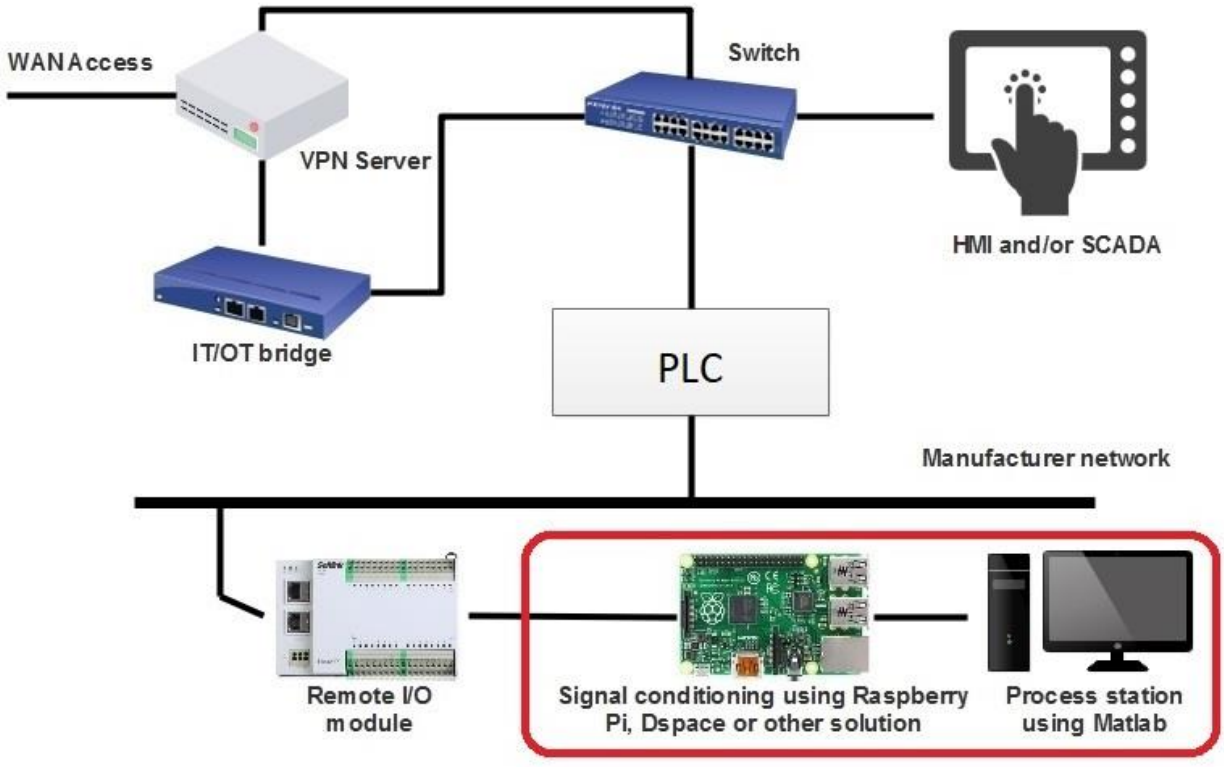

Figure 1: Network schematic of the system. Made using Edraw max and images. (Hipel, n.d.) (Raspberry Pi, 2020) (ipc2u, n.d.)

The idea for the project came from a collaboration between IUT and Exera. I will be working on the simulation on the process station and the signal conditioner which interfaces with the I/O module. The name of the project is Simulated operative process: Monitoring of tank, and when it comes to simulations of process systems there are many benefits.

Industrial equipment is incredibly expensive and having the capability of simulating it will lead to great savings and can also give access to systems that previously were too expensive. In a simulation you are in control of every parameter and can easily manipulate and change things in no time. This contrasts to the real world, where for example the changing of physical components can take hours or days and has an associated cost. A simulation has no extra requirement for utilities. No extra water, sewage, power, gas/heat or anything else. It is compact and scalable, allowing multiple systems to be simulated on only one computer. It is safe for the operator and for everyone else, emitting no gasses, fumes or heat, and having no moving parts. The advantages are nearly endless.

To satisfy the requirements of Exera, an industrial solution based on PLC and an industrial network driving and supervising a process is needed. The process itself does not need to be complex, which is why a simple water tank has been chosen. This solution will be very small, can easily be replicated and will allow many participating manufacturers to install their solution in the same room.

IUT is interested in this project because it could be used as a lab exercise for their students, where the students can practice using PID-control (which is part of the curriculum) on the simulated process. An example lab has already been provided from IUT. The lab, as well as a presentation of the tournament and the rules can be found under attachments.

Objective of the project and tasks

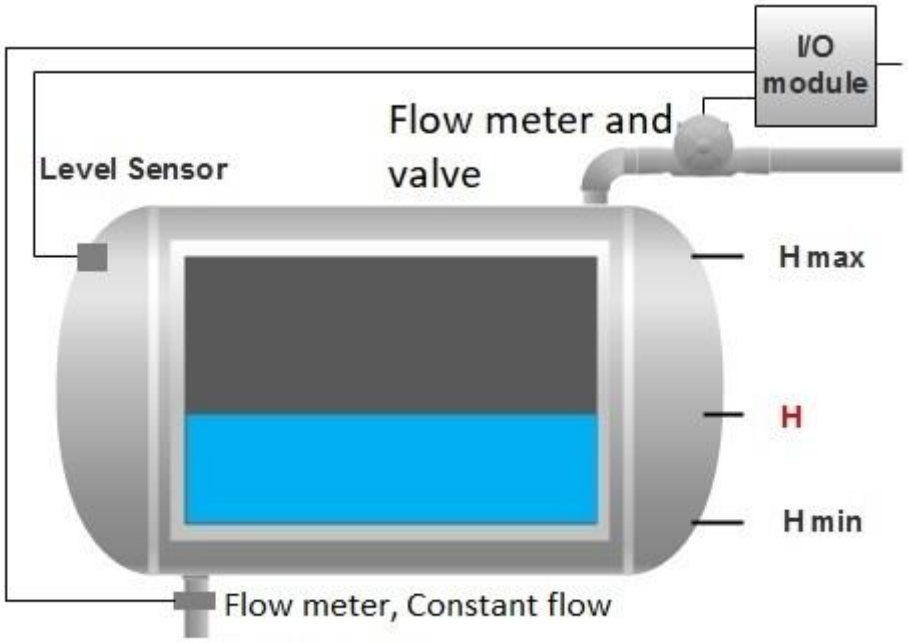

Figure 2: Tank schematic. Made using Edraw max.

The objective of the project is to create a simulation of a water tank on a computer the way described in appendix 2 of the tournament document. It states:

The outflow shall be constant, D_{out} = Constant. The inflow D_{in} will be randomly selected between $D_{out}/2$ and $2*D_{out}$ when the valve is open. The height, H is measured continuously by a sensor which provides the information to the plc. If the height is less or equal to H_{min}, the plc will command the inflow valve to open. When H is equal to or greater than H_{max}, the plc will command the inflow valve to shut. The information about the state of the valve and the flow as well as H_{max} and H_{min} shall be sent to the plc. The simulation shall have a graphical display as well, illustrating the state of the tank and its parameters.

The suggested solution by IUT is to use Matlab on the process station in combination with D-space or preferably raspberry pi as the signal processor. There are many possible solutions and robustness of the system is a priority. Starting out, the process can be broken down into several tasks and central problems.

Central problems

1. How to simulate the tank with waterflow
   How to simulate sensor
2. How to make graphical display and connect to the parameters of the tank
3. How to use IO for physical interaction and to deliver and receive info from the PLC
4. How the signal conditioner will send signals to the simulation program and vice versa
5. Is it necessary to have a PLC that can be connect to the system to show that it works? If so, this needs to be programmed as well.

Tasks

1. Discover options for simulation on process station → e.g. Matlab Simulink, TIA, python, Siemens Simatic HMI or Simit, intouch
2. Discover other options than the suggested one → e.g. Full simulation on raspberry pi and eliminate process station, or D-space or microcontroller instead of raspberry pi
3. Compare solutions and find out how the various components can interact before deciding which solution to go for.
4. Create flowchart for the program → This will further break down the process into various steps. However, it is not appropriate to do before a solution has been selected
5. Write the program and connect the components together
6. Continuously document the process and write report at the end

Limitations

Only one solution will be picket for the system and a basic model with the defined controls and parameters shall be developed. I shall stick to the confines of the project as stated in the tournament document.

The solution used in the tournament is compact and small because it is preferable if all participating manufacturers can install the equipment in one room.

The duration of the tournament is one year. This also creates a limitation on the various solutions that could have been developed. The system must be kept continuously operational throughout the entire period or must be tolerant to black outs and temporary loss of internet connection or similar problems. Finally, it should preferably be maintenance free.

Project execution plan

Activity plan

An activity plan containing the central parts of the project and the obligatory requirements has been made. It contains the starting and ending date as well as the dedicated time. The plan is made so that various dependencies have been considered.

Activity	Number	Start date	End date	Time (hours)
Meeting 1	1	23.03	27.03	3
submitting text and images for expo	2	30.03	31.03	14
Looking into various solutions for the project	3	01.04	07.04	28
Compare and select solution	4	08.04	10.04	21
Make program chart	5	13.04	14.04	14
Start programming/simulating the tank	6	15.04	24.04	35
Set up a blog	7	20.04	22.04	12
Submitting special needs/requirements Expo	8	23.04	24.04	3
Making graphical interface	9	27.04	15.05	105
Meeting 2 and meeting confirmation	10	30.04	03.05	4
Documenting the process	11	01.04	18.05	30
Writing the report	12	18.05	05.06	105
submitting title in student-web	13	01.06	02.06	2
Finishing the blog	14	01.06	07.06	12
Submitting project report in Inspera	15	06.06	07.06	2
Expo	16	15.06	16.06	16
Sum				406

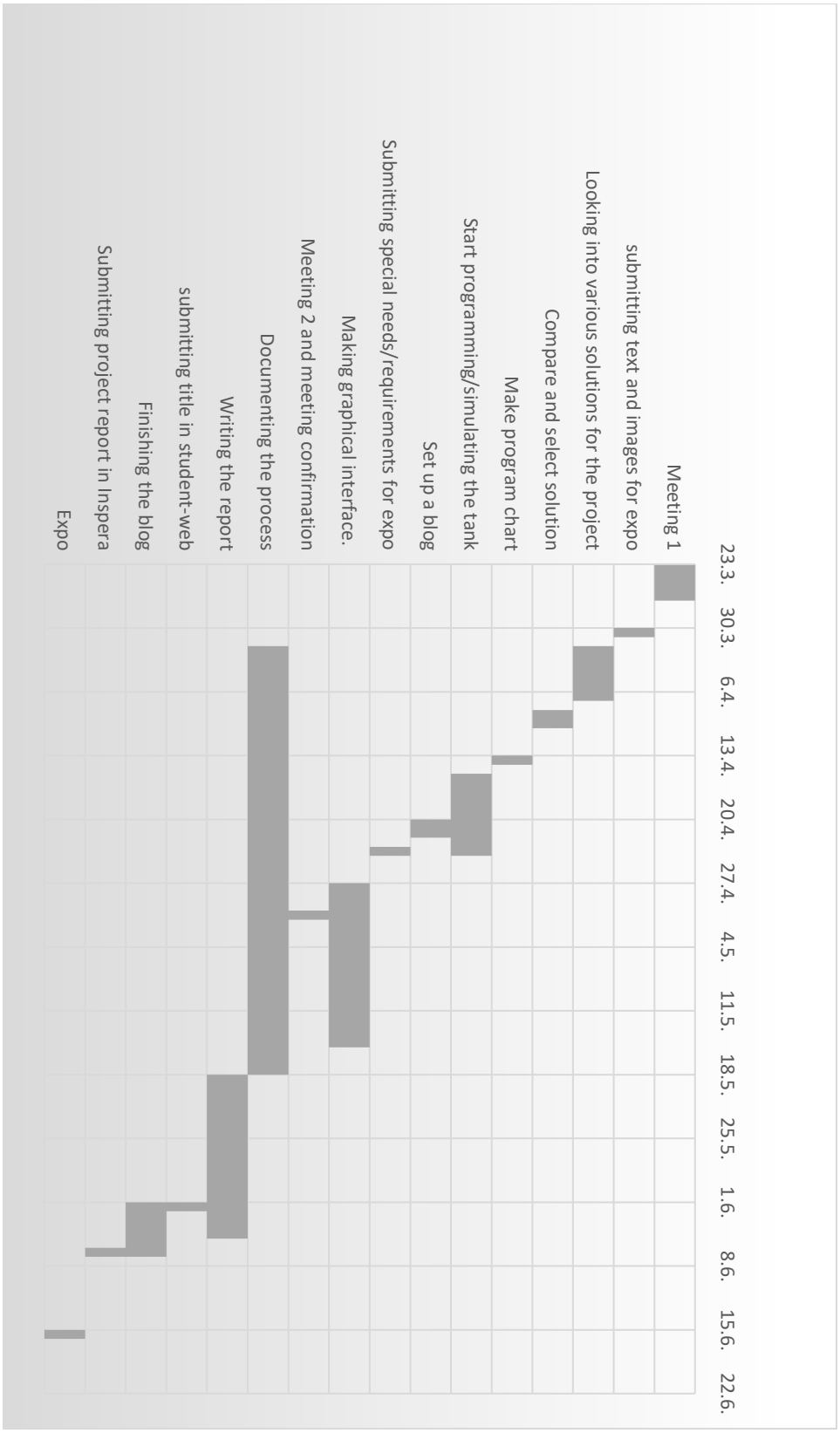

Figure 3: Gantt chart showing planned activity

Milestones and deadlines

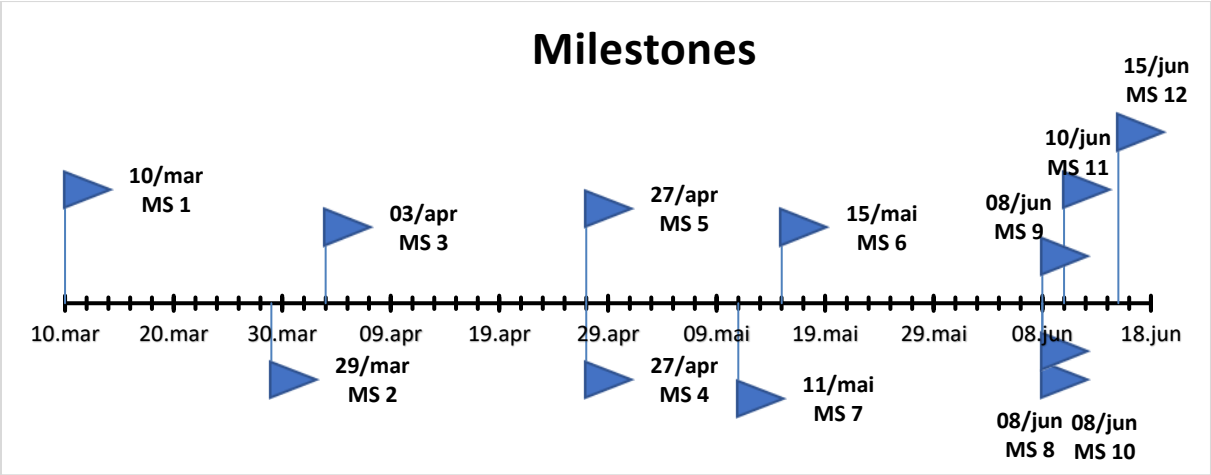

Figure 4: Milestone Chart.

Date	Milestone	Name
10.mar	MS 1	Prosject start
29.mar	MS 2	My deadline for the Pre project report
03.apr	MS 3	Deadline for submitting text and images for expo
27.apr	MS 4	Deadline for making of Blog
27.apr	MS 5	Deadline for submitting special needs/requirements for expo
15.mai	MS 6	Meeting confirmation
11.mai	MS 7	Deadline for meeting requirement
08.jun	MS 8	Deadline for submitting title in student-web
08.jun	MS 9	Deadline for finishing the blog
08.jun	MS 10	Deadline for submitting project report in Inspera
10.jun	MS 11	End of stay in France
15.jun	MS 12	Expo

Solution methodology

As stated in the activity plan, I will look at various solutions for simulation programs, see various solutions for communication between the process station and the I/O module. Then compare and pick solution. Make a flowchart, make a program for the signal conditioner and ensure that the signal conditioner and the simulation program can communicate, make a program for the tank, make a program for the graphic interface. Then I will put it all together into a complete solution.

It is not essential to use any scholarly sources or special searching tools to find the various solutions/programs. The internet is full of open source solutions and tutorials. The information needed can be found by simply using google and YouTube to find similar projects, then find the webpages with the documentation for the various programs/solutions. It has already been suggested that I use MATLAB/Simulink and raspberry pi. For this solution the documentation as well as examples are available on MATLAB's and raspberry pi's webpages.

To answer my central problems, I will look at other similar projects and read the documentation of the various solutions. This is the correct way of solving my task because my project is a practical one where the goal is to develop a finished solution that is robust.

Resources and costs

No budget or resource plan has been made for the project. Expected materials needed include a raspberry Pi, a micro controller or a D-space controller. It is common for all universities to have all of these. If that is not the case, the price for a good microcontroller or a raspberry Pi is less than 500 kr. If needed, IUT will provide any of these upon request.

Attachments

Contract between contractor and client

Tournament document, "*TOURNOI EXERA DE HACKING*"

Example of Lab provided by IUT, *"industrial communication labs"*

References

Commission technique « Cybersécurité des systèmes industriels » Exera. (2020, January 21). TOURNOI EXERA DE HACKING TESTS D'INTRUSION SUR AUTOMATES ET ÉLÉMENTS ASSOCIÉS.

Hipel. (n.d.). *hmi-icon*. Retrieved from Hipel.

ipc2u. (n.d.). *Softlink Distributed Fieldbus I/O modules*. Retrieved from ipc2u: https://ipc2u.com/news/productnews/softlink-distributed-fieldbus-i-o-modules/

McAfee. (n.d.). *What is Stuxnet*. Retrieved from McAfee: https://www.mcafee.com/enterprise/en-us/security-awareness/ransomware/what-is-stuxnet.html

Piggin, R. (2016). *Cyber security trends: What should keep CEOs awake at night.* Retrieved from ResearchGate: https://www.researchgate.net/profile/Richard_Piggin/publication/293809327_Cyber_security_trends_What_should_keep_CEOs_awake_at_night/links/5df11e8b299bf10bc3544759/Cyber-security-trends-What-should-keep-CEOs-awake-at-night.pdf

Raspberry Pi. (2020, 03 13). Retrieved from Wikipedia: https://en.wikipedia.org/wiki/Raspberry_Pi

The New Jersey Cybersecurity and Communications Integration Cell. (2017, August 10). *Stuxnet*. Retrieved from NJCCIC: https://www.cyber.nj.gov/threat-profiles/ics-malware-variants/stuxnet