M.Sc. in Information Technology Architecture, Engineering and Construction

Colm Prenderville MIEI
114222336

PROJECT

Submitted as part of continuous
assessment for the subject of
Computer Mediated Communication

for

Prof. Matevez Dolenc

University College Cork, Ireland

Chosen topic:

IT in BIOMASS WASTE ENGINEERING, SUPERVISORY CONTROL and DATA ACQUISITION (SCADA) SYSTEM

Submittal date: 6th of November 2014

Chapter 1

1.1 Introduction

The project as a case study for this assignment is the Milton Keynes Waste Recycling Project fines stabilization facility. It is a waste to energy plant, currently under construction due for completion in June 2016. It will process 30,000 tons p/a of municipal solid waste fines derived from primarily domestic waste. This material waste has high methane potential. It is proposed that harnessing the gas though anaerobic digestion is the most preferred method of extraction. The concept of waste to energy is relatively new in the UK and it is seen as a new way forward to deal with domestic waste, with only 5% post processing will disposed of in landfill. The production of the gas to energy and sending back onto the national grid reduces carbon footprint, it is looked at a revolutionary way to manage waste material.

Approximately 5,000 tons P/A of bulking materials will be added to achieve sufficient porosity within the waste. The enables the agents work its way through the raw material within the fermenters. It is expected that 30,000 tons of MSW fines when subjected to dry fermentation, has the capacity to generate approximately 110 m3 biogas per ton of fresh material. Studies have shown in other European countries how beneficial this relatively new technology can be for client profitability, moreover than ever before when we introduce clever IT software we can manipulate to yield the plants maximum potential.

1.2 Building element and processes

Before we discuss the plants software and technologies, and to understand the interface of both, we must first must describe the buildings core elements in basic form. The following is a list of the major structural components within the development, with each of the elements are controlled or monitored by IT in some form. (fig1)

- The fines reception area. This is where the bulk waste material is imported to the facility and material is sieved and cleansed of all foreign waste prior to use.
- Nine fermentation chambers, material from the reception area is placed in the fermenters for 28 days and heated to 60degrees for gas extraction.
- Six Aerobic Composting Zones, after the materials used in the fermenters it is sent here for the initial drying stage.
- Pasteurization Tunnels. The tunnels are heated up to 90 degrees to remove any unwanted bacteria from the material before it is finally removed from the plant, and used as agricultural waste or bagged for gardening.
- Percolate Storage Tank. One of the more important elements, the percolate tank carries the agent that is sprayed over waste in the fermenters to activate the substrate .
- Leachate Tank is a back up to the percolation tank and collects leachate from the pasteurization tunnels.

- 1 Biofilter with flare stack discharge, this is used when the gases are deemed to be impure for use in the fermenters, here is where is burned off into the atmosphere.

- 1 Gas scrubber, cleans the gas prior to sending to the turbines to create electricity

- 2 CHP 600KW engines, this is the turbine creating the electricity sending it back on the national grid.

- 1 Operations control room or HMI (Human Interface Machine) this is where all the data from the plant operation is controlled locally, or remotely. This project will be controlled both locally and from Germany.

1.3 Plant layout

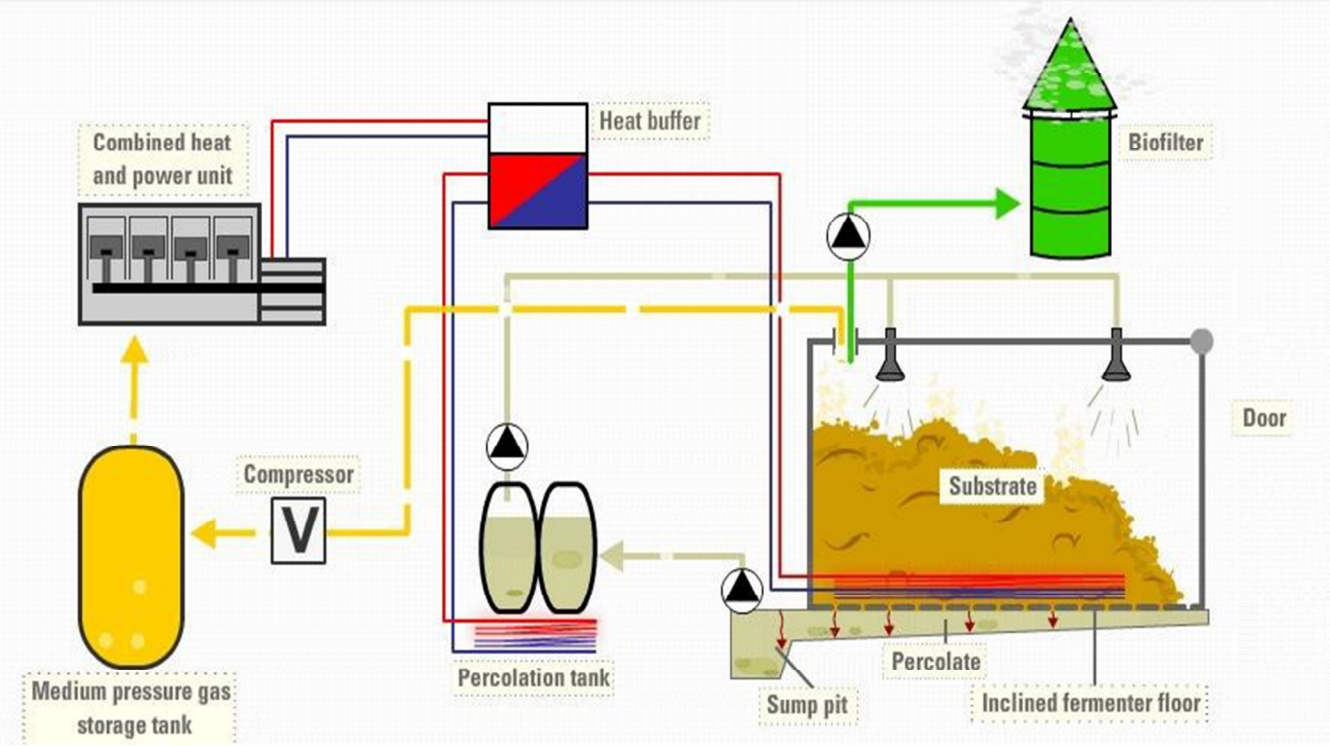


Fig 1.

Chapter 2

2.1 The software

The software known as SCADA, is an acronym for Supervisory Control and Data Acquisition. It is a software that is used for process control, to gather real time data from plant floors inhabitable or restricted areas. It comprises of a network of intelligent devices that interfaces and interacts with sensors and control outputs. It congregates and reads information from independent systems, and reports in real time from local and geographically remote locations. It combines telemetry and data acquisition that allows users to send and receive commands to distant facilities, which will be discussed in greater detail later on in this report.

2.2 The uses of SCADA uses in modern day.

It is somehow overlooked or perhaps not appreciated is how SCADA interacts in our everyday life. It controls most of the things that we can unknowingly take forgranted to mention a few;

- Manufacturing: The SCADA systems regulates industrial automation robots, monitor processes and quality control.
- Buildings, facilities and environments: Facility managers use SCADA to control HVAC, refrigeration units, lighting and entry systems.
- Electric power generation, transmission and distribution: Electric utilities use SCADA systems to detect current flow and line voltage, to monitor the operation of circuit breakers, and to take sections of the power grid online or offline.
- Water and sewage: Municipal water companies use SCADA to monitor and regulate water flow, reservoir levels, and pipe pressure.
- Mass transit: Transit authorities use SCADA to regulate electricity to subways, automation for traffic signals on rail and road systems. it uses GPS to track and locate trains and buses.
- Traffic signals: SCADA regulates traffic lights, controls traffic flow and detects out-of-order signals.

Through this brief description how much it comes into our daily lives, one can now have some appreciation, but with this it comes a risk. Careful consideration is needed when programming the software and to the level of protection required. Again this depends on what the is primary purpose, and its vulnerability to attack. There have been many recorded instances where attacks have happened, with the potential to cause great harm.

From what we have mentioned up to now SCADA can be argued to be an almost bespoke software, as every process plant, automated workshop or transit system in most cases have its own individual uniqueness. Born out of a need for a user-friendly front-end control system containing PLCs. SCADA is now at the forefront of software automation technology. HMI (Human Machine Interface) SCADA supports the way

today's operators need to work with the most powerful capabilities. In this modern environment we continue to seek new methods and tools that can enable them to do more with less.

2.3 The System

SCADA is a system with many data elements called points. Each point is a monitor, or sensor and these points can be either hard or soft. A hard data point can be an actual monitor; a soft point can be viewed upon as an application or software calculation. Data elements from hard and soft points are usually always recorded and referenced logged to create a time stamp or history. It joins together independent systems that measure and report in real time, both local and geographically to remote distributed processes. It is a combination of telemetry and data acquisition, that enables a user to send commands to distant facilities and collect data from them. Telemetry is a technique used in transmitting and receiving data over a medium. Data acquisition is a method of collecting the data from the equipment being controlled and monitored for human interface.

Chapter 3

3.1 SCADA feasibility and suitability assessment

A project charter is the first step in the plants methodology of its requirement and how it functions. It can take place in the define step of DMAIC (Define, Measure, Analyse, Improve, Control), and the charter can make or break a successful project. The Project Management team through the project charter, must identify the need and limits of the software, and prepare estimate costs for setup and operational stage. A comprehensive review must be carried out to ensure the software and programming requirements are fully met to optimise the use of the plant.

For these large scale operations such as energy plants, industry professionals provide a framework known as the bodies of knowledge (BOK). This is a structured frame work that is recognised by Project Management Institute (Fig 2.)

The chart below provides a list of knowledge areas that are all assets of this software, it can be seen as an early troubleshooter to assess the software's true suitability to the plant. Or part of what is required to develop, execute on the part of software and HMI supervision. It is for the plants overall protection and optimisation. It has proven to deliver and enhance the value of the plants data and its information assets. Without going into too much detail we can see at a glance the usefulness to carry out this study to categorise, eliminate, or introduce certain items that will enhance the software further at this very early stage.

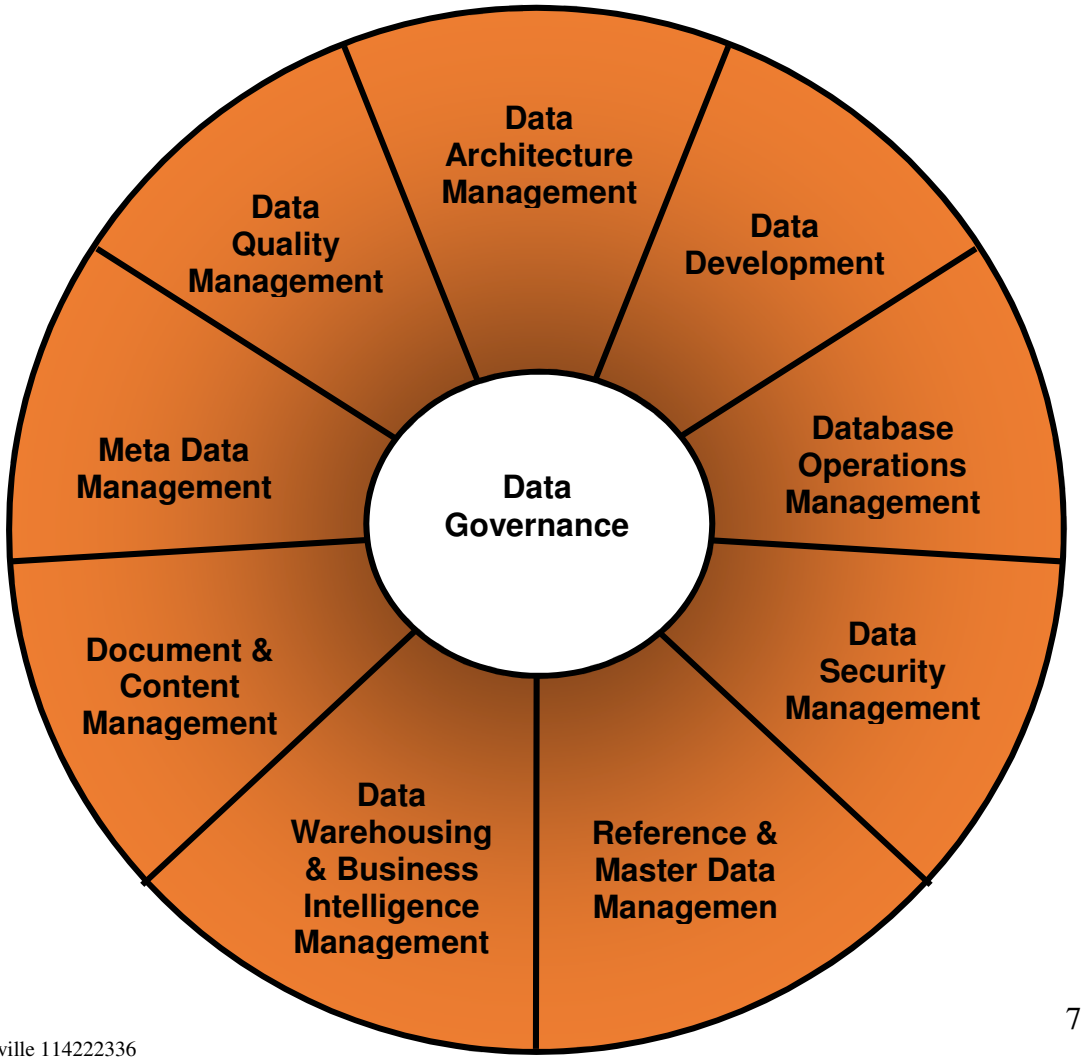


Fig 2.

3.2 Use case diagram

As we have discussed the goal is to supervise, control, monitor and acquire data for the process plant systems and to ensure optimization, safety and efficiency. (Fig 3)

Actors:

1. Field Devices
2. Local Control Center (LCC)
3. Remote Telemetry Units (RTU)
4. Master / Central Control Terminal Unit (MTU)
5. Operator
6. Supervisor

User cases

1. System Shut Down / Startup
2. Gather Field Information
3. Perform Local Control
4. Transfer Field Information
5. Manage Field Information
6. Perform Remote Control
7. Analyze System State
8. Schedule Task
9. Balance Load
10. Adjust Settings
11. Check Status
12. Manage Logging

User Case Diagram

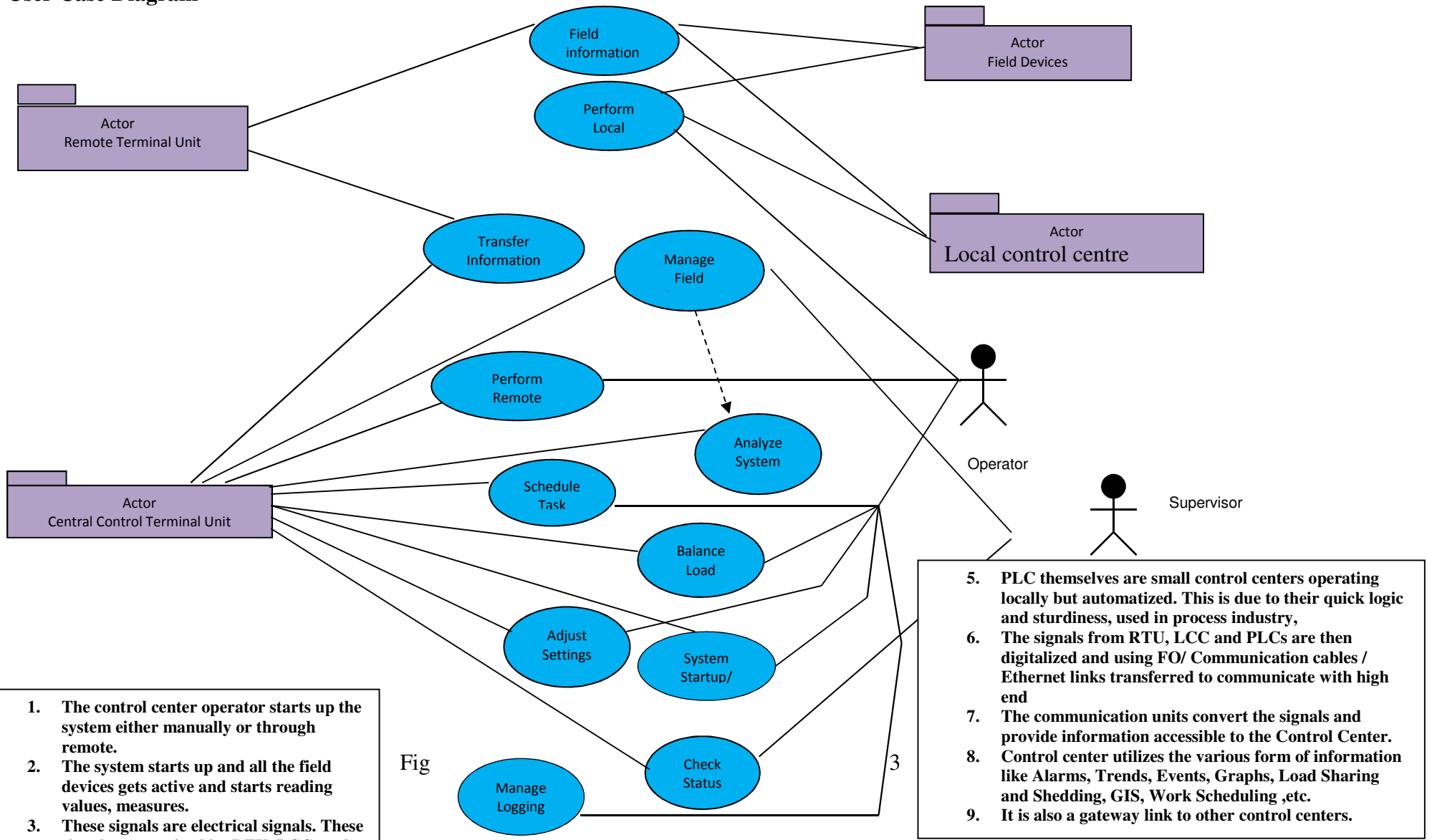


Fig 3

1. **The control center operator starts up the system either manually or through remote.**
2. **The system starts up and all the field devices gets active and starts reading values, measures.**
3. **These signals are electrical signals. These signals are received by RTU, LCC, and PLCs**
4. **LCC is responsible to manual operation from the site, in case of emergency or shutdowns**

5. **PLC themselves are small control centers operating locally but automatized. This is due to their quick logic and sturdiness, used in process industry,**
6. **The signals from RTU, LCC and PLCs are then digitalized and using FO/ Communication cables / Ethernet links transferred to communicate with high end**
7. **The communication units convert the signals and provide information accessible to the Control Center.**
8. **Control center utilizes the various form of information like Alarms, Trends, Events, Graphs, Load Sharing and Shedding, GIS, Work Scheduling ,etc.**
9. **It is also a gateway link to other control centers.**

Chapter 4
Control components within the Program

4.1 Maintenance and Repair Operation

The intelligence within the software creates and intelligent Maintenance Repair Operation (MRO) or remote monitoring and diagnostic systems. This cuts overall production costs, improves quality, minimises downtime and increases operational efficiency. We are all too familiar with the term *'Predict and prevent'*. Unresponsive outdated systems without this intelligence can lead to major plant malfunctions and further costs. Examples of such can be from a weak or faulty telemetry unit allowing poor quality volatile gas quality being sent to the 1.2M GBP CHP units. The SCADA system will detect such anomalies or abnormal signals to run system diagnostic check. The parameters of the telemetry unit is programmed into the software, therefore sudden changes instigate secondary telemetry readings to either keep the plant operational or send an alarm to the engineers for support.

4.2 Major control components

The control server hosts the DCS or PLC supervisory control software that is designed to communicate with lower-level control devices. The control server accesses subordinate control modules over an LAN or wireless networks.

SCADA Server or Master Terminal Unit (MTU). The SCADA Server is the device that acts as the master in a SCADA system. Remote terminal units and PLC devices (as described below) located at remote field sites act as slaves.

Remote Terminal Unit (RTU). The RTU, also called a remote telemetry unit, is special purpose data acquisition and control unit designed to support SCADA remote stations. RTUs are field devices often equipped with wireless radio interfaces to support remote situations where wirebased communications are unavailable. Sometimes PLCs are implemented as field devices to serve as RTUs; in this case, the PLC is often referred to as an RTU.

Programmable Logic Controller (PLC). The PLC is a small industrial computer originally designed to perform the logic functions executed by electrical hardware (relays, drum switches, and mechanical timer/counters). PLCs are controllers with the capability of controlling complex processes, and they are used substantially in SCADA systems and DCSs. Other controllers used at the field level are process controllers and RTUs; they provide the same control as PLCs but are designed for specific control applications. In SCADA environments, PLCs are often used as field devices because they are more economical, versatile, flexible, and configurable than special-purpose RTUs.

Intelligent Electronic Devices (IED). An IED is a "smart" sensor/actuator containing the intelligence required to acquire data, communicate to other devices, and perform local processing and control. An IED could combine an analog input sensor, analog output, low-level control capabilities, a communication system, and program memory in one device. The use of IEDs in SCADA and DCS systems allows for automatic control at the local level.

Human-Machine Interface (HMI). The HMI is the IT software and hardware that allows human operators to monitor the state of a process under control, modify control settings to change the control objective, and manually override automatic control operations in the event of an emergency. The HMI also allows a control engineer or operator to configure set points or control algorithms and parameters in the controller. The HMI also displays process status information, historical information, reports, and other information to operators, administrators, managers, business partners, and other authorized users. The location, platform, and interface may vary a great deal.

Data Historian. The data historian is a centralized database for logging all process information within the control system. Information stored in this database can be accessed to support various analyses, from statistical process control to enterprise level planning.

Input/Output (IO) Server. The IO server is a control component responsible for collecting, buffering and providing access to process information from control sub-components such as PLCs, RTUs and IEDs. An IO server can reside on the control server or on a separate computer platform. IO servers are also used for interfacing third-party control components, such as an HMI and a control server.

Chapter 5 Core processing elements of the SCADA system

5.1 Data acquisition

Sensors, either digital or analog directly interfaces with the managed systems inputs/outputs, water flow, valve states, temperature probes, pressure sensors. The point sites are known as field sites, as mentioned in the use case diagram which are the data sources. (Fig 4)

The telemetries send and receive electronic signals between 4-20 milliamps. In this case the heating of the fermenter floor slab will range from 16-60 degrees. Therefore the SCADA software is programmed to understand 4 milliamps = 16 degrees and so on rising, as the temperature increases the electrical current increases informing the RTU's.

The kind of used in this industry are known as *'Thermistors'* a commonly known temperature sensor used in appliances. The same operations or methodologies will apply to all field sites, flow computers, Rod pump controllers, Plunge lift controllers, compressors, vapour recovery systems and tank level sticks the information is transmitted through an electronic signals and displayed on the HMI SCADA monitors. The RTUs consist of programmable logic converter which can be set to specific requirement. For example, in the thermal power plant the percolate flow can be set to specific value, or it can be changed according to the requirement if it detects a dry substrate in the fermenters.

Network (LAN) the signal that is transmitted back to the RTU, PLC or the DCS controller and communicated through the architectural peers via LAN or wireless connection.

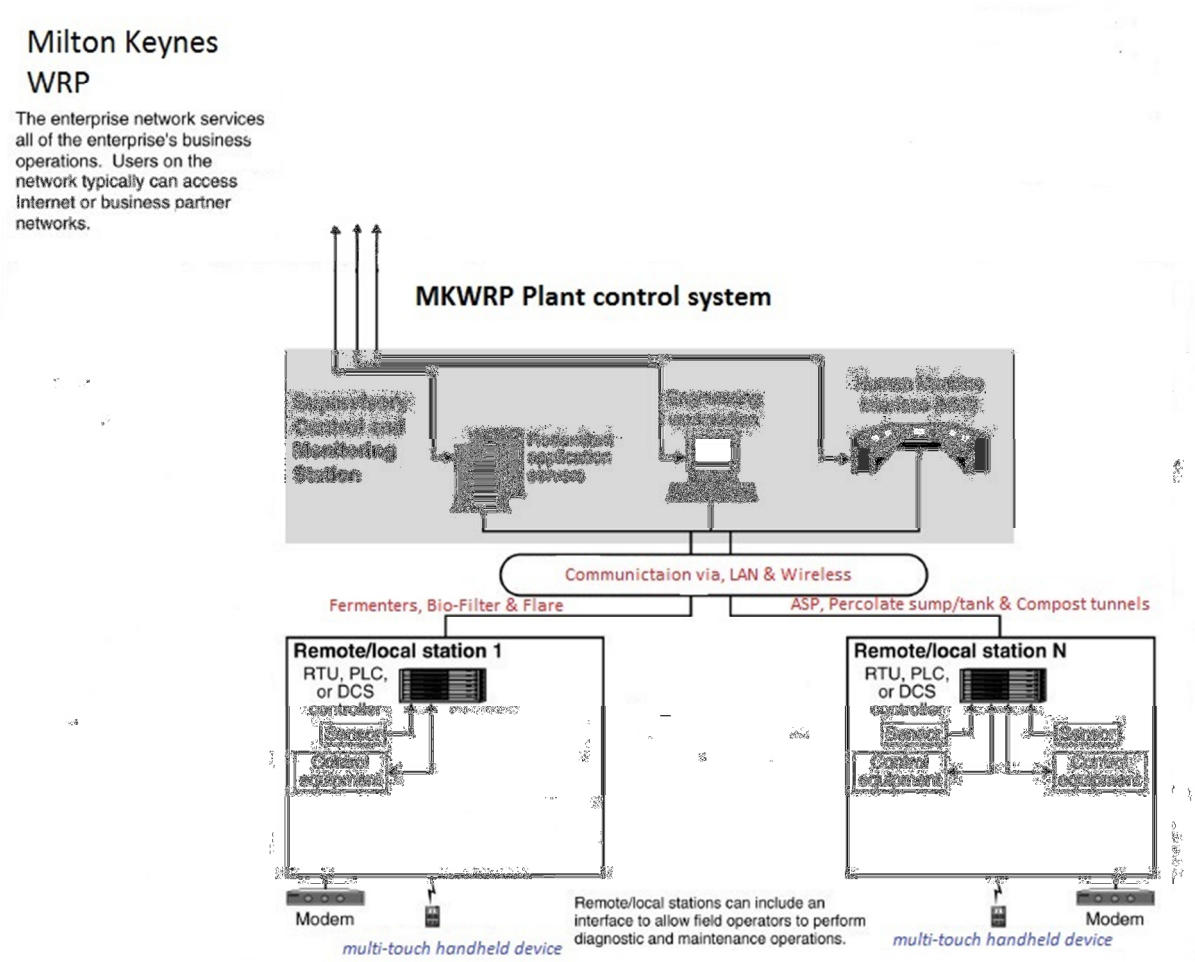


Fig 4

5.2 Data communication

The SCADA system controls peer-to-peer network architecture. It automatically seeks out its peers. Through this it seamlessly exchanges control information in engineering units, across the Local Area, it's a centralized system which monitors and controls entire area. It is purely a software package that is positioned on top of hardware.

A supervisory system gathers data on the process, and sends the commands control to the process. The SCADA a remote terminals unit which utilises standard IP technology (3rd. generation). SCADA Cloud Control System gives it a powerful Distributed Control System (DCS).

The cloud (4th generation) somewhat new to SCADA is creating a revolution in systems architecture, because it provides very high redundancy, virtually unlimited data storage, and worldwide data access. This is now extended to phone apps for immediate notification and plant control. The user can log in and manipulate the plants operation in real time, but as discussed earlier in this report with cloud data communication, one must pay very careful consideration on what possible risks or eventualities will pass at if a catastrophic hack occurs. This we will discuss on security in chapter 5.

5.3 Data presentation

A Human machine interface or HMI is the apparatus which presents the data to operator, and through which the human operator controls the processes (Fig 6). A HMI is linked to the SCADA systems databases and software programs, to provide plant room trends, diagnostics and management information. Presenting the information graphically in the form of a mimic diagram. The mimic diagram provides an integrated flow chart of each of the processes in each area as we have discussed earlier.

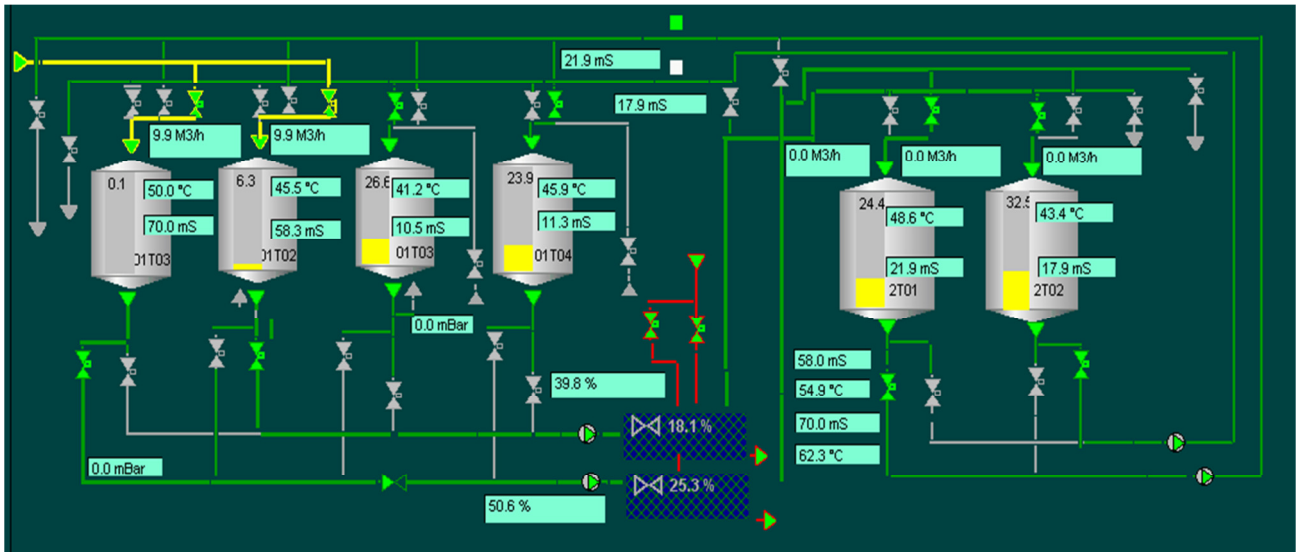


Fig 6

From here the human operator can identify how the plant is performing. Typically the operator locally or in Germany can log into the plant system and manipulate its operations.

5.4 Control

The supervisory control and monitoring system for the facility typically contains redundant application servers, an engineering workstation and a HMI. Both the remote and local station contains RTU's, a PLC or DCS (Distributed controller system) which receives and interprets the signals from the sensors transmits the information through LAN or wireless to the supervisory control and monitoring system. (Fig 7)

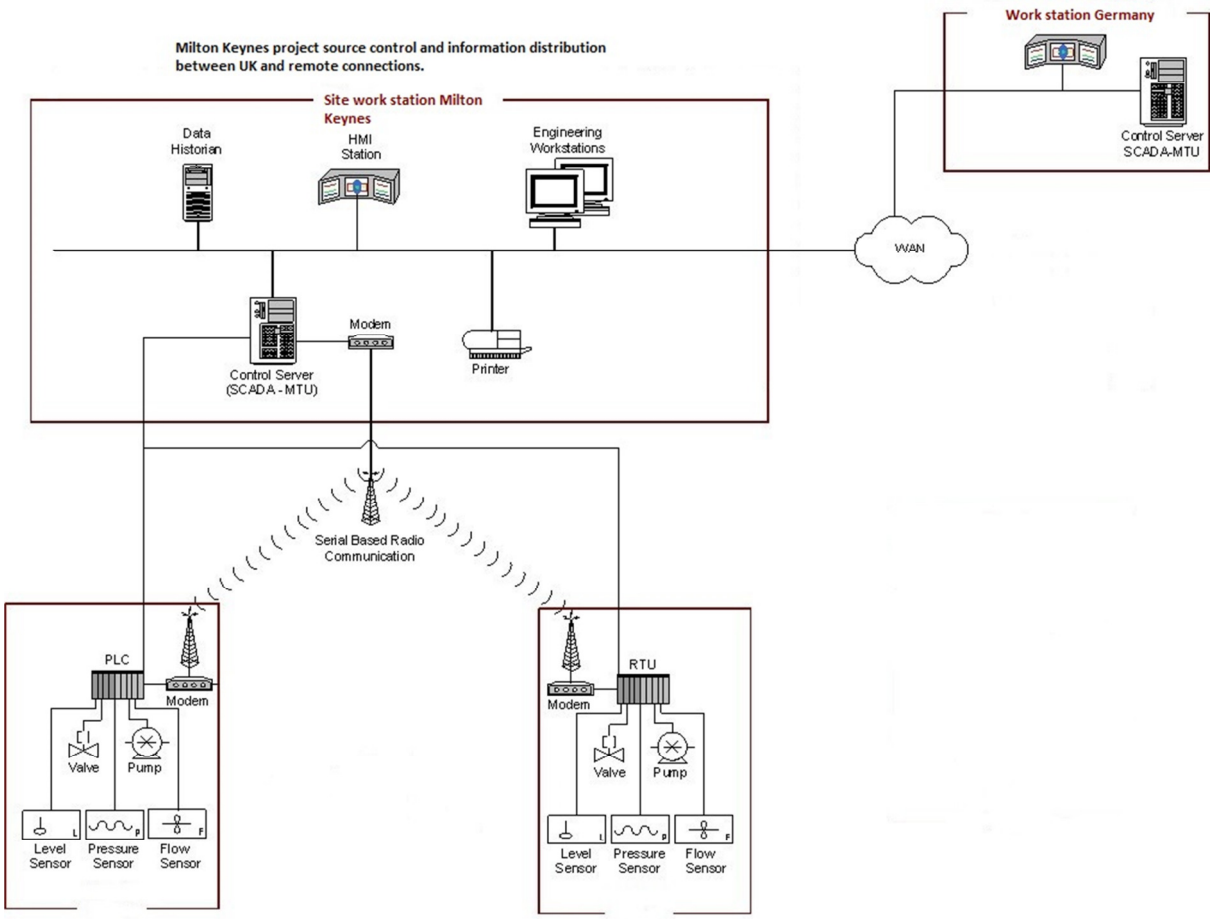


Fig 7

Control assets, execute write back commands to send new data point values from the HMI or relayed back from the system architecture back to the field devices. It can receive Alarms and view notifications of potentially threatening situations in the operation. The control benefits SCADA software has more than other IT automation programmes, is its increased response to potential equipment problems and take corrective action quickly and more efficiently. Raise awareness and improve communication by making field data available to anyone in the organization requiring access to it. Developing more accurate and consistent reporting with improved data collection and display.

Chapter 6: Security

Security threats to the control systems can come from numerous sources, including adversarial sources. Disgruntled employees, malicious intruders, and natural human errors and accidents and equipment failures. To protect against adversarial threats it is necessary to create a defensive in depth strategy for the program.

6.1 Understand the Business Risk

The first step in improving the security of process control systems is to gain a thorough understanding of the business risk in the context of electronic security. Business risk is a function of threats, impacts and vulnerabilities. Only with a good knowledge of the business risk can an organisation make informed decisions on what should be the appropriate levels of security protection.

6.2 Implement Secure Architecture

Designing a secure architecture for a control system can be a difficult exercise as there are so many different types of systems in existence and so many possible solutions, some of which might not be appropriate for the process control environment. Given limited resources it is important that the selection process ensures that the level of protection is commensurate with the business risk and does not rely on one single security measure for its defence.

6.3 Firewall deployment for SCADA and process control networks

This guide documents the pros and cons of architectures used to separate the SCADA and process control network from the Enterprise network. These range from hosts with dual network interface cards to multi-tiered combinations using firewalls, switches and routers.

6.4 Establish Response Capabilities

The capability to respond to both alerts and incidents is an important part of a process control security framework. Obtaining management support, determining responsibilities, establishing communication channels, drafting policies, and procedures, identifying pre-defined actions, providing suitable training and exercising the whole process prior to incidents enables a quick, effective and appropriate response which can minimise the business impacts and their cost, possibly avoiding such incidents taking place in the future.

6.5 Improve Awareness and Skills

Raising awareness is potentially the single most valuable action in the ongoing task of process control security. Raising awareness endeavours to ensure all relevant personnel have sufficient knowledge of process control system security and the potential business impact of lapses in security. Personnel need to know what to do to prevent attacks and what to do in the event of an incident.

6.6 Manage Third Party Risk

The security of an organisation's process control systems can be put at significant risk by third parties, e.g. vendors, support organisation and other links in the supply chain, and therefore warrants considerable attention. Technologies that allow greater interconnectivity, such as dial-up access or the internet, bring new threats from outside of the organisation. Third parties must therefore be engaged as part of the process control security programme and steps should be taken to reduce the associated risk.

6.7 Engage Projects

Process control systems are usually installed with an expectation of a long service life and minimal changes to these systems during their lifetime. However saying this for all control systems in use is probably an over generalisation. In many organisations there are often a number of process control system related projects underway at any point in time, any of which could have security implications.

An important aspect to manage during the life cycle of a SCADA system is the implementation of all security features proposed by SCADA vendors, in the form of updates or product patches.

Personnel in charge of SCADA maintenance and installation must be aware of the features enabled for their systems, and must be able to properly configure them. In many cases, it has been observed that newer SCADAs are deployed with basic security features, disabling security settings to ensure ease of installation, and to provide maximum usability.

SCADA users must be aware of the necessity of security features are mandatory to provide the maximum level of security and robustness of systems. Also, in these cases it’s suggested that careful risk assessment of the consequences of reducing all the security features is needed. This is where one must revert back to the Project Charter as discussed in chapter 3.

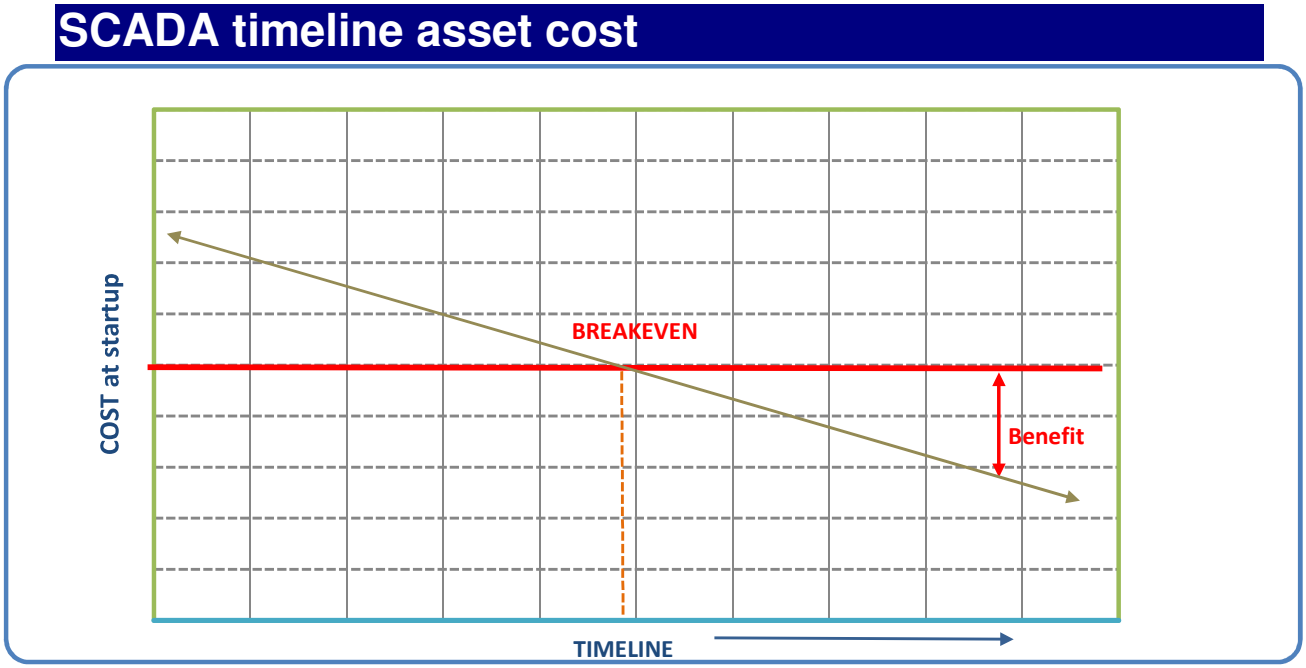
Chapter 7 Cost

The more complex or vast communication choices required by the end users will have, a substantial impact on the cost. Primarily the obvious choice without going into great detail is for the process plant to operate seamlessly without downtime this needs consideration when analysing the cost.

The big benefit of SCADA is that operators can extract much more data from programmable controllers. PLC totals all flows in the plant, data is easily retrievable by an operator at his desk. And to give operators information on when to change day units, the PLC also calculates motor run times.

In addition, programmable controllers monitor many more alarms, rather than manual checks. These alarms might be triggered by high level or low pressure switches. They might also be set off by a pump's failure to start or a valve not closing. The PLCs give operators an early warning that something has gone wrong - before the process can be impaired by a system failure.

While SCADA systems are costly - in terms of equipment, software, and operator education - savings in plant operation are significant enough to justify the expense in most cases.



A reduction of SCADA cost over time makes the initial use of it feasible

Chapter 8 The future

The adaptation of open community in the 90's offered a myriad of SCADA component choices. Integration server, prices dropped for instrumentation and computers. Cellular emergence, satellite and communication options now provides a new means of connecting to remote, restricted or uninhabitable locations.

As new communication systems continue to evolve the choices that owners and investors have become more affluent and affordable. The longer term plan is for interconnecting autonomous plants into a centralised management and or a decentralised control paradigm. This provides a platform to reduce on micromanagement and operatives. This *'mothership'* approach will be further increased by the further evolution of telemetry devises.

8.1 Industrial trends

On a summation of the generations we can acknowledge that

1. The incremental cost to expand it capabilities to additional assets is decreasing
2. The amount of data being gathered in increasing
3. Basic logic control is becoming decoupled from the operator, thereby reducing the importance of the HMI component of the software

8.2 Importance of upgrading Legacy Systems

Legacy systems are those which are continue to be used despite relatively poor performance and compatibility. For those the increased adaptability and flexibility of new computer hardware and software offers an opportunity for organisations. As major advancements are made in the IT sector, legacy systems are more vunerable to attacks. 3rd generation systems that operate without proper firewalls can lead to catastrophic effects. A typical legacy system may use a leased dial up line for communication, isolating it out the open and unprotected from cyber-attacks. It's common for legacy systems having been in operation for many years to be assumed safe, the *''long standing'* notion.

Conclusion

As the costs are expected to decline into the future. Simultaneously larger organisations will seek to use the software across all operational spectrums functioning as more of a large control group, able to operate autonomously at increasingly higher levels based on fewer inputs from operational personnel. A myriad of methodologies will be programmed into the software allowing organisations to develop and introduce larger SCADA systems without incurring unreasonable additional or staffing costs. The value of a pure HMI component of SCADA software as we know today will decline relative to the many other emerging benefits SCADA will offer. The overall benefits to install such IT within an organisation reap huge benefits maximising the processes within the plant and allowing for expansion.

LIST OF ABBREVIATIONS

BOK	Bodies of Knowledge
DMAIC	Define, Measure, Analise, Improve, Control
DCS	Distributed Control System
GPS	Gloobal Positioning Sattelite
HMI	Human Interface Machine
IED	Intelligent Electrical Devise
IO	Input/Output
LAN	Local Area Network
LCC	Local Control Centre
MRO	Maintenance Repair Operation
MTU	Master Terminal Unit
PLC	Programmable Logic Controller
SCADA	Supervisotry Control And Data Aquisition

Bibliography/References

1. Sinclair, Hassan *'An Intrusion detection system for Supervisory Control and Data Acquisition'*. 2001 Information Security Institute and Faculty of Information Technology, Brisbane, Australia.
2. Tracy Amaio PH.D *'How to protecy serial comunications'* 2011 SEQIM. Inc
3. Blair P. Sooley. *'The future of SCADA'* May 2011 white paper. Florida Water Resources Journal.
4. Motorola *'Wireless Communications for SCADA Systems'* BCWWA 2008
5. Keith Stouffer, Joe Falco, Karen Kent *'Guide to Supervisory Control, Data Aquistion and Industrial Systems Security'* National Institue of Standards and Technology. US department of Commerce September 2006
6. Meha Garg 'SCADA software architecture' Dept. of Computer Science and Engineering, Florida 2008
7. http://resources.infosecinstitute.com/improving-scada-system-security/
8. http://www.nsa.gov/ia/_files/factsheets/scada_factsheet.pdf
9. https://www.dhs.gov/sites/default/files/publications/csd-nist-guidetosupervisoryanddataccquisition-scadaandindustrialcontrolsystemssecurity-2007.pdf

10. http://www.schneider-electric.co.uk/sites/uk/en/products-services/services/solutions/power-management/pcmd.page