University of Southern Queensland
Faculty of Engineering and Surveying

Implementing Industry Best Practice Alarm Management

A dissertation submitted by
Daniel Snelgar

In fulfilment of the requirements of
Courses ENG4111 and 4112 Research Project

Towards the degree of
Bachelor of Engineering (Electrical and Electronic)

Submitted: October 2015

Abstract

This dissertation investigates how alarm management practices can be implemented at a large industrial facility, and what effect this could have on alarm system performance. Poor performing alarm systems create an environment where alarms of high importance can be missed or operators are desensitised to the alarm system. Alarm system performance has been a factor in several high consequence industrial accidents.

The project was conducted at a large coal fired power plant which uses modern Process Control and Human Machine Interface systems. The project site has never employed any alarm management practices in the past and is seeking to implement alarm management practices based on *ISA-18.2-2009 Management of Alarm Systems for the Process Industries.*

The requirements of industry best practice alarm management were researched and identified. Alarm management processes were created and adopted by the project site. New software tools were developed to support the alarm management processes.

The alarm system performance at the project site was measured using these software tools. The worst performing alarms over a six month period were identified. By investigating the causes of the worst performing alarms improvements were identified that could reduce the alarm rate by 40%.

Disclaimer

University of Southern Queensland
Faculty of Health, Engineering and Sciences

ENG4111 & ENG4112 *Research Project*

Limitations of Use

Certification

I certify that the ideas, designs and experimental work, results, analyses and conclusions set out in this dissertation are entirely my own effort, except where otherwise indicated and acknowledged.

I further certify that the work is original and has not been previously submitted for assessment in any other course or institution, except where specifically stated.

Daniel Snelgar
Student Number: 0050022704

___________________________ (Signature)

29th October 2015 (Date)

Acknowledgements

I would like to acknowledge the project site (who have requested to remain unnamed for commercial reasons) for opportunity to conduct this research project at their facility. Particularly the engineering staff that me gave access to their systems and gave their time to support the project.

I would especially like to thank my wife, Kristy, as without her support I could not have embarked, and completed, the journey to complete a four year Bachelor degree program while we both worked full-time and raised a family.

Contents

List of Figures

List of Tables

Chapter 1 – Introduction

1.1. The Worst Case Scenario

"He was blasted into the air, struck a solid object with his head and hit the ground with liquid, dirt and stones pelting him at high velocity. He felt as if he were being shot at by a machine gun. Wherever he crawled he continued to get pelted. He smelt nothing because he was holding his breath. Eventually he saw a glimmer of light and crawled in that direction. He must have come out from behind something that was sheltering him, because he was rolled over and again exposed to the blast. He had his eyes closed. He crawled into the clear and noticed two other blackened persons crawling towards the control room. Blood was flowing from an injured eye. He glanced over his shoulder and saw white vapour everywhere. GP905 had been skewed at an angle and there was still a loud roar of vapour and liquid" (Longford Royal Commission, 1999).

Figure 1 – Photo of explosion at the Longford facility (Longford Royal Commission, 1999)

This is the moment a plant disturbance turned into an industrial accident at the Longford gas plant in Victoria, Australia in 1998. This is the extreme case of what can go wrong. Perrow describes normal accidents as "rare but inevitable in interactively complex, tightly coupled systems. Some complex systems with catastrophic potential are just too dangerous to exist, not because we do not want to make them safe, but because, as so much experience has shown, we simply cannot" (Perrow, 2011).

This appeared to be case for the nuclear power industry as a result of the Fukushima nuclear incident in 2011 on which Perrow bases his paper. A year after the disaster all but two of Japan's nuclear reactors had been shut down due to fears of nuclear power.

In 2015 there are now 24 reactors in the process of seeking approval to restart (World Nuclear Association, 2015).

The nature of industrial processes means that there are hazards to be controlled. The nuclear power industry has radiation and heat, which if not controlled can melt reactors and contaminate the environment with radioactive material. The hydrocarbon industry processes highly flammable materials which can explode if not contained. Pesticide manufacturing involves handing poisonous chemicals. Accidents occur when control of hazards is lost. The results can be catastrophic.

1.2. Automation and Control in the Process Industry

The process industry is concerned with the transformation of raw products into more complex products. This is achieved by the transfer of mass or energy or the reaction of chemicals to combine or separate raw products. Industrial processes usually consist of a complex arrangement of tanks, vessels, and other fixed equipment such as mixers, heat exchangers and furnaces. Materials are moved throughout the process with machinery such as pumps, valves, compressors and material conveying systems. Examples of industrial processes are oil and petroleum refining, natural gas processing, fertiliser and pesticide manufacturing, chemical manufacturing and in the case of the project site, large scale power generation.

Industrial processes are controlled using automation and control technologies. Sensors measure process conditions and send signals to a control system. The control system determines what actions to take to regulate the process and sends signals to control elements. Control systems have evolved from mechanical systems to microprocessor based computer systems such as a Distributed Control Systems (DCS) or Programmable Logic Controllers (PLC's).

Figure 2 – Early (left) and modern (right) central control room

Personnel who supervise and control industrial processes are call operators. Most often they work from centralised control rooms. Operators interact with the process using a Human Machine Interface (HMI). *Figure 2* shows and early control room to the left and modern control room to the right. The early control room comprises of panels with gauges, dials, lights and buttons, each in a fixed position on the panel. The modern control room features multiple computers systems with a graphical user interface. This control room also has a large display monitor giving and overview of the whole process.

Automation and control is designed to keep a process conditions on target or within normal operating conditions. Upsets or abnormal situations can arise where the process exceeds normal operating conditions. This can result in a loss of product quality, an interruption to production, or worse, the loss of assets or human lives due to catastrophic failures.

When the automation cannot keep the processes at the target or in normal operating conditions operators are alerted to the abnormal situation by alarms. This alerts the operator of the abnormal situation such that they can take action to return the process to normal conditions. If the exceedance continues automated supervisory actions may intervene and shut down the process. *Figure 3* shows the relationship between the control system, the operator and the process conditions.

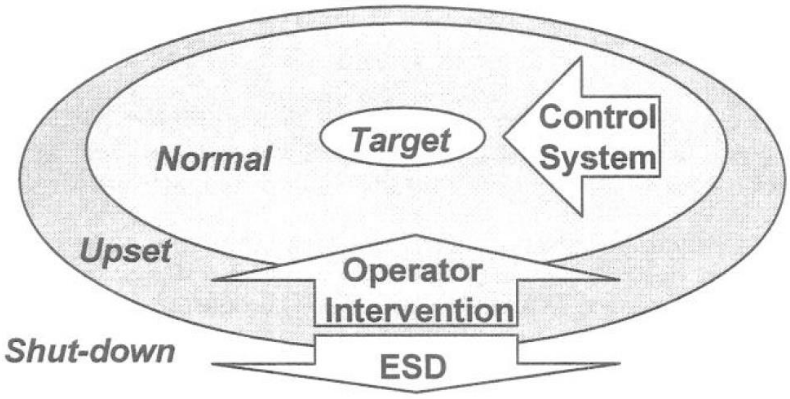


Figure 3 – Relationship between Control System, Operator and the Process (EEMUA, 2007)

1.3. The Alarm Problem

Early alarm systems comprised of panels that had individual indicators for each alarm. The number of alarms was limited to the physical space available to install the indicators and the cost to construct it. There may have been only one to two hundred different alarms in a control room. The advent of modern computer based HMI systems meant the cost and effort of adding new alarms reduced significantly. All that was required was some simple software configuration and a new alarm could be implemented. As the cost and effort was low there was a tendency to add alarms 'just in case' or for 'information only'. It was thought that adding an alarm made the plant safer. Modern industrial facilities now may have many thousands of configured alarms. *Figure 4* shows the growth of configured alarms at industrial facilities.

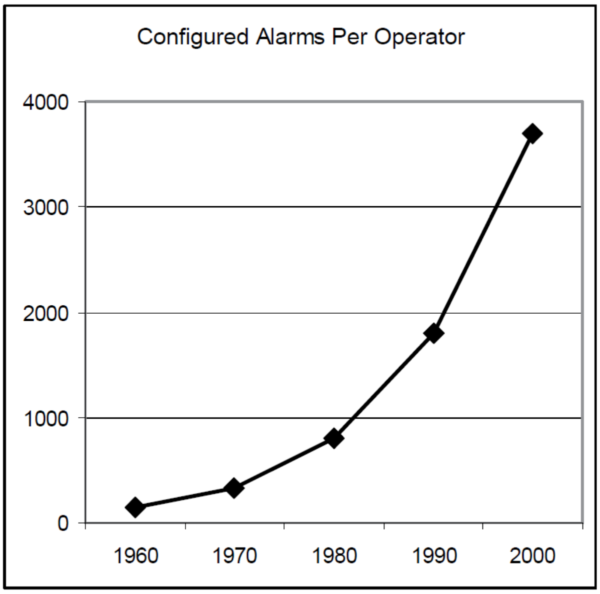


Figure 4 – Growth of Alarms *(Hollifield & Habibi, 2001)*

All of the configured alarms do not create a problem on their own. The problem occurs when alarms activate. Each alarm requires the operator to identify the cause, decide what action to take, then take the action and monitor the process response. This takes time, which means there is a finite number of alarms an operator can effectively manage over period of time. This is where the problem begins – operators receiving more alarms that they can effectively manage.

For large industrial facility there are usually many different contractors and vendors that supply and construct the subsystems that make up the total plant. Each of the contractors and vendors are responsible for identifying the alarm requirements for their subsystem. There is usually no common approach across all of the contractors and vendors and the plant owner or end user also has limited involvement. Many alarms are added for information only while others are added as it thought to be safer and more conservative to add an alarm.

Once the facility is begins commercial operation the alarm system is normally not maintained to any performance standard. Alarms are usually added as a result of learnings of incidents that occur at the facility site over time. Learning from past events is a sound practice but there is often no consistent methodology employed to implement new alarms.

Operators begin to mask alarms mentally – they learn that specific alarms have in the past not lead to undesirable consequences so they may be ignored. They also learn some of the key alarms to look out for – these are alarms that occur regularly and have led to undesirable consequences in past if ignored.

From time to time some alarms activate and de-activate at high rates, taking over the alarm system. This can go on for hours and some time event days. This is tolerated as by now the alarm system is not seen as an overly useful tool anyway.

This is most common scenario for an alarm system that pre-dates industry best practice. In Australia some industry sectors apply industry best practice alarm management, while some specific organisations have also embraced it. For some facilities a lack of good alarm management practices still continues to a problem.

The solution to the alarm problem is not singular. What is required is an array of technical solutions and pragmatic work practices – something that is right at home to a professional engineer.

1.4. Project Summary

The aim of this project was to develop and implement systems and tools such that project site could sustain industry best practice alarm management practices. The project was conducted at one of Western Australia's largest coal fired power plants. For commercial reasons the project site has requested to remain unnamed. Also note that the author is not currently employed by, or part of any commercial relationship with the project site.

The project site uses modern automation technologies and HMI systems similar to those described in current industry best practice alarm management guidelines and standards. The project site has never employed any alarm management practices. It is known that the alarm performance at the site exceeds current industry best practice metrics, thought the full extend was unknown.

Unbeknown to the author at the time of negotiating the nature and scope of the project the project site received a corporate engineering directive stating they are to implement an alarm management practices based on *ISA-18.2-2009.* The project site is relying on this project to initiate its compliance with the engineering directive.

Background information on modern control systems is firstly presented. The research aspects of the project included past industrial accidents that have elements of alarm management in their causes, the development of alarm management guides and standards and current industry best practice for alarm management.

Based on the research of current industry best practice for alarm management an alarm management procedure was created for the project site – the 'Alarm Philosophy'. Some of the requirements of the Alarm Philosophy could not be met by the functional capabilities of project site's control system infrastructure – a 'Master Alarm Database' and 'Alarm Reporting Tool'. Software engineering techniques were used to develop these functional capabilities.

The worst performing alarms for the first six months of the year were identified. Case Studies were performed using a systems integration engineering approach. The predicted improvement to the alarm performance based on the results of the case studies is presented.

1.5. Abbreviations

ANSI	American National Standards Institute
ASCII	American Standard Code for Information Interchange
ASM	Abnormal Situation Management (as in ASM Consortium)
DCS	Distributive Control System
EEMUA	the Engineering Equipment and Material User Association
HMI	Human Machine Interface. A computer system were
HSE UK	Health and Safety Executive of the United Kingdom
IEC	International Electrotechnical Commission
ISA	International Society of Automation
SQL	Structured Query Language
TCP/IP	Transmission Control Protocol / Internet Protocol
UTC	Coordinated Universal Time
VBA	Visual Basic for Applications

Chapter 2 – Modern Process Control Equipment

A control system is “a system that responds to input signals from the equipment under control and/or from and operator and generates output signals that cause the equipment under control to operate in the desired manner” (ISA, 2009).

The modern control system is an industrial computer system. It comprises of both hardware and software to perform automation and control. The control system also provides an interface for operators to monitor and intervene when required. An operator’s role can vary depending on the size of the plant and the complexity of the automation implemented in the control system. The level of automation can be simple where operators have to determine when to control individual pieces of equipment, or it may be complex and all-encompassing where an operator’s main role is monitoring and supervision of the process.

The project site uses a DCS as its control system. The following provides a simplified description of how automation and control is implemented in a modern DCS system. In most cases the description is applicable to most DCS’s though some of the specific features and terminology of the project site’s DCS are used.

2.1. Field Equipment

Field equipment can be generally classed as measurements or drives. Measurements and drives interface to the control system using an Input / Output (I/O) interface. This is where there is a physical connection to the control system using wires. This enables electrical and electronic signals to be exchanged between the control system and the field equipment. The equipment must be chosen and configured correctly to ensure that the signals are compatible with the I/O interface. Wireless technology is also beginning to find its way into industrial automation and control.

2.1.1. Measurements

Measurements devices read the value of process variables. Process variables can include the temperature or flow rate of gasses, fluids or materials; the pressure, level or mass of a fluid or material in a tank or vessel; the chemical properties of a liquid such as pH or conductivity; the concentration of a particular component molecule in a gas. Process variables can also include the physical position or status of equipment or machinery such as a valve open, a pump running or an actuator arm extended.

Measurement devices are considered to be either ‘analog’ or ‘digital’. These terms are legacy in nature and do reflect the way the signals are processed – being a computer system all signals are digitised. The term ‘analog’ refers to values that are continuous. They may take on any value within the resolution of an analogue to digital conversion or the floating point representation of the process variable. The term ‘digital’ refers to values that are discrete. It has a set of particular values which normally reflect a state such as On or Off, Open or Closed.

‘Analog’ measurement devices are often called transmitters. A single transmitter is designed to read one specific type of process variable and transmit this value to the control system in real time. Most transmitters use a sensing element that changes its physical properties or reacts in a known way when exposed to the process. The transmitter then uses electronics, which may also be microprocessor based, to measure the response. An example is a pressure transmitter where the pressure in the process exerts force on a measuring cell. The force on the measuring cell causes capacitance of the measuring cell to change. The electronics in the transmitter measure the change in capacitance and convert this to a value that is in pressure units.

The transmission of the process variable from the transmitter to the control system is normally via an analogue electrical current or voltage signal over wires. The I/O interface performs an analogue to digital conversion of the electrical signal, upon which the process variable is available for use by control algorithms in the control system. More modern transmitters may also use a serial communications interface to transmit process variables to the control system as a floating point numbers.

'Digital' measurement devices are essentially switches. They may be used to measure the physical position of piece of equipment, the status of a machine or other plant subsystem, or the position of an operator push button or selector switch. They may also be used determine if a process variable in within a predetermined limit. Such an example is a pressure switch. Pressure in the process acts on a diaphragm within the switch. When the pressure in the process reaches a pre-determined value deflection of the diaphragm operates a mechanical switch. It is now not uncommon for modern process switches to use similar technology as a transmitter. Instead of transmitting a continuous value the electronics operates a switch when the process value goes beyond a pre-determined limit.

A 'digital' measurement device is wired in an electrical circuit with the I/O interface. By supplying voltage to the switch and measuring electrical current the I/O interface can determine if the switch is open or closed. When the switch is open no current will flow through the circuit. When the switch is closed current will flow through the circuit. The I/O interface assigns a binary value of '0' to an open switch and a binary value of '1' to a closed switch. Within the control system the user is able to assign meaningful text to state of the binary value. In the case of the pressure measurement a binary value of '1' can be assigned the state of pressure HIGH and binary value of '0' can be assigned to the state of pressure NOT HIGH.

Figure 5 shows some typical measurement devices. In the fore ground the two blue devices are pressure transmitters. The process connection is via a small pipe to the main process pipe. The measuring cell is at the base of the transmitter. To the right of the pressure transmitters the white devices are temperature transmitters. A temperature probe extends into the main process pipe.

Figure 5 – Typical measurement devices

2.1.2. Drives

Drives are the final control elements in the process cause the equipment under control to operate in the desired manner. Drives include motor driven equipment such as pumps and conveyors which move materials through the process; valves and dampers which control the flow of materials; electrical switches which control high voltage or high current devices; or audible and visual indicators. Like measurement devices, drives can be considered to be either ‘analog’ or ‘digital’.

‘Digital’ drives are drives that have discrete states. For example, a motor may be running or stopped. A valve may be open or closed. A ‘digital’ drive can operated manually by an operator or automatically as part of a simple on-off feedback control algorithm or a complex sequence that controls many final elements.

The control system’s I/O interface issues commands to the drive by operating ‘digital’ outputs. The ‘digital’ output is normally an electromagnetic relay or a solid state electronic switch. The closing of the switch sends electrical current to the drive. The amount of current the I/O interface can deliver is relatively small. It does not have enough power to directly control a ‘digital’ drive. Pilot devices control other energy sources which operate the drive. For a motor drive the pilot device is an electromagnetic relay which in turn activates a larger electromagnetic relay that controls the flow of electric power to the motor. For a valve the pilot device is an electromagnetic operated solenoid valve. When the solenoid valve is activated it routes compressed air to a pneumatic actuator, which in turn provides mechanical energy to drive a valve to the required position.

It is normal practice to monitor the status of a drive as a measurement in the control system. For a motor an auxiliary switch on the main electromagnetic relay is used to determine if it is running. For a valve a position switches connected to the shaft of the valve can be used to determine its position. The control system can use the status measurements to detect discrepancies between the commanded stated and the actual state. Discrepancies occur if a device fails to move when commanded, or if there is a malfunction in the drive that causes an unexpected change from the commanded state.

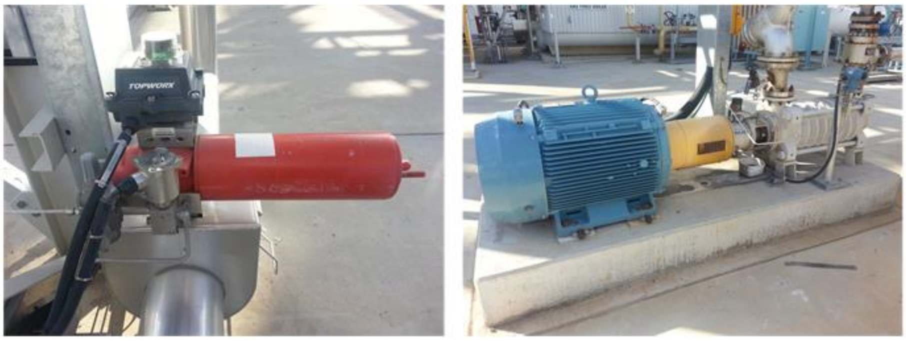


Figure 6 – Typical 'digital' drives

Figure 6 shows some typical 'digital' drives. On the left is a pneumatic operated on-off valve. The red object is the pneumatic actuator which provides motive force to turn the valve shaft through 90 degrees, which in turn opens and closes the valve. Note that this valve in encased in thermal insulation directly below the actuator and cannot be seen. The solenoid valve which controls the supply of pneumatic air is mounted in front of the actuator. Mounted on top of the actuator is a box that contains switches to detect when the valve is in the closed or open position. On the right is a motor driven pump. The supply of electrical power to the motor is from a centralised switchboard where the electromagnetic relays can switch electrical power to the motor.

'Analog' drives are special drives that can operate over a continuous range of positions. They are normally used in regulatory control. 'Analog' drives require specific hardware to operate and cannot easily be adapted from 'digital' drives. To control the speed of a motor specially designed power electronics are required to adjust the frequency of the motor supply voltage. For a valve special positioning hardware is required. It uses the valve shaft travel position to adjust the amount of compressed air pressure in the valve's pneumatic actuator, and hence its position.

Figure 7 shows typical 'analog' drives. On left is a control valve. The mechanical components that regulate the flow of material are inside the valve body which is directly in line with the pipework. Above the valve body is the positioning hardware and the pneumatic actuator is at the top. On the right is an air duct with a louver damper inside. This uses a pneumatic ram and levers to provide the turning force to position the louvers. The black box with three gauges the positioning hardware.

Figure 7 – Typical 'analog' drives

2.2. DCS Infrastructure

The DCS is an industrial computer system. The user develops application software to perform the automation and control to suit the process. The software is loaded into DCS controllers where it controls the process in real time.

2.2.1. DCS Controller Hardware

Control systems must provide high availability and reliability. Hardware failures or system crashes may result in lost production and can be very costly for plant owners. The firmware within the controllers is designed to operate in very controlled manner where resourcing of CPU and memory is tightly controlled. This ensures continuous operation over many years without system crashes. The construction of the DCS hardware is usually more robust than that of consumer electronics. The DCS hardware is designed to last for well over a decade.

Failures do occur so here are several methods employed to ensure availability. One method is the use of a dual redundant controller. This is where a secondary controller is loaded with the same application software as the primary controller. If the primary controller fails the secondary controller immediately takes over control. The failed controller can then be replaced while the secondary controller is active. The method employed at the project site is to distribute the control software in many (100's) small controllers. The failure of a single controller only represents a very small portion of the plant and it is likely that the failure will not result in a loss of production.

Control systems are designed to be scalable. This makes them suitable for use in small process plants and very large plants. The number of I/O signals can range from hundreds to tens of thousands. Apart from processing power and memory one if the limiting factors of a controller is the number of I/O signals that it can handle. In a medium sized plant is likely that more than one controller will be required for all of the automation and control tasks. This requires an effective inter-controller communications system. The inter-controller communications must also provide high availability and reliability to avoid costly down time in the case of a hardware failure.

Control system vendors originally developed their own serial communications network hardware and protocols. The networks are normally arranged in redundant pairs. This ensures that the network is always available in the case of a network failure.

Modern control systems are now employing Ethernet TCP/IP communications networks for inter-controller communications. The traffic on these networks is still tightly controlled and not mixed with general day to day business networks. Although Ethernet TCP/IP is not deterministic, by managing traffic and bandwidth it has proven to be suitable for process control and automation. The Ethernet TCP/IP networks are still arranged in redundant pairs to ensure that the network is always available in the case of a hardware failure.

Many control system vendors are now also using common communications protocols on Ethernet TCP/IP communications networks. Object Linking and Embedding (OLE) was developed by Microsoft to allow software developers to link data between software applications. This has been used in the industrial automation industry. OLE for Process Control (OPC) is an extension of OLE technology. Devices such as controllers may run as an OPC server and allow an OPC client to access data within controller.

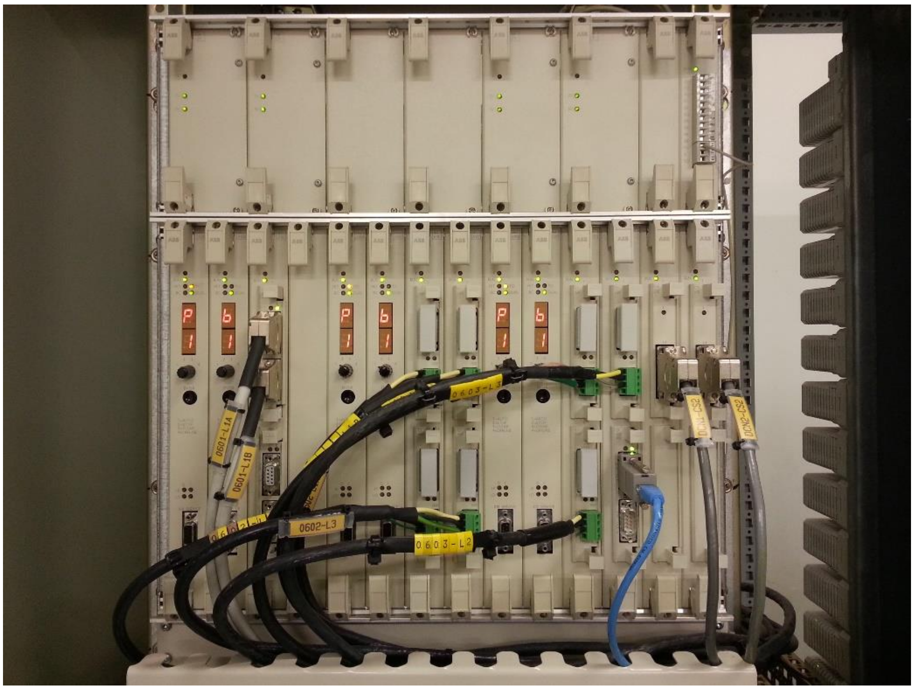


Figure 8 – Rack mounted DCS controllers

Figure 8 shows a rack mount DCS controller system. The rack contains three pairs of redundant controllers. The controllers are the cards with seven segment LED display. ‘P1’ are the active controllers, ‘b1’ are the backup or standby controllers. To the extreme right are two inter-controller network interface cards. In the top section of the rack are four redundant power supply cards.

Figure 9 – Backplane mounted DCS controllers

Figure 9 shows a backplane mounted DCS Controller system. The two cards to the very left are a power supply card and DCS controller pair. The next two cards are a backup power supply and DCS controller. Each controller has two Ethernet TCP/IP RJ45 network connections on the bottom to connect to the inter-controller network.

2.2.2. DCS I/O Interface

The functionality of the I/O interface was described in Section 2.1. This section will expand on the hardware and how it relates to the DCS controllers. The hardware for the I/O interface can be arranged in several ways. The traditional method is used a single circuit board or card assembly for each type of I/O – ‘analog’ input card; ‘analog’ output card; ‘digital’ input card; and ‘digital’ output card. The number of I/O points on each card is normally eight, sixteen or 32. The cards have terminals where the physical wiring to the field equipment can be connected. In *Figure 9*, to the right of the power supplies and DCS controllers are local mounted I/O cards.

The I/O interface may also be located remote to the controllers. This type of configuration requires special I/O controllers at the DCS controller and the remote I/O interface. The two I/O controllers are then connected with a dedicated serial communications network. Refer back to *Figure 8*, to the right of each controller are I/O controllers. *Figure 10* shows a group of remote I/O cards with an I/O controller at the top.

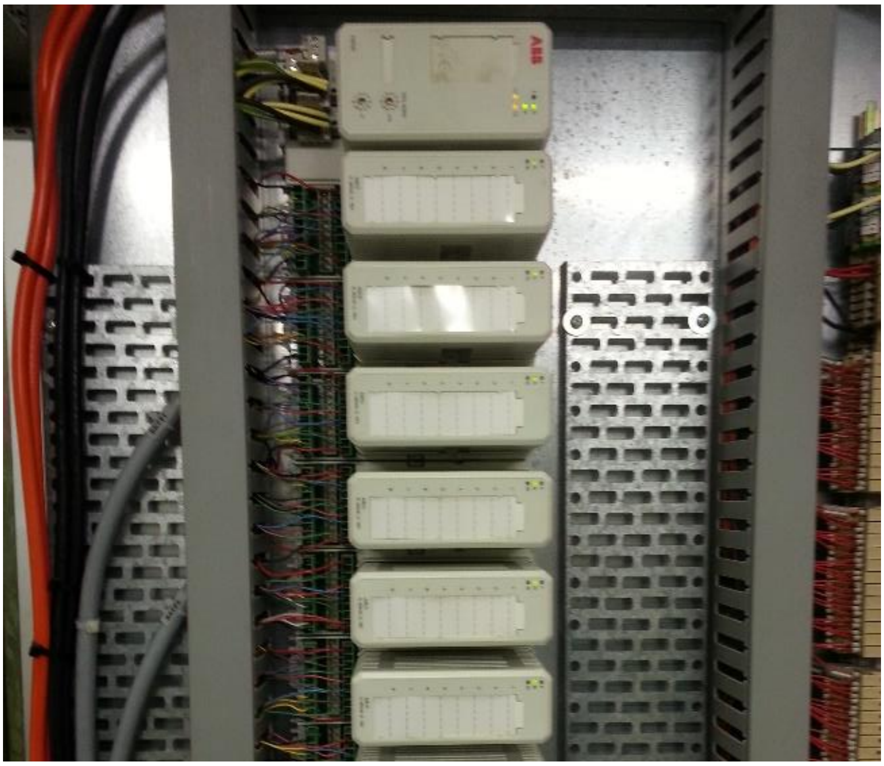


Figure 10 – DCS I/O Cards

2.2.3. Controller Software

The application software is what the user develops to effect the required automation and control tasks. It is a mixture of closed loop feedback control algorithms using both measurements and drives and the direct feedforward control of drives. Higher levels of automation can also be implemented using sequences where groups of drives are controlled at specific times or when measurements are at specific values. It is also possible to implement higher levels of control on closed loop feedback systems where target values are set by other closed loop feedback control algorithms.

Many variables can be created and manipulated by the application software. The concept of ‘analog’ and ‘digital’ signals still exists in the application software. ‘Analog’ values are used as real numbers and can be used in mathematical operations. ‘Digital’ values are used in Boolean operations. ‘Digital’ signals can be created from ‘analog’ signals by performing a comparison, i.e. is ‘analog’ value ‘A’ greater than ‘analog’ value ‘B’ – the result being either true of false. At the project site these are referred to as limit values. They are often used as alarms

The development of the application software is performed using engineering tools that are specially designed for the control system. The engineering tools are normally installed on a dedicated computer terminal. The terminal is permanently connected to the control system via the controller inter-communications network. This allows the application software to be loaded on to controllers when required. The terminal normally called an engineering station. Engineering stations developed from specially designed computer systems for this purpose only to personal computers with specific software to build and load the application software to the controllers.

Programming languages for industrial control systems have been specifically designed for automation and control tasks. The functionality mainly focuses on regulatory control, drive control, Boolean algebra, sequences to operate groups of equipment and mathematical operations. Most control system vendors have developed their own versions of programming languages. In 1993 an international standard was developed for programming languages – IEC 61131-3 Programmable controllers - Part 3: Programming languages (IEC, 2013). This standard identities Ladder Logic, Function Block, Structured Text, Instruction List as well Sequential Function Chart for sequences. Many control system vendors had input to this standard and the languages in standard captured much of what was already used. The project site uses Function Block and Sequential Function Chart languages which are closely aligned to this standard.

The application software is normally grouped based on specific automation and control tasks. The groupings are often called loops, functions or modules. The groupings represent the smallest block of code that can be individually programmed. Each block of code is given a unique name, or Tag.

Tags are normally alpha numeric strings that provide some clue to the purpose of the software grouping. ANSI/ISA-5.1-2009 Instrumentation Symbols and Identification (ISA, 2009) is widely used in industrial industries to designate Tag names for field equipment and software groupings in control systems. Within the power generation industry the KKS tagging system is widely adopted in power plants across the world. The KKS tagging system is administered by the VGA Group (VGA Group, 2015). The project site utilises the KKS tagging system for both physical equipment designation and the groupings of software code, which are referred to as Functions.

Normally the loops, functions or modules are further grouped into several hierarchal levels based on which plant subsystem, plant area and/or processing unit the software is associated with. The project site DCS further groups Functions into Function Groups and then plant areas.

2.3. Human Machine Interface

The HMI provides the means for operators to interact with the application software. The interface is a computer terminal with a graphical user interface. The terminal is normally called a HMI station. Similar to an engineering station, HMI stations developed from specially designed computer systems to personal computers with specific software for control and monitoring. Depending on the size of the plant it is possible that there may be many operators required to operate the plant. Each operator required a HMI station. These can be located in one central control room or in several control rooms spread throughout the plant. It is common for the HMI station to used multi monitor displays.

HMI stations are permanently connected to the control system via the controller inter-communications network. This enables real time data exchange between the HMI and the DCS controllers. The HMI system may also have a network connection to the engineering station. The engineering station is used to configure all of or parts of the HMI interface as it is closely aligned to the application software.

2.3.1. Graphical Displays

The most common method to present the interface to an operator is via graphical displays. There may be dozens to 100's of different graphical displays for a plant depending on its size. Each display is made up of shapes that depict specific areas of the plant. The shapes represent plant elements such as tanks, pipes and vessels. The layout of each graphic is such that it associates the graphic to either the physical layout of the plant, the flow of the process materials through the plant or the tasks an operator may be required to perform.

Interactive elements are added to the displays that represent measurements and drives. These elements provide real time indication of the value and status of the measurements and drives. By selecting these elements pop-up windows open displaying further information. These windows, often referred to as a Faceplate, provide the means to operate drives. Drives may be stopped or started, set points and control modes may be changed, sequences and higher level control algorithms may also be controlled.

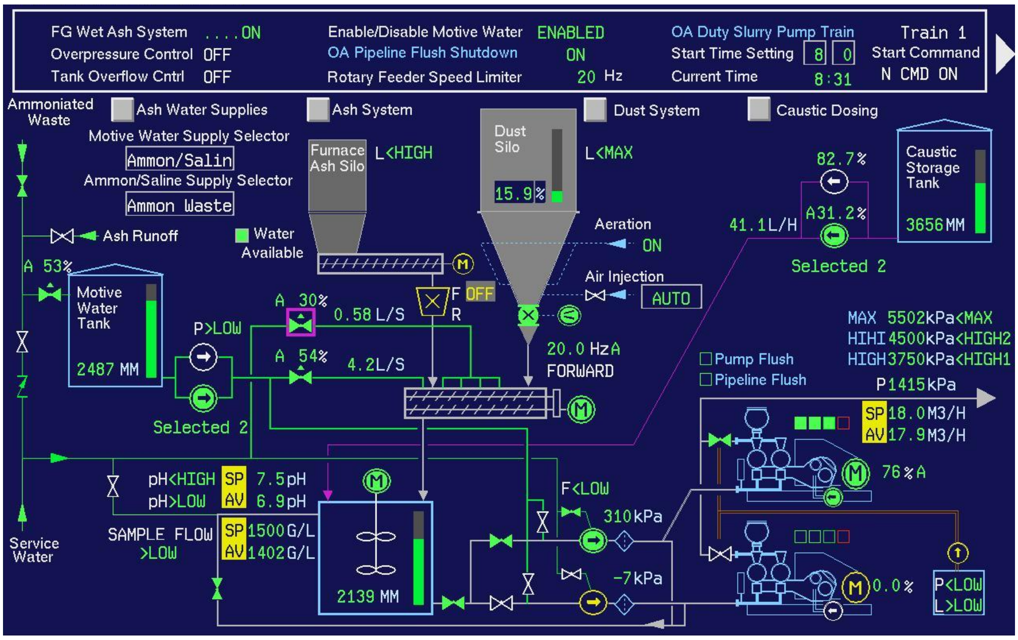


Figure 11 – Graphical display for plant area

The displays are normally grouped in a similar fashion to software groupings – using several hierarchal levels based on which plant subsystem, plant area and/or processing unit the display is associated with.

Figure 11 shows one of the graphical displays from the project site. Many interactive elements can be seen, such as the value of process variables and symbols representing drives. As an example a pump is depicted as a circle with an arrow inside. When highlighted white pump is off; when highlighted green the pump is running; and, when highlighted yellow the control system has detected a diagnostic fault with the pump. *Figure 12* shows the same graphic but with a Faceplate selected for a valve. The set point and control mode of the closed loop controller associated with this valve may be altered via the Faceplate

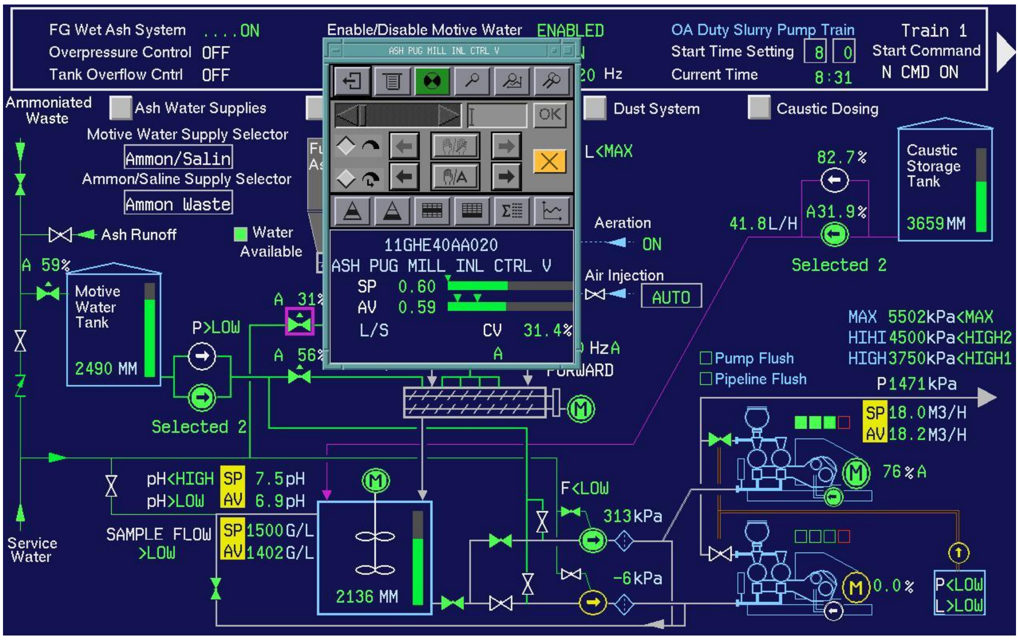


Figure 12 – Graphical display for plant area with pop-up Faceplate

2.3.2. Alarms and Events

In general an Alarm or Event is any 'digital' signal from the application software that is specifically selected for use in the HMI. Alarms and events are configured as part of the application software. Alarms are specific 'digital' signals that represent a condition that requires the operator's attention. Events are specific 'digital' signals that may be used to drive dynamic elements on graphical displays or their activation is to be recorded for review at a later stage. Events also include changes in the status of drives and any commands made by operators.

Alarms are assigned a priority. This provides guidance to operators when determining which alarm to respond when several are active. It is most comment to have either three priorities – Low, Medium or High, or four priorities – Low, Medium, High and Critical. A colour is also associated with each priority. The project site uses red for High priority alarms, orange for Medium priority alarms and yellow for Low priority alarms yellow. Priority colour schemes are typically user selectable on newer control systems.

There may also be specific priorities relating to diagnostic alarms. Diagnostics alarms include measurement signals that are outside of their configured range or drive discrepancy alarms. The diagnostic alarms do not require any configuration by the user. They are built into the control system when using measurements and drives in the application software.

When an alarm activates it is presented to an operator in several ways. Firstly elements on the HMI graphic display associated with the alarm may change to the priority colour. Secondly, alarms may produce an audible warning the operator. The tone or sound of the audible waring can be different for different priorities. Finally, an alarm list is provided. This is a list of every alarm activation. The list may be ordered based on chronological order of activation, the priority of the alarm, or a combination of other these and other attributes. The alarm list may be filtered to only present alarms from certain areas of the plant, or certain priories, or other attributes of the alarm.

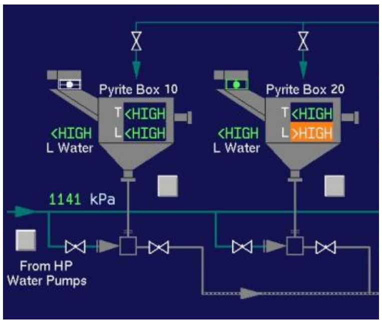


Figure 13 – Alarm on graphical display

Figure 13 shows how alarms are represented on graphical displays on the project site. Highlighted in orange is a priority 2 alarm associated with the level in the hopper. The alarm state or text associated with this 'digital' signal in the alarm state is '>HIGH'. To left there is another hopper where the high level alarm is not active. The text for the normal state is '<HIGH'.

Figure 14 shows the alarm list display at the project site. This list has been sorted by priority. In the top left hand corner the total number of active alarms for each priority is shown.

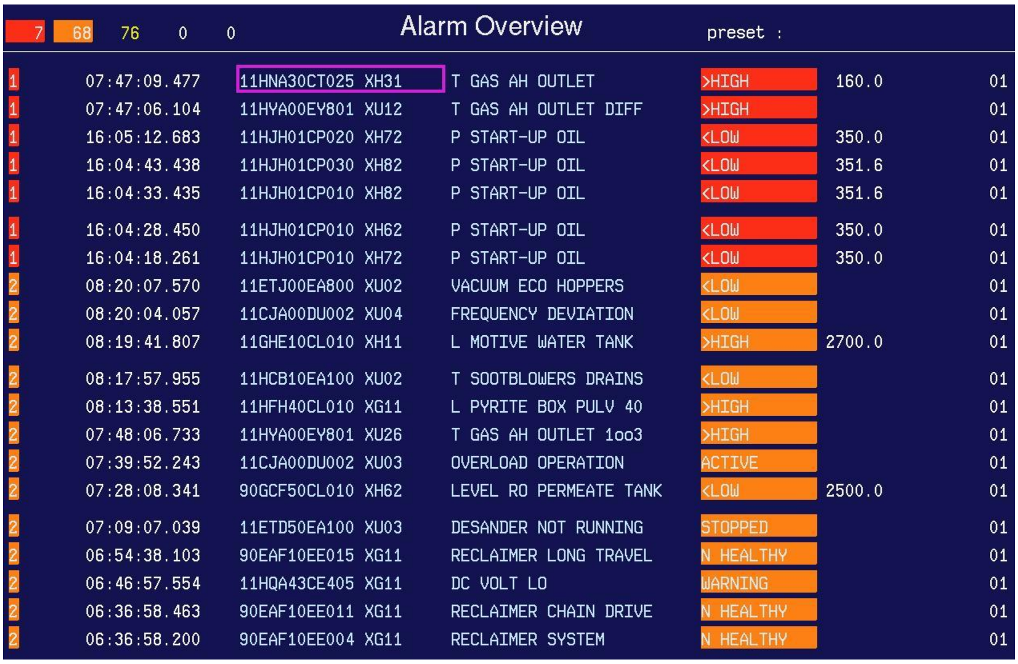


Figure 14 – Alarm List display

2.3.3. Alarm Handling

Within the application software an Alarm is either active or not active. On the HMI the alarm can have further attributes which affect how it is presented to an operator. Alarm handling describes how these attributes are handled. One of these attributes is the Acknowledgment. This is best described by explaining the alarm handling at the project site. When an alarm becomes active is considered to be active and not acknowledged. In this state the element on the HMI graphic flashes in the priority colour and the auditable alert is triggered. The alarm also appears on the HMI alarm list display with its alarm text flashing in the priority colour. When the operator acknowledges the alarm it is then considered to be active and acknowledged. The audible alert will silence and the element on the HMI graphic will hold steady in the priority colour. In the alarm list text will also hold steady in the priority colour.

Once the conditions that triggered the alarm have cleared the alarm will be considered non active. The element on the graphic will revert to its normal colour and the alarm will disappear from the alarm list. The project site also the possibility of masking the alarm. An alarm masking is a signal in the configured in the application software. If this signal is in an active state when the alarm actives the HMI will transition it directly to Active and Acknowledged.

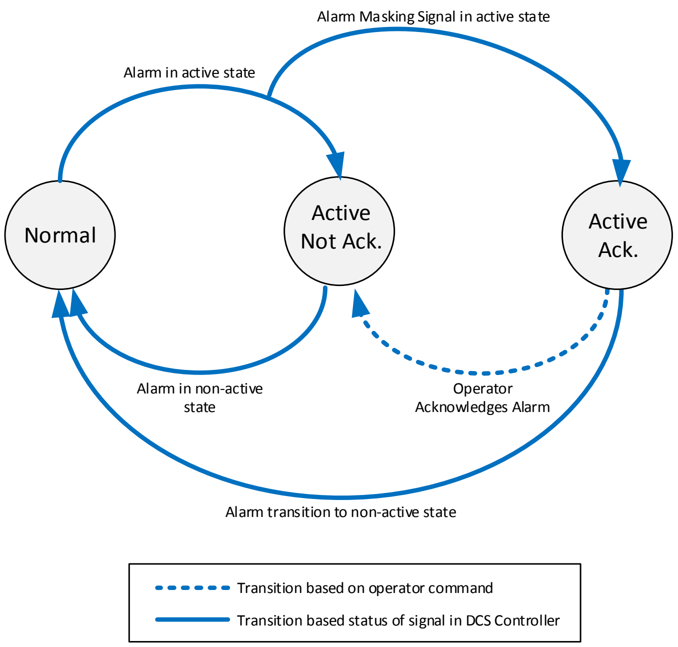


Figure 15 – Alarm Handling transition diagram for project site

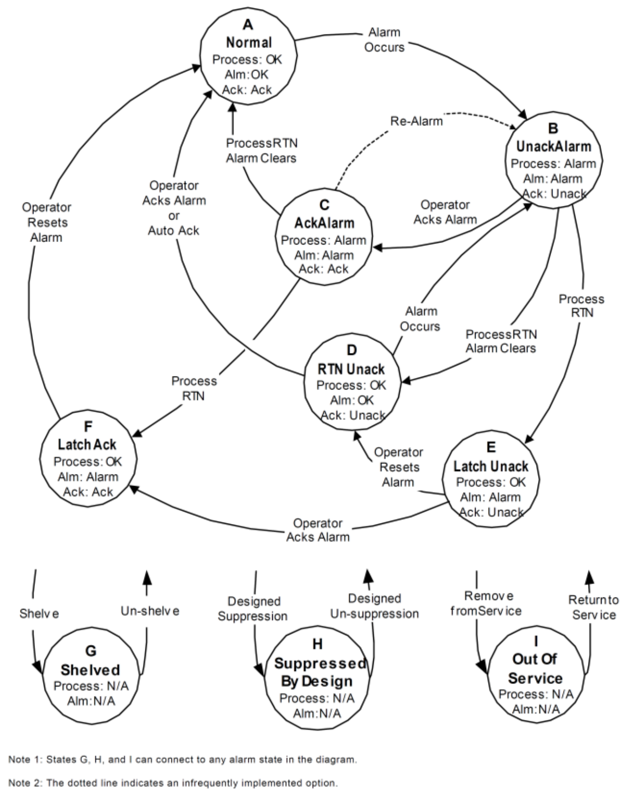


Figure 16 – Alarm Handling transition diagram from ISA-18.2-2009 *(ISA, 2009)*

Alarm handling techniques can differ slightly among Control System vendors. Recommended practice for alarm handling is now defined in several industry guides and standards.

Figure 15 shows the alarm handling transition diagram from the project site. *Figure 16* shows the recommended alarm handling transition diagram from ISA-18.2-2009 Management of Alarm Systems for the Process Industries. Note that the project site HMI cannot functionally meet the requirements of ISA-18.2-2009.

2.4. Historical Data

Historical data is collected for reporting and investigation purposes. HMI systems have a limited capacity to store both 'analog' and alarm and event historical data. Depending on the control system it is normally in the range of days to weeks. The long term storage of data from the control system is normally achieved using a Historian.

A Historian is a computer system that has specific software to read and store 'analog' and alarm and event data from the DCS. They can have a direct connection to the inter-controller network or a TCP/IP network connection directly to a HMI station. Most modern Historian systems now utilise OPC data communications to read data from the DCS. There may be many years of 'analog' and alarm and event data for 1000's of different tags. The data can be stored using proprietary database software, or commercially available database platforms such as Oracle and Microsoft SQL Server.

'Analog' data is normally collected using exception based rules. An example of an exception base rule is as follows:

> Read the value of an 'analog' signal every 10 seconds. If the difference between the current value and the last value stored is more than 0.1% of its range then store the current value in the database along with the current time, otherwise do not store a value.

The exception based method is an efficient means to store data. Data is only stored when needed, as opposed to potentially recording the same or similar value at regular intervals. This reduces the size of the database. All alarm and event activations and deactivations are captured and stored in database tables.

Historical data is used for reporting and review. 'Analog' data may be trended using special client software packages. *Figure 17* shows a screen shot from a Historian trending software package. It is displaying over two months of data in a single window. Most Historian systems also have an interface that allows the data to be exported to spreadsheets. Reports templates can be created with in spreadsheets and run manually or on a schedule. An Example of a scheduled report at the project site is a weekly report that shows coal tonnages used each day.

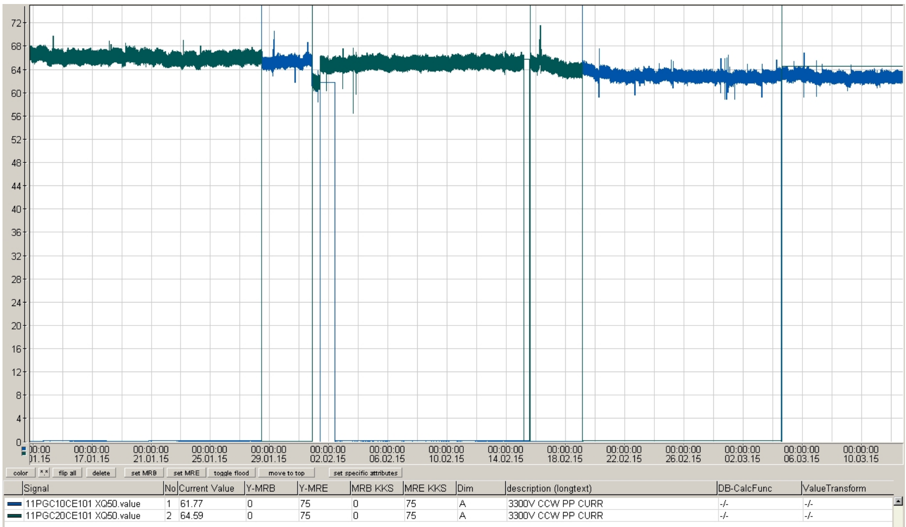


Figure 17 – Historian Trend Tool

Seq #	Timestamp	Event Type	Level	Tag	Alarm Type	Module Desc	Content	Desc1	State	Category	Area	Unit
32929484	28/10/15 13:21:28	EVENT	4-INFO	FI6606		H653A filter raw water	I/O Input Failure	FI6606/AI1	ACTIVE	PROCESS	A650P	K6511/EQM_H653A
32929483	28/10/15 13:21:24	ALARM	05-MAINTENANCE	CTRL-J6312	ADVISE_ALM		[MULT]Assigned IO: CHARM Integrity Error - J6314, CHM2-01, AI Charm	ADVISE	ACT/ACK	HARDWARE	AREA_K0600	
32929482	28/10/15 13:21:23	EVENT	4-INFO	FI6606		H653A filter raw water	Module Failure Active	Error Cleared	ACTIVE	PROCESS	A650P	K6511/EQM_H653A
32929481	28/10/15 13:21:23	EVENT	4-INFO	FI6606		H653A filter raw water	I/O Input Failure	Error Cleared	ACTIVE	PROCESS	A650P	K6511/EQM_H653A
32929480	28/10/15 13:21:22	EVENT	4-INFO	FI6606		H653A filter raw water	Module Failure Active	FI6606/AI1	ACTIVE	PROCESS	A650P	K6511/EQM_H653A
32929479	28/10/15 13:21:22	EVENT	4-INFO	FI6606		H653A filter raw water	I/O Input Failure	FI6606/AI1	ACTIVE	PROCESS	A650P	K6511/EQM_H653A
32929478	28/10/15 13:21:22	ALARM	05-MAINTENANCE	CTRL-J6312	ADVISE_ALM		[MULT]Assigned IO: CHARM Integrity Error - J6314, CHM1-11, AI Charm	ADVISE	ACT/ACK	HARDWARE	AREA_K0600	
32929477	28/10/15 13:21:18	ALARM	05-MAINTENANCE	CTRL-J6312	ADVISE_ALM		[MULT]Assigned IO: CHARM Integrity Error - J6314, CHM2-01, AI Charm	ADVISE	ACT/ACK	HARDWARE	AREA_K0600	
32929476	28/10/15 13:21:16	EVENT	4-INFO	FI6606		H653A filter raw water	Module Failure Active	Error Cleared	ACTIVE	PROCESS	A650P	K6511/EQM_H653A
32929475	28/10/15 13:21:16	EVENT	4-INFO	FI6606		H653A filter raw water	I/O Input Failure	Error Cleared	ACTIVE	PROCESS	A650P	K6511/EQM_H653A
32929474	28/10/15 13:21:14	EVENT	4-INFO	FI6606		H653A filter raw water	Module Failure Active	FI6606/AI1	ACTIVE	PROCESS	A650P	K6511/EQM_H653A
32929473	28/10/15 13:21:14	EVENT	4-INFO	FI6606		H653A filter raw water	I/O Input Failure	FI6606/AI1	ACTIVE	PROCESS	A650P	K6511/EQM_H653A
32929472	28/10/15 13:21:14	ALARM	05-MAINTENANCE	CTRL-J6312	ADVISE_ALM		[MULT]Assigned IO: CHARM Integrity Error - J6314, CHM1-11, AI Charm	ADVISE	ACT/ACK	HARDWARE	AREA_K0600	
32929471	28/10/15 13:20:16	EVENT		SEQ_C103_STT	SEQ_LOG_ALM	C103 Ore Start/Run Sequence	Starting new egg batch	COS	INACT/ACK		AREA_K0100	K10102/EQM_C103
32929470	28/10/15 13:21:10	ALARM	05-MAINTENANCE	CTRL-J6312	ADVISE_ALM		[MULT]Assigned IO: CHARM Integrity Error - J6314, CHM2-01, AI Charm	ADVISE	ACT/ACK	HARDWARE	AREA_K0600	
32929469	28/10/15 13:20:14	EVENT		SEQ_C103_STT	SEQ_LOG_ALM	C103 Ore Start/Run Sequence	Starting new egg batch	COS	ACT/ACK		AREA_K0100	K10102/EQM_C103
32929468	28/10/15 13:21:08	ALARM	05-MAINTENANCE	CTRL-J6312	ADVISE_ALM		[MULT]Assigned IO: CHARM Integrity Error - J6314, CHM1-11, AI Charm	ADVISE	ACT/ACK	HARDWARE	AREA_K0600	
32929467	28/10/15 13:21:07	EVENT	4-INFO	FI6606		H653A filter raw water	Module Failure Active	Error Cleared	ACTIVE	PROCESS	A650P	K6511/EQM_H653A
32929466	28/10/15 13:21:07	EVENT	4-INFO	FI6606		H653A filter raw water	I/O Input Failure	Error Cleared	ACTIVE	PROCESS	A650P	K6511/EQM_H653A
32929465	28/10/15 13:20:12	EVENT		PAL1119	DISC_ALM	C103 Ore Blow Egg	Change From Normal Value 0	CFN	ACT/ACK	PROCESS	AREA_K0100	K10102/EQM_C103
32929464	28/10/15 13:21:06	EVENT	4-INFO	FI6606		H653A filter raw water	Module Failure Active	FI6606/AI1	ACTIVE	PROCESS	A650P	K6511/EQM_H653A
32929463	28/10/15 13:21:06	EVENT	4-INFO	FI6606		H653A filter raw water	I/O Input Failure	FI6606/AI1	ACTIVE	PROCESS	A650P	K6511/EQM_H653A
32929462	28/10/15 13:20:12	EVENT		PAH1119	DISC_ALM	C103 Ore Blow Egg	Change From Normal Value 0	CFN	INACT/ACK	PROCESS	AREA_K0100	K10102/EQM_C103
32929461	28/10/15 13:21:00	ALARM	05-MAINTENANCE	CTRL-J6312	ADVISE_ALM		[MULT]Assigned IO: CHARM Integrity Error - J6314, CHM2-01, AI Charm	ADVISE	ACT/ACK	HARDWARE	AREA_K0600	
32929460	28/10/15 13:20:58	EVENT	4-INFO	FI6606		H653A filter raw water	Module Failure Active	Error Cleared	ACTIVE	PROCESS	A650P	K6511/EQM_H653A

(32929909 to 32928910) 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 ...

Figure 18 – Historian Alarm and Event Tool

Alarm and event data may also be used for reporting and review using client software packages and spreadsheet tools. *Figure 18* shows a screen shot from a Historian Alarm and event package. It is listing alarm and events in chronological order for a selected time period. This list may be filtered by any of the attributes and any time period.

Historian systems are normally connected to the business Ethernet network. The client software packages are normally installed on computes on the business Ethernet network. This enables staff other than operators to view and analyse data as required.

The Ethernet connection is normally controlled with a firewall which restricts TCP/IP traffic. This is for both security and performance purposes. Unwanted traffic in the control system can impact performance, while malicious attacks can be perpetrated on unsecured connections.

Chapter 3 – The Usual Suspects – Industrial Incidents

The nature of industrial processes means that there are hazards to be controlled. Sometimes control of these hazards is lost and the results can be catastrophic. The following three accidents can only be described this way.

3.1. Milford Haven

The explosion at the Texaco Refinery, Milford Haven United Kingdom in 1994 is the industrial accident that is referenced most often when discussing alarm management. It directly referred in the first page of EEMUA 191 (EEMUA, 2007) and in countless whitepapers on alarm management. The accident was investigated by HSE UK, the United Kingdom's regulator for workplace health and safety. The following is a simplified account based on the HSE UK (HSE UK, 1997) official investigation of the accident.

The beginnings of the accident can be traced to plant disturbances caused by an electrical storm before 9:00am on the 24th of July. A lightning strike caused a power dip, resulting in much of the plant shutting down and a small fire to break out. Operators spend the next few hours trying to restart the plant. One of the tasks required was to refill a process vessel with hydrocarbon liquids. The automated outlet value on vessel was supposed to be open but it did not operate correctly. It was indicating to the operators that it was open when it was not. This created confusion with the operators as they could not understand why the vessel would not fill.

Throughout the morning there were several attempts to fill the vessel. The closed outlet valve caused it to overpressure each time. To relieve the overpressure the vessel was vented to a flare system where the hydrocarbons are vented and burned in the atmosphere. Prior to the flare the hydrocarbons pass through a vessel known as a knock out drum. Liquids in the vented hydrocarbons are captured so only gas is passed to the flare.

Liquids passing into the flare system can cause an overpressure which the pipework is not designed to take. A pump-out system was fitted to remove the liquids from the knock out drum. A prior modification to the pump-out system for other purposes had a side effect of reducing its capacity to remove liquids from the knock out drum. The knock out drum was fitted with a high level alarm to warn operators when there was too much liquid in the knock out drum.

During the morning the vessel pressure relief operated three times, with the last time at 12:36 for 36 minutes. At 12:56 a high level alarm for the knock out drum activated, though there was no evidence that it was seen. As the liquid hydrocarbons continued to flow the knock out drum was filled beyond its design capacity. This caused liquid hydrocarbons to exit the knock out drum in the pipework to the flare. At 13:12 the pipework could no longer hold pack the pressure of the liquid hydrocarbon and the pipework ruptured. Twenty tonnes of hydrocarbon was released and the resulting vapour cloud found an ignition source and exploded.

The explosion injured 26 people, none seriously, though the report states that one of the mitigating factors was the fact that the accident occurred on a Sunday there were relatively few employees on the site. The report itself does not put a cost on the damage but the HSE UK information sheet titles Better Alarm Handling (HSE UK, n.d.) suggests that the accident "caused damage of around £48 million and significant production losses".

The report identified the following causes:

- The valve being shut when it indicated it was open
- Modification to the flare without the consequences being fully accessed
- The HMI did provide the necessary overviews to adequately diagnose the problem
- Attempting to continue operation when the plant should have been shut down
- The failing of the company to take overall perspective, focussing on local and immediate issues instead of trying to determine the root cause
- Failures of the company's systems for:
    - Assessing risks from plant and procedure modification
    - The use of programmable electronic systems
    - The Management of inspection and maintenance

3.2. Longford Gas Plant

The explosion at Esso's Longford Gas Plant, Victoria Australia resulted in the deaths of two people. The state of Victoria lost its natural gas supply for two weeks causing major economic losses as the state's industry ground to a halt. Many people who relied on natural gas for their homes also suffered hardship. A government of Victoria formed a Royal Commission to investigate the accident. The following is a simplified account based on Royal Commission (Longford Royal Commission, 1999) investigation of the accident.

The accident had its beginnings on the night shift prior. The plant was being prepared to operate at higher production rates. The plant was dealing with higher than normal volumes of liquid hydrocarbons. The was due a hydrocarbon supply which was rich with liquids and a process vessel that had been out of service and accumulating liquids was being returned to service.

By the time the day shift took control of the plant one cold hydrocarbon liquid began to flow into an oil stream bound for a one of the plant heat exchangers. This on its own did not present a problem as long as the heat source for the heat exchanger – warm lean oil flow was maintained. Process disturbances eventually caused a shutdown of the lean oil pumps at 08:19, at which point an alarm was activated to warn the operator. At 08:30 the operator attempted a restart of the lean oil pumps but was unsuccessful.

The heat exchanger then cooled to point where flange joints on the pipework attached to the heat exchanger deformed and began to leak liquid hydrocarbon. Without the warm lean oil flow the temperature in the heat exchanger dropped to -48^{o}C by 09:30, causing embrittlement of the heat exchanger metal. The plant operators spent the morning trying to return the plant to normal operation. They did not associate any hazards with the loss of the lean oil flow other than off spec production and leaks at the heat exchanger flanges.

At around 12:17 the lean oil flow was reintroduced and started to heat you the heat exchanger. At 12:25 the rapid heating caused it to fail catastrophically. Ten tonnes of hydrocarbon escaped and found an ignition source and exploded. There were several more explosions and many spot files. Two workers were killed and eight were injured in the explosions and fires.

The report identifies the real causes of the accident as:

- Incorrect actions following the shutdown of the lean oil pumps
- Insufficient knowledge of the dangers of associated with the loss of the lean oil flow
- Deficiencies in operator training
- Lack of operating procedures to deal with the process conditions encountered on the day

3.3. Three Mile Island

The accident a Three Mile Island nuclear power plant, Dauphin County, Pennsylvania United States of America in 1979 caused a partial meltdown of a reactor. No people were injured and there was negligible release of radioactive materials but the clean-up lasted for almost 15 years and cost an estimated cost of $1 billion dollars. It is also attributed to stalling the expansion of the nuclear power industry in the United States. Although the accident does not involve use of modern process control systems it does highlight some of issues surrounding abnormal situations and alarm management.

The reactors at Three Mile Island have two water circuits. The primary water circulates through the reactor core, to the steam generator and the returns to the reactor core. Secondary water circulates through the steam generator, where it is turned to steam, through the steam turbine generator. It is then condensed and returned to the steam generator. Energy as heat is transferred from the reactor core to the primary water, from the primary water to the secondary water. The heat energy is converted to mechanical energy in the turbine generator. The primary water is radioactive as it is exposed to the reactor core. The following is a simplified account based on the official (The Presidents Commission on The Accident at TMI, 1979) report off the accident.

The accident began late on the 28th of March 1979 at 04:00 when pumps feeding secondary water to the steam generator shut down. Without secondary water the reactor automatically went into a shutdown – control rods are dropped into the reactor core to stop the nuclear reaction. Although there is no longer a nuclear reaction the radioactive materials in the reactor continue to produce enough heat such that primary water is still required to prevent damage to the reactor.

During this type of shutdown it is normal for a pilot operated relief valve open to release the pressure in the primary water system. Thirteen seconds after it opened the pressure in the primary water system returned to normal and the pilot operated relief valve was supposed to close but it did not. It did indicate to operators that it was closed.

There are three emergency cooling pumps for the secondary water which did start as required, though the valves on each of the two emergency cooling water lines were closed and no emergency water was reaching the steam generator. Two minutes into the accident the high pressure injection pumps started and began to deliver water directly to the reactor. The operators were not aware that the pilot operated relief valve had not closed. Due to the open pilot operated relief valve radioactive water was escaping the reactor. Another knock on effect was that the water level instrumentation in the reactor core did not respond accurately

As the accident developed the operators restricted the flow of the high pressure water injection pumps as they were concerned that they could overfill the reactor core, a situation known as ‘going solid’. They did not correctly diagnose the situation as being caused by the pilot operated relief valve. The accident was now escalating as reactor core was no longer covered with water and began to overheat.

The temperature of pipe downstream of the pilot operated relief valve also indicated it was over 200^{o}F. One of the plant procedures stated that temperatures over 200^{o}F indicated the pilot operated relief valve is open. The operators testified to that it was normal for the temperature to be high due to a leaking pilot operated relief valve or other valves leaking. The operators did not consider the temperature of the pipe as significant.

Two hours and 22 minutes after the accident began it was determine that the pilot operated relief valve was stuck open. A manual valve near downstream from the pilot operated relief valve was closed and the primary water system was contained. By this point 32000 gallons of radioactive water had escaped through the open valve. It was not until 10:30 that the high pressure injection pumps were finally able restore the reactor water level above the core. The temperature of the reactor was brought under control over the next day. By this time the reactor was damaged beyond repair.

The report made the following assessment of the significant events:

- The event was initiated by equipment failures
- Operators were not able to recognise the actual conditions in the plant
- Operator training did not prepare them the situation
- Operators took incorrect actions, and failed to take correct actions which escalated what would have been a minor incident to the actual accident

3.4. The Alarm System’s Role in these Accidents

What is not captured in the descriptions of these accidents is the tension and frustration operators were experiencing. In all three accidents the operators were dealing with abnormal situations. In each case there were many attempts to bring the plant back to normal operation. The operators were struggling to understand what was really happening. At Three Mile Island one of the operators testified that he “would have liked to have thrown away the alarm panel. It wasn't giving us any useful information" (The Presidents Commission on The Accident at TMI, 1979). The alarm systems that were supposed to support them were adding the frustration.

Common to all the accidents are the flood of alarms. At Three Mile Island "During the first few minutes of the accident, more than 100 alarms went off, and there was no system for suppressing the unimportant signals so that operators could concentrate on the significant alarms" (The Presidents Commission on The Accident at TMI, 1979).

At Milford Haven the report stated that "the chances of the operators restoring control by manual intervention decreased the longer the upset condition persisted. This was because they became progressively overloaded with an increasing barrage of alarms" and "alarms were being presented to operators at the rate of one every two to three seconds. Alarms going off this frequently resulting in operators cancelling them because of their nuisance value without necessarily recognising what they meant" (HSE UK, 1997).

Recognising that there is an alarm condition is only the first part in managing an abnormal situation. It is important that the consequences are well understood. At Longford within ten minutes of the lean oil pumps stopping operators has attempted to restart them but could not. Operators knew they had to restart the lean oil system, but they only associated the situation with off spec production, not the potential to cause the catastrophic failure of the heat exchanger.

One of the expert witnesses at the Longford Royal Commission stated that in the industry "hazards associated with the loss of the lean oil flow were well known" (Longford Royal Commission, 1999). Hopkins suggests (Hopkins, n.d.) that it was the failure of the operators to respond to the alarms that led to the failure of the lean oil system which subsequently caused the cold temperature embrittlement failure of the heat exchanger. If the operators had understood the consequences of they may have the loss of the lean oil system they might

The normalisation of abnormal situations is another problem highlighted in these accidents. At Longford "there was evidence that in the GP1 control room it was common for a large number of alarms to be active at any one time." At Three Mile Island operators stated in the normal operation it was not uncommon to have more than 52 alarms active (The Presidents Commission on The Accident at TMI, 1979). In the Three Mile Island accident operators had been normalised to the situation of high temperature on the pilot operated relief valve pipework which should have indicated that the valve was open. Although no alarm is attributed to this situation is demonstrates how situations that are documented as abnormal become normalised.

In all three accidents the alarms system did not support operators, they impeded the operators. This was not due the situations. There were systematic failures in the design and management of the alarm systems. At Longford "One of the operators gave evidence nuisance alarms had the capacity to distract operators and frequently did. They could become very repetitive and could result in more important alarms not being picked up or noticed because their warning signals were lost amongst the numerous other alarms" (Longford Royal Commission, 1999). At Three Mile Island

“The danger of having too many alarms was recognized by Burns and Row during the design stage, but the problem was never resolved” (The Presidents Commission on The Accident at TMI, 1979)

The alarm systems did not cause these accidents. There were many systematic causes. The accidents transitioned from disruptive incidents to major accident thought the loss of situational awareness. An analysis of 32 major process industry accidents by the ASM Consortium (ASM Consortium, 2013) showed that 50% of failures by operators were due to a loss of situational awareness. Alarm systems must add to situational awareness, not detract from it.

Chapter 4 – The Development of Alarm Management

The alarm problem pre-dates the modern control system. Problems were identified prior to the Three Mile Island accident in 1979 though there were no coordinated efforts to solve them. The modern control system saw a rapid increase in the number of configured alarms. This amplified the alarm problem.

4.1. Early Work and Research (Pre 2000)

The first coordinated effort to tackle the alarm management was in the USA in 1989. Honeywell, a control system vendor, identified the growing problem of alarms on modern computer based HMI systems. They convened a task force with 25 of their clients to investigate the problem. This effort became more focussed in 1992 when Honeywell and four companies (Amoco, Chevron, Exxon and Shell) formed the Abnormal Situation Management (ASM) Consortium. ASM believed "that the alarm system was but a part of the larger issue of the management of unexpected process upsets" (ASM Consortium, n.d.).

By 1994 four more companies (BP, Mobil, NOVA Chemicals, and Texaco) had joined ASM. The consortium applied for, and received funding from USA's National Institute of Standards and Technology's (NIST) Advanced Technology Program for research funding. This was a significant in the fact that the consortium of private companies provided $8.5 million of their own funds. This funding was matched closely by NIST.

The research project had a duration of four years and focussed on developing software based decision support tools and consistent information management for process plant operators. NIST (NIST, 2009) suggests that as a result of the research project that ASM generated on average savings of $800 000 a year for a process plant and increases production from 95% of capacity 99%, and there are over 120 operating plant with ASM's Alarm Configuration Tool.

The next major event in alarm management was as a result of the 1994 explosion at the Texaco Refinery, Milford Haven United Kingdom. The HSE UK began looking closely at how poorly managed alarm systems affect safety. In 1996 HSE UK funded a research project "to survey alarms systems in the power and chemical industries and hence identify and report current industry best practice" (Bransby & Jenkinson, 1997). The research project covered:

- visits to 15 plants, discussions where held with a range of staff, operations, engineering and managerial
- questionnaires of 96 operators,
- visits to three company engineering or R&D centres to discuss alarm system standards
- questionnaires of five engineers involved in specifying or procuring alarm systems
- a literature review on alarm systems
- discussions with members of industry associations

The conclusions of the research project recommended that alarms of little value be identified and re-engineered, the use of alarm system performance monitoring to drive improvements and control system manufacturers provide alarm handling features that users require. Above all the conclusions pointed to the need for a greater understanding of the impacts alarm system performance in relation to both financial and safety risks.

In 1997 the Institution of Electrical Engineers (IEE) in the United Kingdom hosted a colloquium titled “Stemming the Alarm Flood”. Both the HSE UK research team and the ASM Consortium presented papers based on the work they were performing. It seemed that there was now a common understanding in the process industry of the problems associated with poor performing alarm systems. Companies were applying techniques that were been identified by ASM’s research to improve alarm systems. BP presented a paper on it current practices for alarm management. It highlights that “advanced solutions are never a ‘fix’ for bad basic practices” (Brown & O'Donnell, 1997).

The first attempt to provide a common solution to the alarm problem was by EEMUA in the United Kingdom. EEMUA was heavily involved in the HSE UK research project. Prior to this involvement it had been considering developing a best practice guidance document (Bransby & Jenkinson, 1997). In 1999 EEMUA Publication 191, Alarm Systems – A Guide to the Design, Management and Procurement was released. As well as learnings from the HSE UK research project the ASM Consortium also provided input.

EEMUA 191 is a guidance document, not a standard. In 2000 the HSE UK released a “Better Alarm Handling” information sheet recommending EEMUA 191 be used as guidance. The HSE UK inspector’s tool kit (HSE UK, n.d.) also suggests that it is “vital that significant (i.e. more than 300 alarms) new DCS systems going in are designed to EEMUA principles and we should enforce on this. For existing systems enforcement to carry out a review is appropriate where there is evidence of problems (e.g. large numbers of standing alarms on the system).”

4.2. Development of Standard (Post 2000)

In 2001 the Norwegian Petroleum Directorate, the government agency for administration and regulation of the Norwegian oil and gas resources, produced the guidance document YA-711 Principles for Alarm System Design. This guidance document contained much of the guidance of EEMUA191 in a more direct and concise manner. In 2003 NAMUR, the German based User Association of Automation Technology in Process Industries also released the guidance document NA102 – Alarm Management, again based on EEMUA 191.

The ASM Consortium released a guideline document in 2003, Effective Alarm Management Practices. Initially ASM considered the EEMUA performance metrics as too aggressive but research in 2004 showed that they were appropriate (Metzgar, 2009). The guideline document provides examples from ASM member’s sites as well as the rationale for recommendations it makes. It has been updated six times, with the most recent in 2009. It was initially only available to ASM members, but the latest update is available for purchase.

2003 was also the year that ISA began working on an alarm management standard. ISA is a non-profit professional association in the process automation and control industry. Many of its standards have been recognised by ANSI and also adopted by the IEC. Its standards are developed using volunteer committees of professionals.

In 2007 EEMUA released an update to EEMUA 191. The ASM Consortium Director wrote in the Foreword that the ASM Consortium considers EEMUA 191 “represent the best publically available benchmark of industry good practice for alarm management” (EEMUA, 2007). A third edition of the EEMUA 191 was also released in 2013.

The Electrical Power Institute (EPRI), a research and development organisation based in the USA and funded by the electric utility industry, published a guideline document Alarm Management and Annunciator Applications Guidelines in 2008. This was developed in close consultation with company called PAS, of which Bill Hollifield is the Principle Alarm Management Consultant.

In 2009 the voting members of the ISA18 committee approved ISA-18.2-2009 Management of Alarm Systems for the Process Industries. ANSI adopted the standard as ANSI/ISA-18.2-2009. Two of the voting committee members have both produced books on the subject of alarm management. Bill Hollifield is one of the authors of The Alarm Management Handbook – A Comprehensive Guide in 2006. This was updated in 2009 and a version is also published by the ISA. Doug Rothenberg produced Alarm Management for Process Control in 2009. Both books describe methods to manage alarm systems that comply with ISA-18.2. They also provide expanded guidance and explanations for some techniques to apply to specific alarm problems.

The American Petroleum Institute (API) is a trade association based in the USA that represents the USA’s oil and gas industry. In 2010 it published API-RP-1167 Pipeline SCADA Alarm Management in 2010. This document summarises the requirements of ISA-18.2, and it as a normative reference.

The International Electrotechnical Commission (IEC) is a non-profit organisation that produces standards for electrical and electronic related technologies. Its standards are created in a similar manner to the ISA – using technical committees for development and voting to approve standards. It began working on IEC62682 Management of Alarms Systems for the Process Industries in 2010. Its structure is identical to ISA-18.2 and it has no new sections, though some minor changes have been made (Hollifield, 2015). The major different is that many recommendations using the term “should” have been made mandatory with the term “shall”. It was released in 2014.

The development alarm management has been driven the process automation and control industry. The EEMUA and ASM industry groups were the early pioneers. Their research and involvement in alarm management built the foundations for the current standards and knowledge of alarm systems. This knowledge is now forms the international standard in the form of IEC 62682. The work of the ASM Consortium continues to explore abnormal situations and the human factors involved in detecting and restoring normal plant operation.

Chapter 5 – Alarm Management Best Practice

When determining alarm management best practice three main sources were used:

- ISA-18.2-2009 Management of Alarm Systems for the Process Industries
- EEMUA 191 – Alarm Systems, A Guide to Design, Management and Procurement
- ASM Consortium Guidelines – Effective Alarm Management Practices

These three documents present the most up to date alarm management practices. All three documents share a common lineage as the organisations that created these documents have collaborated during the development of alarm management methodologies. ISA-18.2-2009 was immediately adopted as an ANSI standard in the Unites States of America and has now been released as an international version as IEC62682-2014, cementing these methodologies as best practice worldwide.

5.1. When and How Alarms Should Be Used

Alarms have a specific purpose and purpose should be understood by those who are designing and implementing alarm. The ISA-18.2-2009 definition of an alarm is:

> "An audible and/or visible means of indicating to the operator an equipment malfunction, process deviation, or abnormal condition requiring a response." (ISA, 2009).

This definition agrees with one of the key design principles of the EEMUA 191 which states:

> "Every alarm should have a defined response." (EEMUA, 2007)

Common understanding of the definition of an Alarm is important and the ISA-18.2-2009 definition has been adopted for this project.

In Section 2.3 the HMI was discussed and the audible and/or visual means by which operators are alerted to alarms was described. This is normally fixed by the control system vendor. Newer control systems have flexibility to change these attributes slightly to suit end user requirements. It is usually only end users who are well versed in alarm management that would modify the default configuration to suit specific requirements in their Alarm Philosophes.

End users decide which process conditions will activate an alarm. This means that end users have the most scope to design and implement poor alarms. This section focusses on how to use alarming effectively.

There a many models that depict how alarms should be used. Most of these models use the concept of layers as depicted in *Figure 19* and *Figure 20*. The first layer is when the process is operating at normal process conditions. The control system is primarily used to keep process variables at set point or target values, as show in *Figure 19*. This ensures production quality, efficient use of process inputs and the continued reliable operation of the plant equipment and machinery.

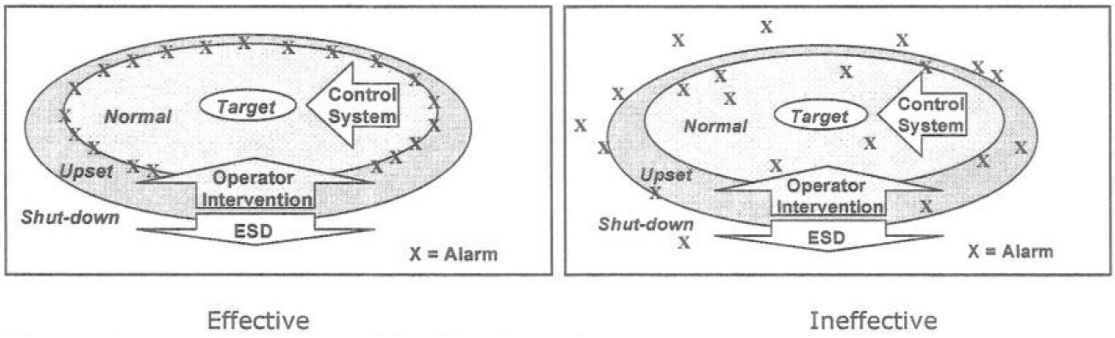


Figure 19 – EEMUA 191 Effective Alarm System *(EEMUA, 2007)*

There are times when the control system can no longer keep the process at normal conditions. The reasons for this could be that there are set of circumstances that were not considered in the original design or equipment has malfunctioned and is not operating correctly. The process conditions will begin to deviate from normal conditions. This is referred to a process upset or a process disturbance.

If the process continues to deviate it will likely reach a point where the process conditions exceed the safe operating parameters of the plant and equipment. At this point the safety of people and the environment may be at risk, or the financial impact of the loss of product quality or damage to the equipment may exceed the cost of continued production. At this point automated supervisory actions may intervene and shut down the process. This may be in the form of a controlled shutdown over a period of time or an Emergency Shut Down (ESD as depicted *Figure 19*) where the process is halted immediately, or a combination of both. This is known as the shutdown layer. The shutdown may be performed by the control system or an independent shutdown system.

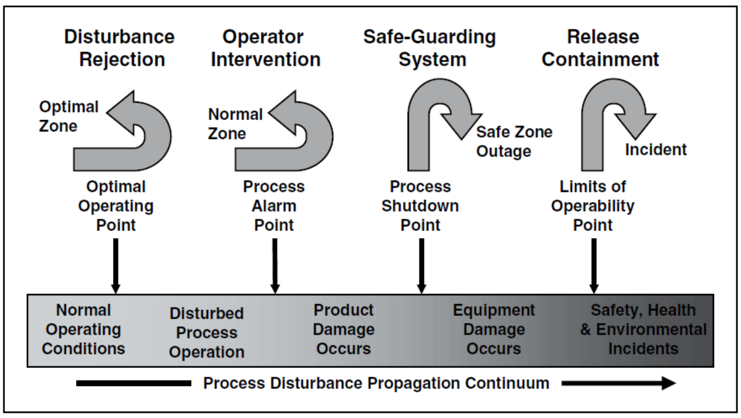


Figure 20 – Process Disturbances and Layers of Protection *(Hollifield & Habibi, 2001)*

While in the process disturbance layer an operator may be able to intervene in order identify and correct the cause of the process disturbance and return the process to normal conditions. If they are able to do this then production can continue. The purpose of an alarm is to alert the operator that the process in deviating from normal conditions and they will need to take action to return the process back to normal conditions. Failure to do so will result in undesirable consequences.

The speed at which the process transitions from one layer to the next can vary greatly. For instance, steam turbine over speed is particularly dangerous and can happen in a matter of seconds. There is no time for an operator to take action to prevent the shutdown layer if alerted to the turbine speed deviating from normal speed. On the other hand if a tank is being filled with liquid and a shutdown layer is installed to prevent a tank overflow an operator may have many minutes to take action if alerted to the tank level being too high.

Figure 19 shows to versions of the same model. On the right is ineffective alarming. Alarms in the normal process conditions layer require no action. Alarms in the shutdown layer are too late – there is now the consequence of lost production. Alarms depicted in the disturbance or upset layer are time dependant – there must be enough time for an operator to take the necessary action to return the process to normal conditions. This must be taken into context when interpreting the left of *Figure 19*. The transition from the process disturbance or upset layer to the shutdown layer is time bound. Understanding the time it takes for the transition from the start of the disturbance layer to the start of the shutdown layer makes for an effective alarm. If the time is too short then the detection of the process disturbance may be able to be changed to provide more time.

The action an operator needs to take, or the response, is the most important aspect of the alarm. The definition of an alarm includes the phrase “requiring a response”. This dispels the idea that some alarms should be used ‘For Information Only’. It also means that ‘lazily’ placed alarms have no place either. ‘Lazily’ placed alarms are those whose only purpose is a catch all. They are normally placed at the operating limits of plant of equipment or near the shutdown limits. They are seen as being safe or conservative. When specifying these alarms there is normally no consideration of the operator response or if there is time for the operator to reposed before a shutdown occurs. Pre shutdown warning alarms are useful but they must accompanied with a specific response and enough time to perform the response.

There should also be some additional limitations on the use of alarms. In *Figure 19* the control system can be seen as the primary means to keep the process at normal conditions. This should be the case – alarms should not be used to prompt operators to take actions that the control system can do.

Alarms should not be the last layer. *Figure 20* shows that the ‘Shutdown Point’ prevents the process from reaching the ‘Limits of Operability Point’. This is the point where the process may no longer be contained by the plant and equipment. The consequence of exceeding this point is catastrophic failure. It is not the role of an alarm to prevent this. It may be used in addition to, but not the sole layer for this type of consequence.

5.2. Common Alarm Problems (and Treatment Options)

The unwritten goal of Alarm Management is to have an alarm system that the operator trusts. When alerted to an alarm they should interrupt their current task with the confidence that the alarm contains important information. Alarm problems erode this confidence in the alarm system.

5.2.1. No Response Required

No Response required means that the alarm was likely added for information only or as a result of an overcautious approach to alarms. By definition alarms require a response. This alarm problem conditions the operator to expect some alarms will not likely require a response.

The treatment option for this alarm is to simply remove it.

5.2.2. Unknown Response

Unknown Response is when an operator receives the alarm but does not why or what to do. This could be due to non-intuitive descriptors or a lack of documentation. The response to these alarms will be delayed as the operator may have to consult with other operators, supervisors, maintenance, or engineering personnel to determine the response. This alarm problem creates a sense of frustration. If this alarm activates during an Alarm Flood it will likely add to the tension operators may be experiencing.

The treatment option for these alarms is to rationalise it with close attentions to the descriptor and ensure the documentation captured during rationalisation is available to the operator.

5.2.3. Unknown Consequences

Unknown Consequences is when an operator knows how to return the process to normal conditions but they do not the understanding of the consequences of not responding to the alarm. This becomes and alarm problem when the operator is trying to prioritise several alarms – this alarm may be incorrectly prioritised over other alarms.

The treatment option for these alarms is to rationalise it and ensure the documentation captured during rationalisation is available to the operator.

5.2.4. Alarming Normal Conditions

Alarming Normal Conditions occurs when an alarm point is used as a trigger or condition in the automation of a subsystem. A typical example is an automated sequence that fills a tank with liquid where the high level alarm also stops the filling sequence. This alarm problem conditions the operator to expect some alarms will not likely require a response.

The treatments options are to either remove the alarm or separate the control point from the alarm point. If the alarm it to be kept it should be justified by the rationalisation process.

5.2.5. Trip/Shutdown Activated

Trip/Shutdown Activated alarms may operate with no pre-warning that the process upset has resulted in a shutdown. These alarms are generally too late to be of any use.

The treatment option is to review the alarming strategy of the subsystem to ensure alarms are activated with enough time to take action to avoid the shutdown. Note that it may be necessary to alarm to an operator that a specific subsystem has shut down as they may then need to perform specific tasks. For shut down situations alarm masking should be used to eliminate alarm flooding.

5.2.6. Standing Alarms

Standing alarms (or stale alarms) are alarms that remain active for prolonged periods of time – normally more than 24 hours. This can be because the alarm points have been selected incorrectly or the process in being operated incorrectly. Another cause is that out of service subsystems or equipment are generating alarms. An example is a low temperature alarm. If during normal operation the process is above ambient conditions then low temperature alarms will be active when out of service. Standing alarms create many problems:

- they can fill the alarm list
- priority one standing alarms diminish the concept of alarm priority
- the plant maybe being operated in an unsafe manner if the alarm points have been selected incorrectly
- there is effectively no alarm if the alarm is already active
- they conditions the operator to ignore particular alarms – a problem is there is a genuine activation

The treatment options depend on the cause. If the cause is due to equipment being out of service then alarm masking can be used, otherwise careful consideration of the alarm's purpose and then rationalisation is required.

5.2.7. Alarm Floods

ISA-18.2-2009 defines an alarm flood as

> "A condition during which the alarm rate is greater than the operator can effectively manage (e.g. more than 10 alarms per 10 minutes)." (ISA, 2009)

Alarm floods normally occur when there is a shutdown of subsystem or major parts of the plant. Many process variables transition from their normal operating values to ambient conditions – creating many alarms. Process disturbances can also cascade to other subsystems creating multiple alarms. The alarm flood normally occurs at a time when the operator in under a lot of stress. Important alarms can be missed as many alarms appear and scroll through the alarm list.

Alarm floods are perhaps the hardest alarm problem to treat. To prevent alarm floods during shutdowns requires alarming strategies to be developed that consider the whole subsystem. Alarm masking needs to be employed to many alarms.

Alarm floods during process disturbances an upsets are harder still. They are hard to predict so most often the only way is design them out once they occur. This requires very diligent alarm performance monitoring looking for alarm flood conditions.

If the background alarm rate is greater than 10 per 10 minutes then the alarm system may be in a constant state of alarm flood. If this is the case then efforts need concentrate on getting the alarm rate to manageable levels before considering alarm floods.

5.2.8. Fleeting Alarms

Fleeting alarms (or chattering alarms) occur when noisy signals or faulty equipment cause alarms to repeatedly activate and clear in rapid succession. Fleeting alarms take over the alarm system such that it no longer useful. They can account for 1000's of alarm activations in a single day. It is one of the most common problems that affect alarm performance.

Figure 21 shows how fleeting alarms occur. Consider a process variable oscillates due to noise in the process. Now consider the average value of the process variable – it is increasing and does cross the alarm point. The oscillations cause the alarm to active and deactivate 10 times in this figure, though it was only needed once. This effect can be severely amplified if the oscillations are more frequent. The problem is worse when large oscillations push a normal process value to it alarms point. This type of fleeting alarm can occur for many hours.

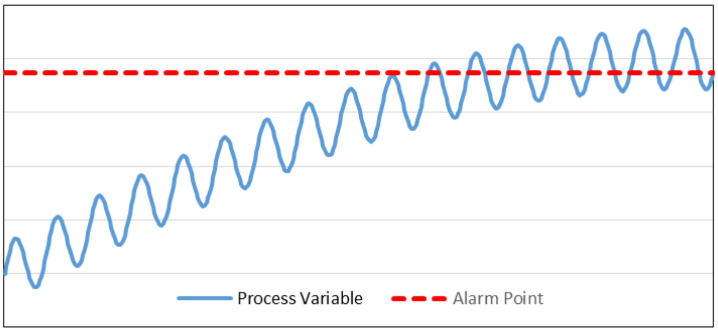


Figure 21 – Fleeting Alarm

Fleeting alarms can also be caused by faulty equipment. If this is the case then immediate action should be taken to rectify the situation. A fleeting alarm that takes over the alarm system such than no other alarms can be discerned should not be tolerated for any length of time.

There are several treatment options for fleeting alarms:

- Filtering of the process variable before it is processed. Caution as this could affect control response if the process variable used for control
- Delay Time (or De-bounce Timer) which means the process value should exceed the alarm limit for a predetermined amount of time before it is activated.

- Hysteresis, which is adding a dead band or 'backlash' to the reset of the alarm.

EEMUA 191 makes recommendations for filter times and EEMUA 191 and ISA-18.2-2009 make the same recommendations for Time Delay and Hysteresis. These recommendations are based on the process variable being measured. These recommendations are shown in *Table 1*

Table 1 – Recommendations for Filter Time, Time Delay and Hysteresis

Variable Type	**Filter Time (seconds)** (EEMUA, 2007)	**Time Delay (seconds)** (EEMUA, 2007) (ISA, 2009)	**Hysteresis (%)** (EEMUA, 2007) (ISA, 2009)
Flow	2	15	5
Level	2	60	5
Pressure	1	15	2
Temperature	0	60	1

5.2.9. Alarm Masking

Alarm masking (or Suppressed by Design) is not an alarm problem – it is a treatment option for several alarm problems though. The ISA-18.2-2009 definition is:

> "3.1.73 Suppressed by Design
> A mechanism implemented within the alarm system that prevents the transmission of the alarm indication to the operator based on plant state or other conditions." (ISA, 2009)

Alarm masking can be used to prevent alarms from activating under circumstances where there would be no response required. The classic example is alarms associated with dual redundant subsystems. While one subsystem is out of service or on standby some of the alarms may be active. Alarm masking is implemented to detect when the alarms are not required and prevent them from activating. The simplest application of this is to use Boolean and logic with the alarm conditions and the masking conditions. Consider a tank with a discharge pump and a low level alarm. If the system was out of service, i.e. the discharge pump is not running the low level alarm is not required. Using alarm masking the alarm activation logic would look like this:

> Low Tank Level AND Discharge Pump Running

If there was no alarm masking and system was out of service the low level alarm would activate. The alarm masking prevents an unnecessary alarm.

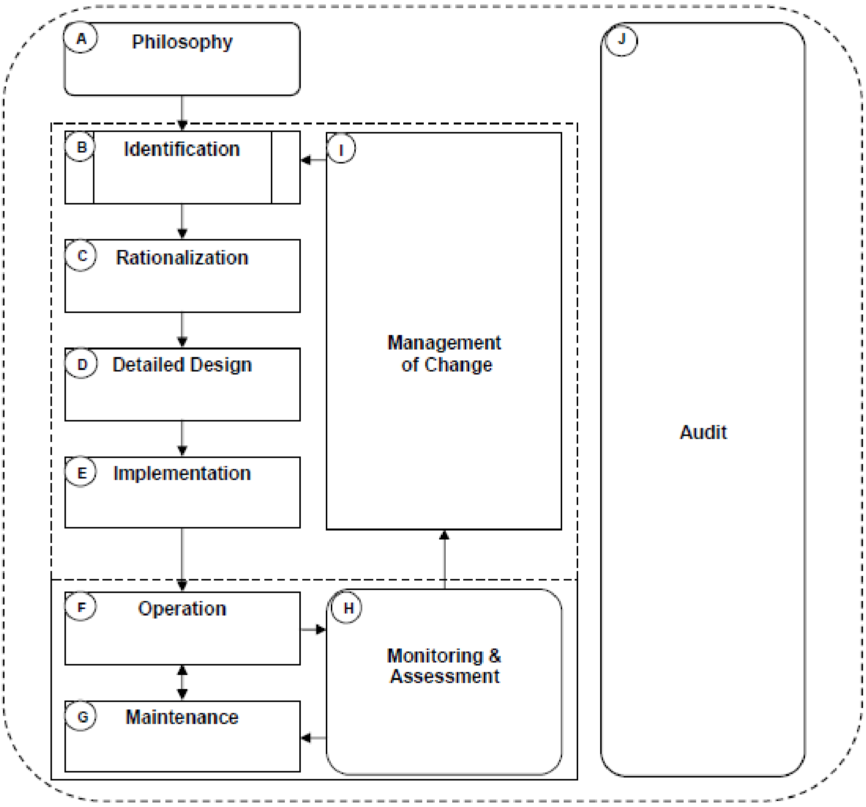
Alarm masking is a powerful tool for preventing both standing alarms and limiting alarm floods during plant shutdowns.

5.3. How Alarm Systems Should Be Managed

Alarm management is a continuous improvement cycle in the same manner as the Shewhart cycle of Plan – Do – Check – Act. This is evidenced by the fact that

ISA-18.2-2009, EEMUA 191 and the ASM Consortium all place very high importance on performance monitoring of the alarm system to drive alarm management.

This cycle firstly starts with a definition of the process and the problems that may occur. Methodologies and approaches are identified as well as the goals and measures of success. A feedback loop is then employed where changes are made the process or system under continuous improvement. The effect of changes on the process or system are measured and then compared to the goals and measures of success. Based on the results further changes are made to improve the process or system and the cycle repeats. The ISA-18.2-2009 Alarm Management Lifecycle is shown in *Figure 22*.



Note 1: The box used for stage B represents a process defined outside of this standard per 5.2.1.2.

Note 2: The independent stage J represents a process that connects to all other stages per 5.2.1.10

Note 3: The rounded shapes of stages A, H, and J represent entry points to the lifecycle per 5.2.2.

Note 4: The dotted lines represent the loops in the lifecycle per 5.2.4.

Figure 22 – ISA-18.2-2009 Alarm Management Lifecycle *(ISA, 2009)*

ISA-18.2-2009 and EEMUA 191 both propose comprehensive planning requirements as the first stage in Alarm Management. The EEMUA 191 guidance is to create a 'Site Alarm Management Strategy' while ISA-18.2-2009 defines an Alarm Philosophy as:

> "A document that establishes the basic definitions, principles, and processes to design, implement and maintain an alarm system." (ISA, 2009)

Some of the key requirements are of these documents are:

- Definitions to ensure common understanding – particularly the definition of an alarm
- Roles and responsibilities for alarm management
- Principles and guidance for the design of alarms
- The Rationalisation process
- Performance metrics
- Collection of alarm and event data

The roles are key requirements for successful and sustainable alarm management. Generally engineering staff are involved alarm management. They have the technical knowledge of the plant and equipment and the control system. The ASM Consortium recommends that the company management support for alarm management be established (ASM Consortium, 2009). The expectation is that an Alarm Philosophy or management strategy will become an official site procedure. This ensures company management will support the alarm management efforts. Hollifield and Habibi suggest that without company management support alarm improvement efforts will not get far (Hollifield & Habibi, 2001).

ISA-18.2-2009 and EEMUA 191 both impress the need for operator to be involved in alarm management, particularly alarm design. The operators are the end users of the alarm system so their input is vital. They also have intimate knowledge of the process as it does operate, which may be a little different to how it is designed to operate. Their input is an invaluable resource.

Hollifield and Habibi suggest that an Alarm Champion role be created. This role is responsible for the coordination of the alarm management activities. They also suggest that without this role sustained improvement is very unlikely (Hollifield & Habibi, 2001).

5.3.1. Rationalisation

Alarm rationalisation has three important roles. Firstly it is must vet alarms to ensure they meet the criteria to be an alarm. Secondly it the primary design process were the requirements for the alarm are identified and standardised. Finally, it is the means by which to document alarms.

ISA-18.2-2009 recommends that rationalisation be performed using a team. The ASM Consortium provides an example of a site that uses a multidisciplinary team. The team approach ensures all stakeholders are involved in the design.

To rationalise an alarm the following questions should be asked:

- What is the functional description of the alarm?

- What are the consequences of not responding to the alarm?
- What are the possible causes of the abnormal situation?
- How long does the operator have to respond
- What is action should the operator take?

The last question is what decides if the alarm is required, remembering the definition of an alarm means that response is required. If no response is required then the alarm is not justified.

Some of the key technical aspects of the alarm should also be determined during rationalisation. This includes alarm masking, delays times, hysteresis values and the text for the alarm. One of the most important aspects is the alarm Priority.

Alarm priority provides operators with guidance for two aspects. Firstly, if there are several alarms active at the same time the alarm priority can, as the name suggests, assist in prioritising which alarms to respond to first. Secondly the priority can provide a suggestion of how quick the response needs to be. An operator's tasks are varied and not limited to monitoring and responding to alarms so any additional guidance to prioritise the alarm response with other tasks is important.

ISA-18.2-2009 provides no specific guidance for how to set the priority of an alarm. EEMUA 191 suggests that prioritisation should be a risk based determination on the consequences of the not responding to the alarm. It presents three methods ranging from quantitative to qualitative.

Table 2 – ASM Consortium Example Prioritisation Matrix *(ASM Consortium, 2009)*

	Potential Consequences		
Response Time	**Production/ Quality**	**Plant Asset/ Reliability**	**Safety/ Environmental**
Less than 1 minute	Medium	High	High
1 to 10 minutes	Low	Medium	High
10 to 30 minutes	Low	Low	Medium

The first method quantifies the risk in terms of safety, environmental and financial consequences a then considers the time the operator have to respond – either less than three minutes or greater than three minutes. Being quantitative this method requires an accurate understanding of the financial consequences and conversions of safety and environmental consequences so they can be compared side by side. The ASM Consortium guidelines present an example method though the consequences have only been classified, not quantified. There are also there are there time bands when considering the alarm response time. The example is shown in *Table 2*.

In their book Alarm Management: A Comprehensive Guide (Hollifield & Habibi, 2001) Hollifield and Habibi propose a combination of a semi-qualitative risk assessment with prioritisation matrix in the ASM guidelines. The risk matrix is used to determine the consequence severity of not responding to the alarm – either Minor, Major or Serve.

The prioritisation matrix and an example of a semi-qualitative risk matrix are shown in *Figure 23*. As with any risk based approach an organisation must calibrate the risk matrix to suit their own risk appetite. This should normally be aligned to corporate their risk management policies.

An important part of the rationalisation process is documentation. EEMUA 191 (EEMUA, 2007) and the ASM Consortium guidelines recommend that a computerised alarm database be created and used throughout the life of the facility. ISA-18.2-2009 suggests that rationalisation be documented in a 'Master Alarm Database'.

Maximum Time To Respond	**Consequence Severity: MINOR**	**Consequence Severity: MAJOR**	**Consequence Severity: SEVERE**
More than 30 Minutes	If possible, re-engineer the alarm so it has the characteristic of urgency.		
10 to 30 minutes	Priority 3 (P3)	P3	P3
3 to 10 minutes	P3	P2	P2
Less than 3 minutes	P2	P1	P1

Impact Category	**Severity: NONE**	**Severity: MINOR**	**Severity: MAJOR**	**Severity: SEVERE**
Personnel Safety	No injury or health effect	Any alarm for which operator action is the primary method by which harm to a person is avoided, shall non-exclusively utilize Priority 1. See the alarm philosophy section on "Alarms that Prevent Harm to Personnel."		
Public or Environment	No effect	Local environmental effect ... Does not cross fence line ... Contained release ... Little, if any, clean up ... Negligible financial consequence ... Internal or routine reporting requirements only	Contamination causes some non-permanent damage ... Single complaint ... Single exceedance of statutory or prescribed limit ... Reporting required at the local or state agency level	Limited or extensive toxic release ... Crosses fence line ... Impact involving the community ... Repeated exceedances ... Uncontained release of hazardous materials with major environmental impact and 3rd party impact ... Extensive cleanup measures and financial consequences ... Reporting required at the state or federal agency level
Costs / Production Loss / Down-time / Quality	No loss	Event costing less than $10,000. ... Reporting required only at the department level	Event costing $10,000 to $100,000 ... Reporting required at the site level	Event costing more than $100,000 ... Reporting required above the site level

Figure 23 – Prioritisation Matrix and Semi-quantitative Risk Matrix *(Hollifield & Habibi, 2001)*

This database is should become the master data for alarm configuration. If a change to an alarm is required the correct work flow is to rationalise the alarm, document it in the Master Alarm Database. It is then implemented into the DCS configuration based on the information in the Master Alarm Database. The work flow should not work backwards where changed are made in the DCS configuration first and then back filled into the Master Alarm Database.

Documenting the alarm also captures one of the key components of Alarm Management – the correct operator response to the alarm. Considering that an alarm system may consist of 1000's of alarms it is not practical to expect an operator to know the correct response to every alarm. Making this information available to operators is required. Newer HMI platforms now include the ability to integrate the Master Alarm Database to the HMI so the operator has direct access to this information when an alarm activates.

5.3.2. Performance Monitoring

Performance Monitoring closes the continuous improvement process loop. Alarm activation data is analysed and compared against performance metrics. If any metrics are exceed then the individual alarms causing the performance metric exceedance are identified – these are called Bad Actors. Bad Actors are investigated to establish the root cause of the performance issue and changes are made to ensure they no longer cause performance issues.

In some cases Bad Actors are a result of poor alarm design. The treatment options for these alarms are to apply the best practice techniques such alarm masking, hysteresis and time delays. Sometimes the operation of the subsystem needs to be observed. Unreliable and faulty equipment can cause Bad Actor alarms. The treatment option for these alarms is not in the scope of alarm management. It usually requires engineering and maintenance personnel to investigate and correct the issues with the equipment. In some cases the alarm itself does not fit the definition to be an alarm. No investigation of alarm rates or subsystem operation will change the fact that the alarm is just not required. The treatment option for these alarms is removal. In some instances there is a combination of several alarm problems which are the cause of a Bad Actor.

Using the data in the alarm and event database Alarm reports are produced which analyse the chronological nature of the data. Reports are produced over various periods. ISA-18.2-2009 recommends that analysis of alarm performance should be conducted with data over a period of at least 30 days. It is not uncommon thought have daily, weekly and monthly alarm reports.

One of the key performance metrics used is the average alarm rate. This alarm rate should only consider alarms for the plant area that the operator is actually monitoring – not the whole site, unless of course, the operator monitoring the whole site. ISA-18.2-2009, EEMUA 191 and the ASM consortium all recommend that the 'likely to be acceptable' alarm rate for an operator 150 alarms per day. This works out to be approximately one alarm per ten minutes. This is based on the time it takes for the operator recognise the alarm, decide the correct course of action, take the action and monitor the return to normal process conditions. This must be completed along with the operator's other tasks. ISA-18.2-2009, EEMUA 191 and the ASM consortium also recommend that the 'maximum manageable' alarm rate is 300 alarms per day.

A full list of the ISA-18.2-2009 performance metrics can be seen in *Figure 24*. This is the most comprehensive list of performance metrics available the current industry guides and standards. Note that it may not be necessary or appropriate to implement all performance measures identified in *Figure 24*. This judgement must be made based on the needs, size and complexity of the site. The alarm rate should always remain the key performance metric though.

Alarm Performance Metrics Based upon at least 30 days of data		
Metric	**Target Value**	
Annunciated Alarms per Time:	Target Value: Very Likely to be Acceptable	Target Value: Maximum Manageable
Annunciated Alarms Per Day per Operating Position	~150 alarms per day	~300 alarms per day
Annunciated Alarms Per Hour per Operating Position	~6 (average)	~12 (average)
Annunciated Alarms Per 10 Minutes per Operating Position	~1 (average)	~2 (average)
Metric	**Target Value**	
Percentage of hours containing more than 30 alarms	~<1%	
Percentage of 10-minute periods containing more than 10 alarms	~<1%	
Maximum number of alarms in a 10 minute period	≤10	
Percentage of time the alarm system is in a flood condition	~<1%	
Percentage contribution of the top 10 most frequent alarms to the overall alarm load	~<1% to 5% maximum, with action plans to address deficiencies.	
Quantity of chattering and fleeting alarms	Zero, action plans to correct any that occur.	
Stale Alarms	Less than 5 present on any day, with action plans to address	
Annunciated Priority Distribution	3 priorities: ~80% Low, ~15% Medium, ~5% High or 4 priorities: ~80% Low, ~15% Medium, ~5% High, ~<1% "highest" Other special-purpose priorities excluded from the calculation	
Unauthorized Alarm Suppression	Zero alarms suppressed outside of controlled or approved methodologies	
Unauthorized Alarm Attribute Changes	Zero alarm attribute changes outside of approved methodologies or MOC	

Figure 24 – ISA-18.2-2009 Performance Metrics *(ISA, 2009)*

Alarm reports can be presented many different ways. It is common to present alarm rates in graphic format. This allow for quick visualisation of how well the alarm system is performing overall. Tables showing actual alarm performance for each performance metric are also used – *Figure 25* shows an example. This report uses the performance metric of daily alarm rate; the peak alarm rate, which looks at the number of alarms in a 10 minute period; alarm flooding; fleeting alarms; the top ten percentage; and, standing alarms.

Performance Metric	This Week	Last Week	Benchmark	Unit
Average Alarm Rate Per Operator				
U100/200/500	1.91	1.62		
U300	1.68	1.31	< 1.0	Alarms / 10 minutes
U400/650	0.50	0.62		
U550	0.47	0.64		
Peak Alarm Rate Per Operator				
U100/200/500	55	18		
U300	29	42	< 10	Alarms / 10 minutes
U400/650	12	28		
U550	13	14		
Alarm Flooding				
U100/200/500	4.27	2.18		
U300	2.58	1.59	< 1%	% of time
U400/650	2.48	1.09		
U550	0.20	0.10		
Chattering Alarms	0	0	0	No. of alarms
Top 10 Alarms Occurrence	43.1	34.8	< 5%	% of total alarms
Standing Alarms	69	58	< 5	No. of alarms

Figure 25 – Example of alarm report results against performance metrics

A common analysis to include in an alarm report is a top alarm table. This is most frequently occurring alarms in the reporting period. Normally the top ten, 20 or 50 alarms are presented in descending order of their total activations. This allows several performance metrics to be interpreted easily, as well as the identification Bad Actors. The table can be used to quickly direct efforts to improve and maintain the alarm rates. Some of the key columns are included are the total count of activations as well as the percentage of the total count (as percentage of the total activations in the reporting period). Another useful column is the cumulative percentage of each alarm, working down the table.

Alarm	Description	DCS	Priority	Count	Percent	Accum
PI1114::HI_ALM	Coke Conveying to C201A/B	DV	Medium	62	44.93	44.93
SEQ_C102_STT::INTLK_ALM	C102 Coke Start/Run Sequence	DV	Low	18	13.04	57.97
XCV1107::FAIL_ALM	C102 Coke Blow Egg Discharge	DV	Low	18	13.04	71.01
PIC1116::LO_ALM	Nitrogen to C103 Ore Blow Egg	DV	Low	8	5.80	76.81
TI1101::HI_ALM	Coke to Online C201A/B	DV	Low	7	5.07	81.88
KYI1002::HI_ALM	Coke Feed Delay	DV	Low	6	4.35	86.23
TI1102::HI_ALM	Ore to C201 Chlorinator	DV	Low	5	3.62	89.85
KYI1001::HI_ALM	Ore Feed Delay	DV	Low	3	2.17	92.03
SEQ_C103_STT::INTLK_ALM	C103 Ore Start/Run Sequence	DV	Low	3	2.17	94.20
XCV1115::FAIL_ALM	Ore to C201 Chlorinator	DV	Low	2	1.45	95.65

Figure 26 – Example of Alarm Top Alarm Table

Figure 26 shows and example of a top alarm table from a daily alarm report. This is an example of how it could be interpreted:

- The top alarm looks to be a fleeting alarm – there are 62 activations while the next ranked alarm has only 18 activations.
- The second and third alarm have the same number of counts. It is know that the second alarm is a sequence and the third alarm is a valve operated by that sequence – these two alarms are for the same problem so half of the count of these two alarms is not required.

By focusing efforts to deal with the first alarm and ensuring the second alarm and third alarm do not both activate for the same problem could improve the alarm rate by 58% (refer to the second row in the 'Accum'). The third alarm looks to be a problem with the valve – a discrepancy alarm. If maintenance could investigate rectify the valve the third alarm could be eliminated, the overall improvement would then be 71% (refer to the third row in the cumulative 'Accum' column).

This example shows some of the problems identified in alarm reports are not just poorly configured alarms – they are actual problems with the plant or equipment. A well performing alarm system can quickly identify process and equipment problems. This improves can improve the effectiveness of maintenance at a facility. Rothenberg (Rothenberg, 2009) suggests that within six months of practicing a good alarm management regime unplanned maintenance costs by will reduce by 5 – 15%.

Chapter 6 – The Project Site

The project site is one of Western Australia's largest coal fired power plants. For commercial reasons the site has requested to remain unnamed.

6.1. Coal Fired Power Generation Process Description

The following is not exhaustive description of all aspects of the coal fired power generation process. It gives a basic understanding of the industrial process which will help put into context some of the decisions and approaches used to select the correct alarming strategies for Bad Actor alarms. *Figure 16* shows a schematic presentation of the process.

The process of coal fired power generation has largely remained unchanged for many decades. The combustion of coal produces heat energy. The heat energy is used in a Rankine cycle where the heat energy is transferred to water, which is converted to steam. The steam is feed to a turbine where the heat energy is extracted from the steam and converted into mechanical energy. The steam is then condensed back to water and the cycle continues again. The mechanical energy produced in the turbine is used to drive a generator which creates electrical energy.

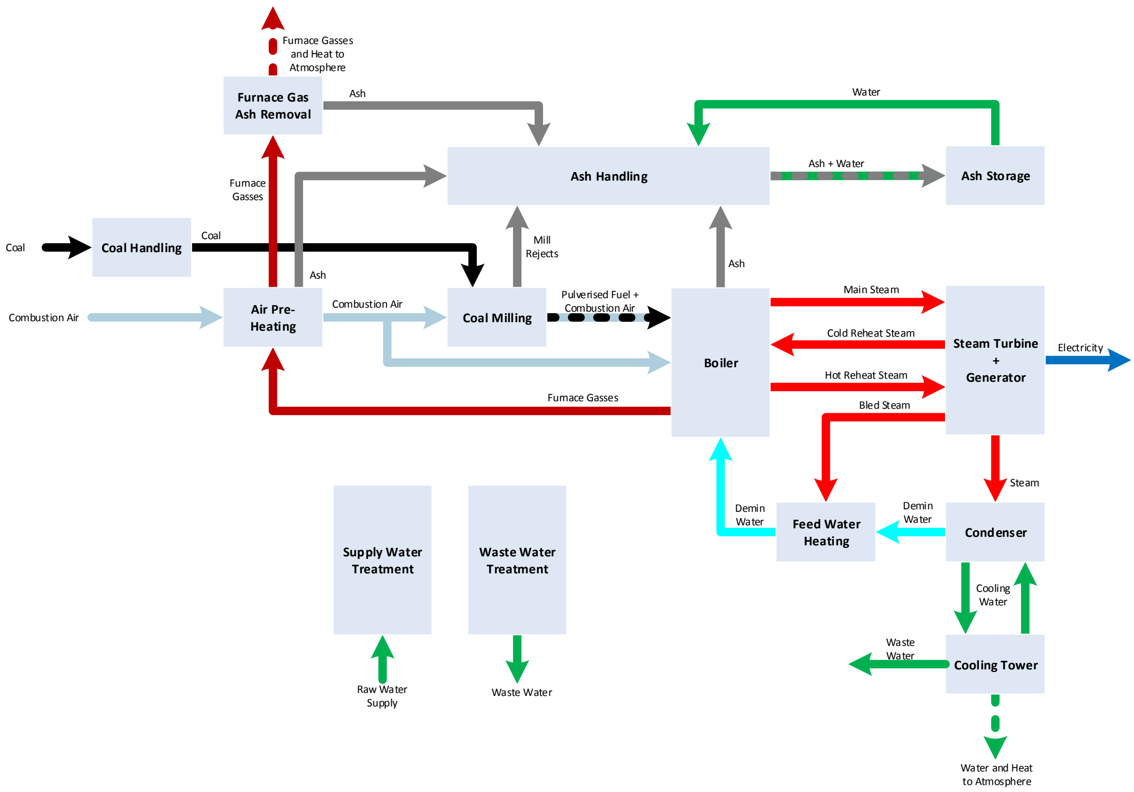


Figure 27 – Coal Fired Power Generation Process

6.1.1. Coal Handling

Coal is delivered to the project site from local mines by an overland conveyor system. The size of the coal is approximately 50mm by 50mm by 50mm. Once the coal is received on site there are two options – it may be conveyed to large hoppers call coal bunkers where it is feed directly into the Boiler furnace or directed to onsite stockpiles. The used of coal from the stockpiles or direct bunkering of the coal is managed based on coal delivery windows and the amount of coal in the coal bunkers. There are several conveyers and transfer points which manage the movement of coal around the site.

6.1.2. Air Pre-Heating

Air for combustion is preheated before being delivered to both the Coal Milling plant and directly to the Boiler. The combustion air pushed into the Boiler using a large fan called a Forced Draft Fan. The heat for the pre-heating is recovered from the Boiler Furnace Gasses. The Furnace Gasses are drawn out of the Boiler using large fans call Induced Draft Fans.

The air pre-heater collects Ash from the combustion of the coal. The ash is removed on a regular basis to prevent ash blockages forming in the air and furnace gas paths. The ash is collected and transferred to the Ash Handling plant several times a day.

6.1.3. Coal Milling

Before coal is feed to the Boiler is it milled to a powder consistency in large machines called Pulverisers. The coal (or Pulverised Fuel) is then blown directly to the Boiler using some of the pre-heated combustion air. The heat also removes any trapped moisture in the coal.

The coal supply contains impurities such as pyrites (iron sulphides commonly found in coal reserves), sand and rock. The Pulveriser is able to separate the out these impurities. The impurities (or mill rejects) are sent to the Ash Handling plant.

6.1.4. Boiler

The Boiler is a large furnace where Pulverised Fuel is combusted. The walls of the furnace are made from metal tubes filled with water that circulates throughout the Boiler. The radiant heat energy from the combustion is absorbed into water and it is converted into steam. The steam is then piped to into heat exchangers where convection heat energy from the combustion gasses super heats the steam. The superheated steam the supplied to the steam turbine.

The water supplied to the Boiler is high quality demineralised water. This ensures that corrosion does not damage the metal components in the Boiler and steam turbine. The quality of the water in the Boiler is closely monitored and controlled. To maintain the quality of the water a portion it is continuously replaced with new water from the Water Treatment Plant.

One of the by-products of the combustion of coal is ash particles. Apart from the environmental considerations of emitting particulate matter to the environment, the ash must be removed from the Boiler to prevent blockages. The Boiler is designed to accumulate ash in specific areas. From these areas the ash can be removed in a controlled manner while the Boiler is operating. The ash is removed using specialised plant and equipment to transfer the ash to the Ash Handling plant several times a day.

6.1.5. Steam Turbine and Generator

The steam turbine consists of three separate turbines connected to a common shaft. The High Pressure turbine converts the heat energy in the Main Steam into mechanical energy. The steam is then sent back to the Boiler again and reheated. The Hot Re-heat Steam is supplied to the Intermediate Pressure turbine where further heat energy is extracted and converted into mechanical energy. The steam is then directed to the Low Pressure turbine where the last possible amounts of heat energy are converted into mechanical energy. Some of the steam in the High Pressure and Intermediate Pressure turbines is directed to the Feed Water Heating plant. This steam is referred to as Bled Steam.

The Generator is a synchronous alternating current generator. The common shaft of the three steam turbines is linked to the rotor of the generator. The rotor contains a rotating magnetic field that is produced using direct current voltage. The Generator casing contains the three phase windings where the electrical power generated and output for transmission to the electrical energy grid.

6.1.6. Condenser

Steam that exits the Low Pressure turbine is cooled in the shell side of a large shell and tube heat exchanger. The steam condenses into water. This is then pumped to the Feed Water heating plant.

Cooling water in the tube side of the condenser is supplied from the Cooling Tower. This water is low quality water. It carries away the latent heat energy recovered from the steam as it condenses into water.

6.1.7. Cooling Tower

The cooling water from the Condenser cascades down the Cooling Tower. Large fans blow air through the cooling water as it cascades down. The removes the heat energy in the Cooling Water. The heat energy is released into the atmosphere and a large amount of water also evaporates. The cooling water is then returned to the condenser.

The evaporation of the cooling water means that significant amounts of water are required to keep the cooling water system full of water. The cooling water is also affected by the accumulation of salts and biological growth. The quality of Cooling Water is closely monitored and controlled. The main method to control the quality of the water is to constantly relace the water with new water from the Supply Water Treatment plant. This creates significant amounts of Waste Water.

6.1.8. Feed Water Heating

To improve the efficiently of the Rankine cycle the feed water is heated bled steam from the steam turbine. A series of shell and tube heat exchangers increase the temperature of the feed water. The bled steam condenses in the shell section of the heat exchangers and is then returned to the feed water

6.1.9. Furnace Gas Ash Removal

Some Ash is left in the furnace gasses after it exits the Boiler and Air Pre-Heating plant. This ash is removed from the Furnace Gasses using electro-static attraction. The ash is collected and transferred to the Ash Handling plant.

6.1.10. Ash Handling

All of the ash from the Boiler, Air Pre-Heater and Furnace Gas Ash Removal is mixed with water so it can be transferred to the Ash Storage area using pumps.

6.1.11. Ash Storage

Ash and water are pumped into a large dam on the site. Here the ash and water are separated. The water drains to central collection point where it is recovered and returned to the Ash Handling plant for reuse.

6.1.12. Supply Water Treatment

Raw Water is supplied to the site and stored in a large dam. The raw water is neither suitable for use as cooling water or boiler water. The Supply Water Treatment plant produces water which able to be used in the cooling water system as well as demineralised water for the boiler. Some waste water is created as a by-product.

6.1.13. Waste Water Treatment

Waste water from the Boiler, Cooling Tower and Supply Water Treatment plant is treated. Salty water is produced and piped offsite for disposal. Other impurities are concentrated and sent to the Ash Storage area.

6.2. Control System Infrastructure Description

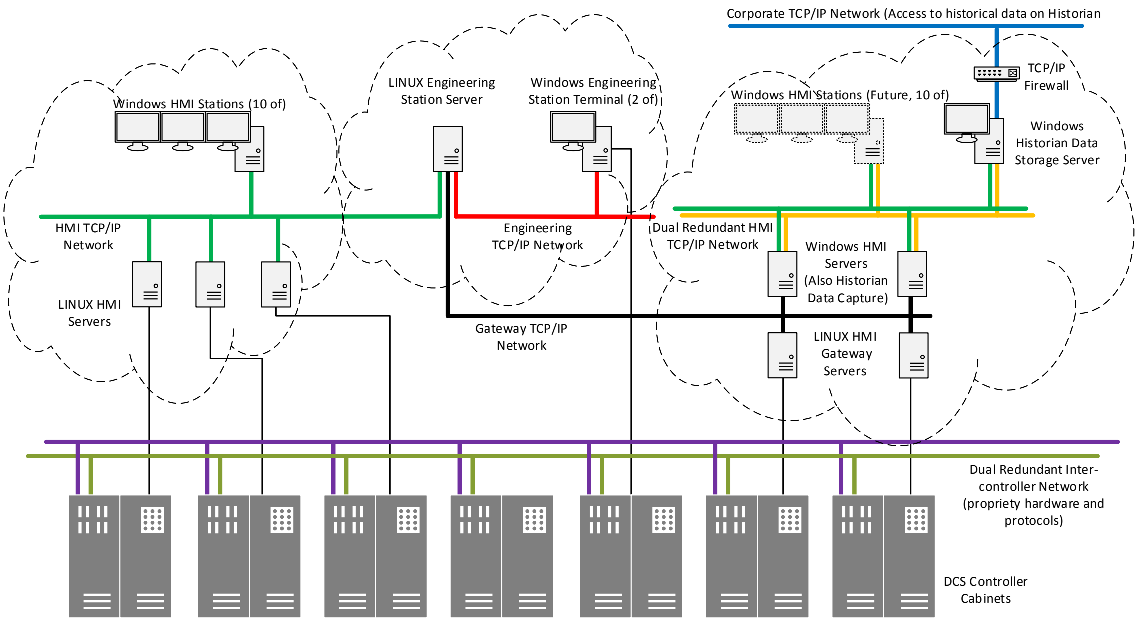


Figure 28 – Site Control System Infrastructure

The following is not exhaustive description of all aspects the control system infrastructure. It gives a basic understanding of the control system infrastructure which will help put into context some of the decisions and approaches used to develop tools such as the Master Alarm Database and alarm reports.

6.2.1. DCS Controllers and I/O Interface

There are twenty DCS controller cabinets which can contain up to 64 cards each. Three types of cards are predominantly used in the control system; a universal input card which can read both 'analog' and 'digital' inputs; a 'digital' drive card which has the required inputs and outputs for a 'digital' drive; and, an 'analog' drive card which the required inputs and outputs for an 'analog' drive. The drive cards also serve as the DCS controllers. The application software is allocated to the drive cards. Some of the drive cards are only used for application software and do not have a connection to any drives.

The controller cabinets are spread through several areas in the plant. A proprietary dual redundant inter-controller network links all of the controller cabinets. There are specialised serial communications cards for interfacing to the HMI system and engineering stations.

6.2.2. HMI System

There are two HMI systems in use at the project site. The first system is the original system that was installed when the site was constructed. This system can be seen in the left clouded region in *Figure 28*. This system is the primary HMI used for operation of the plant. The system is based on three Linux HMI servers. There is a Thinwire Coaxial TCP/IP connection from the each HMI server to a specialised serial communications card. This is the communications interface that connects the HMI server to the inter-controller communications network. This allows the HMI server to access all required signals throughout control system.

The HMI server acts as a central data concentrator for the current status and values of process variables, alarm handling and forwarding operator commands to the DCS controllers. The HMI servers use the X-Window system (a windowing system for Unix/Linux type operating systems) to provide the HMI interface to Windows based HMI stations. There are 10 HMI stations throughout the plant. Only five HMI stations are available for control of the plant. Three are located in the central control room and one each in the Coal Handling plant and Water treatment plant. The other HMI stations are for engineering and management access to view the operation of the plant. These are located in offices around the plant.

The second HMI system is a newer system. This system was installed as a part of an upgrade to replace the primary HMI system. This upgrade has stalled and has not been completed. There are plans to resume the upgrade in the near future. This system can be seen in the right clouded region in *Figure 28*. It uses Linux based 'Gateway' servers with the same type of Thinwire Coaxial TCP/IP connection to the inter-controller communications network as the primary HMI system. A Windows based HMI server is then paired to each Gateway server. The HMI server would act as a central data concentrator for HMI stations but none have been installed. There are two Gateway/HMI server pairs for redundancy. There also a dual redundant TCP/IP HMI network for the new HMI system.

6.2.3. Engineering System

The engineering system comprises of a LINUX based server with two Windows based engineering stations. This system can be seen in the central clouded region in *Figure 28*. The server is the central of a database for the configuration of the application software. The engineering stations are where the applications software is developed. There is an RS232 serial link from each engineering station to specialised serial communications cards. This is the communications interface that connects the engineering stations to the inter-controller communications network. This allows the engineering stations load the application software to any of the DCS controller cards.

The engineering station connects to three TCP/IP networks – the engineering network; the primary HMI network; and, the 'Gateway' network, which is part of the new HMI system. It acts as a TCP/IP Router for these networks. HMI configuration information for the application software is sent to each of the HMI systems via these networks.

6.2.4. Historian System

The Historian is part of the new HMI system – this is one of the reasons why both HMI systems are still active. The Historian is integrated into the new HMI system. This system can be seen in the right clouded region in *Figure 28*. This Historian server is a Windows based server running proprietary database software to store 'analog' data and Microsoft SQL Server to store alarm and event data.

The Historian server connects to the dual redundant TCP/IP HMI network. It uses OPC communications protocols to collect 'analog' data from the HMI servers. Alarm and event data is transferred to the Historian using propriety software on the HMI servers. In the case of one of the HMI server's failing the other will continue to be available for the Historian and data storage will continue uninterrupted. In the event of a failure of the Historian server the HMI servers will buffer data until the HMI server is available again. All the buffered data will then be transferred to the Historian, meaning no data will be lost.

The Historian server also has a connection to the business TCP/IP network via a TCP/IP firewall. This allows client applications on the business network to access data on the Historian. Client Proprietary software tools are installed on many computers on the business network to access both 'analog' and alarm and event data. There are also Microsoft Excel Addin's that allow both 'analog' and alarm and event data to be exported into spreadsheets for further analysis.

Chapter 7 – Alarm Philosophy

The structure of the Alarm Philosophy is explained in the following sections. This is not a complete recount of the document. It explains some of the rationale behind the development of the Alarm Philosophy. The Alarm Philosophy document itself can be found in Appendix D.

When developing the Alarm Philosophy there were three considerations. Firstly it is expected that the Alarm Philosophy will mature as the site journeys towards sustainable alarm management practices. For this reason the Alarm Philosophy does not attempt to fully comply with ISA-18.2-2009. Attempting full compliance is likely to overwhelm the site and jeopardise the success of their alarm management program.

The second consideration was the technical capability of the DCS at the project site. It pre-dates standards and guides such as ISA-18.2-2009 and EEMUA 191. It does not have the technical capabilities or features to be fully compliant with requirements of an alarm system identified in these standards and guides. Some limitations and work arounds must be in place.

The final consideration was the resourcing at the project site. Like many organisations the personnel at the project site are very busy with many tasks. Trying to implement a new system of work that heavily impacts many personnel could also jeopardise the success of their alarm management. The Alarm Philosophy is focused on developing some operational discipline in the alarm management and improving the daily alarm rate, which is the main problem area at this time.

7.1. Alarm Management Roles

The development of the Alarm Management Roles, where possible, avoided allocating individuals to roles. Instead the roles were mainly allocated to departments. The roles reflect the actual groups that already exist at the project site. The roles identified in the Alarm Philosophy are:

- Site Management Team
- Alarm Champion
- Asset Engineering
- Production
- Maintenance

The Site Managements Team is the most significant role is alarm management. They must provide the resourcing to complete the activities required. The resourcing includes all of the physical resources as well as the time resources of site personnel. Without the support of the Site Management Team alarm management will fail.

The Alarm Champion role was created so a single person could coordinate all of the activities required for successful and sustainable alarm management. This is the only role which does not exist at the project site at present. This is not a new position at the project site, rather a responsibility should be assigned to a person with skills in control systems as they knowledge of the control systems and alarms system, as well as skills in systems integration engineering. This provides the right skill set for driving alarm management.

The role of the Production department is important to the success of the alarm management efforts. The operators are the members of the Production department. They are the end users of the alarm system. The Production department need to hold the Alarm Champion to account for the performance of the alarm system.

The role of the Asset Engineering and Maintenance is to provide the technical expertise to support alarm management. These groups have knowledge of the design intent and operating limits of the plant and equipment.

7.2. Alarm Management Model

The Alarm Management Model was developed to provide a visual means to identify the activities and systems involved in alarm management. It also reinforces the continuous improvement nature of alarm management.

The core of the Alarm Management Model (shown in blue in *Figure 29*) includes the following:

- Rationalisation
- Master Alarm Database
- Management of Change – a work process to manage technical changes at the facility, although not in the scope of the Alarm Philosophy it is important to define how alarm management relates to Management of Change
- DCS Configuration – this reflects the actual alarm as configured via the engineering station. Its position in the Alarm Management Model reflects that Rationalisation should always be performed on new alarms and the Master Alarm Database is now the master data for alarm configuration, i.e. where the specification the alarm configuration is held.
- Real-time Control – this reflects that fact that the configuration and subsequent loading of this configuration into the DCS controllers is what actually results in alarms
- Alarm and Event History Collection – this reflects the Historian where the chronological data on the activation of alarms and events is collected.
- Alarm Performance Reporting

Another feature of the Alarm Management Model is the work flow entry points. Three workflow entry points are identified:

- Existing Alarms (the orange start point in *Figure 29*) – as there has been no alarm management at the project site all existing alarms have not been designed as per the Alarm Philosophy. It therefore may be prudent to pro-actively rationalise some of these alarms. This may include all alarms from a particular plant subsystem, e.g. all alarms on the generator; or, alarms that are similar in function from several different subsystems, e.g. all electrical current alarms for high voltage motors.

- New alarms (the grey start point in *Figure 29*) – may be required due to new plant equipment being installed or personnel may have identified new alarming strategies to assist operators in the management of abnormal situations.
- Bad Actors (the green start point in *Figure 29*) – are identified in the alarm reports.

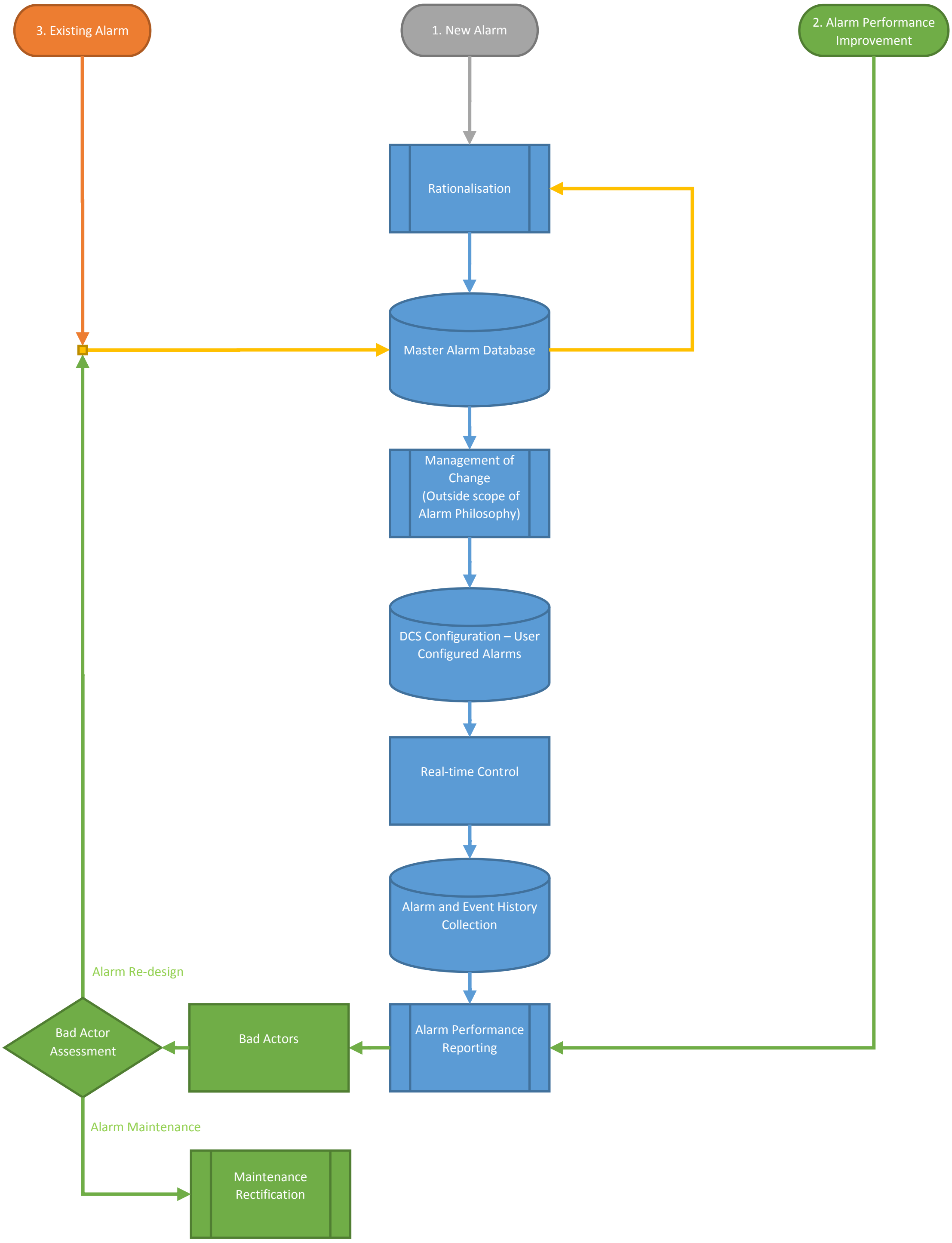


Figure 29 – The Alarm Management Model

The final feature of the Alarm Management Model is Bad Actor resolution (shown in the green in *Figure 29*). There are two possible treatment options for Bad Actors. The first is the Maintenance Rectification. Alarm maintenance issues include faulty equipment, mal-operation or insufficient protection offered by the process control layer. The resolution does not require the alarm to proceed through the Alarm Management Model.

The second treatment option for Bad Actors is Alarm Re-design. This requires the alarm to proceed through the Alarm Management Model, i.e. it is to be rationalised. This will result in changes and improvements to eliminate the performance issues. It is then documented in the Master Alarm Database and then installed in the DCS controller using site's Management of Change process.

7.3. Alarm System Description

The importance of the Alarm System Description section is to define the alarm system. This importance of this is twofold. It clarifies the capabilities of the alarm system and also identifies its limitations.

The alarm system at the project site pre-dates recommendations from both EEMUA 191 and ISA-18.2-2009. Many of the technical requirements identified in these documents do not exist at the project site. An example is the alarm handling capabilities identified ISA-18.2-2009, including states such as 'Shelved', 'Suppressed by Design' and 'Out of Service'.

One of the features of the HMI is alarm masking. The application software only provides a signal reference to activate the alarm masking. The implementation of alarm masking does not match the ISA-18.2-2009 definition. In the HMI alarm masking only prevents the alarm from making an audible sound and flashing, i.e. it will progress directly to the Active and Acknowledged state (refer back to Section 2.3.3 and

Figure 15 for details). The alarm will still appear in the Alarm List, in an alarm state on graphical displays and also be recorded in the Historian as an alarm activation.

It is not recommended to use this feature be used on the project site as it does not fit the definition in ISA-18.2-2009. Instead alarm masking should be implemented in the application software that is loaded into the DCS controllers. Note that it was found that the HMI alarm masking feature was seldom used. It was more common to see alarm masking implemented in the application software.

7.4. Alarm Rationalisation

This is where the alarm rationalisation process is defined. ISA-18.2-2009 (ISA, 2009) suggests that this process should utilise a team approach, which was adopted. The Alarm Philosophy identifies the site personnel who are required at all times, as well as requiring other expertise as needs dictate. The Alarm Champion is nominated as the leader of the rationalisation process.

The rationalisation process also includes specific guidance avoid badly designed alarms. The guidance includes:

- The definition of an alarm
- Ensuring a control system layer is used – alarms should not be used to guide normal operation
- Ensuring the alarm is no the last layer – there should be a shutdown layer
- Ensuring alarms are not used to prevent harm to people
- Alarms are not be used for 'information only'
- Grouping of alarms with the same response

The rationalisation process captures the DCS configuration information required to implement the alarm in the application software. A functional description of the alarm is also required. This may be as simple as a process variable exceeding a predefined limit or a complex series of Boolean logic on several different conditions, or a combination of both. Any time delays, hysteresis and alarm masking are also considered. Selecting these three attributes correctly can prevent the alarm creating problems in the future such as fleeting alarms and standing alarms.

The following items are what really define an alarm. If these points cannot be addressed, especially the corrective actions, then the alarm cannot be justified.

- Consequence of No Action or Incorrect Action
- Maximum Time for Operator to Respond
- Potential Causes
- Corrective Actions

Determining the consequence may require several areas of expertise. This is the benefit of using a multi-disciplinary team in the rationalisation process. It is also expected that this information will be accessible to an operator in real time. The corrective actions must be in the context of actions the operator can understand and actually take. This is the importance of having an operator as part of the process.

Another important part of the rationalisation process is selecting an appropriated alarm priority. The alarm management corporate directive issued to the project site included an example prioritisation matrix as proposed by Hollifield and Habibi in the book Alarm Management: A Comprehensive Guide (Hollifield & Habibi, 2001). This matrix has been adopted for the project site. *Table 3* shows the risk matrix as used in the Alarm Philosophy.

A semi-quantitative risk matrix was developed to accompany the prioritisation matrix. One of the advantages of this type of risk matrix over a fully qualitative method is that it requires less resourcing to use. *Table 4* shows the alarm consequence matrix used in the Alarm Philosophy.

Table 3 – Alarm Prioritisation Matrix

Maximum Time for operator to respond	Consequence		
	Minor	Major	Severe
>30 minutes	Event	Event	Event
10 to 30 minutes	3	3	2
3 to 10 minutes	3	2	2
<3 minutes	2	1	1

Table 4 – Alarm Consequence Matrix

Consequence Category	Consequence		
	Minor	Major	Severe
Safety	Any alarm that prevents harm to personnel shall be Priority 1. *Alarms shall not be used as the primary layer of protection to prevent harm to personnel		
Environment	Local clean up required	Major clean up required Incident report to corporate level	Offsite clean up required Breech of License conditions or incident report to regulator
Assets Damage or Loss	Damage or loss <$10K	Damage or loss >$10K	Damage or loss >$100K
Business Interruption	Loss of availability of redundant equipment	Temporary loss of generating capacity <24 hours	Unit Trip or Shutdown Temporary loss of generating capacity >24 hours
Asset Integrity	Any Alarm that protects Asset Integrity shall be Priority 2. *Asset Integrity is related to consequences of continued operation outside of safe operating windows where consequences may be reduced asset life or a scheduled plant shutdown to make repairs.		

Two of the consequence categorises in *Table 4* were developed specifically for the Alarm Philosophy. Alarms should not be used as the last layer of protection to prevent undesirable consequences. A shutdown layer should be used in the case were there has been no action or incorrect action in response to an alarm. Based on this it is likely that for the bulk of alarms the consequences of no action or incorrect action will result in some sort of shutdown. The Business Interruption consequence category was created for this reason.

The Asset Integrity consequence category was created as the project site has been issued another engineering directive covering asset integrity and safe operating windows. Plant and equipment may be operated at conditions that do not result in immediate consequences, and therefore would not result in an alarm being created. Prolonged operation at these conditions may result in shortened asset life so should therefore be prevented. An example is the creep lift metal components operating at very high temperatures. Alarms in this category are automatically assigned a Priority of 2. They require the operator to adjust operation of the plant to ensure it is operating within safe operating windows.

7.5. Alarm Performance Monitoring

In order to monitor the alarm system performance regular reports are required to analyse the historical alarm and event data stored on the Historian. The definition of an alarm for the reporting is "all priority 1, 2, 3 and Maintenance alarms". This represent alarms which the operator is expected to provide a response. For the alarm reports Disturbance alarms have been ignored. This is based on ISA-18.2-2009, clause 9.3.2 which states:

> "Those alarms for which the console operator's primary response is simply to relay the information to the appropriate person or group for action (e.g. instrument diagnostics alarms) should be reviewed if an alternative method exists the transfer the information without burdening the operator or the alarm system." (ISA, 2009)

This coincides with current practice on the project site where Disturbance alarms are filtered out of alarm displays. Disturbance alarms are diagnostic type of alarms. In most instances they do not necessarily represent a condition that requires a response from an operator. Disturbance alarms should be monitored regularly (daily) by technical personnel.

Common reporting periods for alarm reports are monthly, weekly and daily. For the project site only monthly and weekly reports were chosen. This is as a result of two factors. Firstly the baseline alarm rate is an order of magnitude higher than the recommend performance metrics. There are consistent Bad Actors that are generating a significant portion of the alarms. Focusing on daily alarms may shift focus to the fleeting alarms that may only create an issues for a day. These alarms are important to resolve but the focus must initially remain on the alarms that will give the most sustained improvement.

Secondly the project site resourcing is limited and finite. The project site is not prepared to resources alarms management on a day by day basis. The monthly reports will keep the focus on sustained improvement. The weekly reports will give glimpse of alarms that may be creating a short term performance issue while still keeping the longer term objectives in focus.

The chosen alarm metrics for the alarms reports are Alarm Priority Distribution, Top Alarms and Daily Alarm Total. These alarm reporting metrics do not reflect all of those recommended as best practice. The Alarm Priority Distribution includes Maintenance priority alarms. These are not included in any of the recognised performance metric. The ideally there should be no maintenance alarms, though some will exist. It was decided not redistribute the recommend distribution of the recognised metric to include Maintenance alarms. Instead a target of less than 5% of the total alarm count for Maintenance alarms was set.

The alarm reports will also include three tables of top alarms. The tables will include the count, percentage and cumulative percentage. The first table is the Top Alarms – this will list the top twenty alarms in the reporting period based on count. The second table is the Top Maintenance Alarms – this will list to top ten maintenance alarms. Although Maintenance alarms are included in the Top Alarms analysis splitting them out gives a diagnostic for the maintenance department. The third table is the Top Disturbance Alarms – this will list the top ten Disturbance priory alarms. These alarms are not included of any analysis and there are no performance metrics associated with these alarms. Like the Maintenance priority alarms this gives diagnostic for the maintenance department.

Some important metrics have been left out. Alarm flooding has been left out of the metrics because based on the definition of an alarm flood the project site is in a permanent state of alarm flood. Standing alarms have been left out because the baseline alarm rates result in the operators using a sequence of event display for alarms. This effectively filters out standing alarms to the operator. These metrics are important and it is envisaged that these metrics will be used in the future. For now the initial focus remains on improving the daily alarms rates to within the recommend performance metrics.

Chapter 8 – Master Alarm Database

The project site does not have a complete list of all the alarms configured in the DCS application software. There is no means to easily extract a list of all the configured alarms in the DCS application software. The Alarm Philosophy requires that a Master Alarm Database be the master data for all configured in the DCS application software. The Master Alarm Database was developed to support the documentation requirements of the Alarm Philosophy and capture to all of the alarms that are configured in the DCS application software.

8.1. Existing Alarm List

When the site was constructed a comprehensive set of Operations and Maintenance (O&M) manuals were provided by Engineering, Procurement and Contraction (EPC) contractor. Within these manuals a hard copy Alarm List was included. The Alarm List from the O&M manuals was converted to an electronic copy in a Microsoft Excel spreadsheet at some time in the past. Neither the hard copy version, or the electronic version have been maintained, i.e. as new alarms were added to the DCS have not been added to the Alarm List. It is also not known how comprehensive the Alarm List was at the time the project site was handed over after construction. The hard copy Alarm List is sometimes used by operators, though not all know of its existence. Only a few of engineering staff know of the existence of the electronic copy.

The Alarm List comprises of five columns. The first four are based on the DCS configuration of the alarm, while the fifth column is titled 'Cause/Action'. *Table 5* has an explanation of the Alarm List columns.

Table 5 – Columns in the Alarm List

Column	Explanation
KKS Tag	The KKS tag
Description	The text descriptor
Status	Text for the Alarm State
Priority	The priority of the Alarm – 1,2 or 3
Cause/Action	A description of the possible cause of the alarm and/or action to take when it activates

The Alarm List identifies 4863 alarms, of these:

- 386 have no entry in the Cause /Action column
- 225 are identified as 'Information Only'
- 113 suggest to refer to O&M manuals for guidance
- 79 have a limited explanation and then suggest to refer to O&M manuals for guidance
- 36 suggest to refer to engineering staff for guidance

Note: *Table 6* has examples of each of these cases.

This suggests that a little over 80% percent of the alarms in the Alarm List may have had some reasonable consideration into the Cause/Action text. In some causes this is true – the first row of *Table 6* does provide some guidance to the operator to identify why the alarm is active. In other cases the Cause/Action text is not helpful – refer to the second row of *Table 6*. The Cause/Action text only assumes faulty equipment is the cause. There is no reference to process conditions that may be the cause.

Table 6 – Examples from the Alarm List

KKS Tag	Description	Status	Prio	Cause Action
11LDF10CP030 XH62	PRESSURE CPP INLET	<LOW	3	Insufficient inlet pressure for the condensate polisher to function correctly. Check condensate extraction pumps are in service and that the polisher is not isolated from the condensate system. Check that the pressure switch has not been isolated from the condensate system.
11LBG30CP004 XG11	AUX STM PRESS 2 (CRH)	HIGH	2	AUX-STM pressure is high. Faulty transmitter. Check and rectify. Check and replace if necessary
11LBG30CP014 XG11	CRH CV AIR FAIL SW	FAIL	2	
90GBL10EE108 XG11	SUPP WTR TRF P2 CTL VOLT	HEALTHY	3	Information Only
90BMA00CE010 XG11	415V MEAS CUB UV	FAULT	3	Refer to LV switchgear O&M volume 2of3 section3.
11PAD60CE402 XG11	3300V CT FAN 6 THEROVLD	WARNING	3	Motor thermal overload alarm .. Refer to MV switchgear O&M section 3.
11QUA10CQ045 XH11	FW AT ECO 1NL -ACID CTY	>HIGH	2	Refer station chemist for action.

The Alarm List information was kept for the Master Alarm Database. Although a significant portion (>20%) of the guidance in the Alarm List may be of questionable quality, this information may assist in the rationalisation of existing alarms.

8.2. Extraction of DCS Configured User Alarms

There is no method view all of the configured User Alarms in the DCS. The engineering station provides limited lists of the configured alarms. The lists are restricted to alarms within a single Function Group, or the Function Groups for a single alarm. The lists cannot be exported in any way.

8.2.1. Alarm Objects in the HMI

Alarms are configured as part of the application software. The engineering station includes two distinct tools for the configuration of alarms. The first tool is used for the building the application software. ‘Digital’ signals can be created in several ways:

- As limit values from an ‘analog’ signal, e.g. the value has exceeded a pre-defined limit
- A ‘digital’ measurement, e.g. a pressure switch

- The result of Boolean algebra on other 'digital' signals, e.g. valve x is open and pressure y is greater than z

This application software is loaded and processed by the DCS controllers.

The second tool is used for building the objects that form the HMI. The objects are dynamic elements that provide the means for the user to interact with the application software. They are the basic building blocks of the HMI graphical user interface. Objects can include, but are not limited to the following types:

- 'Digital'
- 'Analog'
- Drives

The objects are loaded into and processed by the HMI system.

Some of an object's attributes are configuration information, such as the KKS tag of a process variable. Other attributes are read from the DCS controller such in real time, such as the value of process variable. Some of the attributes are determined by the HMI system, such as acknowledged or not acknowledged state of an alarm. Alarms are a subset of the 'digital' objects. If the priority attribute of a 'digital' object is 1, 2 or 3 then it is an alarm; otherwise it is simply an event.

Much of the following information is not documented within the control system. It was reversed engineered by inspection. The output of the HMI tool is the configuration attributes for all the HMI objects. This is spread across four main types of files ASCII text files. Each files type has a specific suffix, they are:

- .BSIG files – contains configuration attributes for 'digital' objects
- .SIG – contains configuration attributes for 'analog' objects
- .KRS – contains confirmation attributes for drive and controller objects
- .FGR – contains a list of all objects in a function group

The BSIG files are of interest as they contain the configuration of all of the alarm objects.

All of the HMI configuration files reside in a directory on the Linux based engineering station server. The HMI servers have access to this directory. As part of the setup and maintenance of the HMI servers engineering personnel can request the HMI server to update/refresh its configuration of HMI objects. The HMI server will read the files from the directory on the engineering station server and convert these into the actual runtime objects.

As described in Section 2.2.3 the application software is divided into Functions (smallest block of code that can be individually programmed), and the grouped into Function Groups. This hierarchy is maintained in the HMI configuration. There are 396 function groups at the project site.

Each file type is named after a Function Group. All Function groups are named in the format of NNAAANNAA, where 'N' is a numeric character and 'A' is an alphabetic character. The name of the BSIG file for Function Group 11HFC10EA would be '11FHC10EA.bsig'

There is no known limit to the number of 'digital' objects that may appear in a BSIG file, though the maximum found was 439 'digital' objects in file 90CYE00EU.bsig.

There are 13 attributes that define a 'digital' object. The attributes are shown in *Table 7*. Note that the control system is of German origin so many of the attributes are based on German abbreviations.

Table 7 – 'Digital' signal attributes defined in BSIG file

Attribute in BSIG file	Explanation
SIGTYP	Always has a value of 'B', used to signify the next signal in the list
SIGKZ	The KKS tag
SIGBEZ	The text descriptor
SIGEINH	The engineering units if the 'digital' value is associated with a limit valve
SIGADR	The DCS controller address - this is used so the HMI can read the actual value – either 0 or 1 for 'digital' objects
SIGDAT	Data type for the signal – system use
ZUST_1	Text to display when the 'digital' value is 1
ZUST_0	Text to display when the 'digital' value is 0
ZUST_LOG	The 'digital' value that represents the active (alarm) state
PRIO	The priority of the signal 0 – event, 1,2 and 3 are alarm priorities
BGREWERT	The numerical value if the signal is associated with a limit valve
MF_SIG	System use
SPERR_KZ	Masking Signal – if this signal is active then the alarming in the HMI is blocked

The last item in *Table 7* is the Masking Signal. As stated in Section 7.3 and the Alarm Philosophy it is recommended that this feature not be used at the project site.

The configuration attributes the HMI objects in ASCII text files is serialised. That is, it is not presented in a table. It is a list of the attributes for each object in a specific and repeating order.

The following is an extract of BSIG file for Function group 90CYE00EU:

```
SIGTYP: 'B'
SIGKZ: '90SGA40AP010 XG11'
SIGBEZ: 'FPSTN PRESS MAINT RUN'
SIGEINH: ''
SIGADR: '1 206 32 034 06'
SIGDAT: 0
ZUST_1: 'ALARM'
ZUST_0: 'N ALARM'
ZUST_LOG: 1
PRIO: 3
BGREWERT:
MF_SIG: 'N'
SPERR_KZ: ''


SIGTYP: 'B'
```

```
SIGKZ: '90SGA40AP010 XG12'
SIGBEZ: 'FPSTN PRESS MAINT FLT'
SIGEINH: ''
SIGADR: '1 206 32 034 07'
SIGDAT: 0
ZUST_1: 'ALARM'
ZUST_0: 'N ALARM'
ZUST_LOG: 1
PRIO: 2
BGREWERT:
MF_SIG: 'N'
SPERR_KZ: ''
```

The first object '90SGA40AP010 XG11' is for the running status of the fire pump station maintenance pump. This signal has a priority of 3, so it is an alarm. The alarm state is when the 'digital' value is '1', which has the text descriptor of 'ALARM'.

The second object '90SGA40AP010 XG12' is for the fault status of the fire pump station maintenance pump. This signal has a priority of 2, so it is an alarm. The alarm state is when the 'digital' value is '1', which has the text descriptor of 'ALARM'.

The following of the BSIG file for Function group 11ETJ00EA:

```
SIGTYP: 'B'
SIGKZ: '11ETJ00EA006 XU01'
SIGBEZ: 'VACUUM ECO SYSTEM <20kPa'
SIGEINH: ''
SIGADR: '1 039 16 003 02'
SIGDAT: 1
ZUST_1: 'ACTIVE'
ZUST_0: 'N ACTIVE'
ZUST_LOG: 1
PRIO: 0
BGREWERT:
MF_SIG: 'N'
SPERR_KZ: ''
```

The object '11ETJ00EA006 XU01' is for a pressure measurement exceeding a pre-defined limit. This signal has a priority of 0, so it is an event. When 'digital' value is '1', the text descriptor is 'ACTIVE'. When 'digital' value is '0', the text descriptor is 'N ACTIVE'.

Note that these extracts do not show the header and footer information that is present in the files.

8.2.2. Development of BSIG Parser Tool

In order to capture all of the configured alarms a tool has been developed to extract all of the 'digital' objects defined in the 395 BSIG files. The result is a single flat table that represents all of the 'digital' objects that are defined in the application software and configured for use by the HMI. This table includes alarms and events. The alarms are a subset of this configuration.

The BSIG Parser Tool was developed using a VBA procedure in Microsoft Excel. The output is sent to a spreadsheet. When developing the BSIG Parser Tool the following requirements and constraints where placed:

- All of the HMI configuration files directory will be copied off of the engineering server into a local working directory onto the computer running the BSIG Parser Tool.
- No further manual manipulation of the HMI configuration files is to be done, i.e. the BSIG Parser Tool must be able to process the files as copied from the engineering station server.
- The BSIG Parser Tool must be able process required files automatically, i.e. it must be able to determine which files in the directory to process automatically without the user specifying individual files to process.
- The BSIG Parser Tool must ensure each file is processed completely.
- The BSIG Parser Tool must also capture the Function Group that each 'digital' object originates from.
- The BSIG Parser Tool must not create duplicate entries as some digital objects appear in multiple Function Groups

The method employed to extract the data the ASCII text files was text parsing. Parsing is the process where text is split up to smaller blocks of text based on specific characters and symbols, this included control characters such as carriage return and line feed. Parsing is an appropriate choice as structure of all of BSIG files is predictable and consistent.

There were 14 attributes of interest identified for the output of the parser. *Table 8* shows the output attributes and how they map to the attributes contained in the BSIG file. The BSIG file attribute SIGTYP is not used as it is always 'B' for 'digital' objects.

Table 8 – Headers for BSIG Parser Tool output

Column	Column Header	Attribute in BSIG file
1	Tag KKS	SIGKZ
2	Description	SIGBEZ
3	Engineering Units	SIGEINH
4	P14 Address	SIGADR
5	Data Type	SIGDAT
6	Text for Value 1	ZUST_1
7	Text for Value 0	ZUST_0
8	Alarm State	ZUST_LOG
9	Priority	PRIO
10	Limit Value	BGREWERT
11	MF_SIG	MF_SIG
12	Masking Signal	SPERR_KZ
13	Number of FGs	N/A
14	Function Groups	N/A

Two additional fields have been added. Function Groups is sourced from the file name. Number of Function Groups is included as a 'digital' object can appear in multiple Function Groups – this attribute is determined once all of the BSIG files have been processed. Both of these attributes are useful reference to the configuration in the application software.

As there is no routable IP network connection to the engineering station to the business network the files were transferred using portable USB mass storage media. The HMI configuration files reside in a subdirectory called 'PBS_Daten' on the engineering station server. This complete subdirectory, including all other file types, can be copied to the same subdirectory where the BSIG Parser Tool spreadsheet resides. This is important as the tool uses relative references for file operations.

The operation of the BSIG Parser Tool is as follows:

The BSIG Parser Tool firstly sets up the headers as per *Table 8* in the output spreadsheet. Variables such as the row and column index pointers for the output spreadsheet, and the working directly path are initialised.

The procedure uses to main loops. The first, or outer loop, is the File Handling Loop. At the start of the procedure a list of all of the files with the '.bsig' extension is collected using the VBA 'DIR' command. This command will store the first file name with the BSIG extension into a string variable. When looping through files the next BSIG file name can easily be retrieved using the 'DIR' command – this will update the string variable with the next file name.

Some of the BSIG files to not contain 'digital' objects. These files do not follow the naming convention of NNAAANNAA.bsig. If a filename does not follow this convention then the file is skipped.

The Function Group name is extracted from the BSIG file name. It is stored so it can be added to the Function Group attribute for each of the 'digital' object in the BSIG file. The file Handling Loop terminates when the DIR command returns and empty string as the next filename. This means all the BSIG files have been process by the File Handling Loop.

In each operation of the file handling loop the BSIG file contents are processed. To read the contents of the BSIG files the VBA 'Open' and 'Line Input' commands were used. The intent of these commands is read ASCII files line by line. The Line Input command relies on ASCII control characters to determine the end of a line. VBA expects to see a Carriage Return (ASCII character code 13) followed by Line Feed (ASCII character code 10) at the end of each line. As the BSIG files are sourced from a Linux based system each line ends with a single Line Feed control character. This meant that the Line Input command could not detect each line individually. The whole file contents were read as a single line.

To work around this issue is was decided to manage BSIG file lines as part of the text parsing. This option was chosen over manipulating the files prior to parsing. It is possible to add a Carriage Return control character in the correct location. This would require a separate process and potentially another application to manipulate the BSIG files. This would also risk corrupting the BSIG files before they are parsed.

The second, or inner loop, is the Line Handling Loop. The BSIG file is then parsed in this loop. Its operation is as follows:

The next line of text from the BSIG files contents is extracted by searching and tracking the position of the Line Feed control characters. Note that the code ignores blank lines.

If the line begins with the text 'SIGTYP' (which means the start of the next object) the output spreadsheet row index is increased by one and the column index is reset to 1. The name of the Function Group and Number of FGs (set to '1') is also written to the output spreadsheet using the row index and a fixed column numbers.

If the line does no begin with the text 'SIGTYP' the line represents an attribute that is to be written to the output spreadsheet. The text after the ':' character is extracted from the line and written to the output spreadsheet using the row index and column index as the destination reference. The 1 column index is then increased by 1 and the Line Handling Loop repeats.

The Line Handing Loop terminates when there is no more text to search. Once terminated the next operation of the File Handling Loop begins.

A check was implemented to ensure each BSIG file is completely processed. The was implemented to as there was some doubt that larger BSIG files could be read without some of the contents being truncated when using 'Line Input' command.

The last line of each BSIG files starts with the text 'E_DA'. This is part of a string of text indicating the date the engineering station generated the file. By checking the last line of the BSIG file as read by the 'Line Input' command it can be confirmed that the file was processed completely.

If the file is not completely processed then a message is presented to the user to indicate that the file was not fully processed. Note that no files were incorrectly processed by the BSIG Parser Tool.

The final part of the BSIG Parser Tool is the removal of duplicate entries. On the engineering station it is possible to place a 'digital' object in more than one Function Group. Note that the maximum found was for 'digital' object '11HJQ04CP010 XH11', which was in 52 Functions Groups.

The text parsing will create an entry for every 'digital' object it encounters. This means that the parsing will have created multiple entries for a single 'digital' object where it is in multiple Function Groups. Simply deleting duplicates was not an option as the Function Group information was to be retained, i.e. how many and which Functions Groups is the 'digital' object in.

The attribute Number of FGs was included for this purpose. Some additional code was added to the VBA procedure to remove duplicates but retain all Function Group information.

Firstly all of the rows in the output spreadsheet are sorted alphabetically by KKS Tag Name and Function Group. This groups all duplicates together. Starting with the third row as the current row the following loop operates:

If the KKS Tag Name in the current row and the row above are the same then:

- append the Function Group name in the current row to the Function Group name in the row above, and
- increment the Number of FGs value in the row above the current row by one, and
- delete the current row

Else

- increment the current row number by 1

This loop terminates when the current row is empty.

This loop progressively deletes duplicate 'digital' object entries while retaining Function Group name and keeping count of the number of Function Groups the 'digital' object was in.

The operation of the program can be seen visually in *Figure 30*, *Figure 31* and *Figure 32* – note the cross referencing of program flow across the three sheets. The full VBA code listing of the BSIG Parser Tool can be found in Appendix B.1.

The BSIG Parser tool was developed as an intermediary stage in developing the Master Alarm Database so no user interface was developed. It is not envisaged that the project site will require the use of the tool as the Master Alarm Database is the now master data for the alarm configuration.

The BSIG Parser Tool identified 13811 different alarms and events in the DCS configuration. Of this 7084 where identified as alarms. A screen shot of the output of the BSIG Parser Tool can be seen in Appendix B.2

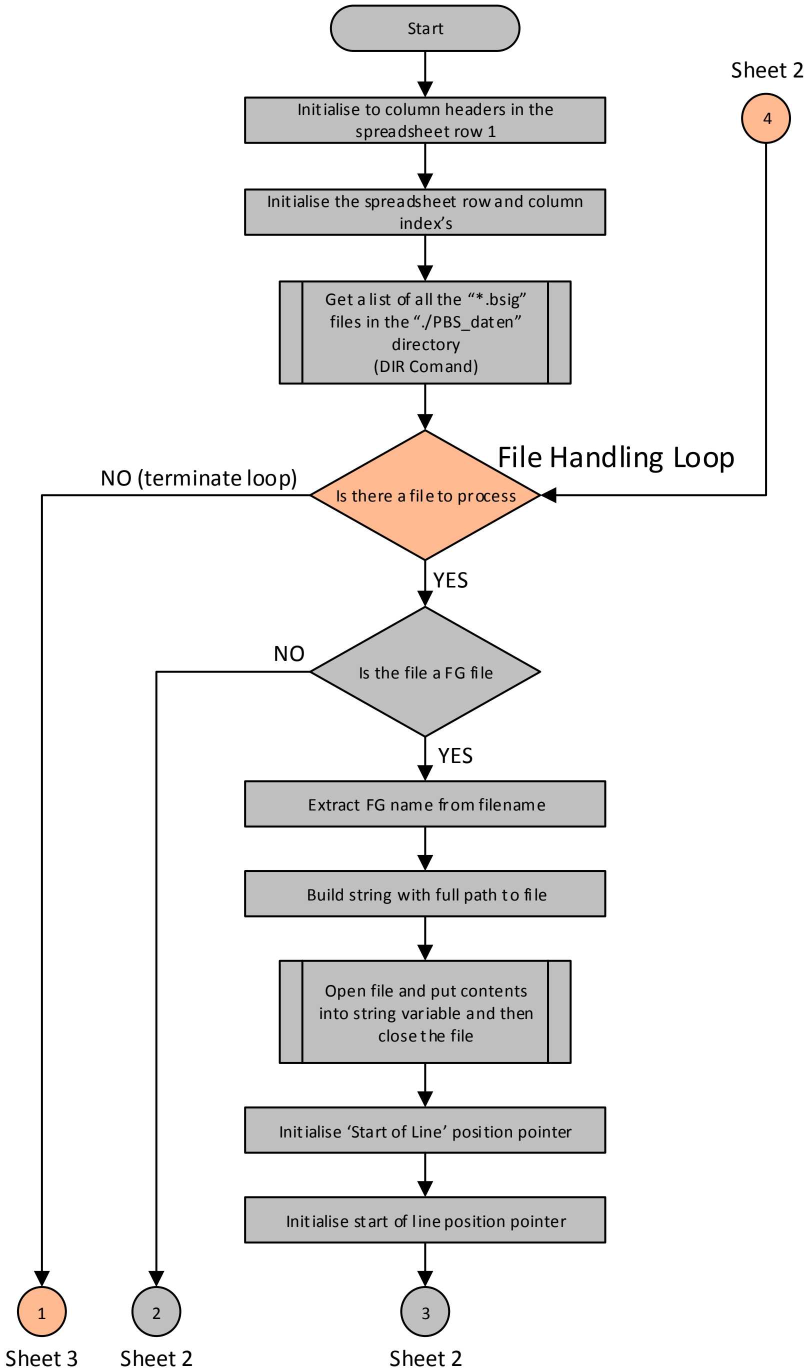


Figure 30 – BSIG Parser Tool flow chart – Sheet 1

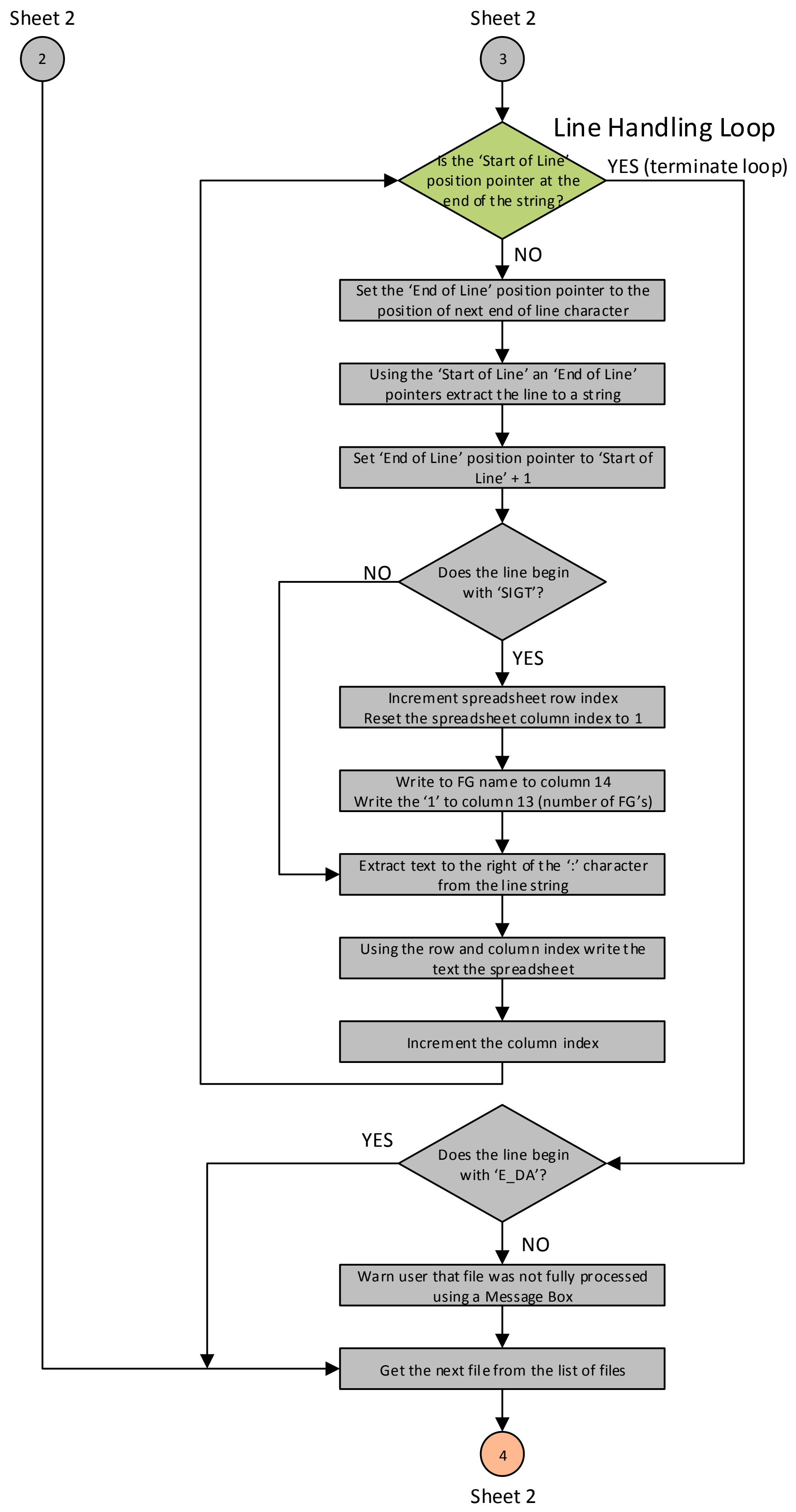


Figure 31 – BSIG Parser Tool flow chart – Sheet 2

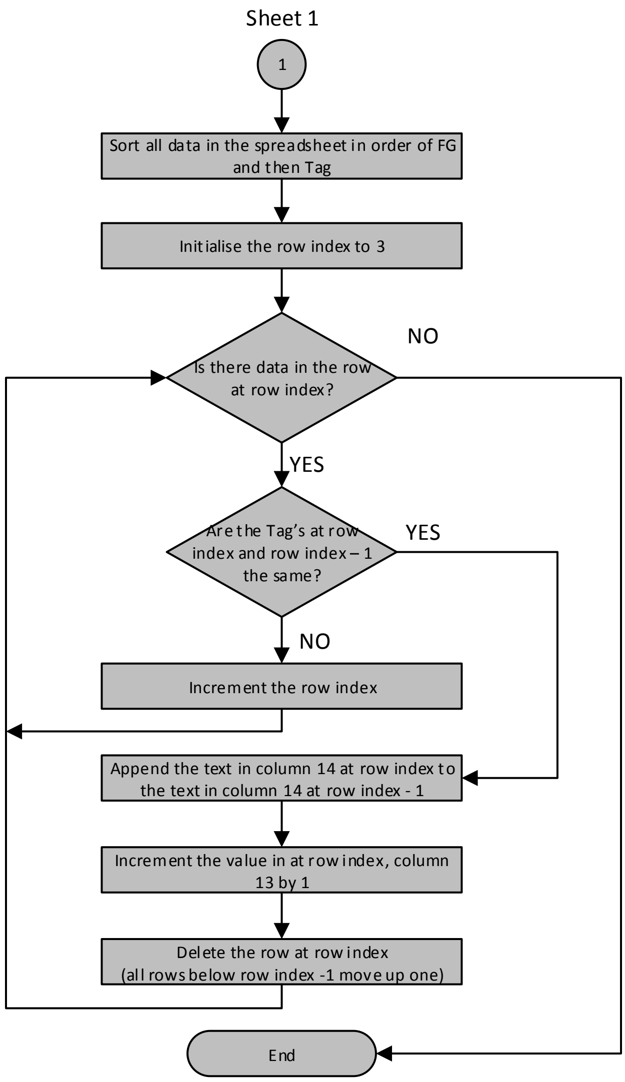


Figure 32 – BSIG Parser Tool flow chart – Sheet 3

8.3. Compilation of the Master Alarm Database

The Master Alarm Database is the combination of the Alarm List with the output of the BSIG Parser Tool structured in a manner that supports the documentation requirements identified in the Alarm Philosophy. To complete the Master Alarm Database the output from the BSIG Parser Tool was expanded to include all required fields identified in the Alarm Philosophy. The data from the Alarm List was then added. To complement the Master Alarm Database a Rationalisation template and Alarm Help feature was also added.

8.3.1. Master Alarm Database

The format chosen for the Master Alarm Database was a Microsoft Excel spreadsheet. This format was chosen for several reasons:

- The Master Alarm Database is a single flat table, which is suitable for spreadsheet
- It is faster to develop than relational database software
- It may be replaced by a commercial product, hence development efforts may be wasted

Alarm Philosophy defines the documentation requirements for the Master Alarm Database. This was the basis for design of the Master Alarm Database. *Table 9* shows the fields created for the Master Alarm Database with an explanation of the each. To aid in the useability Master Alarm Database the fields were grouped. Each grouping is colour coded in Master Alarm Database sheet (same colour coding is used in *Table 9*). The grouping used for the fields is as follows:

- KKS Tag – the unique identifier for each alarm. This is the same as the KKS Tag the alarm has in the DCS
- DCS Configuration – includes all information required to implement the alarm in the DCS application software
- Alarm Guidance – the consequence, cause and action information for the alarm. This is the information that operators need for alarm help.
- Risk Assessment – the risk assessment information used to determine the priority
- General – general administrative information

To construct the Master Alarm Database fields in *Table 9* where used to create the blank database in a spreadsheet. The Output from the BSIG Parser was then imported to the spreadsheet. *Table 10* shows how BSIG Parser Tool output fields where mapped to Master Alarm Database fata fields.

Table 9 – Master Alarm Database Data Fields

KKS Tag		KKS Tag of the alarm signal
DCS Configuration	Description	The text descriptor of the signal
	Alarm Text	The text descriptor for the alarm state
	Normal Text	The text descriptor for the non-active alarm state
	Priority	Priority of the alarm as configured in the DCS
	Type	A choice of :Measured Limit Value Calculated Limit Value Measured Binary Logic
	Alarm Set Point or Logic Conditions	The functional description is the DCS configuration required to implement the alarm. This is the alarm set point or logic conditions that will activate the alarm
	Time Delay	Time delay applied to the alarm
	Hysteresis	Hysteresis applied to the alarm
	Masking Conditions	Identity any logic conditions in the DCS which can be used to prevent the alarm from activating unnecessarily, i.e. sub-system or equipment shutdown which may generate an alarm that is unnecessary
	# FGs	How many Function Groups the alarm is in
	FG	The names of the Function Group(s) the alarm is in
Alarm Guidance	Consequence if no or incorrect action is taken	What is the consequence if no action or the incorrect action is taken - assume any shutdown layers will operate
	Possible Cause	What are the potential causes of the abnormal situation
	Corrective Action	What is the corrective action to be taken to return the process to normal operation
	Time to Respond	How long does the operator have to respond to the alarm in order to prevent the abnormal situation from escalating to the consequence
Risk Assessment	Safety	Refer to the Risk Matrix in the Alarm Philosophy
	Environment	
	Asset Business	
	Recommended Priority	
	Priority	
General	Comments	Any additional comments or justifications should be noted here
	Rationalised Yes / No	Since all alarms have never been rationalised all have been set to 'No'. Set to yes once each alarm is rationalised
	Rationalisation Team	The names and function of those in the session should be recorded here
	Date of Last Rationalisation	The date of the rationalisation session

Table 10 – Mapping of BSIG Parser output to Master Alarm Database data fields

BSIG Parser Output (refer to *Table 8*)	**Master Alarm Database Field (refer to Table 9)**
Tag KKS	KKS Tag
Description	Description
Engineering Units	Not uses
P14 Address	Not used
Data Type	Not used
Text for Value 1	These map to Alarm Text and Normal Text depending on the value of Alarm State
Text for Value 0	
Alarm State	Not used - See above
Priority	Priority
Limit Value	Not used
MF_SIG	Not used
Masking Signal	Not used
Number of FGs	# FGs
Function Groups	FGs

The mapping is direct except for the BSIG Parser Tool output field of 'Text for Value 1' and 'Text for Value 0'. The Master Alarm Database uses the fields 'Alarm Text' and 'Normal Text'. The mapping of these fields is dependent on the BSIG Parser Tool output field 'Alarm State'. If the value of 'Alarm State' is '1' then 'Text for Value 1' was mapped to 'Alarm State' and 'Text for Value 0' was mapped to 'Normal Text'. If the If the value of 'Alarm State' is '0' the mapping was opposite. A simple VBA procedure was created to perform the import of the BSIG Parser Tool output (code not provided).

The Data from the Alarm List was then imported to the Master Alarm Database. The Alarm List has only one text field for alarm guidance – 'Cause/Action'. In the Master Alarm Database there are three fields for alarm guidance. It was decided to map the 'Cause/Action' text into the 'Possible Cause' field. There was no rationale behind this choice – it was an arbitrary decision.

A simple VBA procedure was created perform the import of the Alarm List (code not provided). This procedure looked for KKS Tag matches in the Alarm List and Master Alarm Database. Whenever there was a match the 'Cause/Action' text was copied to the 'Possible Cause' field. For the import the Master Alarm Database was assumed to be the master data as it was derived from the actual DCS configuration, as well as the fact that the Alarm List has not been maintained.

To complete the Master Alarm Database an introduction and instructions were added as well as the field definition – *Table 9*. Note that the instructions refer to the Rationalisation Template describe in Section 8.3.2.

The instruction sheet is documented as follows:

Introduction

This is the Master Alarm Database. It is the master data for Alarms on site. Alarms should not be changed in the DCS configuration without first being identified in this database.

Instructions

1. Prior to the rationalisation session create a copy of the Rationalisation Template and name if after the KKS tag name of the Alarm and fill as many of the DCS Configuration fields as possible.

2. During the rationalisation session fill in all of the fields

Note: if an alarm is to be removed leave all other fields blank and indicate in the comments section that it is to be deleted and the reasons why

3. After the alarm rationalisation session correct site Management of Change procedures should be followed to implement any alarm changes in the DCS configuration, a copy of the completed Alarm Template sheet should be attached to this documentation.

4. Once the DCS Configuration is up to date the information on the Alarm Template sheet for the alarm should copied the Master Alarm Database Sheet and the Alarm Template sheet for the alarm sheet then removed from this file. If an alarm is to be deleted remove its entry in the Master Alarm Database sheet. It is recommended to keep copies of the Alarm Template sheet for alarms in a separated file for reference, especially deleted alarms.

A screen shot of the Master Alarm Database sheet can be seen in Appendix B.3. A screen shot of the instruction sheet can be seen in Appendix B.4

8.3.2. Rationalisation Template

To aid in the rationalisation of alarms a Rationalisation Template was created. This sheet has all of the fields in the Master Alarm Database. Prior to rationalisation a copy of the template should be made each alarm that is to be rationalised. The rationalisation information can them be added during the rationalisation session. A screen shot of the Rationalisation Template can be seen in 0.

One of the features of the Rationalisation Template is an automated determination of the alarm priority based on the prioritisation matrix and risk matrix defined in the Alarm Philosophy. The determination is performed using formulas within the spreadsheet. *Figure 33* shows an example where a Severe consequence with a Maximum Time to respond of 3 to 10 minutes has been selected. The recommend priority has automatically and correctly selected to Priority 2. *Figure 34* shows the same selections, though this time a Safety consequence has been added. The recommend priority has automatically and correctly selected to Priority 1.

Consequence if no or incorrect action is taken					
	Safety	Environment	Asset Damage or Loss	Business	Asset Integrity
Severe				x	
Major					
Minor					

Maximum Time to Respond	
> 30 Minutes	
10 to 30 min	
3 to 10 min	x
Less than 3 min	

Maximum Time to Respond	Consequence		
	Minor	Major	Severe
> 30 Minutes	Event	Event	Event
10 to 30 min	3	3	2
3 to 10 min	3	2	2
Less than 3 min	2	1	1

Recommended Priority	2

Figure 33 – Rationalisation template priority selection

Consequence if no or incorrect action is taken					
	Safety	Environment	Asset Damage or Loss	Business	Asset Integrity
Severe				x	
Major	x				
Minor					

Maximum Time to Respond	
> 30 Minutes	
10 to 30 min	
3 to 10 min	x
Less than 3 min	

Maximum Time to Respond	Consequence		
	Minor	Major	Severe
> 30 Minutes	Event	Event	Event
10 to 30 min	3	3	2
3 to 10 min	3	2	2
Less than 3 min	2	1	1

Recommended Priority	1

Figure 34 – Rationalisation template priority selection with safety consequence

8.3.3. Alarm Help Interface

The Master Alarm Database spreadsheet is not suitable tool for operators. It is quite cumbersome to find specific consequence, cause and action information for an alarm. An Alarm Help Interface was added so the required alarm information could be accessed without having to navigate through the spreadsheet. The Alarm Help Interface only displays information that is relevant to operators.

It is envisaged that a copy of the Master Alarm Database will be made available to operators in the Central Control Room. They have access to the computer on the business network immediately adjacent to one of the HMI stations. The computer is used by operators on a regular basis for electronic operating logs so it a good candidate to use the Master Alarm Database with the Alarm Help Interface active.

The Alarm Help Interface provides a means to quickly search for a specific alarm and retrieve the documented information operators would require. A simple User Form was added to the Master Alarm Database spreadsheet to show the following information for a KKS Tag:

- Descriptor
- Alarm Text
- Consequence if no or incorrect action is taken
- Potential Causes
- Corrective Action

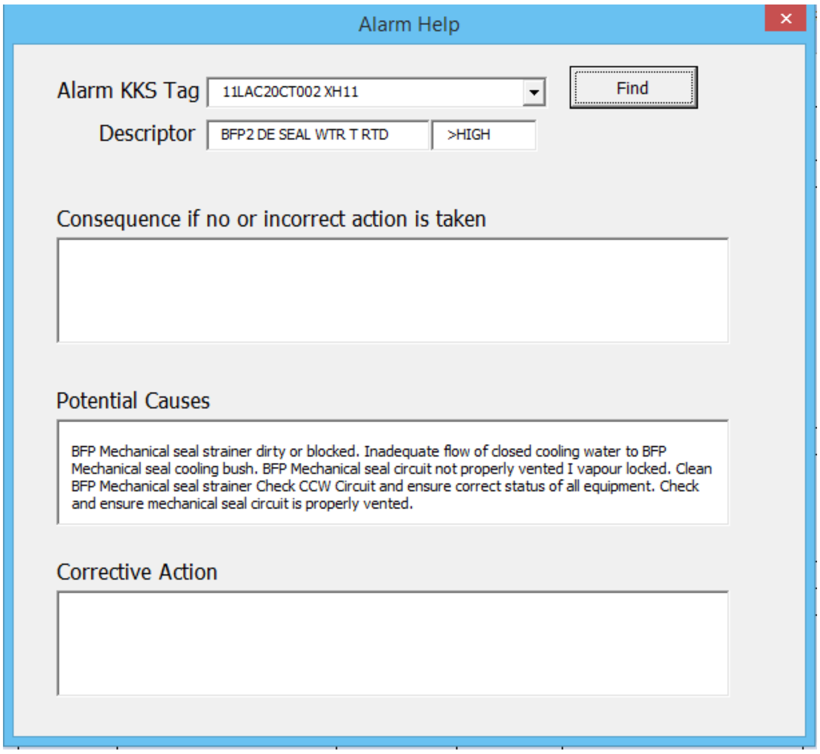


Figure 35 – Screen Shot of Alarm Help Interface

The Alarm Help Interface can be activated by selecting the 'Alarm Help' button in the top left hand corner of the Master Alarm Database sheet (refer to Appendix B.3). When the Alarm Help User Form first opened VBA code populates the Alarm KKS Tag combo box will a list of all of the alarms in the Master Alarm Database spreadsheet.

To find an alarm the user can either use the drop down to scroll to the required alarm or they can begin typing a KKS. The list will automatically begin to filter to the first match it finds in the list. It will continue to filter as typing continues.

To retrieve the information from the Master Alarm Database the 'Find' button on the User Form is selected. This calls a VBA procedure which searches the Master Alarm Database spreadsheet for the alarm that in the KKS Tag Combo box. Using the row number of the alarm as a reference the User Form is populated with the required information. If the alarm cannot be found the all field a cleared except for the Descriptor field, which will display ‘Not Found’.

The Alarm Help interface can be seen in *Figure 35*. The full VBA code listing of the Alarm Help Interface can be found in Appendix B.6.

Chapter 9 – Alarm Report Tool

The Alarm Reporting Tool was developed to support the alarm performance metrics identified in the Alarm Philosophy, refer to Section 7.5 for details.

9.1. Test Environments

As time on the project site is limited a test environments were implemented to allow development of the alarm reporting tools. The test environments replicate the SQL database named "PlaCoEvents" on the Historian. Data from the project site Historian was exported and the imported to the test environments.

Table 11 – Alarm and Event Table Definition

Column Name	Data Type	Comment
EVENT_ID	bigint	Event ID number assigned by SQL server
ts_subsystem	datetime	Date and timestamp of alarm/event in UTC in the format: YYYY-MM-DD HH:MM:SS.000
ts_subsystem_ms	char(3)	Millisecond of alarm/event
ts_notify	datetime	Same as ts_subsystem but time shifted by -8 hours
ts_notify_ms	char(3)	Always '000'
tag_name	nvarchar(100)	Tag name of the HMI object that is the source of the alarm/event as configured in the engineering station and loaded to the DCS controller
tag_description	nvarchar(100)	Text descriptor of the HMI object that is the source of the alarm/event as configured in the engineering station and loaded to the DCS controller
tag_status	nvarchar(100)	HMI system generated descriptor of Alarm condition
tag_limit	nvarchar(100)	Date and timestamp of alarm/event in local time in the format: MM/DD/YY HH:MM:SS
Line_name	nvarchar(50)	Always '800xA'
area_shortID	nvarchar(50)	Always '143413803'
area_longID	nvarchar(100)	Always 'Null'
ev_longdescription	nvarchar(100)	Always 'Null'
ev_shortdescription	varchar(50)	Always blank
ev_comment	nvarchar(400)	Always 'Null'
ev_modif	nvarchar(100)	Always 'Null'
ev_prio	smallint	Priority of alarm/event
info_01	nvarchar(100)	Blank if the row is for an alarm/event transitioning to any 'Active' state, "CLEARED' if the row is for an alarm/event returning to a 'Normal' state
info_02	nvarchar(100)	Always '0x0'
Field_A	nvarchar(100)	Priority of alarm/event (different numbering system)
Field_B	nvarchar(100)	Always 'SIMP'
Field_C	nvarchar(100)	Always '20'
IO	nvarchar(20)	Always blank
ev_ws	nvarchar(50)	Always blank
CompuNo	nvarchar(70)	Always blank
tag_shortdescription	nvarchar(100)	HMI system generated descriptor of Alarm condition
ev_quitt	nvarchar(50)	Always 'Null'
ev_tS_quitt	nvarchar(50)	Always 'Null'

The scope of test system was limited to the alarm and event table “tbl_events”. This table stores all of the alarm and event data collected by the HMI servers. By inspecting the SQL database configuration a specification of the table was created – it can be seen in *Table 11*. Note that this definition is only considered for alarms and events as a result of the application software. Some alarms and events are recorded that are sourced from the HMI server and Historian. These are not presented to operators, so they have been ignored for this project.

Two test environments were required to complete to development of the Alarm Reports. The test environments were created in virtualized operating systems. VMWare Player was used to create and manage the virtualised test environments. VMWare Player is free for non-commercial use.

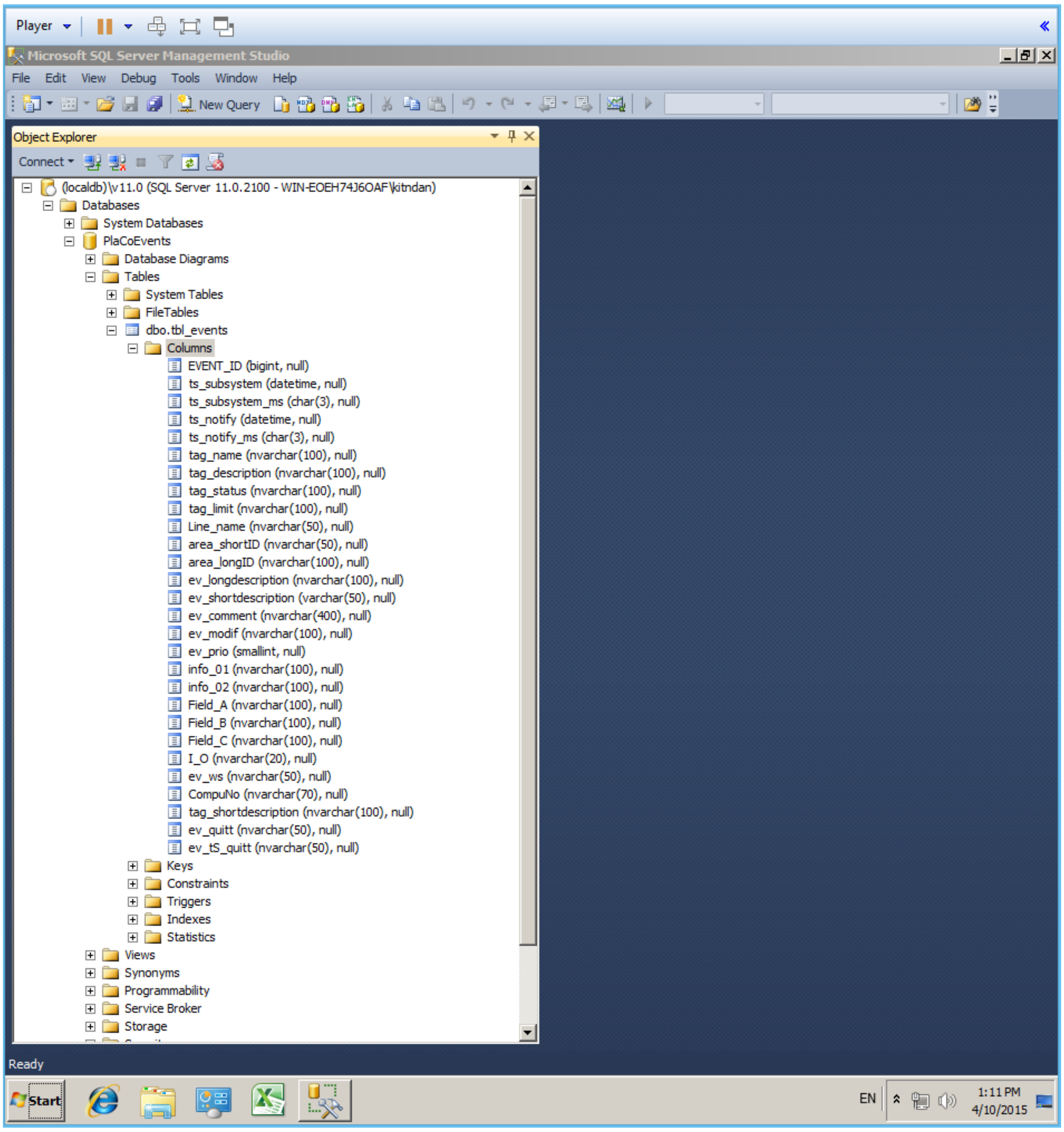


Figure 36 – Screenshot of LocalDB Test Environment

The first test environment was created using Microsoft SQL LocalDB 2012 on a Windows 7 Operating System. LocalDB is aimed at application developers. It is simple to install and manage and free to use. It is based on the 2012 edition of MS SQL Server. Local DB has a database size limitation of 10GB and it does not accept remote connections. The LocalDB 2012 software was administered using Microsoft SQL Management Studio Express 2012. *Figure 36* shows a screen shot of the test environment with table 'tbl-events' created.

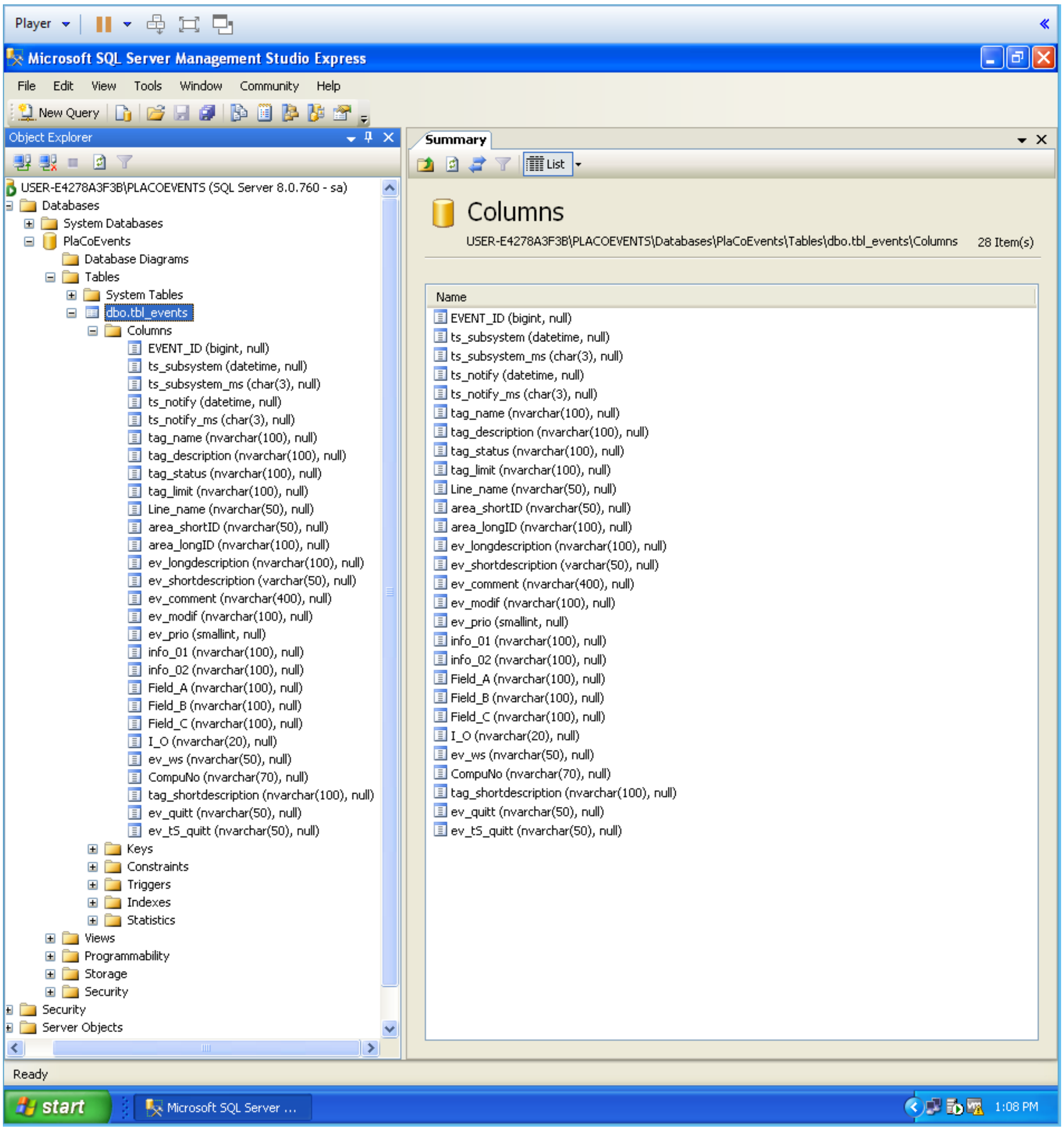


Figure 37 – Screenshot of MSDE Test Environment

The second test environment was created using Microsoft MSDE2000A on a Windows XP Operating System. The use of MSDE is aimed at users with small databases. It is free for non-commercial use. It is based on the 2000 edition of MS SQL Server though it has some built in performance limitations. MSDE2000A has a database size limitation of 2GB and it does accept remote connections. The MSDE2000A software was administered using Microsoft SQL Management Studio Express 2005. *Figure 37* shows a screen shot of the test environment with table 'tbl-events' created.

The size of SQL database at the project site was approximately 380 MB per month. With 1000 days of stored data the total size of the database is approximately 12 GB. The total database would not fit into the either test environment. It was decided to only use data from the 1st of January 2015 for the project. For development of the reports and data analysis of the alarms and events the LocalDB test environment was used. All of the data for 2015 could fit into the 10GB size limitation.

The alarm reports will be installed on a computer on the business Ethernet network. The reporting tools must be able to connect to the Historian SQL database over a TCP/IP network connection. For this reason the MSDE2000A test environment was used for testing. This test environment is based on the same version of SQL as the Historian at the project site - MS SQL Server 2000. This allows any compatibility issues to be minimised before site testing. The size limitation of 2GB of MSDE200A meant only several months of actual data could be imported to the database. This was enough to test the ability to connect using a TCP/IP network and see if there were any compatibility issues between the two versions of SQL in the test environments.

9.2. Historian Event Table Considerations

Prior to creating the Alarm Report Query there were some issues in the way the Historian records alarms and events from the DCS that had to be addressed. Firstly, the new HMI system uses slightly different alarm priority numbering than the original HMI system. If the alarm reports are to be interpreted correctly then the priorities have to be redressed to the same priorities that operators are using in the primary HMI system. The difference in the priorities between the two systems is shown in Table 12. Note that only User and System priorities from the ‘Alarm Type’ column will be used in the alarm reports. These other Alarm Types are system events.

Table 12 – Priority Mapping for Historian and HMI

Historian Priority	Primary HMI Priority	Description	Alarm Type
1	1	User Priority 1	User
2	2	User Priority 2	User
3	Maintenance	Maintenance Alarms	System
4	3	User Priority 3	User
5	N/A	HMI system alarms	N/A
8	Disturbance	Bad Data	System
9	Disturbance	Switchgear Disturbance	System
11	Event	Event	N/A
13	Event	Drive in test position	N/A
14	Event	Logic overrides by user	N/A
15	N/A	Auto Disturbance in drive control	N/A
17	N/A	HMI system events	N/A

Secondly, during the development of the SQL queries it was found that some User Alarms can double up in the alarm reports. This is because the Historian records the alarm twice if the alarm originates from an ‘analog’ limit value where the ‘analog’ value is also used in drive object – one alarm is recorded for the drive object and another is recorded for 'digital' object. This does not reflect what actually happens in the primary HMI, only one alarm is generated.

On inspection it was seen that all entries in the alarm and event table for 'digital' objects have a 17 character KKS tag. This is made up of a 12 character KKS tag of the application software Function, a space character and a four character signal extension. All entries in the alarm and event table for drive objects only have a 12 character KKS – the tag of the application software Function. To prevent this double up only User Alarms with a character length of 17 characters are considered. This ensures only the alarm associated with the 'digital' object is counted in the alarm reports.

Finally, the reference date and time for alarms and events is recorded in three different columns – refer back to *Table 11* for details. In column 'ts_subsystem' the UTC time is recorded. In column 'ts_notify' the date and time shifted by eight hours is recorded. This was thought to be local time at the project site as it was eight hours ahead of UTC. Closer inspection of the date and time in this column showed that the time shift to convert the time to local time was actually applied in the wrong direction, making the date and time in this column time shifted by 16 hours from local time.

In the column 'tag_limit' the date and time in is shown correct to local time. The data in this column is stored as 'text' datatype. This means it may not be interpreted as a date correctly by SQL queries. This could create errors when processing alarm reports.

The other two columns store data as a 'datetime' data type. These columns can be safety used in calculations involving dates. For this reason all analysis of dates will be performed using the column 'ts_subsystem' with eight hours added to convert to local time. Note that the millisecond value of date and times will be ignored for alarm reporting.

9.3. Alarm Report Query

The alarm report query is based on the use of temporary tables. Temporary tables are allocated memory on the SQL server host computer during the query execution. This allows for data to be manipulated as required while not interfering with the alarm and event data in the database tables.

The alarm report query uses the following temporary tables (note that temporary tables are denoted with a '#' character at the start their name):

- #working – all of the alarms in the reporting period. This allows actions such as returning the priority and correcting the time to be performed only on these records of interest.
- #prioritydistribution – this table the is the total count of alarm in the reporting period grouped priority 1, 2, 3 and Maintenance priority
- #topalarms – this table is the top ten priority 1, 2, 3 and Maintenance priority alarms in the reporting period
- #topmaintenance – this table is the top ten Maintenances priority alarms in the reporting period

- #topdisturbance – this table is the top ten Disturbance priority alarms in the reporting period
- #dailyrate – this table the is the total count of alarm in the reporting period grouped per day

The following is functional explanation of alarm report query. It is shown as flow chart in *Figure 39*. The full SQL code listing of the alarm report query can be found in Appendix C.1.

The first task of the query is to delete any of the temporary tables if they already exist. The temporary tables are deleted at the end of the query, but they may already exist if the query did not finish correctly the last time it was run.

The #working table is created by selecting all records from the table 'tbl_events' in database 'PlaCoEvents' that have occurred in the reporting period based on local time. The selection is also limited to records which:

- Have a priority of 8 or 9 (is a System alarm)
- have a priority or 1, 2 or 4 (is a User Alarm) and KKS tag text is 17 characters
- the value in column 'info_01' is not 'CLEARED' (this means the record is for a transition to Alarm state)

Once the #working table has been created the column 'ts_subsystem' is converted to local time by adding eight hours to each time entry. The priorities are converted to those used in the primary HMI:

- 8 and 9 to 6 (6 is a holding priority as 4 is being used)
- 3 to 0 (0 is used for Maintenance priority in the alarm reports)
- 4 to 3
- 6 to 4 (4 is used for the Disturbance priority in the alarm reports)

The #working table is now the source for all further queries. The total number of alarms (Priority 1, 2, 3 and Maintenance) in the reporting period is calculated and stored in a variable. This will be used for further processing.

The table #prioritydistribution is created by selecting the total count of all alarms (Priority 1, 2, 3 and Maintenance) grouped and sorted by priority. A column is created where the count of each priority is divided by the stored total to give a fraction of the total. This is used as the percentage.

The table #topalarms is created by selecting the top 20 alarms (Priority 1, 2, 3 and Maintenance) by count and sorting by the total. A column is created where the count of each alarm is divided by the stored total to give a fraction of the total. This is used as the percentage.

The table #topmaintenance is created by selecting the top 10 Maintenance priority alarms by count and sorting by the total. A column is created where the count of each alarm is divided by the stored total to give a fraction of the total. This is used as the percentage.

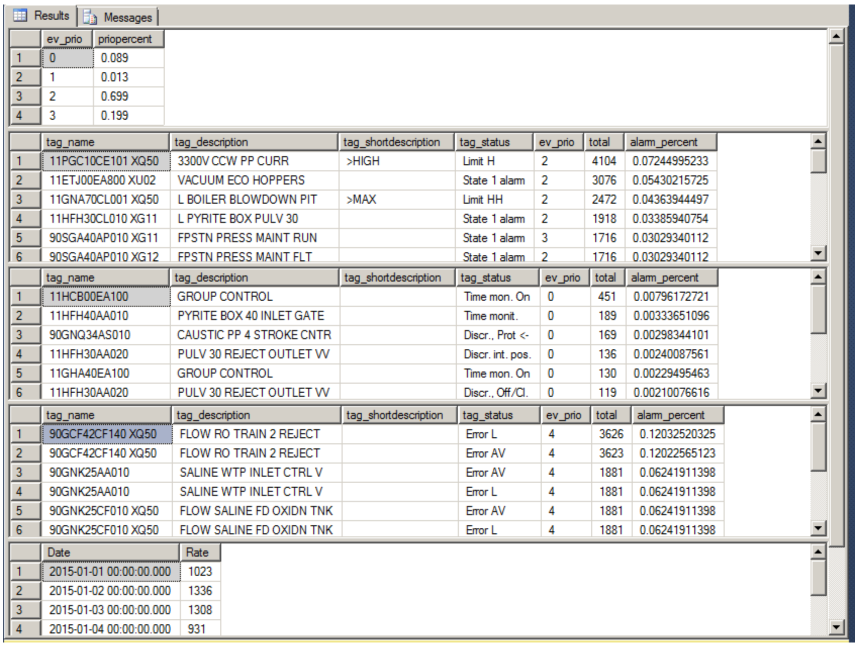
The variable storing the total count of alarms is recalculated as the total number of Disturbance priority alarms. The table #topdisturbance is then created by selecting the top 10 Disturbance priority alarms by count and sorting by the total. A column is created where the count of each alarm is divided by the stored total to give a fraction of the total. This is used as the percentage.

The table #dailyrate is created by selecting the total count of alarms (Priority 1, 2, 3 and Maintenance) grouped and sorted by date.

The temporary tables #prioritydistribution, #topalarms, #topmaintenance, #topdisturbance and #dailyrate are the output of the query.

The final task is to delete all of the temporary tables. This ensures that the memory the tables are using is released. The scope of any variables is only while the query is running and therefore they do not need to be released from memory programmatically.

The output of the alarm report query in Microsoft SQL Management Studio Express 2012 can be seen in *Figure 38*


Results | Messages

	ev_prio	priopercent
1	0	0.089
2	1	0.013
3	2	0.699
4	3	0.199

	tag_name	tag_description	tag_shortdescription	tag_status	ev_prio	total	alarm_percent
1	11PGC10CE101 XQ50	3300V CCW PP CURR	>HIGH	Limit H	2	4104	0.07244995233
2	11ETJ00EA800 XU02	VACUUM ECO HOPPERS		State 1 alarm	2	3076	0.05430215725
3	11GNA70CL001 XQ50	L BOILER BLOWDOWN PIT	>MAX	Limit HH	2	2472	0.04363944497
4	11HFH30CL010 XG11	L PYRITE BOX PULV 30		State 1 alarm	2	1918	0.03385940754
5	90SGA40AP010 XG11	FPSTN PRESS MAINT RUN		State 1 alarm	3	1716	0.03029340112
6	90SGA40AP010 XG12	FPSTN PRESS MAINT FLT		State 1 alarm	2	1716	0.03029340112

	tag_name	tag_description	tag_shortdescription	tag_status	ev_prio	total	alarm_percent
1	11HCB00EA100	GROUP CONTROL		Time mon. On	0	451	0.00796172721
2	11HFH40AA010	PYRITE BOX 40 INLET GATE		Time monit.	0	189	0.00333651096
3	90GNQ34AS010	CAUSTIC PP 4 STROKE CNTR		Discr., Prot <-	0	169	0.00298344101
4	11HFH30AA020	PULV 30 REJECT OUTLET VV		Discr. int. pos.	0	136	0.00240087561
5	11GHA40EA100	GROUP CONTROL		Time mon. On	0	130	0.00229495463
6	11HFH30AA020	PULV 30 REJECT OUTLET VV		Discr., Off/Cl.	0	119	0.00210076616

	tag_name	tag_description	tag_shortdescription	tag_status	ev_prio	total	alarm_percent
1	90GCF42CF140 XQ50	FLOW RO TRAIN 2 REJECT		Error L	4	3626	0.12032520325
2	90GCF42CF140 XQ50	FLOW RO TRAIN 2 REJECT		Error AV	4	3623	0.12022565123
3	90GNK25AA010	SALINE WTP INLET CTRL V		Error AV	4	1881	0.06241911398
4	90GNK25AA010	SALINE WTP INLET CTRL V		Error L	4	1881	0.06241911398
5	90GNK25CF010 XQ50	FLOW SALINE FD OXIDN TNK		Error AV	4	1881	0.06241911398
6	90GNK25CF010 XQ50	FLOW SALINE FD OXIDN TNK		Error L	4	1881	0.06241911398

	Date	Rate
1	2015-01-01 00:00:00.000	1023
2	2015-01-02 00:00:00.000	1336
3	2015-01-03 00:00:00.000	1308
4	2015-01-04 00:00:00.000	931

Figure 38 – Output of SQL Query in SQL Management Studio

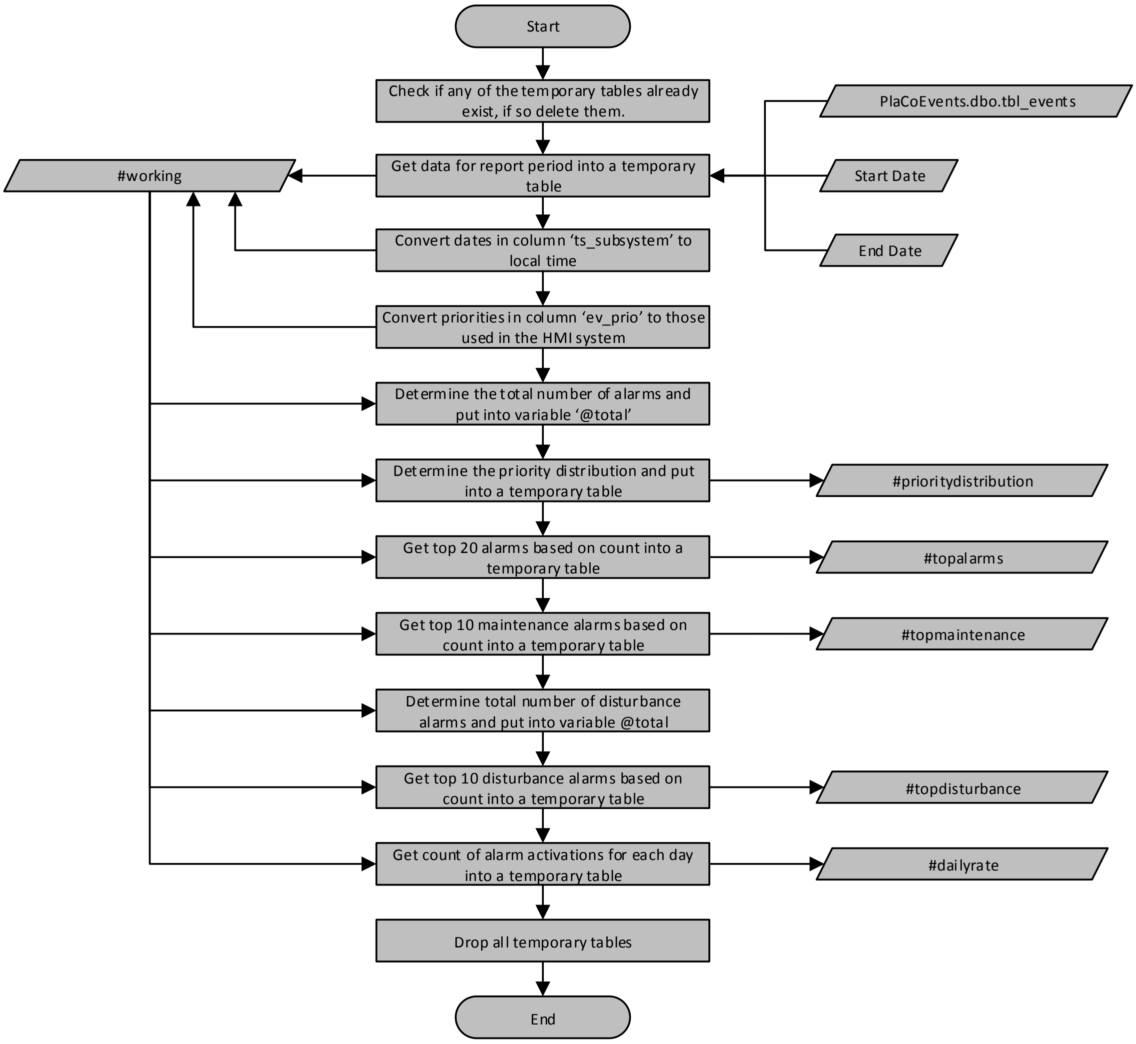


Figure 39 – Alarm Report SQL Query flow chart

9.4. Development of Alarm Report Tool

The alarm report query on its own is not a suitable tool to create alarm reports. The output requires manual manipulation by the user in order to present the data in a meaningful way. To provide a useful tool the alarm report query was further developed into the Alarm Report Tool. The alarm reports will be installed on a computer on the business Ethernet network as installing software on the control system infrastructure is not permitted. To be a useful tool it must be able to produce a report that is suitable for printing without further processing or manipulation by the user

The Alarm Report Tool was developed for Microsoft Excel 2010. A Microsoft Excel spreadsheet solution was chosen as:

- The application is widely used at the project site
- VBA has an interface to SQL Server
- The alarm report query output tables can be easy placed into a spreadsheet

- Data can easily be converted to a chart/graphical format if required

9.4.1. User Interface

To simplify the user interface only two selections are required. First any date within the reporting period, and second the reporting period, either weekly and monthly. This means the user does not have to manually determine the start and end date of the report. Based on these two selections the Alarm Report Tool will determine the start date and end date for the alarm report SQL query.

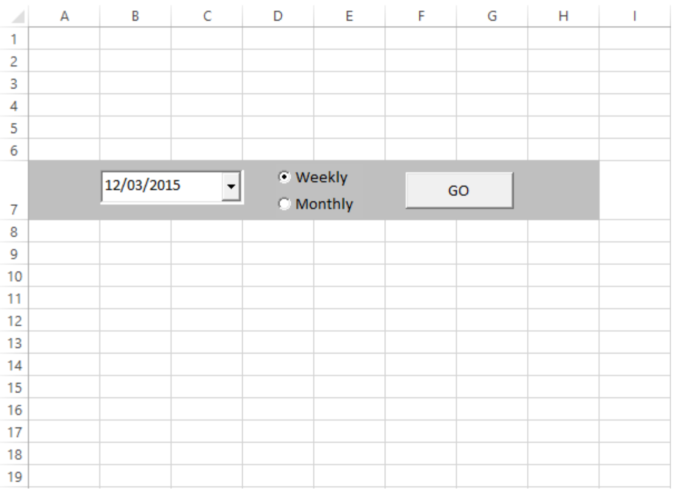


Figure 40 – Screen shot of the Alarm Report Tool user interface

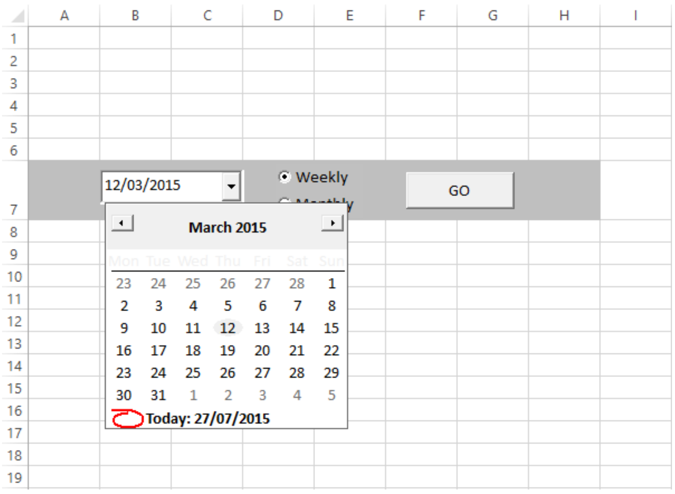


Figure 41 – Screen shot of the Alarm Report Tool user interface date selection

The user interface of the Alarm Report Tool was implemented on a worksheet. This is the only worksheet visible to the user. On this worksheet there is a date selector drop down box, report period radio button and a 'Go' button. When the user presses the

'Go' button the report an alarm report is generated based on the selections made. A screen shot of the user interface worksheet can be seen in *Figure 40*.

To improve the user interface the date selector drop down box uses a graphical month calendar. This is part of the Microsoft Windows Common Controls-2 6.0 (SP6) library. *Figure 41* shows a screen shot of the calendar drop down.

9.4.2. SQL Interface

To enable remote access to the alarm and event data on the Historian an SQL interface is needed. The SQL interface passes queries the SQL database and receives data as a result of the queries. The output of the SQL interface is placed onto a spreadsheet in the correct location to build the alarm report. The SQL interface will be embedded in the Alarm Report Tool.

A VBA SQL interface was developed using Microsoft ActiveX Data Objects (ADO). ADO has the capability to interface to SQL databases. In order to use ADO in VBA two specific libraries are required:

- Microsoft ActiveX Data Objects 6.0 Library
- Microsoft ADO Ext. 6.0 for DDL and Security

Two specific ADO objects from the ADO library were used for the alarm reports. The 'Connection' object can open a unique session to a data source using the 'Open' method. The connection can be to a remote server at any routable TCP/IP address. As well as managing the connection to the data source the 'Connection' object also has an 'Execute' method which can issue commands to the data source. The 'Recordset' object has an 'Open' method where commands that return data can be issued the data source.

To connect to the SQL server using the 'Open' method a connection string is required. The connection string is a series of parameters and their values in a single ASCII text string. The parameters required for the project site and MSDE test environment differ to those needed for the LocalDB test environment. The connection string used for the project site is as follows:

```
Provider=SQLOLEDB; Data Source=PGIM01,1433; Initial
Catalog=PlaCoEvents; User Id=xxxxxxxx; Password=xxxxxxxx
```

The parameters used in the connection string are:

- Provider – a reference to the ADO object so it knows the type of connection
- DataSource – a routable IP address or Host name of the data source where the SQL server is running, note the IP port number can also be specified.
- Initial Catalog – the name of the SQL database
- User Id – a user who has security access to perform the required commands
- Password – the password of the user

The connection string for the LocalDB test environment is specific to an instance of the LocalDB SQL database. It can be seen in *Figure 43*, cell reference R2C1 (Row 5, Column 1 – note RnCn notation will be used to reference spread sheet cells from now). The Data Source parameter needed to be updated each time the SQL server started in test environment as the alpha numeric characters after 'LOCALDB#' were different each time.

The alarm report query has five specific commands that output data. The data returned data is called a record set. Each of these record sets is of predicable size with only the daily alarm rate having any variability. This depends on whether the reporting period is weekly or monthly, and then the number of days in the month. It is only the number of rows that can vary. The five record sets that will be returned data from the alarm report query are shown in *Table 13*.

Table 13 – Alarm Report Query Record Sets

Alarm Metric	SQL Temporary Table Name	Rows X Columns
Alarm Priority Distribution	#prioritydistribution	4 X 1
Top Alarms	#topalarms	20 X 7
Top Maintenance Alarms	#topmaintenance	10 X 7
Top Disturbance Alarms	#topdisturbance	10 X 7
Daily Alarm Total	#dailyrate	up to 31* X 2

* Depending on whether the report is weekly or monthly, and then the number of days in the months

To coordinate the commands that will return records sets the alarm report query was split into groups. Groups of commands that will return a record set then processed by the 'Recordset' object. All the other commands are processed by the 'Connection' object. The splitting of the command groups must maintain the order of the command as per the alarm report query. The 'Connection' object can process multiple commands. The 'Recordset' object can also process multiple commands, though the SQL server may not be able service the request. It was found that the LocalDB test environment running MS SQL Server 2012 could service requests for multiple record sets, while the MSDE2000A test environment based on MS SQL Server 2000 could not service requests for multiple record sets.

Based on this the alarm report query was split into seven groups of commands – all of the commands prior to the first record set, five separate commands for the five record sets, and then a final group for the remaining commands.

The output of the SQL interface needs to be placed onto spreadsheet to build the report. The Alarm Report Tool features a report template and sheet configuration sheet. The report template is a blank report with place holders for all titles and record sets. To complete an alarm report all that is required is to place the record sets in the returned from alarm report query into the appropriate place holders. A screen shot of a portion of the report template can be seen in *Figure 42*. The report template worksheet is usually hidden from the user. It can be unhidden using the Excel interface.

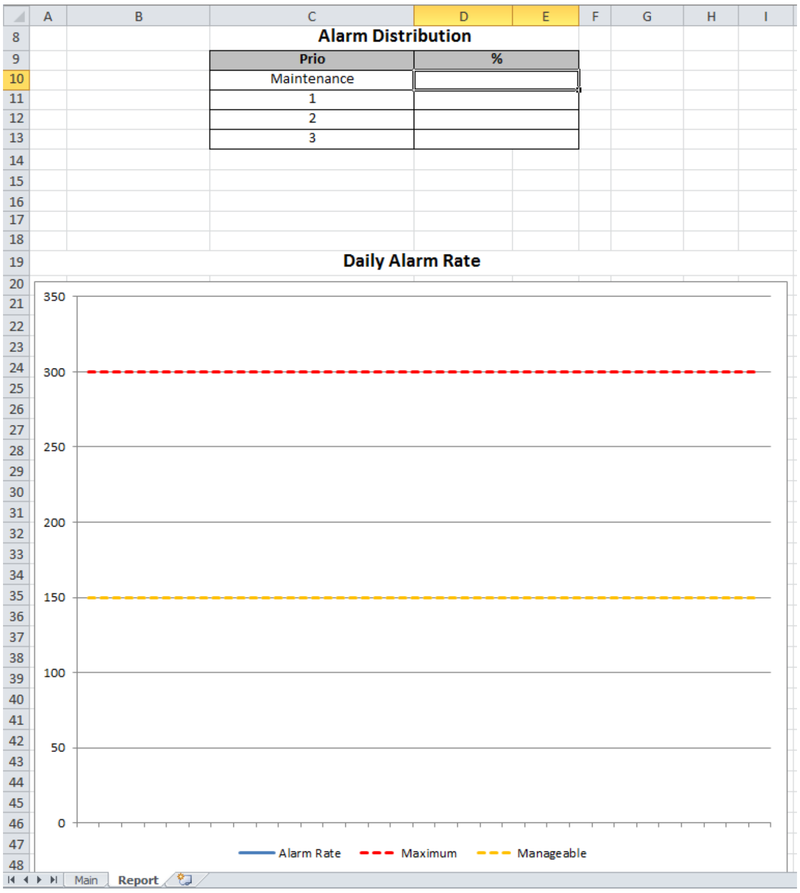


Figure 42 – Screen shot of Alarm Report Tool report template worksheet (part of)

A configuration sheet was also implemented. It has all of the SQL commands and configuration information required to execute the alarm report query. It was implemented so the configuration information could be modified without having to access the VBA code. The configuration sheet has two sections. The first contains the SQL Connection string. The second section contains the groupings of SQL commands that will be processed by the SQL interface. A screen shot of the configuration sheet can be seen in *Figure 43*. The configuration worksheet is usually hidden from the user. It can be unhidden using the Excel interface.

If the grouping of SQL commands is expected to return a record set a cell reference (row and column of first cell where the record set will be placed on the report template) is specified in the cells to the right of the SQL commands. If there is a cell reference then the code will assume a record set will be returned and the SQL commands will be processed using the 'Recordset' object. If there is no cell reference then the code will assume no record set will be returned and the SQL commands will be processed using the 'Connection' object.

As an example consider the Alarm Priority Distribution dataset. In *Figure 43* the SQL command in R5C1 return the temporary table #prioritydistribution as a record set. *Table 13* shows that this record set will be 4 rows by 1 column. In the two cells to the right of the SQL command is the first cell where the top left cell of the record set will be placed on the report template – R10C4. In *Figure 42* at R10C4 is the column for the Alarm Priority Distribution. The other commands returning record set will work in the same manner.

	A	B	C
1	**SQL Connection String**		
2	Provider=SQLOLEDB.1;Integrated Security=SSPI;Persist Security Info=True;Initial Catalog=PlaCoEvents;Data Source=np:\\.\pipe\LOCALDB#0840986E\tsql\query;Use Procedure for Prepare=1;Auto Translate=True;Packet Size=4096;Workstation ID=WIN-EOEH74J6OAF;Use Encryption for Data=False;Tag with column collation when possible=False		
3	**SQL Query**	**Row**	**Column**
4	/* Clean up temp tables */ IF OBJECT_ID('tempdb..#working') IS NOT NULL DROP TABLE #working IF OBJECT_ID('tempdb..#topalarms') IS NOT NULL DROP TABLE #topalarms IF OBJECT_ID('tempdb..#topmaintenance') IS NOT NULL DROP TABLE #topmaintenance IF OBJECT_ID('tempdb..#topdisturbance') IS NOT NULL DROP TABLE #topdisturbance IF OBJECT_ID('tempdb..#prioritydistribution') IS NOT NULL DROP TABLE #prioritydistribution IF OBJECT_ID('tempdb..#dailyrate') IS NOT NULL DROP TABLE #dailyrate		
5	select priopercent from #prioritydistribution order by ev_prio	10	4
6	select tag_name, tag_description, tag_status, tag_shortdescription, ev_prio, total, alarm_percent from #topalarms order by total desc	57	2
7	select tag_name, tag_description, tag_status, tag_shortdescription, ev_prio, total, alarm_percent from #topmaintenance order by total desc	82	2
8	select tag_name, tag_description, tag_status, tag_shortdescription, ev_prio, total, alarm_percent from #topdisturbance order by total desc	97	2
9	select Date, Rate from #dailyrate order by Date	113	2
10	/* Clean up temp tables */ IF OBJECT_ID('tempdb..#working') IS NOT NULL DROP TABLE #working IF OBJECT_ID('tempdb..#topalarms') IS NOT NULL DROP TABLE #topalarms IF OBJECT_ID('tempdb..#topmaintenance') IS NOT NULL DROP TABLE #topmaintenance IF OBJECT_ID('tempdb..#topdisturbance') IS NOT NULL DROP TABLE #topdisturbance IF OBJECT_ID('tempdb..#prioritydisturbance') IS NOT NULL DROP TABLE #prioritydistribution IF OBJECT_ID('tempdb..#dailyrate') IS NOT NULL DROP TABLE #dailyrate		

Figure 43 – Screen shot of Alarm Report Tool configuration worksheet

The SQL interface runs as a subroutine with needing two parameters passed to it. They are the start date and the end date of the reporting period. To pass these parameters to the SQL command text two place holders are used – STARTDATE and ENDATE. Prior to executing the command a VBA string find and replace command replaces the place holders with the actual dates passed to the sub routine. The resulting line of the SQL code in the SQL configuration sheet is as follows:

```
and ts_subsystem > dateadd(hh, -@timeshift,'STARTDATE') and
ts_subsystem  < dateadd(hh, -@timeshift,'ENDDATE')
```

The operation of the SQL subroutine can be seen in *Figure 44*. Sources (configuration worksheet) and destinations (report template worksheet) are shown shaded in green. The full VBA code listing of the SQL subroutine can be found in Appendix C.2.

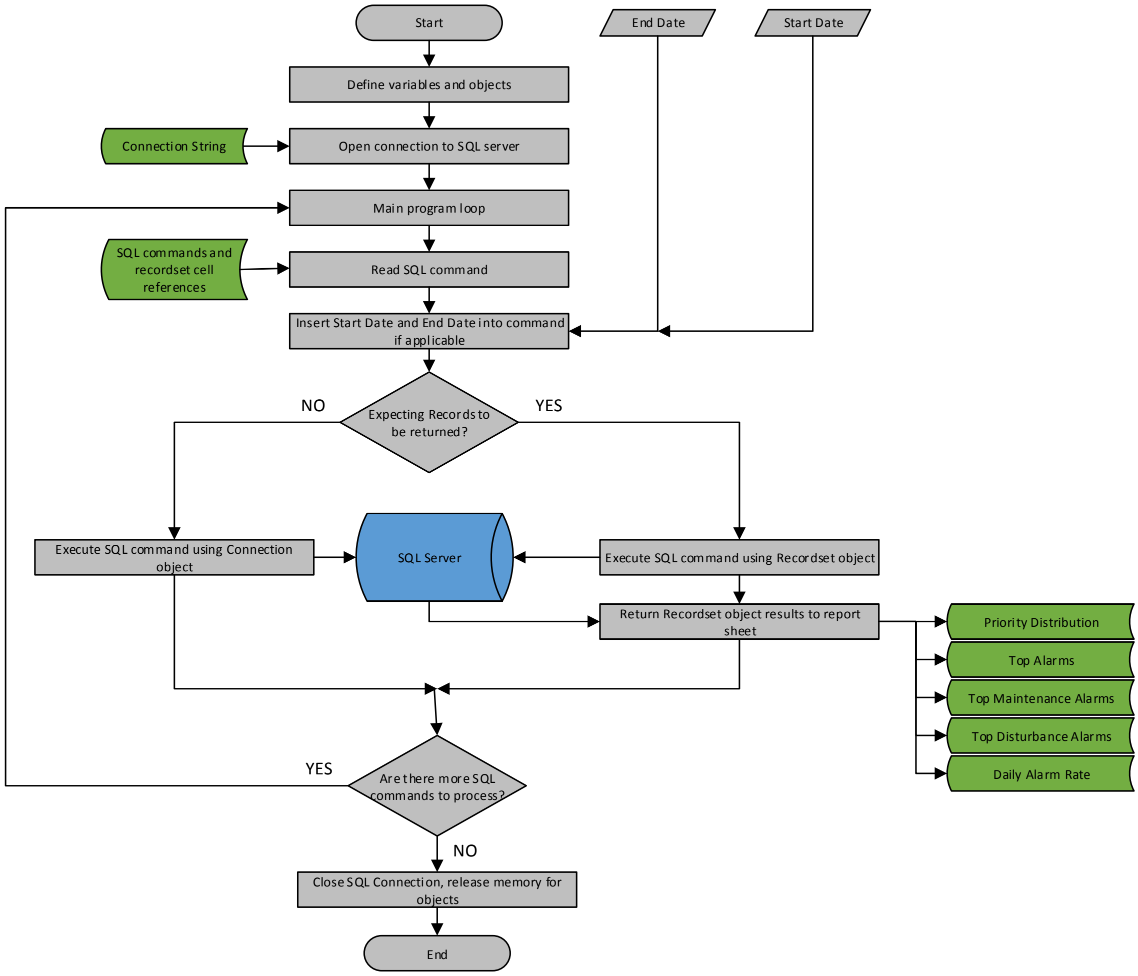


Figure 44 – SQL Subroutine flow chart

9.4.3. Report Generation

Report generation coordinates the operations required to create a finished alarm report. It involves the determination of the start and end dates for the reporting period, calling the SQL subroutine and converting the report template worksheet to the finished alarm report. The code for the report generator is called whenever the 'Go' button on the user interface worksheet is pressed.

The report generator must determine the start and end date as the user interface only provides a date within the reporting period and the actual reporting period – weekly or monthly. If a weekly report is chosen the start date is the Monday prior the selected date. If the selected date is a Monday then the selected date becomes the start date. The end date is then calculated as the following Monday. If a monthly report is chosen the start date is the first day of the month of the selected date. The end date is then calculated as the first day of the following month. The start and end dates are stored as variables to be passed the SQL subroutine.

During report generation a copy of the report template is made and named in the format of 'Weekly *YYYYMMDD*' or 'Monthly *YYYYMM*01'. The dates used are the start date of the report. The SQL subroutine is then called which populates the alarm report with the record sets returned by the SQL interface.

Once the SQL subroutine has finished the alarm report title and subtitle are updated. Weekly alarm reports are titled 'Weekly Alarm Report' with a subtitle 'Monday, *month_name DD, YYYY*'. The monthly reports are titled 'Monthly Alarm Report' with a subtitle '*month_name YYYY*'.

Once of the features of the alarm report is a chart showing the daily alarm rate for the reporting period. The chart shows the daily alarm rate as well as the alarm rate performance metrics of manageable (150 alarms per day) and maximum (300 alarms per day). The chart uses data from the Daily Alarm Rate record set. *Figure 45* shows the charts for the Daily Alarm Rate from a monthly and weekly alarm report. The chart is preconfigured in the report template with its source data from the Daily Alarm Rate record set. This record set is of variable length. For a weekly report it contains values for seven days. A monthly report could contain values for either 28, 29, 30 or 31 days.

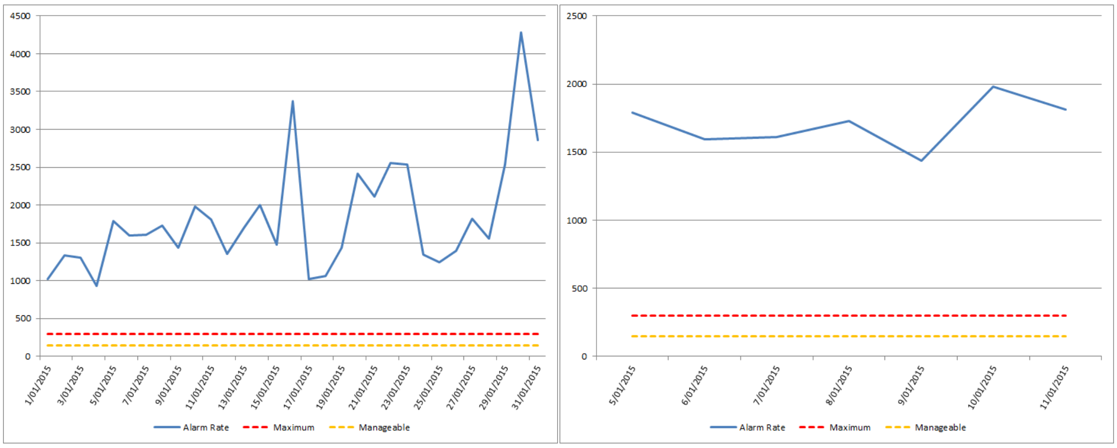


Figure 45 – Charts for Daily Alarm Rate from monthly (left) and weekly (right) alarm reports

To ensure that all possible lengths are catered for the report template is preconfigured for a duration of 31 days. The SQL subroutine will only populate the required number of rows based on the reporting period – weekly or monthly. If there are less than 31 days in the reporting period the chart will show days with no values. To ensure that the chart displays only days in the reporting period the report generator will trim empty rows in the Daily Alarm Rate table in the alarm report. This automatically resizes the chart.

Once the alarm report has been completely populated and formatted the worksheet is transferred to a new Excel file. It is then up to the user to save this file. The alarm report layout and format has set so the all of tables and charts do not break across pages if printed or saved to a document format. The Alarm Report Tool can then be used to generate another alarm report or closed. No saving is required for the Alarm Report Tool as it stores no data locally.

The operation of the ReportGenrator can be seen in *Figure 46*. Sources (user interface worksheet) are shown shaded in green. The full VBA code listing of the ReportGenrator can be found in Appendix C.3

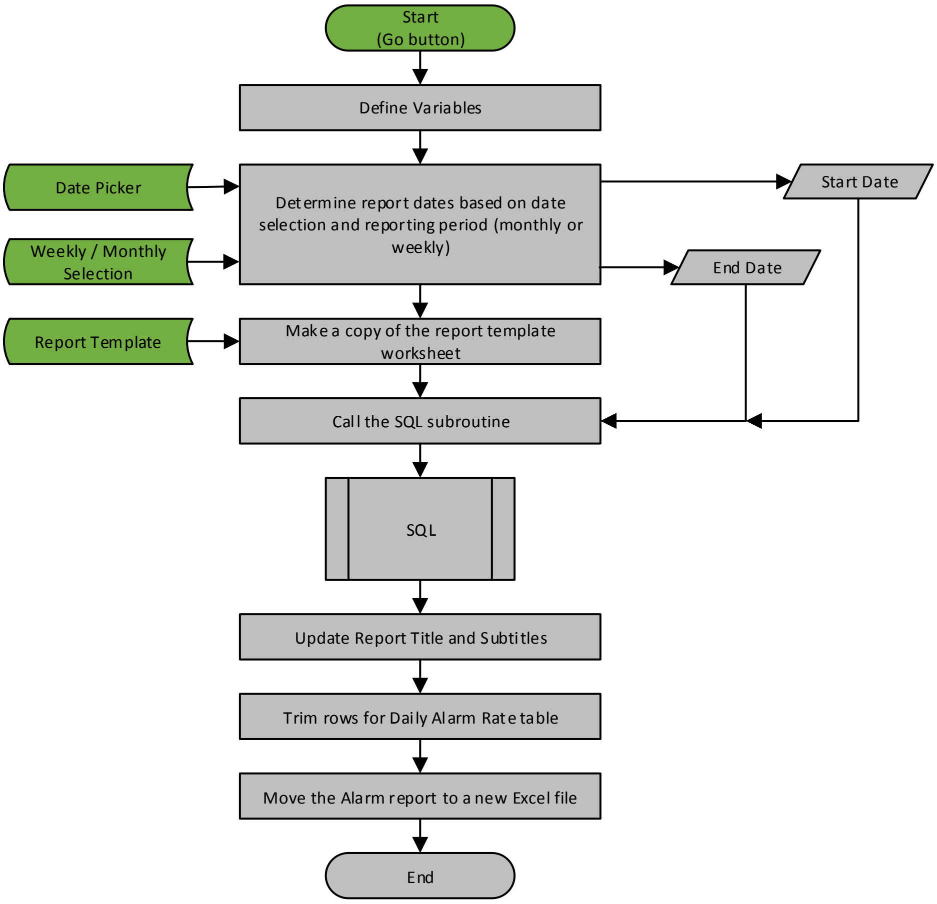


Figure 46 – ReportGenerator flow chart

Chapter 10 – Resolution of Bad Actors

With all parts of the Alarm Management Model in place efforts shifted to resolving some of the Bad Actors. It was decided to focus on the worst performing alarms in the first six months of the year, i.e. the start of January 2015 to end of June 2015. To identify the worst performing alarms in this period the SQL Alarm Report Query was used. By modifying the start and end dates to suit the top twenty alarms (shown in *Table 14* as well as the daily alarm rate (shown in *Figure 47*) was determined.

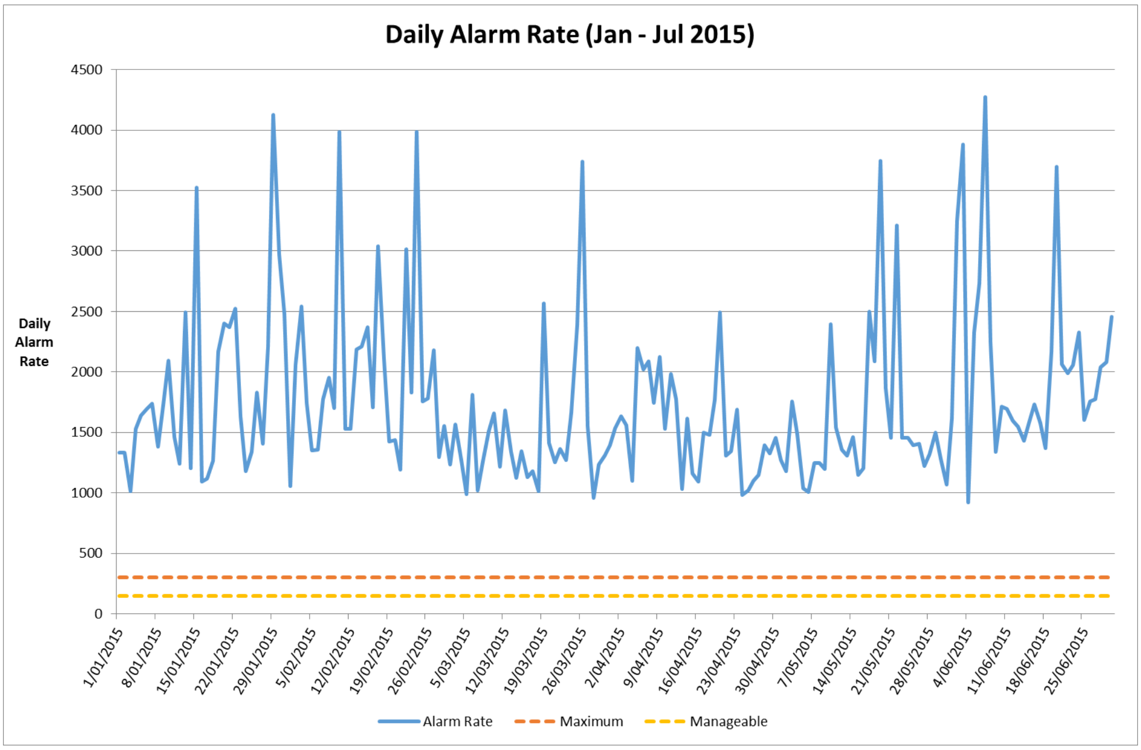


Figure 47 – Daily Alarm Rate – January to June 2015

The top 18 alarms *Table 14* account for just over 40% of all alarms from January to June 2015. Where possible the top 18 have been grouped where the alarms are similar in nature. This resulted in nine groupings. The alarm count for each grouping can be seen in *Table 15*. For each grouping a case study has been performed. The case study includes a description of the subsystem from which the alarms originate; an investigation into what is causing the alarm to be a Bad Actor; and, then recommendations are presented on what methods and/or changes could be employed to precent the alarm form continuing to be a Bad Actor.

Table 14 – Top Twenty Alarms – January to June 2015

Rank	KKS Tag	Description	Prio	Count	%	Cum %
1	11ETJ00EA800 XU02	VACUUM ECO HOPPERS	2	17537	5.52%	5.52%
2	11HFH30CL010 XG11	L PYRITE BOX PULV 30	2	13739	4.33%	9.85%
3	11HFH50CL010 XG11	L PYRITE BOX PULV 50	2	10031	3.16%	13.01%
4	11HFH40CL010 XG11	L PYRITE BOX PULV 40	2	8687	2.74%	15.75%
5	11PGC20CE101 XQ50	3300V CCW PP CURR	2	8312	2.62%	18.37%
6	90GNK35CQ010 XU13	SALINE WTP OUTLET pH	3	8097	2.55%	20.92%
7	11HFH20CL010 XG11	L PYRITE BOX PULV 20	2	6823	2.15%	23.07%
8	90SGA40AP010 XG11	FPSTN PRESS MAINT RUN	3	6008	1.89%	24.96%
9	90SGA40AP010 XG12	FPSTN PRESS MAINT FLT	2	6008	1.89%	26.85%
10	90GNK35CQ010 XQ50	PH SALINE BSTR PP RECIRC	2	5753	1.81%	28.66%
11	90GNK35CQ010 XQ50	PH SALINE BSTR PP RECIRC	2	5643	1.78%	30.44%
12	11HFH10CL010 XG11	L PYRITE BOX PULV 10	2	5361	1.69%	32.13%
13	11HCB10EA100 XU02	T SOOTBLOWERS DRAINS	2	5315	1.67%	33.81%
14	11CJA00DU002 XU04	FREQUENCY DEVIATION	2	4805	1.51%	35.32%
15	90GNK35CQ010 XQ50	PH SALINE BSTR PP RECIRC	2	4585	1.44%	36.76%
16	11PGC10CE101 XQ50	3300V CCW PP CURR	2	4217	1.33%	38.09%
17	11HDA01CP003 XG11	DP SDCC HYDR OIL FILTER	2	4193	1.32%	39.41%
18	90ECJ20CW010 XQ50	WEIGHTOMETER T2C	2	4055	1.28%	40.69%
19	11QUA10CQ075 XQ50	DOWNCOMER WATER OXYGEN	2	3673	1.16%	41.85%
20	11HFC30EA800 XU01	PULVERIZER 30 RATIO	2	3139	0.99%	42.84%

Table 15 – Alarm Count for the Nine Case studies

Rank	Description	Count	%	Cum %
1	Pulveriser Reject Hopper Level	44641	14.07%	14.07%
2	Water Plant pH	24078	7.58%	21.65%
3	Economiser Ash System Vacuum	17537	5.52%	27.17%
4	Closed Cooling Water Pump Current	12529	3.95%	31.12%
5	Fire System Maintenance Pump	12016	3.78%	34.90%
6	Sootblower Drain Temperature	5315	1.67%	36.57%
7	Frequency Deviation	4805	1.51%	38.08%
8	SDCC Hydraulic Oil Filter Differential Pressure	4193	1.32%	39.40%
9	Coal Conveyer Weight Meter	4055	1.28%	40.68%

This approach mimics how the project site should manage Bad Actors. An understanding of the operation of the subsystem from which the alarm originates is required in order to understand the purpose and importance of the alarm.

Techniques for the investigation of Bad Actors also vary. In some cases Bad Actors are a result of improper use of alarm management best practice. The treatment options for these alarms are to apply the best practice techniques such alarm masking, hysteresis and time delays. These types of issues are identified in analysing the alarms rates and alarm duration times and then looking at how these treatment options would improve the alarm rate.

Sometimes the operation of the subsystem needs to be observed. The problem can be unreliable or faulty equipment – in this case engineering and maintenance personnel need to investigate and correct the issues with the equipment. The problem could also be that the alarm design does not fit the purpose of the alarm – this requires and understanding of the subsystem so the deficiencies in the alarm design can identified.

In some cases the alarm itself does not fit the definition to be an alarm. No investigation of alarm rates or subsystem operation will change the fact that the alarm is just not required. The treatment option for these alarms is removal. In some instances there is a combination of some or all of these techniques to understand the root cause of a Bad Actor.

10.1. Pulveriser Reject Hopper Level

This section investigates alarms 11HFH10CL010 XG11, 11HFH20CL010 XG11, 11HFH30CL010 XG11, 11HFH40CL010 XG11, 11HFH50CL010 XG11, ranked 12, 7, 2, 4 and 3 in *Table 14*. These alarms account for 14.07% of all alarms in the period of January 2015 to June 2015.

10.1.1. System Description

The coal delivered to the pulverisers for milling contains impurities such as pyrites (iron sulphides commonly found in coal reserves), sand and rock. The Pulveriser is designed to reject these materials so only Pulverised Fuel (PF) is the delivered to the boiler furnace. There are five Pulverisers at the project site, with four required to maintain the plant's Maximum Continuous Rating (MCR).

Gravity causes the Pulveriser rejects to fall into a Reject Hopper. To detect that the Reject Hopper is full a level switch is used. The level switch uses a motor driven paddle wheel which normally rotates feely. When solid rejects fill the hopper the paddle wheel is physically prevented from turning. A clutch mechanism detects the paddle wheel is no longer turning and operates a mechanical switch. The level switch assembly operates in an extreme environment where there is dirt and dust and the temperature may exceed 200 ^{0}C. A schematic representation of the system is depicted in *Figure 48*.

Each hopper has its own automated sequence which empties the rejects. This operates in a similar manner as the Economiser Ash System – i.e. using an ejector to create a vacuum to draw the rejects out of the hopper. The sequence takes a little over two minutes to complete a reject cycle of a single hopper. There are normally anywhere from a 100 to 150 reject operations per day across the four running pulverisers. The sequences were originally configured to run automatically based on timers, but this was found to be inadequate and is not used. The switch is connected to a DCS 'Digital' input which activates the alarm. The Alarm List has no Cause/Action text for this alarm. Operators now use the alarm as a prompt to start the sequence.

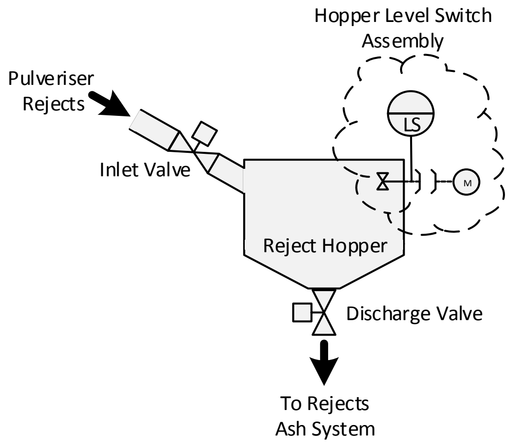


Figure 48 – Pulveriser Reject Hopper

10.1.2. Investigation

Using the LocalDB test environment an SQL query was run to extract all alarm activations and deactivations for level alarms. The duration of each alarm in was then determined. Sorting the alarm durations into groups to observe the distribution of the alarm count proved problematic. The jamming of the switch creates to different problems. Firstly the switch jams intermittently for short periods of time – this appears to be creating many fleeting alarms. Secondly the switch jams and does not return to normal operation for a long time – this produces alarms with an abnormally long duration.

The normal expected duration of the alarm is a somewhere between 45 seconds to one minute. The sequence takes about 30 second to start the high pressure water and open the valves. After 45 seconds the hopper is beginning to empty so it is expected that the alarm will clear as the rejects clear the paddle wheel. This assumes that an operator starts the sequence when the alarm activates.

Figure 49 shows the duration distribution grouped into 15 second intervals for each pulveriser. It can be seen there is a spike in the number of alarms in the 45 – 60 second time range. It is likely these alarms are an associated with the correct operation of the level switch. There are a large number of alarms in the 0 – 15 and 15 – 30 second ranges. It is likely that these are fleeting alarms caused by the intermittent jamming of the switch. There is also large number of alarms in the >300 second range. It is likely that these alarms are due to the level switch jamming completely. The large spike is due to the cumulative effect of the alarms in the >300 second range. There is no actual spike if the range is expanded beyond an hour. It is assumed that most of the contribution in the >300 second range is due to the switch jamming. This is based on discussions with site personnel.

If the assumption is made that accurate operation of the level switch is when the alarm duration is between 30 seconds and 300 seconds then on average, across all pulverisers, the alarm is accurate only 23% of the time. This can be seen in *Table 16*.

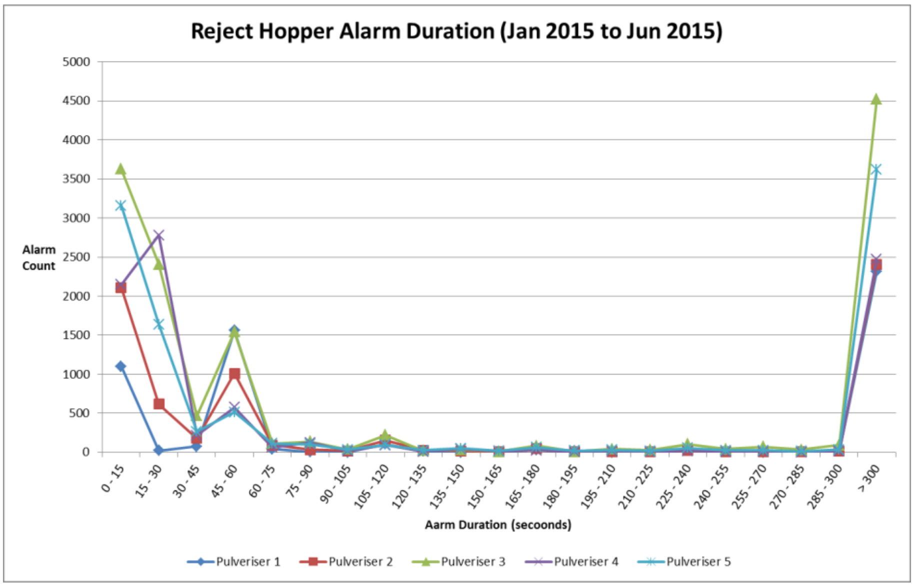


Figure 49 – Pulveriser reject sequence operation January - June 2015

Table 16 – Reject Hopper Level Alarm Duration – All Pulverisers

Alarm Duration	Level Alarm Count				
	Pulveriser 1	Pulveriser 2	Pulveriser 3	Pulveriser 4	Pulveriser 5
< 30	1124	2726	6033	4926	4797
30 - 300	1919	1670	3101	1262	1515
> 300	2316	2406	4521	2468	3617
Total	5359	6802	13655	8656	9929
Percent 30 - 300	36%	25%	23%	15%	15%
				Average	23%

10.1.3. Recommendations

Before there is any attempt to correct this Bad Actor alarm the reliability of the level switches must be addressed. The level switches in their current form are not fit for purpose. Possible solutions are to use a different technology or perform more maintenance on the switches to ensure they operate correctly. This is outside the scope of alarm management on its own.

When the reliability issues are resolved there will still be a residual alarm problem of Alarming Normal Conditions. Operators activate a reject sequence when the high level alarm activates. At 100 operations per day this would take two thirds of the performance metric of 150 alarms per day. It is recommended that the operation of the reject sequence automated based on the operation of the high level switch. The abnormal situation that should be alarmed is if the high level switch is still active after the completion the reject sequence. If this occurs then an alarm should be activated and further automated operation of the sequence prevented until the situation can be investigated and resolved.

10.2. Saline Water Plant pH

This section investigates alarms 90GNK35CQ010 XU13, 90GNK35CQ010 XQ50 <LOW, 90GNK35CQ010 XQ50 >HIGH and 90GNK35CQ010 XQ50 <MIN, ranked 6, 10, 11 and 15 in *Table 14*. These alarms account for 7.58% of all alarms in the period of January 2015 to June 2015.

10.2.1. System Description

All waste water on site is treated in the Waste Water Treatment plant. Once treated the water is held in large storage tanks ready for disposal offsite.

The final stage in Waste Water Treatment plant is the adjustment of the water pH to 7.0 using acid. The water level in the pH Adjustment Tank is maintained by a level control valve – the level control valve only allows water to be pumped to the storage tanks if the level in the pH Adjustment Tank is at set point. This maintains a buffer of water in the pH Adjustment Tank. The pH of the water is controlled by adding acid to the water as it first enters the pH Adjustment Tank. The acid feed rate is controlled by variable speed pump. A schematic representation of the system is depicted in *Figure 50*.

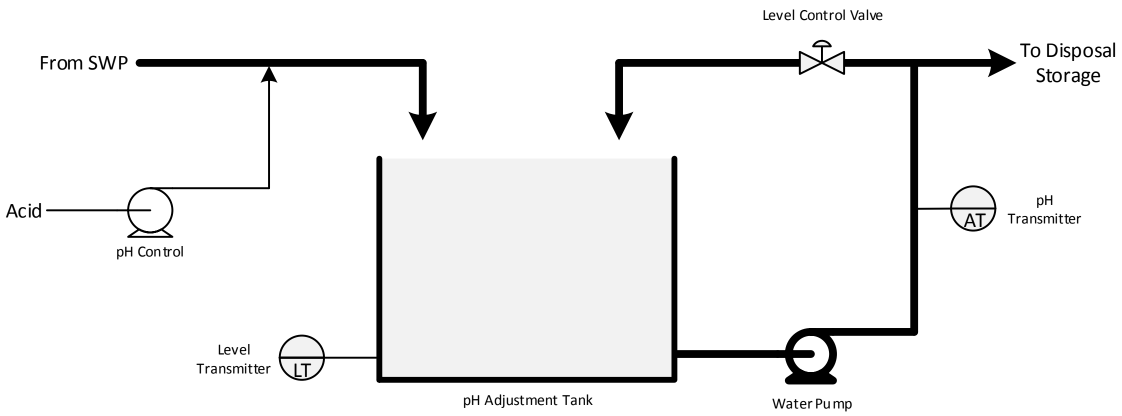


Figure 50 – Waste Water Treatment plant Final pH Control

A pH transmitter is used for both control and alarming of the pH. The summary of alarms is shown in *Table 17*. Note that all of these alarms use alarm masking configured in the application software to precent activation if the Waste Water Treatment plant is not in service. If either the <MIN or >MAX alarm is active for more than 30 minutes the DCS will shut down the SWP.

The Alarm List offers the following text as the Cause/Action for alarm 90GNK35CQ010 XU13:

> "PH adjustment of the saline water leaving the SWTP is malfunctioning effecting to much acid dosing. Check to ensure that the acid dosing group is in auto. The saline water treatment plant will shutdown if low pH continues."

The Alarm List offers the following text as the Cause/Action for alarm 90GNK35CQ010 XQ50 <MIN:

> "PH of the saline water at the outlet of the saline water treatment plant is less than the minimum allowable pH for ocean discharge and therefore should the saline water treatment plant be running in automatic mode the saline plant will trip. Should the saline plant be running in manual mode the operator should decrease or stop acid dosing as required. Change the acid outlet pH setpoint as required prior to re-starting the plant in automatic mode. Should the pH < min occur during startup and the pH activation timer (90GNLOODU151) be set less than 15 minutes, this timer may be extended to assist in obtaining steady state pH control without initially tripping the plant."

The Alarm List has no Cause/Action text for the other alarms in *Table 17*.

Table 17 – SWP Final pH Control Alarms

Alarm Tag	Status	Prio rity	Explanation	Rank in Top 20
90GNK35CQ010 XQ50	<MIN	2	pH <6.7	15
90GNK35CQ010 XQ50	<LOW	2	pH <6.3	10
90GNK35CQ010 XQ50	>HIGH	2	pH >8.3	11
90GNK35CQ010 XQ50	>MAX	2	pH >8.6	N/A
90GNK35CQ010 XU13	LOW	3	pH is more than 0.56 below current pH control set point	6

10.2.2. Investigation

The pH control was observed using the historian. *Figure 51* shows the trend of two different time periods. The trends show that the control of the pH is oscillatory. When comparing to other time periods this trend is typical. The oscillations match the alarms that are being seen – both high pH and low pH alarms.

The likely problem is that the oscillations are caused by poor tuning of the Proportional plus Integral (PI) controller in the DCS. When the pH level falls too low the acid pump turns off. The pH rises and then the acid pump is turned on again. The over aggressive tuning of the PI controller causes the pH level to fall very rapidly again stopping the pump. This cycle repeats over and over. The continuous control algorithm has essentially been degraded to an on/off controller.

Historically this loop has been hard to tune as there are several disturbance variables that are not accounted for, such as:

- Flow rate of water in to the pH Adjustment Tank is not the same
- Strength of the acid can vary

- Mechanical stroke of the acid pump can be, and does get adjusted locally, therefore affecting the process gain.

The oscillatory nature of the control has little affect final pH of the water as the oscillations are generally centred on the pH set point – the large volume of the storage tank helps to ‘dampen’ out the final pH. The only noticeable side effect of the oscillations is the number of alarms generated.

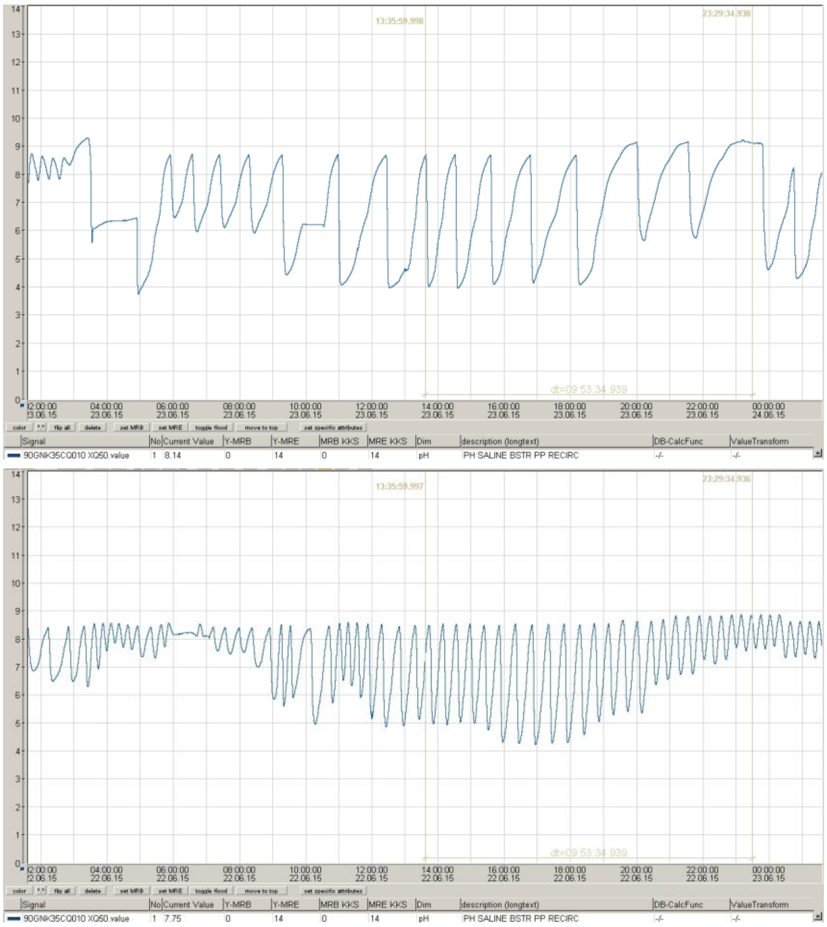


Figure 51 – Trends of SWP Final pH Control

10.2.3. Recommendations

The ideal solution is to improve the control of the pH. This would remove the oscillations and therefore the alarms. It may be possible to make the loop tuning much less aggressive. This would stop the resulting on/off control action that is being seen. A side effect would be an increase in the settling time of the pH control but this may be tolerable given the dampening effect of the large storage tank. The Alarm List text for alarm 90GNK35CQ010 XQ50 <MIN hints to a settling time in the order of 15 minutes. The trends in *Figure 51* show with the current tuning the controller is able to reduce the pH level from over 8 to a little over 4 in several minutes. This seems overly aggressive if a settling time of 15 minutes was originally expected and the shutdown is at 30 minutes.

In regard to the alarms, there are three alarms to monitor low deviations of pH and two alarms for high deviations. Three of these alarms should be deleted so there is only a single alarm for a low pH deviation and a single alarm for high pH deviation. Appropriate alarm masking and time delays and hysteresis should be applied to these alarms.

10.3. Economiser Ash System Vacuum

This section investigates alarm 11ETJ00EA800 XU02, ranked 1 in *Table 14*. This accounts for 5.52% of all alarms in the period of January 2015 to June 2015.

10.3.1. System Description

One of the areas in the Boiler that ash accumulates is the Economiser Ash Hoppers. The ash hoppers are emptied at regular intervals while the boiler is operating. Failure to remove the ash will result in the hoppers filling. Once full the ash will blow over to the Air Heater and cause a blockage.

The Economiser Ash System is a fully automated subsystem to remove ash from the economiser ash hoppers. The system uses an ejector to produce a vacuum which draws the ash out of the bottom of the hoppers. The ejector is operates by supplying high pressure water to the narrow section of a venturi. This produces a vacuum at the inlet of the venturi. The inlet of the venturi is piped to the ash hoppers where an automated valve opened to allow the ash to be drawn out. Ash enters the ejector inlet and mixes with the water. The water and ash is directed to the ash handling plant for disposal. A schematic representation of the system is depicted in *Figure 52*.

The Economiser Ash System is controlled by a DCS sequence which operates as follows:

1. Start the high pressure water pump. The next step is activated when:
   - the water pressure switch confirms that the high pressure water is above the required pressure, AND
   - the pressure transmitter indicates that the pipework pressures is less than -10 kPa
2. Open the Hopper 4 discharge valve. The next step is activated when:
   - 60 seconds has elapsed, AND
   - the pressure transmitter indicates that the pressures is greater than -20 kPa
3. Close the Hopper 4 discharge valve. The next step is activated when:
   - Hopper 4 discharge valve is confirmed closed
4. Repeat steps 2 and 3 for Hoppers 3, 2 and 1
5. Stop the high pressure water pump after 10 minutes

The system is monitored by Priority 2 alarm 11ETJ00EA800 XU02. The alarm activates if "the pressure is greater than -10 kPa while any ash hopper valve is open". The Alarm List has no Cause/Action text for this alarm.

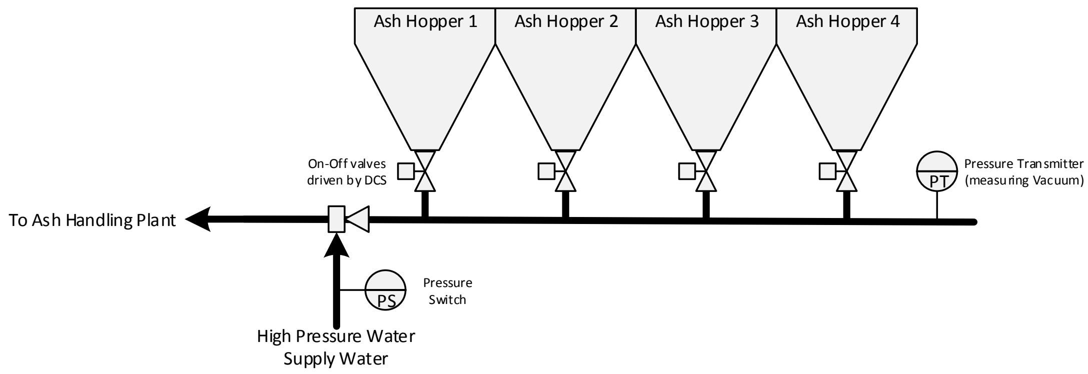


Figure 52 – Economiser Ash System

10.3.2. Investigation

Using the LocalDB test environment an SQL query was run to extract all alarm activations and deactivations for KKS tag 11ETJ00EA800 XU02. The duration of each alarm in was then determined – *Table 18* shows the results. Very few alarms are in the range of 0 – 20 seconds. This indicates that the alarm is not a fleeting alarm.

Table 18 – Economiser Vacuum Alarm Duration

Duration (seconds)	Alarm Count
0 - 20	337
20 - 40	211
40 - 60	1513
60 - 80	15419
80 - 100	5
> 100	50

The typical operation of the Economiser Ash System was observed using the historian. A trend of pipework vacuum over typical cycle can be seen in *Figure 53*. It shows the pressure reducing to approximately -23kPa at the start of the sequence. When the first discharge valve opens the pressure then increases as the ash is drawn out of the hopper. The sequence holds the discharge valve is open for at least 60 seconds. In this time the pressure increases from -30kPa to -4kPa. This is repeated for the three other hoppers. When comparing to other time periods this trend is typical. The alarm activates when the pressure greater than -10kPa. This does not appear to be an alarm condition as the normal operation sees the pressure at -4kPa.

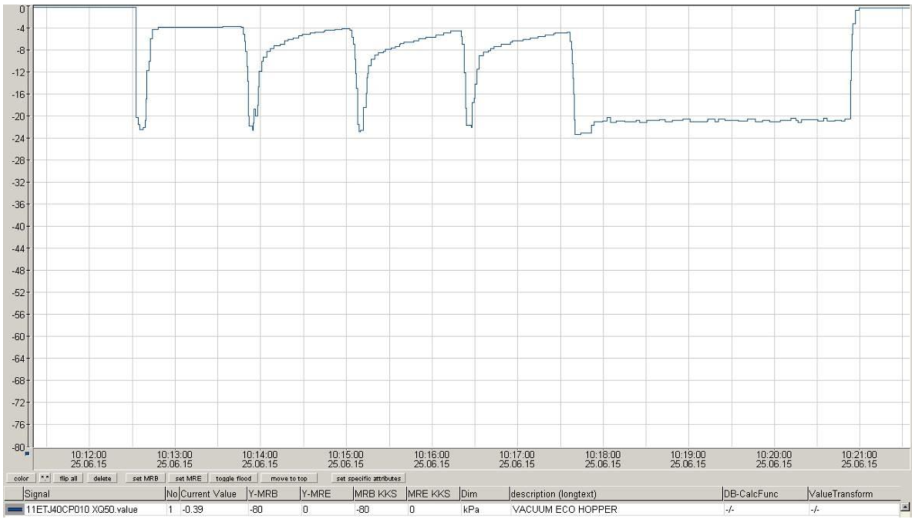


Figure 53 – Trend of Economiser Vacuum during sequence

After discussing the alarm with site operators and engineering personnel it was suggested that the purpose of the alarm may be to indicate that there is a hole in pipework. It appears that this alarm problem is a combination of No Response Required and Unknown Response.

10.3.3. Recommendations

The alarming strategy for the economiser vacuum should be reviewed. It is possible that an alarm could be used to detect holes in the pipework but the validity of this should be confirmed by engineering personnel. The possibility of using the economiser vacuum to detect blockages could also be investigated – if the pressure does not rise shortly after the discharge valve opens then there is likely a problem.

10.4. Closed Cooling Water Pump Current

This section investigates alarms 11PGC10CE101 XQ50 >HIGH and 11PGC10CE101 >HIGH, ranked 5 and 16 *Table 14*. These alarms account for 3.95% of all alarms in the period of January 2015 to June 2015.

10.4.1. System Description

The Closed Cooling Water (CCW) System supplies cooling water to many heat exchangers in the plant. Two sets of pumps and shell and tube heat exchangers provide the motive power for the water and remove the heat energy from the system. The system may run at 100% duty with one pump and heat exchanger pair. The other pair can either in standby or being maintained.

The CCW pumps are high voltage (3.3 kV) three phase squirrel cage motors. The motors have a full load current rating of 69.8 A. Power supply for the motors is from a 3.3 kV switchboard. The switchboard has motor electrical control circuits that interface to the DCS, a motor protection device and current transformers (CT's). A current transmitter provides an 'analog' signal to the DCS. Each pump has two alarms are configured as limit values on the ‘analog’ current signal, refer to *Table 19*. The Alarm List has no Cause/Action text for these alarms.

Table 19 – CCW Pump Current Alarms

Limit Value	Value (Amps)	Priority
High	64	2
Max	69.8	1

10.4.2. Investigation

The typical operation of the CCW motor current was analysed using the historian. *Figure 54* depicts a trend of the motor current. Both pumps were operated during this period. The trend shows that the current signal oscillates during operation. When comparing to other time periods this trend is typical.

Using the LocalDB test environment an SQL query was run to extract all alarm activations and clearing events for KKS tag 10PCG20CE101 for the period of the trend in *Figure 54*. The duration of each alarm in was then determined. *Table 20* shows that almost all of the alarms are of a duration of 5 seconds or less. This confirms the alarm problem is a fleeting alarm.

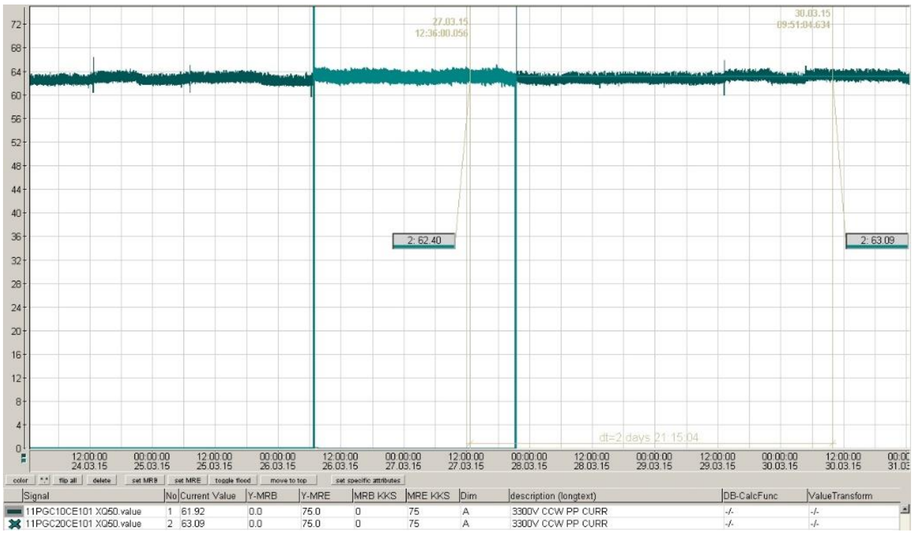


Figure 54 – Trend of CCW motor current

Table 20 – 11PGC20CE101 Alarm Duration

Duration (seconds)	Alarm Count
0 – 5	2120
5 – 10	94
10 – 15	19
15 – 20	8
20 – 25	3
25 – 30	1
30 +	0

10.4.3. Recommendations

Firstly this alarm should be rationalised to ensure that there is a valid operator response to a high motor current alarm. Changing to the other pump and heat exchanger set could be a possible action. If the alarm is still required then hysteresis or a time delay could prevent the oscillations from causing the fleeting alarm.

The best option would be to add filtering the 'analogue' measurement prior to processing the alarm. The current is not used for any other purpose other than indication and alarming so filtering can be applied without any adverse effect. Regardless of the whether the alarm is removed or kept the filtering should be applied to make the measurement more useful.

10.5. Fire System Maintenance Pump

This section investigates alarms 90SGA40AP010 XG11 and 90SGA40AP010 XG12, ranked 8 and 9 in *Table 14*. These alarms account for 3.78% of all alarms in the period of January 2015 to June 2015.

10.5.1. System Description

A piping system distributes fire water across the site. The main uses of fire water on the site are:

1. Fire Hydrants – connection points where a lay flat hoses can be connected, these are generally used by personnel with specific firefighting skills
2. Fixed Fire Hoses – a fire hose on a reel that can be easily operated by any personnel
3. Fire Deluge System – fire sprinkler systems that operate automatically when a fire is detected

If required fire water is delivered using an electrical pump and two diesel pumps. The diesel pumps ensure fire water is available even if there is a power failure on the site. The fire water distribution system is pressurised at all times. As the system comprises of many joints, valves and there is always a small amount of leakage. A smaller Maintenance Pump operates regularly to maintain the pressurised state of the system. A schematic representation of the system is depicted in *Figure 55*.

The pumps are not controlled by the DCS. Each pump is controlled form its own local control panel. This ensures pumps can still operate is the DCS is not be operational, which is possible if there is a major fire. Each pump monitors the pressure of the fire water system using a pressure switch. As the system pressure falls the starting of the pumps is staged. The Maintenance Pump operates first. The Maintenance Pump stops automatically once the system pressure returns to normal. As well as keeping the system pressurised the Maintenance Pump should be able to deliver enough water to operate a single Fixed Fire Hose. If there is a greater demand for fire water the pressure will drop further. The Electric Pump operates next, followed by the two Diesel Pumps. Both the Electric Pump and the Diesel Pumps must be stopped manually.

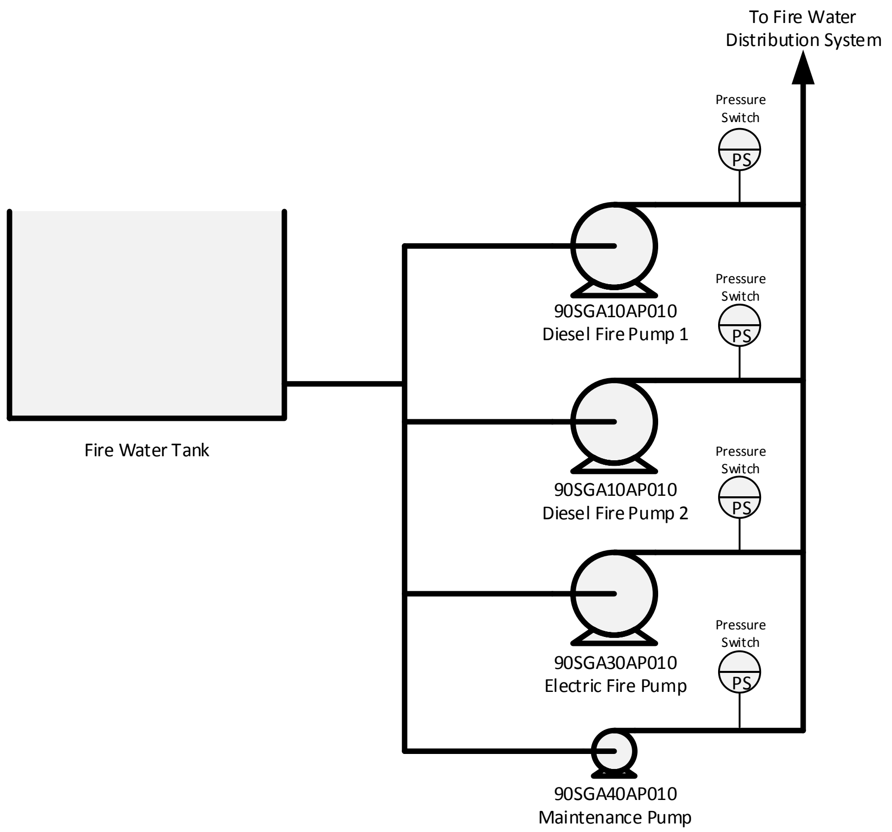


Figure 55 – Fire Water Pumping System

There are two alarms associated with each pump – a pump running alarm and a fault alarm. The alarms originate from the local control panel for each pump. The DCS uses a ‘digital’ input for each alarm. The summary of alarms is shown in *Table 21*.

Table 21 – Fire Pump System Alarms

Alarm Tag	Descriptor	Prio	Explanation
90SGA10AP010 XG11	FPSTN DIESEL 1 RUN	3	Pump is running
90SGA10AP010 XG12	FPSTN DIESEL 1 FLT	2	Local control panel reporting a fault
90SGA20AP010 XG11	FPSTN DIESEL 2 RUN	3	Pump is running
90SGA20AP010 XG12	FPSTN DIESEL 2 FLT	2	Local control panel reporting a fault
90SGA30AP010 XG11	FPSTN MAIN ELEC RUN	3	Pump is running
90SGA30AP010 XG12	FPSTN MAIN ELEC FLT	2	Local control panel reporting a fault
90SGA40AP010 XG11	FPSTN PRESS MAINT RUN	3	Pump is running
90SGA40AP010 XG12	FPSTN PRESS MAINT FLT	2	Local control panel reporting a fault

The Alarm List offers the following text as the Cause/Action for alarm 90SGA40AP010 XG11:

> "System pressure in the fire ringmain is low and the jacking pump is active. Should the jacking pump run for a substantial time, check for leaks in the firemain or for use of a fire hydrant."

The Alarm List offers the following text as the Cause/Action for alarm 90SGA40AP010 XG12:

> "The jacking pump is enabled for operation and is not operating when required. Check pump and its associated drive for faults and correct faults as appropriate."

10.5.2. Investigation

In relation to the pump running alarm there is an obvious problem. The operation of the Maintenance Pump automatically controlled and it is expected under normal operating conditions. In its current form the alarm problem is Alarming Normal Conditions.

The operation of the Maintenance Pump for a prolonged period is an abnormal situation though. The guidance from the Alarm List has the correct causes and actions in regard to the possible use of a Fixed Fire Hose.

The fault alarm activates every time the Maintenance Pump operates. According the wiring schematic for the local panel the fault alarm is configure to activate if the motor thermal overload relay has tripped. If this alarm is active then the pump cannot operate. The fact that this alarm activates when the pump operated indicated that there is a problem with how this panel or wiring have been interface to the panel.

10.5.3. Recommendations

The guidance from the Alarm List is correct is relation to the possibility that a fixed fire hose. An appropriate time delay should be added to filter out the normal operation to pressurise the pipework.

The fault alarm appears to be a fault in how the local panel or the DCS interface to the local panel is wired. The guidance in the Alarm List does not match the configuration of the alarm either. The maintenance department should investigate and rectify this alarm so it operates correctly.

It is also recommended that the all the alarms in *Table 21* be rationalised at the same time so there is a consistent alarming strategy for all of the fire pumps. There should also be a check of the operation of the fault alarms on the other pumps to ensure that they are configured correctly.

10.6. Sootblower Drain Temperature

This section investigates alarm 11HCB10EA100 XU02, ranked 13 in *Table 14*. This alarm accounts for 1.67% of all alarms in the period of January 2015 to June 2015.

10.6.1. System Description

Ash (also referred to as soot) can accumulate on the internal surfaces of the boiler where radiant heat energy and convection heat energy is transferred through the metal components to the water and steam. The coating of these surfaces reduces the heat transfer capability, thereby reducing the performance of the boiler. The most common method to remove this ash is to use high pressure steam the blow the ash off of these surfaces. The ash is then carried through the through the furnace and collected in the Economiser Ash System.

Sootblowers are mechanical devices that direct the steam to the internal surfaces. They are operated by electric motors. When the motor operates nozzles are inserted into the boiler from the access holes. Once the nozzle is inserted a mechanically operated valve allows steam to flow through the nozzles on to the internal surfaces. After a predetermined time the nozzles are retracted and the steam supply is turned off via the mechanically operated valve.

There are 50 sootblowers for the radiant section of the boiler and 40 sootblowers for convention section of the boiler. All sootblowers are controlled from the DCS using and an automated sequence. The selection of which sootblowers will operate during the sequence and when to operate the sequence is set depending on boiler steam and furnace gas exit temperatures.

The steam for the sootblowers is supplied from the boiler superheated steam output. The pressure of the sootblower steam is controlled to 4200 kPa using a valve controlled by the DCS. There is several hundred meters of piping connecting all of the sootblowers to the steam supply. The pipework is arranged in such that there are no dead ends. All of the pipework ends at the sootblower drain valve. The take off line to each sootblower is also as short as possible. These piping arrangements prevent steam condensing into water in the pipework. If water is allowed to enter the furnace through a sootblower it can erode the internal components of the boiler. A schematic simplified representation of the system is depicted in *Figure 56*.

During the start-up of the sootblowing sequence a drain isolation valve and drain control valve both open fully. This directs all of the steam through the pipework. This allows the pipework to be warmed up, again to ensure there is no accumulated water in the system prior to operating a sootblower. Once the system has warmed up the drain control valve closes, but remains partially open so a small amount of steam continuously flows through all of the pipework and to the drain. Again this is to ensure no water accumulates in the pipework

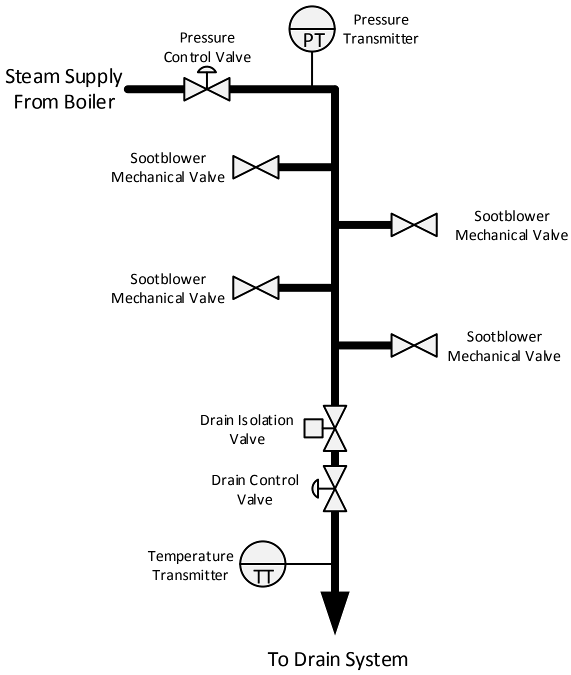


Figure 56 – Sootblowing System (simplified)

Water condenses if the steam is no longer superheated. At 4200 kPa the saturation temperature of the steam is 254 ^{o}C. The temperature of the drain is monitored during operation. If it detects that the temperature is below saturation temperature then alarm 11HCB10EA100 XU02 activates. The alarm is set to at 245 ^{o}C. This relates to a saturation pressure of 3550 kPa. The difference between the supply pressure and the drain pressure is an assumed steam pressure drop through the system. The alarm is masked such that it is only active if the drain isolation valve is open. The Alarm List has no Cause/Action text for this alarm.

10.6.2. Investigation

Using the LocalDB test environment an SQL query was run to extract all alarm activations and deactivations for KKS tag 11HCB10EA100 XU02. The duration of each alarm in was then determined – *Table 22* shows the results. Very few alarms are in the range of 0 – 30 seconds. This indicates that the alarm is not a fleeting alarm.

Table 22 – Sootblower Drain Temperature Alarm Duration

Duration (seconds)	Alarm Count
0 - 60	194
60 - 120	285
120 - 180	956
180 - 240	710
240 - 300	384
300 - 360	855
360 - 420	1913
480 - 540	2
540 - 600	2

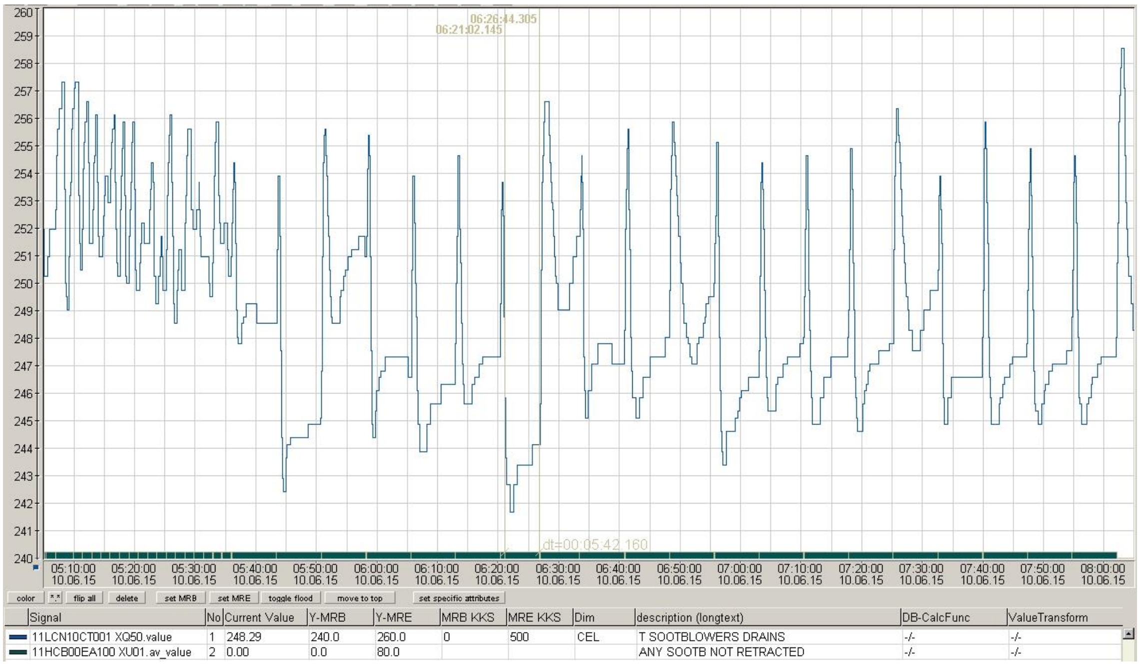


Figure 57 – Trend of drain temperature during operation of Sootblowers

The operation of the sootblowers was observed using the Historian. The radiant area sootblowers take approximately 1.5 minutes to operate, while the convection area sootblowers take just over 7.3 minutes to complete an operation. *Figure 57* shows the drain temperature during the operation of a set of radiant area and convection area sootblowers. As each sootblower operates the temperature initially falls and then recovers. When the convection area sootblowers operate the drain temperature falls either close or below the alarm point. In *Figure 57* 10 of the 13 operations resulted in an alarm. Looking at other time periods it was observed convection sootblowers generally results in anywhere from 3 to 10 alarms each time a set is operated.

The likely scenario is that when a convection area sootblower operated there is a larger pressure drop (and therefore temperature drop) that was assumed when the original alarm was designed. This creates a false alarm that the drain temperature is below the saturation temperature of the steam.

This is backed up by *Table 22* which shows none of the alarms are longer than the run time of the sootblowers – 7.3 minutes (430) seconds. This is also backup by *Figure 58* which shows an alarm rate of anywhere from 10 to 40 alarms per day. This matches the typical trend data for the number of times sootblower operations cause the temperature to fall below the alarm point.

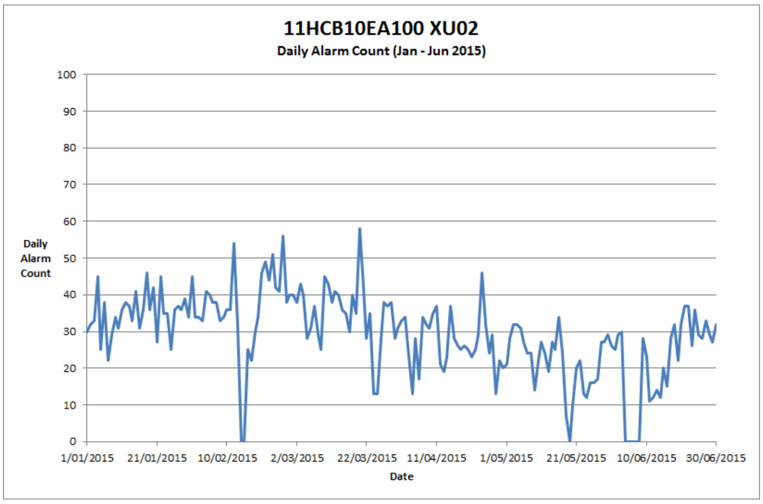


Figure 58 – Sootblower drain temperature Daily Alarm Rate (Jan – Jun 2015)

10.6.3. Recommendations

Firstly it should be determined if the alarm is accurately detecting that water may accumulating in the pipework. If this is the case then the operation of the sootblowing system must be changed so this does not occur. This could be done by taking pressure readings at the drain to see if assumed pressure drop that results in an alarm limit of 245 ^{o}C is valid. This information could then be used to determine a more accurate alarm limit.

10.7. Frequency Deviation

This section investigates alarm 11CJA00DU002 XU04, ranked 14 in *Table 14*. This alarm accounts for 1.51% of all alarms in the period of January 2015 to June 2015.

10.7.1. System Description

All the large power stations in the south west of Western Australia are connected to South West Interconnected System (SWIS). All generators operate at the same speed as they are magnetically coupled. The speed determines the frequency of alternating current produced. This is tightly controlled to 50 Hertz in Australia. In a large grid such as the SWIS only few generators are actually controlling the speed and therefore the frequency of the grid. These generators adjust their mechanical input power to control the speed. Many generators on the grid are operating in load control. They adjust their mechanical input power to meet a specific generated load target. The project site is normally operated in this manner.

If the frequency deviates by a pre-determined level alarm 11CJA00DU002 XU04 activates. The Alarm List has no Cause/Action text for this alarm. If the deviation exceeds a further pre-defined limit the generator controls will trip the generator circuit breaker and remove it from the grid. This will result in the boiler and turbine shutting down also. If the project site is not operating the generator in speed control there is no action an operator may take to correct the situation of a frequency deviation.

10.7.2. Investigation

No specific alarm rate analysis has been conducted for this alarm. If there is a frequency deviation and the generator is not being operated in speed control there is no action the operator can take to correct the situation. Even if the deviation escalates to a complete shutdown of the generator/turbine/boiler the operator cannot correct the situation. The problem with alarm is that there is no response required.

10.7.3. Recommendations

There are two possible solutions to this alarm. The first is to remove the alarm. If the project site feels that operation in speed control mode may be required in the future the alarm should be masked to only activate when operating in this mode.

10.8. SDCC Hydraulic Oil Filter Differential Pressure

This section investigates alarm 11HDA01CP003 XG11, ranked 17 in *Table 14*. This alarm accounts for 1.32% of all alarms in the period of January 2015 to June 2015.

10.8.1. System Description

The SDCC (Submerged Drag Chain Conveyer) removes ash from the bottom of the boiler furnace. The SDCC used a hydraulically driven motor to provide motive force to the conveyer. The hydraulic oil system consists of electrically driven pumps to generate the hydraulic force and control valves to direct oil to the hydraulic conveyor drive. The DCS regulates the speed of the conveyor the control valves.

Cleanliness of the hydraulic oil is important. Particulate contamination can block small passages in the valves and also cause damage to metal components that use polished surfaces and rubber seals to prevent oil leakages. To eliminate particulate contamination a filter system is used. The filter is installed directly downstream of hydraulic pumps. It prevents particulates that are larger than a specific size from entering the hydraulic oil system.

As the filter captures particles the hydraulic pressure drop across the filter increases. The pressure drop will eventually increase to the point where the hydraulic pumps cannot deliver enough pressure to the system. Prior to reaching this point the filter must be replaced with a new one. To indicate that the filter is blocked a differential pressure switch monitors the pressure difference from the inlet to the outlet of the filter. The pressure switch is connected to a 'digital' input on the DCS. Note that the input is configured in such a way that the normal state of the alarm is when the input is in the active state. When the pressure drop exceeds a pre-determined level it operates and activates Priority 2 alarm 11HDA01CP003 XG11 – DP SDCC HYDR OIL FILTER. The Alarm List offers the following text as the Cause/Action:

“SDCC HYD FILTER”

10.8.2. Investigation

Using the LocalDB test environment an SQL query was run to extract all alarm activations and deactivations for KKS tag 11HDA01CP003 XG11. The duration of each alarm in was then determined – *Table 23* shows the results. It shows that all but 15 of the 4193 alarm activations were for a duration of less than one second. This is a classic case of a fleeting alarm.

Table 23 – SDCC Hydraulic Oil Filter Differential Pressure alarm duration

Duration (seconds)	Alarm Count
< 1	4080
1 - 10	98
> 10	17

There are two possible causes of the fleeting alarm. Firstly the alarm was genuine and caused by high pressure across the filter. It should be noted that the pressure will not be constant. It will fluctuate around its operating point. The hydraulic oil is supplied by an electric pump operates at high speed. This causes fluctuations that are a likely to cause the fleeting alarm if the pressure drop approaches the alarm point. The second possibility, given the wiring configuration, is that a loose wiring connection that is vibrating may have also caused the alarm.

Also worth noting in that the 4193 alarm activations all occurred in the period of 18th of February to the 26th of February – over eight days. This shows how fleeting alarm can have a dramatic impact on the alarm system performance over a short period.

10.8.3. Recommendations

Two methods to prevent fleeting alarms are to apply either hysteresis or a time delay. As the alarm originates from a simple pressure switch it is likely that it is not possible to adjust the hysteresis. A time delay is therefore recommended. Guidance from the Alarm Philosophy recommends a time delay of at least 15 seconds be applied to alarms for pressure measurements. This is the minimum time recommended so the rationalisation team may decide that the time can be extended further if appropriate. This depends on the response time required and consequence. The plant can tolerate the SDCC to be shut down while the boiler is operating so a longer time delay could be suitable. To ensure there is not a fault all wiring connections associated with the alarm should also be inspected by maintenance staff.

10.9. Coal Conveyer Weight Meter

This section investigates alarm 90EJC20CW010 XQ50 >HIGH, ranked 18 in *Table 14*. This alarm accounts for 1.28% of all alarms in the period of January 2015 to June 2015.

10.9.1. System Description

There are two coal conveyers that can transport coal from either the overland coal conveying system or coal stockpiles, one is designated as 'T1C' and the other 'T2C'. The coal conveyers have finite capacity to transport coal, normally specified in tonnes per hour. If coal is feed onto the conveyers over this limit the conveyor may be overloaded and damaged, coal transfer points my block or coal spillages may occur. Spillage is dangerous as an accumulation of coal presents a fire hazard. This is a concern as coal can self-combust.

Each coal conveyer has a weight meter measures the instantaneous rate of coal in tonnes per hour and transmits this to the DCS as an 'analog' input. Alarms 90ECJ10CW010 XQ50 (for 'T1C') and 90ECJ20CW010 XQ50 (for T2C) activate when the instantaneous rate of coal is greater than 660 tonnes per hour. The Alarm List offers the following text as the Cause/Action:

> "T2C has exceeded its design capacity of 660 tph. Feed rates should be reduced to prevent chute blockages and coal spills."

10.9.2. Investigation

The first consideration in investigating this alarm was to ask "How many alarms are there on the other conveyor?" Conveyer 'T2C' produced 4055 alarms while 'T1C' only produced 15 alarms for the same period. The next question to ask was "Was one conveyor run more often than the other?" Investigating the run hours for the period shows that conveyor 'T2C' was run for 2613 hours while 'T1C' was run for 1211 hours. Although the conveyor with Bad Actor alarm was run for twice as many hours as the other, this does justify the difference in alarms.

It is likely that there is an accuracy problem with one of the weight meters. The operation of the coal conveyers was observed using the Historian. *Figure 59* shows a trend of the weight meter for T1C and T2C conveyors, and the status the conveyor drive motor. Both are reading significantly different in both value and characteristics. T2C shows a very noisy signal that is likely creating fleeting alarms. After discussing the system with site personnel there is no confidence in accuracy of either weight meter.

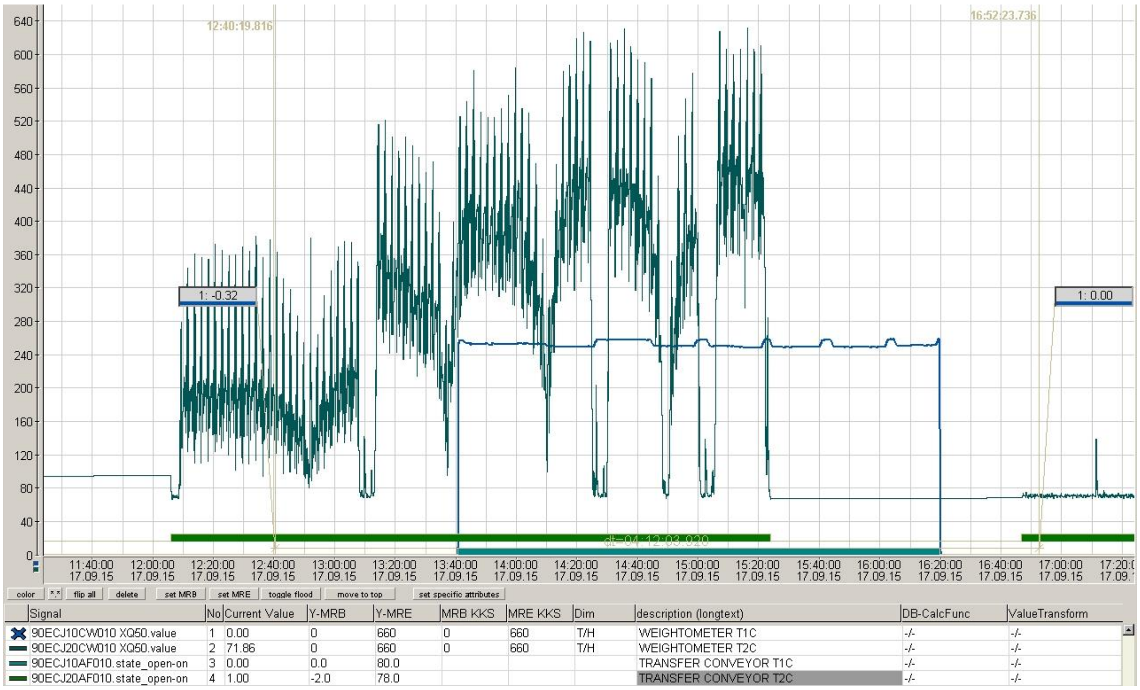


Figure 59 – Trend of coal conveyor weigh meters

10.9.3. Recommendations

Before any further alarm analysis is preformed the accuracy of the weight meters needs to be restored. In the short term the alarms should be disabled as in their current form the alarms are of no use.

10.10. Impact of Removing the Bad Actors

To see to impact of resolving the top 18 Bad Actors daily alarm rate the query was rerun. This time the top 18 alarms were ignored. The assumption made is that all of the Bad Actors would be completely eliminated or reduced such that they would not have any significant effect on the daily alarm rate.

The query was rerun for the period from the start of January 2015 to October 25th 2015. By looking forward from the original dates of the top 18 analysis it can be seen how sustainable the improvements would be. *Figure 60* shows comparison between the actual alarm rate and the predicted alarm rate with the bad actors removed.

The results show that there is an appreciable reduction in the daily alarm rate over the period January to June 2015. There remove of the top 18 Bad Actors has also been sustainable into the second half of 2015. The predicted alarm rate has continued to be significantly lower than the actual alarm rate.

The effect of a single fleeting alarm can be observed in *Figure 60*. The Submerged Drag Chain Conveyor Hydraulic Oil Filter Differential Pressure was a Bad Actor for eight day period in mid-February. During this period there are significant spikes in the actual alarm rate. These are not seen in the predicted alarm rate.

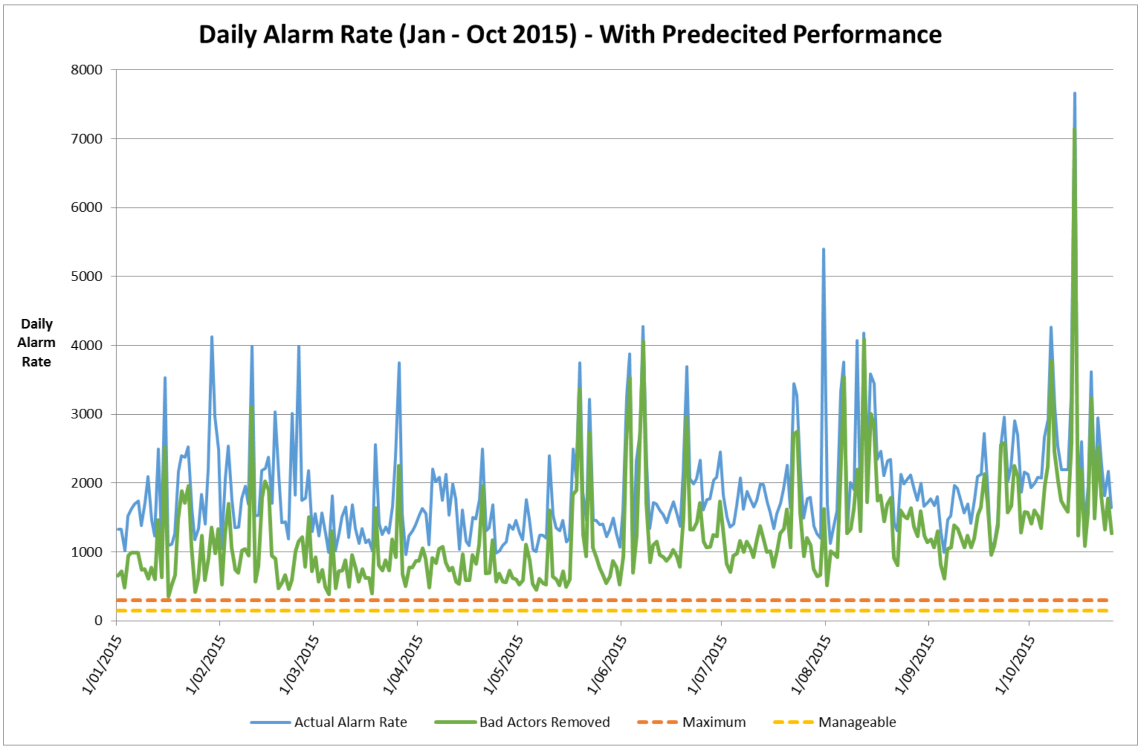


Figure 60 – Daily Alarm Rate Actual and Predicted

There still appear to be many fleeting alarms. There are periods where actual alarm rate is above 3000 alarms per day, with one over 7000. The predicted alarm rate still follows this in most cases. As has been previously stated, fleeting alarms should be dealt with immediately to prevent them taking over the alarm system.

There are two important points that can be inferred from *Figure 60*. Firstly significant effort will be required to reduce the daily alarm rate to below the maximum recommended daily alarm rate and below. The top 18 alarms accounted for approximately 40% of all alarms. To reduce the alarm rate by a further 40% of the actual alarm rate will require the resolution of considerably more Bad Actors.

Secondly, toward the end of September and into October the difference between the actual alarm rate and the predicted alarm rate does appear closer. This is because the actual alarm rate has increased due to alarms other than the top 18 – both actual and predicted are trending upwards. This shows that alarm management is a continuous process. As Bad Actors are resolved others quickly begin to emerge and cause problems.

Chapter 11 – Conclusions and Further Work

11.1. Alarm Philosophy

To comply with the corporate engineering directive for alarm management the project site was required to implement the Alarm Philosophy by the end of June 2015. The Alarm Philosophy was handed to the project site at the start of June. The project site made some slight changes to the document to suit their business requirements. Anecdotally the project site reported that well over 95% of the document was adopted with no changes. The Alarm Philosophy is now an official site procedure. The principal engineer in the organisation has endorsed the Alarm Philosophy and commended the project site for the quality of the document.

Further work for the project site is to ensure the Alarm Philosophy is actually used as the guiding reference for alarm management activities on the site. It is expected that the alarm management practices will mature as the site journeys towards sustainable alarm. Further work is also required to ensure that Alarm Philosophy is updated to reflect any changes to alarm management practices.

11.2. Master Alarm Database

The Master Alarm Database was handed over the project site. The project site now has an up to date list of all configured alarms configured in the DCS. It is too early to determine if there Alarm Help Interface is being used by operators.

Further work for the project site is to investigate is the ability of using Alarm Help as part of the HMI interface. The current HMI will not support this functionality. The project site is now preparing to continue he roll out of the new HMI system and decommissioning the current HMI system. This roll out requires significant development as the existing displays cannot be easily ported to the HMI system. As part of the development of the new HMI system the inclusion of an Alarm Help Interface should be investigated.

It is likely that the current format of the Master Alarm Database is not going to be suitable for long term use. Managing the database in a spreadsheet is cumbersome. Once the project site has decided if it will integrate the alarm help into the HMI system a longer term solution for Master Alarm database can be made. This could be a custom made database or a commercially available product. The chosen solution should continue to support the documentation requirements of the Alarm Philosophy.

11.3. Alarm Report Tool

The Alarm Report Tool was successfully tested on the project site. It was then handed over for use. Alarm reports are now beginning circulated to production, maintenance and engineering departments.

In October 2015 the project site engaged the control system vendor to update the new HMI system to the latest version of the software, as well as replacing the aging hardware. The correct functioning of the Alarm Report Tool is included as one acceptance tests for the update. This shows the project site is committed to continued use of the Alarm Report Tool.

It is expected that the alarm performance monitoring will mature at the project site. The reporting requirements may outgrow the Alarm Reporting Tool. Standing alarm reporting and flooding require a higher level of analysis that would not be supported by simple SQL queries. It is likely that a commercially available reporting tool will be required in this case. A custom tool could be developed as per the Alarm Report Tool, but the complexity of the reporting increases the maintainability of the tools becomes more difficult.

11.4. Alarm Management Practices

Take up of alarm management practices has been slow at the project site. The adoption Alarm Philosophy and including the Alarm Reporting tool in acceptance tests for the new HMI system show that there is a level of commitment. No work has been attempted yet to address the alarm performance though.

The initial challenge for the project site is to reduce the daily alarm rate to the 150 – 300 alarms per day range. The current alarm rate of 1500 alarms per day makes the alarm system almost unusable. The recommendations from the Top 18 Bad actors should be accessed and implemented where possible.

Of these the biggest challenge is the Pulveriser Reject Hopper Level alarms. Collectively these alarms accounted 14% of the alarm count. Part of the solution is outside the scope of alarm management, and has historically been very hard to resolve. The Water Plant pH (7.6%) and Coal Conveyer Weight Meter (1.3%) alarms also require solutions outside of alarm management to resolve, though the resolutions should be achievable using technical expertise at the project site.

The remaining Top 18 Bad Actors are all classic alarm management problems and should be able to be resolved by applying good alarm management practice. These remaining alarms accounted for 17.8% of the total alarm count. Implementing the recommendations will produce quick wins for alarm management at the project site.

Only sustained alarm management will reduce and keep the daily alarm rate in control (150 – 300 alarms per day). Once this is achieved focus should shift to standing alarms and alarm floods created by major process disturbances and shutdowns. The likely solutions to these problems will be to develop alarm masking strategies at the subsystem level. This will require well matured alarm management practices to be successful.

The Alarm Philosophy, Master Alarm Database and Alarm Reporting Tool were road blocks to effective alarm management at the project site. It still remains to be seen if the project site will be able to successfully implement and sustain industry best practice alarm management practices. Now that they have the tools to be successful all they need is the will.

References

ASM Consortium, 2009. *Effective Alarm Managment Practices.* s.l.:ASM Consortium.

ASM Consortium, 2013. *Improving the Operations Team Situation Awareness: Lessons Learned from Major Process Incidents.* [Online]
Available at: https://www.asmconsortium.net/Documents/AM-13-37%20Operator%20Team%20Situation%20Awareness_ReisingBullemer_2013.pdf
[Accessed 31 5 2015].

ASM Consortium, n.d. *ASM Consortium - History.* [Online]
Available at: http://www.asmconsortium.net/defined/history/Pages/default.aspx
[Accessed 17 06 2015].

Bransby, M. L. & Jenkinson, J., 1997. *The Management of Alarm Systems,* Sudbury: HSE Books.

Brown, D. C. & O'Donnell, M., 1997. *TOO MUCH OF A GOOD THING? - ALARM MANAGEMENT EXPERIENCE IN BP OIL.* London, Institution of Electrical Engineers.

EEMUA, 2007. *EEMUA 191 - Alarm Systems, A Guide to Design, Management and Procurement.* London: The Engineering Equipment and Materials Users Association.

Hollifield, B., 2015. *Understanding the New IEC 62682 Alarm Management Standard - A PAS White Paper.* Houston: PAS.

Hollifield, B. R. & Habibi, E., 2001. *Alarm Management: A Comprehensive Guide.* 2nd ed. Research Triangle Park: International Society of Automation.

Hopkins, A., n.d. *Lessons from Esso's Plant Explosion at Longford.* [Online]
Available at:
http://www.futuremedia.com.au/docs/Lessons%20from%20Longford%20by%20Hopkins.PDF
[Accessed 26 4 2015].

HSE UK, 1997. *The Explosion and Fires at the Texaco Refinery, Milford Haven, 24 July 1994,* s.l.: HSE UK.

HSE UK, n.d. *Better Alarm Handling - HSE Information Sheet.* [Online]
Available at: www.hse.gov.uk/pubns/chis6.pdf
[Accessed 17 April 2015].

HSE UK, n.d. *Extract from inspectors toolkit.* [Online]
Available at: http://www.hse.gov.uk/humanfactors/topics/specific1.pdf
[Accessed 17 6 2015].

IEC, 2013. *IEC 61131-3 Programmable controllers - Part 3: Programming languages.* s.l.:International Electrotechincal Commission.

ISA, 2001. *ANSI/ISA-88.00.02-2001 Control Part 2: Data Structures and Guidelines for Languages.* Research Park Triangle(Northern Carolina): International Society of Automation.

ISA, 2009. *ANSI/ISA-18.2-2009 Management of Alarm Systems for the Process Industries.* Research Triangle Park(Northern Carolina): International Society of Automation.

ISA, 2009. *ANSI/ISA-5.1-2009 Instrumentation Symbols and Identification.* Research Park Triangle(Northern Carolina): International Society of Automation.

Longford Royal Commission, 1999. *Report of the Longford Royal Commission,* s.l.: Government Printer for the State of Victoria.

Metzgar, D., 2009. *ASM Alarm Management Guidelines and ISA-18.2: How do they stack up?.* [Online]
Available at:
http://www.controlglobal.com/articles/2009/asmalarmmanagement0910/?show=all
[Accessed 17 6 2015].

NIST, 2009. *ATP Helps Consortium Develop Technology to Prevent Manufacturing Accidents.* [Online]
Available at: http://www.atp.nist.gov/gems/asmc_94-01-0169.htm
[Accessed 17 6 2015].

Perrow, C., 2011. Fukushima and the inevitability of accidents. *Bulletin of the Atomic Scientists,* 67(6), pp. 44-52.

Rothenberg, D. H., 2009. *Alarm Managment for Process Control.* New York: Momentum Press.

The Presidents Commission on The Accident at TMI, 1979. *The Report of The Presidents Commission on The Accident at TMI,* s.l.: US Government Printing Office.

VGA Group, 2015. *KKS Identification System for Power Plants.* [Online]
Available at: http://www.vgb.org/shop/b105e.html?___store=en&___from_store=default
[Accessed 15 June 2015].

World Nuclear Association, 2015. *Nuclear Power in Japan.* [Online]
Available at: http://www.world-nuclear.org/info/Country-Profiles/Countries-G-N/Japan/
[Accessed 30 May 2015].

Appendix A – Project Specification

University of Southern Queensland

FACULTY OF ENGINEERING AND SURVEYING

ENG4111/4112 Research Project

Project Specification

FOR: **Daniel Justin SNELGAR**

TOPIC: Implementing Industry Best Practice Alarm Management

SUPERVISER: Catherine Hills

PROJECT AIM: This project seeks to investigate Process Automation industry best practice for the management of alarm systems. This information will be used to benchmark the selected industrial site, a large thermal power station, against industry best practice alarm metrics for alarms rates and the installed base of alarms. The site's current managements systems associated with alarm management will also be compared to industry best practice alarm management practices so a gap analysis can be created.

PROGRAME: Issue A, 18th March 2015

1) Research the history of industrial alarms, the risks associated with poorly managed alarms systems and some industrial incidents that have been attributed to poorly managed alarms systems.

2) Compare current industry guides and standards, not limited to but specifically:
   a. 'EEMUA 191 Alarms systems – a guide to design, management and procurement'
   b. 'ISA 18.2 Management of Alarm Systems for the Process Industries'
   c. 'IEC 62682 Management of alarm systems for the process industries'

3) Based on current industry guides and standards establish the appropriate aspects and metrics for an industry best practice alarm management system.

For the selected industrial site:

4) Design and implement reporting tools to analyse the archived chronological alarm data and the installed base of configured alarms so they may be compare to industry best practice metrics.

5) Compare the results of the reporting tools against industry best practice metrics and where possible suggest changes to improve alarm performance. Simulate the results of the proposed changes to alarms.

6) Compare the site's management systems associated with alarm management against an industry best practice alarm management system and create a gap analysis.

As time permits:

7) Implement proposed changes to the alarm system and compare against simulated results.

8) Research the cognitive boundaries of human performance and how this relates to the metrics used in industry guides and standards.

AGREED __________________(student) __________________(supervisor)

Date: / /2015 Date: / /2015

Appendix B – Master Alarm Database

Appendix B.1. BSIG Parser Tool Code Listing

```
Sub bsig_parser()

' Set column headers
Cells(1, 1).Value = "Tag KKS"
Cells(1, 2).Value = "Description"
Cells(1, 3).Value = "Engineering Units"
Cells(1, 4).Value = "DCS Address"
Cells(1, 5).Value = "Data Type"
Cells(1, 6).Value = "Text for Value 1"
Cells(1, 7).Value = "Text for Value 0"
Cells(1, 8).Value = "Alarm State"
Cells(1, 9).Value = "Priority"
Cells(1, 10).Value = "Limit Value"
Cells(1, 11).Value = "MF_SIG"
Cells(1, 12).Value = "Masking Signal"
Cells(1, 13).Value = "Number of FGs"
Cells(1, 14).Value = "Function Group"

' Initialise row and column index counters
r = 1
c = 1

' Find the first file with the BSIG extension in the directory
' Note: assuming the files reside in a subdirectory .\PBS_daten relative to this file
strFilePath = ThisWorkbook.Path
strFileName = Dir(strFilePath & "\PBS_daten\*.BSIG")

' File Handling Loop - process while there are still .BSIG files found in the directory
While strFileName <> ""

    ' Some of the BSIG files need not be processed, only files that start with numeric
    ' characters, is not numeric the skip to the next file
    If IsNumeric(Mid(strFileName, 5, 1)) = False Then GoTo skipfile

    ' Extract the Function Group name from the file name
    strFunctionGroup = Right(Left(strFileName, 13), 9)

    ' Build the a string of the file name including the full path
    strFileNameFull = strFilePath & "\PBS_daten\" & strFileName

    ' Open the file an import the contents to a string variable
    ' Note: because the files are sourced for a Linux based computer system the line feed used as
    ' a carriage return is not recognised by VBA, so the Line Input command reads the whole file.
    ' Later we check to ensure the full file has been parsed and the contents have not been clipped
    ' due to string length restrictions
    FileNum = FreeFile
    Open strFileNameFull For Input As FileNum
    Line Input #FileNum, strFileContents

    ' Close the current BSIG file
    Close FileNum

    ' Initialise file index counters
    intStartPos = 1
    intLineNum = 1

    ' Line Handling Loop
    While intStartPos < Len(strFileContents)

        ' Get the next line of the file - Chr(10) is the line feed character
        intEndPos = InStr(intStartPos, strFileContents, Chr(10))
        strLineText = Mid(strFileContents, intStartPos, intEndPos - intStartPos)
        intStartPos = intEndPos + 1

        ' Only process after the 4th line, the line is not blank and the line start with "E_AD"
        If intLineNum > 4 And strLineText <> "" And Left(strLineText, 4) <> "E_DA" Then

            ' If the line starts with "SIGT" then line represents a new signal ...
            If Left(strLineText, 4) = "SIGT" Then

                ' ... increase the row index, reset the column index and write the Function Group
name ...
                r = r + 1
                Cells(r, 14).Value = strFunctionGroup
                Cells(r, 13).Value = 1
```

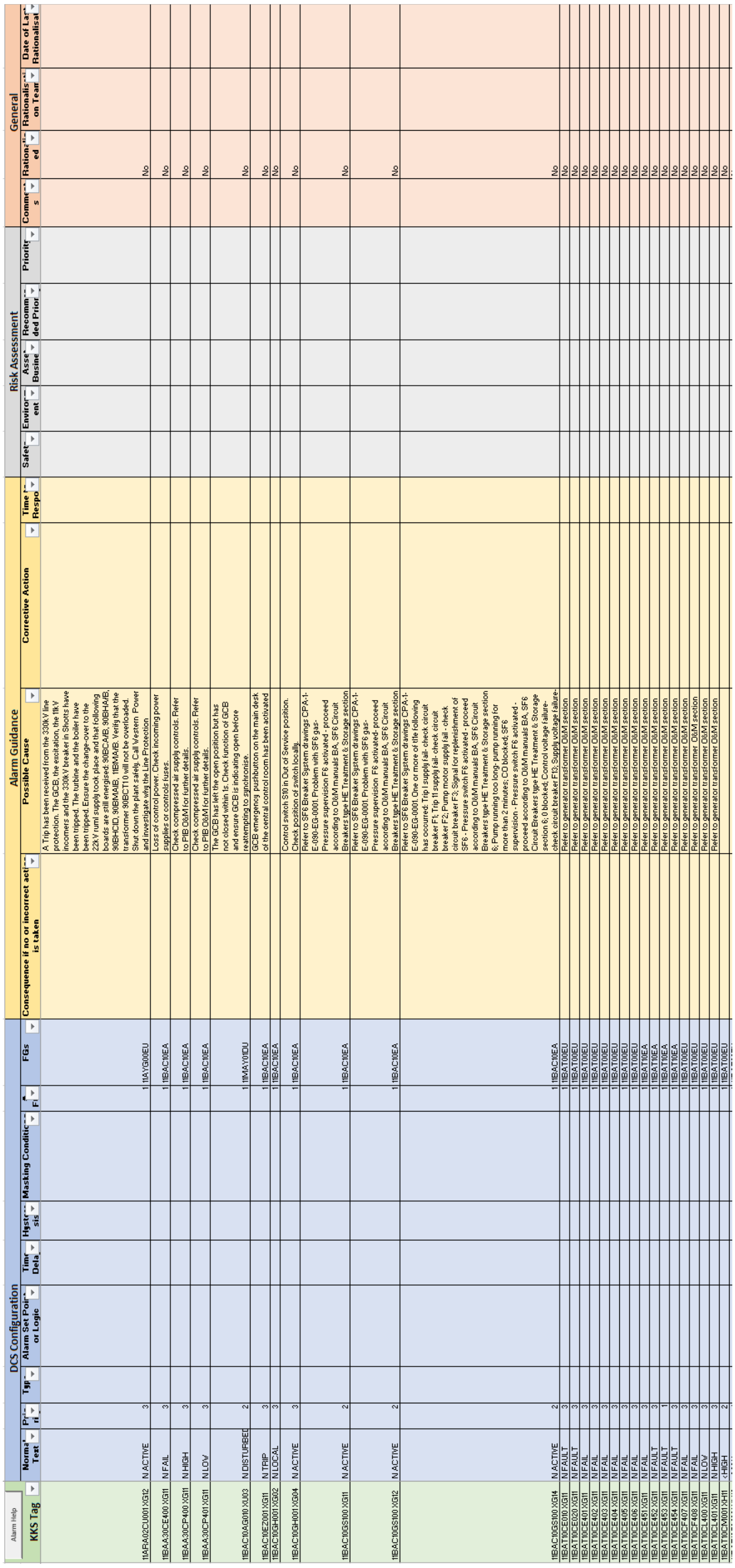
```
                c = 1

            ' ... else the line is a continuation of the signal ...
            Else
                '... split the column name from the data and write the data to the spread sheet
                strCellText = Right(strLineText, Len(strLineText) - InStr(strLineText, ":") - 1)
                strCellText = Replace(strCellText, "'", "")
                Cells(r, c).Value = strCellText
                c = c + 1

            End If

        End If

        ' Increment the line index counter
        intLineNum = intLineNum + 1

    ' Continue the Line Handling Loop
    Wend

    ' Check that the last line of the file begins with "E_DA" - this proves that the complete file
was
    ' imported into the string.  If not captured use a message box to warn
    If Left(strLineText, 4) <> "E_DA" Then

        a = MsgBox("File " & strFileName & " not fully processed", vbOKOnly)

    End If

' If the file was skipped this is where the code jumps to
skipfile:

    ' Find the next file with the BSIG extension in the directory
    strFileName = Dir

' Continue the File Handling Loop
Wend

' Remove duplicates but retain FG information
' Note - a binary signal may be in more than one function group, therefore be in multiple lines.
' We only want the signal once, so the following code removes all duplicates but keeps the Function
' Group information from each duplicate.

' This block of code was created with the aid of the macro recorder
' It sorts all information in order of KKS name and then Function Group
lastrow = Cells(Rows.Count, 2).End(xlUp).Row
Range("A1:M" & lastrow).Select
ActiveSheet.Sort.SortFields.Clear
ActiveSheet.Sort.SortFields.Add Key:=Range( _
    "a2:a" & lastrow), SortOn:=xlSortOnValues, Order:=xlAscending, DataOption:= _
    xlSortNormal
ActiveSheet.Sort.SortFields.Add Key:=Range( _
    "n2:n" & lastrow), SortOn:=xlSortOnValues, Order:=xlAscending, DataOption:= _
    xlSortNormal
With ActiveSheet.Sort
    .SetRange Range("A1:n" & lastrow)
    .Header = xlYes
    .MatchCase = False
    .Orientation = xlTopToBottom
    .SortMethod = xlPinYin
    .Apply
End With

' Initialise row index counter
r = 3

' Loop - while there are binary signals to process keep processing rows
While Cells(r - 1, 1) <> ""

    ' If the current row is the same signal as the row above ...
    If Cells(r - 1, 1).Value = Cells(r, 1).Value Then

        ' ... increment the column  which identifies the number of Function Groups and append the
        ' Function Group name to the Function Group column, then delete the row
        Cells(r - 1, 13).Value = Cells(r - 1, 13).Value + 1
        Cells(r - 1, 14).Value = Cells(r, 14).Value & "," & Cells(r - 1, 14).Value
        Rows(r).Delete

    Else

        ' Increment the row index counter
        r = r + 1
```

```
    End If

' Continue removed duplicates the Loop
Wend

End Sub
```

Appendix B.2. BSIG Parser Tool Output Screen Shot

	Tag KKS	Description	Engineering Units	P14 Address	Data Type	Text for Value 1	Text for Value 0	Alarm State	Priority	Limit Value	MF_SIG	Masking Signal	Number of FGs	Function Group
7530	11LAD70CL012 XH13	HP7 CTRL LEVEL 2 TX		1 033 47 027 09	3	>MAX	<MAX	1	1		N		2	11LCH07EA,11LCH00EA
7531	11LAD70CL012 XH62	HP7 CTRL LEVEL 2 TX		1 033 47 027 05	3	<LOW	>LOW	1	2		N		2	11LCH07EA,11LCH00EA
7532	11LAD70CL013 XH11	HP7 CTRL LEVEL 3 TX		1 033 49 005 03	3	>HIGH	<HIGH	1	2		N		2	11LCH07EA,11LCH00EA
7533	11LAD70CL013 XH13	HP7 CTRL LEVEL 3 TX		1 033 49 005 09	3	>MAX	<MAX	1	1		N		2	11LCH07EA,11LCH00EA
7534	11LAD70CL013 XH62	HP7 CTRL LEVEL 3 TX		1 033 49 005 05	3	<LOW	>LOW	1	2		N		2	11LCH07EA,11LCH00EA
7535	11LAD70CL902 XH21	HP7 CTRL LEVEL TX (2oo3)		1 039 40 004 03	3	>HIGH	<HIGH	1	2		N		3	11LCH07EA,11LAD70DL,11CFA00EU
7536	11LAD70CL902 XH23	HP7 CTRL LEVEL TX (2oo3)		1 039 40 004 06	3	>MAX	<MAX	1	1		N		3	11LCH07EA,11LAD70DL,11CFA00EU
7537	11LAD70CL902 XH72	HP7 CTRL LEVEL TX (2oo3)		1 039 40 004 08	3	<LOW	>LOW	1	2		N		3	11LCH07EA,11LAD70DL,11CFA00EU
7538	11LAD70CL902 XU01	HP7 CTRL LEVEL TX		1 039 40 014 11	1	DISTURBED	N DISTURBED	1	2		N		1	11CFA00EU
7539	11LAD70CL902 XU63	HP7 CTRL LEVEL TX (2oo3)		1 039 40 014 10	1	DISTURBED	N DISTURBED	1	3		N		1	11CFA00EU
7540	11LAE21AA001 XU01	BLR PROT MAIN FUEL TRIP		1 032 06 001 01	1	ACTIVE	N ACTIVE	1	3		N		1	11LAE21EA
7541	11LAE21AA002 XU03	LOW DSH SPRAY WIDE OPEN		1 010 11 004 11	1	ALARM	N ALARM	1	1		N		1	11HAY01DT
7542	11LAE21CG002 YE45	G LOW T DSH SPRAY CV A		0	3	DISTURBED	N DISTURBED	1	3		N		1	11HAY01DT
7543	11LAE22AA001 XU01	BLR PROT MAIN FUEL TRIP		1 032 06 001 03	1	ACTIVE	N ACTIVE	1	3		N		1	11LAE21EA
7544	11LAE22AA002 XU03	LOW DSH SPRAY WIDE OPEN		1 010 11 004 12	1	ALARM	N ALARM	1	1		N		1	11HAY01DT
7545	11LAE22CG002 YE45	G LOW T DSH SPRAY CV B		0	3	DISTURBED	N DISTURBED	1	3		N		1	11HAY01DT
7546	11LAE31AA001 XU01	BLR PROT MAIN FUEL TRIP		1 032 06 001 05	1	ACTIVE	N ACTIVE	1	3		N		1	11LAE21EA
7547	11LAE31AA002 XR02	HIGH T DSH SPRAY CV (A)		1 010 12 004 10	23	MANUAL	N MANUAL		-1		N		1	11HAY01DT
7548	11LAE31AA002 XU03	HIGH DSP SPRAY WIDE OPEN		1 010 12 005 10	1	ALARM	N ALARM	1	1		N		1	11HAY01DT
7549	11LAE32AA001 XU01	BLR PROT MAIN FUEL TRIP		1 032 06 001 07	1	ACTIVE	N ACTIVE	1	3		N		1	11LAE21EA
7550	11LAE32AA002 XR02	HIGH T DSH SPRAY CV (B)		1 010 12 010 10	23	MANUAL	N MANUAL	1	0		N		1	11HAY01DT
7551	11LAE32AA002 XU03	HIGH DSH SPRAY WIDE OPEN		1 010 12 005 13	1	ALARM	N ALARM	1	1		N		1	11HAY01DT
7552	11LAE32CG002 YE45	G HIGH T DSH SPRAY CV B		0	3	DISTURBED	N DISTURBED	1	3		N		1	11HAY01DT
7553	11LAF50AA001 XU01	BLR PROT MAIN FUEL TRIP		1 032 07 001 01	1	ACTIVE	N ACTIVE	1	3		N		1	11LAE21EA
7554	11LAF50AA002 XU03	RH DSH SPRAY WIDE OPEN		1 010 21 046 05	1	ALARM	N ALARM	1	1		N		1	11HAY02DT
7555	11LAF50CG002 YE45	G RH DSH SPRAY CV		0	3	DISTURBED	N DISTURBED	1	3		N		1	11HAY02DT
7556	11LBA10CT001 XH11	T STEAM TERT SH OUTL A		1 034 35 017 03	3	>HIGH	<HIGH		-1		N		1	11HAY01DT
7557	11LBA11CT001 XH11	T STEAM TERT SH OUTL B		1 034 35 019 03	3	>HIGH	<HIGH		-1		N		1	11HAY01DT
7558	11LBA20AA001 XB02	BOILER STOP VALVE		1 032 34 000 04	21	CS CLOSE	N CS CLOSE	1	0		N		2	11MAY02DU,11MAA10EA
7559	11LBA20AA001 XU02	BLR MAIN FUEL TRIP		1 032 34 004 13	1	N ACTIVE	ACTIVE	1	0		N		1	11LBA20EA
7560	11LBA20AA001 XU03	STEAM > TBN INL MET TEMP		1 032 34 004 03	1	ACTIVE	N ACTIVE	1	0		N		1	11LBA20EA
7561	11LBA20AA001 XU04	STEAM PRESS EQUALISED		1 032 34 004 04	1	ACTIVE	N ACTIVE	1	0		N		1	11LBA20EA
7562	11LBA20AA002 XB01	BOILER STOP BYPASS VALVE		1 032 34 001 05	21	CS OPEN	N CS OPEN	1	0		N		1	11LBA20EA
7563	11LBA20AA002 XB02	BOILER STOP BYPASS VALVE		1 032 34 001 04	21	CS CLOSE	N CS CLOSE	1	0		N		1	11MAA10EA
7564	11LBA20AA002 XU02	BLR MAIN FUEL TRIP		1 032 34 004 14	1	N ACTIVE	ACTIVE	1	0		N		1	11LBA20EA
7565	11LBA20AA002 XU03	STEAM > TBN INL MET TEMP		1 032 34 004 08	1	ACTIVE	N ACTIVE	1	0		N		1	11LBA20EA
7566	11LBA20AA002 XU04	STEAM PRESS ADEQUATE		1 032 34 004 09	1	ACTIVE	N ACTIVE	1	0		N		1	11LBA20EA

Appendix B.3. Master Alarm Database Sheet Screen Shot



Alarm Help	DCS Configuration									Alarm Guidance				Risk Assessment					General			
KKS Tag	Normal Text	Pri ri	Typ	Alarm Set Point or Logic	Time Dela	Hyste sis	Masking Conditio	A F	FGs	Consequence if no or incorrect actio is taken	Possible Cause	Corrective Action	Time t Respo	Safet	Enviror ent	Asse Busine	Recomm ded Prior	Priority	Comme s	Rational ed	Rationalis on Team	Date of Las Rationalisat
11ARA02CU001 XG12	N ACTIVE	3						1	11AYG00EU		A Trip has been received from the 330kV line protection. The GCB, the excitation, the 11kV incomers and the 330kV breaker in Shotts have been tripped. The turbine and the boiler have been tripped. Ensure the change-over to the 22kV ruml supply took place and that following boards are still energised: 90BCA/B, 90BHA/B, 90BHCID, 90BMAIB, 11BMA/B. Verify that the transformer 90BCT1 0 will not be overloaded. Shut down the plant safely. Call Western Power and investigate why the Line Protection									No		
11BAA30CE400 XG11	N FAIL	3						1	11BAC10EA		Loss of control power. Check incoming power supplies or controls fuses.									No		
11BAA30CP400 XG11	N HIGH	3						1	11BAC10EA		Check compressed air supply controls. Refer to PIB O&M for further details.									No		
11BAA30CP401 XG11	N LOW	3						1	11BAC10EA		Check compressed air supply controls. Refer to PIB O&M for further details.									No		
11BAC10AG010 XU03	N DISTURBED	2						1	11MAY01DU		The GCB has left the open position but has not closed within 1s. Check function of GCB and ensure GCB is indicating open before reattempting to synchronise.									No		
11BAC10EZ001 XG11	N TRIP	3						1	11BAC10EA		GCB emergency pushbutton on the main desk of the central control room has been activated									No		
11BAC10GH001 XG02	N LOCAL	3						1	11BAC10EA											No		
11BAC10GH001 XG04	N ACTIVE	3						1	11BAC10EA		Control switch S10 in Out of Service position. Check position of switch locally.									No		
11BAC10GS100 XG11	N ACTIVE	2						1	11BAC10EA		Refer to SF6 Breaker System drawings CPA-1-E-090-EG-0001. Problem with SF6 gas-Pressure supervision F6 activated - proceed according to O&M manuals BA, SF6 Circuit Breakers type HE Treatment & Storage section									No		
11BAC10GS100 XG12	N ACTIVE	2						1	11BAC10EA		Refer to SF6 Breaker System drawings CPA-1-E-090-EG-0001. Problem with SF6 gas-Pressure supervision F6 activated- proceed according to O&M manuals BA, SF6 Circuit Breakers type HE Treatment & Storage section									No		
11BAC10GS100 XG14	N ACTIVE	2						1	11BAC10EA		Refer to SF6 Breaker System drawings CPA-1-E-090-EG-0001. One or more of tl1e following has occurred: Trip I supply fail- check circuit breaker F1; Trip 11 supply fail- check circuit breaker F2; Pump motor supply fail - check circuit breaker F3; Signal for replenishment of SF6 - Pressure switch F6 activated - proceed according to O&M manuals BA, SF6 Circuit Breakers type HE Treatment & Storage section 6; Pump running too long- pump running for more than 2 minutes; CO blocked; SF6 supervision - Pressure switch F6 activated - proceed according to O&M manuals BA, SF6 Circuit Breakers type HE Treatment & Storage section 6; 0 blocked; Control voltage failure-check circuit breaker F13; Supply voltage failure-									No		
11BAT10CE010 XG11	N FAULT	3						1	11BAT00EU		Refer to generator transformer O&M section									No		
11BAT10CE020 XG11	N FAULT	3						1	11BAT00EU		Refer to generator transformer O&M section									No		
11BAT10CE401 XG11	N FAIL	3						1	11BAT00EU		Refer to generator transformer O&M section									No		
11BAT10CE402 XG11	N FAIL	3						1	11BAT00EU		Refer to generator transformer O&M section									No		
11BAT10CE403 XG11	N FAIL	3						1	11BAT00EU		Refer to generator transformer O&M section									No		
11BAT10CE404 XG11	N FAIL	3						1	11BAT00EU		Refer to generator transformer O&M section									No		
11BAT10CE405 XG11	N FAIL	3						1	11BAT00EU		Refer to generator transformer O&M section									No		
11BAT10CE406 XG11	N FAIL	3						1	11BAT00EU		Refer to generator transformer O&M section									No		
11BAT10CE451 XG11	N FAIL	3						1	11BAT10EA		Refer to generator transformer O&M section									No		
11BAT10CE452 XG11	N FAULT	3						1	11BAT10EA		Refer to generator transformer O&M section									No		
11BAT10CE453 XG11	N FAULT	1						1	11BAT10EA		Refer to generator transformer O&M section									No		
11BAT10CE454 XG11	N FAULT	3						1	11BAT10EA		Refer to generator transformer O&M section									No		
11BAT10CF407 XG11	N FAIL	3						1	11BAT00EU		Refer to generator transformer O&M section									No		
11BAT10CF408 XG11	N FAIL	3						1	11BAT00EU		Refer to generator transformer O&M section									No		
11BAT10CL400 XG11	N LOW	3						1	11BAT00EU		Refer to generator transformer O&M section									No		
11BAT10CL401 XG11	N HIGH	3						1	11BAT00EU		Refer to generator transformer O&M section									No		
11BAT10CM001 XH11	<HIGH	2						1	11BAT00EU											No		

Appendix B.4. Master Alarm Database Instruction Sheet Screen Shot

Introduction

This is the Master Alarm Database. It is the master data for Alarms on site. Alarms should not be changed in the DCS configuration without first being identified in this database.

Instructions

1. Prior to the rationalisation session create a copy of the Rationalisation Template and name if after the KKS tag name of the Alarm and fill as many of the DCS Configuration fields as possible.
2. During the rationalisation session fill in all of the fields
Note: if an alarm is to be removed leave all other fields blank and indicate in the comments section that it is to be deleted and the reasons why
3. After the alarm rationalisation session correct site Management of Change procedures should be followed to implement any alarm changes in the DCS configuration, a copy of the completed Alarm Template sheet should be attached to this documentation.
4. Once the DCS Configuration is up to date the information on the Alarm Template sheet for the alarm should copied the Master Alarm Database Sheet and the Alarm Template sheet for the alarm sheet then removed from this file. If an alarm is to be deleted remove its entry in the Master Alarm Database sheet. It is recommended to keep copies of the Alarm Template sheet for alarms in a separated file for reference, especially deleted alarms.

Master Alarm Database Fields

	KKS Tag	KKS Tag of the alarm signal
DCS Configuration	Description	The text descriptor of the signal
	Alarm Text	The text descriptor for the alarm state
	Normal Text	The text descriptor for the non-active alarm state
	Priority	Priority of the alarm as configured in the DCS
	Type	A choice of :Measured Limit Value Calculated Limit Value Measured Binary Logic
	Alarm Set Point or Logic Conditions	The functional description is the DCS configuration required to implement the alarm. This is the alarm set point or logic conditions that will activate the
	Time Delay	Time delay applied to the alarm
	Hysteresis	Hysteresis applied to the alarm
	Masking Conditions	Identity any logic conditions in the DCS which can be used to prevent the alarm from activating unnecessarily, i.e. sub-system or equipment shutdown which may generate an alarm that is unnecessary
	# FGs	How many Function Groups the alarm is in
	FGs	The names of the Function Group(s)s the alarm is in
Alarm Guidance	Consequence if no or incorrect action is taken	What is the consequence if no action or the incorrect action is taken - assume any shutdown layers will operate
	Possible Cause	What are the potential causes of the abnormal situation
	Corrective Action	What is the corrective action to be taken to return the process to normal operation
	Time to Respond	How long does the operator have to respond to the alarm in order to prevent the abnormal situation from escalating to the consequence
Risk Assessment	Safety	Refer to the Risk Matrix in the Alarm Philosophy
	Environment	
	Asset Business	
	Recommended Priority	
	Priority	
General	Comments	Any additional comments or justifications should be noted here
	Rationalised Yes / No	Since all alarms have never been rationalised all have been set to 'No'. Set to yes once each alarm is rationalised
	Rationalisation Team	The names and function of those in the session should be recorded here
	Date of Last Rationalisation	The date of the rationalisation session

Appendix B.5. Rationalisation Template Screen Shot

ALARM RATIONALISATION TEMPLATE

KKS Tag		
Description		
Text	**Normal**	**Alarm**
Type	Logic	
Alarm Set Point or Logic Conditions	<The functional description is the DCS configuration required to implement the alarm. This is the alarm set point or logic conditions that will activate the alarm>	
Time Delay		
Hysteresis		
Masking Conditions	<Identity any logic conditions in the DCS which can be used to prevent the alarm from activating unnecessarily, i.e. sub-system or equipment shutdown which may generate an alarm that is unnecessary>	

Consequence if no or incorrect action is taken	<What is the consequence if no action or the incorrect action is taken - assume any shutdown layers will operate>

Potential Causes	<What are the potential causes of the abnormal situation>

Corrective Action	<What is the corrective action to be taken to return the process to normal operation>

Consequence if no or incorrect action is taken					
	Safety	**Environment**	**Asset Damage or Loss**	**Business**	**Asset Integrity**
Severe					
Major					
Minor					

Maximum Time to Respond	
> 30 Minutes	
10 to 30 min	
3 to 10 min	
Less than 3 min	

Maximum Time to Respond	**Consequence**		
	Minor	**Major**	**Severe**
> 30 Minutes	Event	Event	Event
10 to 30 min	3	3	2
3 to 10 min	3	2	2
Less than 3 min	2	1	1

Recommended Priority	**#VALUE!**

Priority	

Additional Comments	<Any additional comments or justifications should be noted here>

Rationalisation Team	<The names and function of those in the session should be recorded here>

Rationalisation Date	

Appendix B.6. Alarm Help Interface Code Listing

```
Private Sub UserForm_Initialize()

' First row in the MasterAlarmDatabase with an alarm
r = 3

' Populate the KKS Tag combo box with all of the alarms in the Master Database
With ComboBox_KKS_Tag

    ' Loop through each item in coloum 1 until a blank cell is found ...
    While Worksheets("MasterAlarmDatabase").Cells(r, 1) <> ""

        ' ... and add the item to the KKS Tag combo box
        .AddItem Worksheets("MasterAlarmDatabase").Cells(r, 1).Value

        r = r + 1

    Wend

End With

End Sub
```

```
Private Sub CommandButton_Find_Click()

' Call the FindAlarm subroutine if the Find button is pressed

Call FindAlarm

End Sub
```

```
Private Sub FindAlarm()

' Get the current alarm selected in the KKS Tag Combo Box
KKS_Tag = ComboBox_KKS_Tag.Value

' If the alarm is not found there will be an error
On Error GoTo NotFound

' For the alarm selected find the row in the Master Alarm Database
r = Application.WorksheetFunction.Match(KKS_Tag, Worksheets("MasterAlarmDatabase").Range("A:A"), 0)
On Error Resume Next

' Populate the fields in the UserForm with the information for selected alarm
TextBox_Descriptor.Value = Worksheets("MasterAlarmDatabase").Cells(r, 2).Value
TextBox_Alarm_Text.Value = Worksheets("MasterAlarmDatabase").Cells(r, 3).Value
TextBox_Consequence.Value = Worksheets("MasterAlarmDatabase").Cells(r, 13).Value
TextBox_Cause.Value = Worksheets("MasterAlarmDatabase").Cells(r, 14).Value
TextBox_Action.Value = Worksheets("MasterAlarmDatabase").Cells(r, 15).Value

Exit Sub

NotFound:
' If the alarm is not found then put 'Not Found' in the descriptor text box
' Empty all of the other text boxes
TextBox_Descriptor.Value = "Not Found"
TextBox_Alarm_Text.Value = ""
TextBox_Consequence.Value = ""
TextBox_Cause.Value = ""
TextBox_Action.Value = ""

End Sub
```

Appendix C – Alarm Reporting Tool

Appendix C.1. Alarm Report SQL Query Code Listing

```
/* Clean up temp tables */
IF OBJECT_ID('tempdb..#working') IS NOT NULL
    DROP TABLE #working
IF OBJECT_ID('tempdb..#topalarms') IS NOT NULL
    DROP TABLE #topalarms
IF OBJECT_ID('tempdb..#topmaintenance') IS NOT NULL
    DROP TABLE #topmaintenance
IF OBJECT_ID('tempdb..#topdisturbance') IS NOT NULL
    DROP TABLE #topdisturbance
IF OBJECT_ID('tempdb..#prioritydistribution') IS NOT NULL
    DROP TABLE #prioritydistribution
IF OBJECT_ID('tempdb..#dailyrate') IS NOT NULL
    DROP TABLE #dailyrate

declare @total decimal(10,3)
declare @timeshift int
set @timeshift = 8

/* Prepare working table for alarm activations in the reporting period */
select *
 into #working
 from PlaCoEvents.dbo.tbl_events
 where (((ev_prio = 1 or ev_prio = 2 or ev_prio = 4) and len(tag_name) = 17)   /* User Alarms */
 or ev_prio = 3  /* Maintenance Alarms */
 or ev_prio = 8 or ev_prio = 9 ) /* Disturbance Alarms */
 and info_01 <> 'CLEARED' and tag_shortdescription <> 'CLEARED'
 and ts_subsystem > dateadd(hh, -@timeshift,'01-01-2015') and  ts_subsystem  < dateadd(hh, -
@timeshift,'02-01-2015')

/* Set column ts_subsytem to local time */
update #working
set ts_subsystem = dateadd(hh, @timeshift, ts_subsystem)

/* Return priorities to DCS values */

/* Set Disturbance Alarms to Priority 6 - temporary!*/
update #working
set ev_prio = 6
 where ev_prio = 8 or  ev_prio = 9
/* Set Maintenance Alarms to Priority 0 */
update #working
set ev_prio = 0
 where ev_prio = 3
/* Set User Priority 4 to Priority 3 */
update #working
set ev_prio = 3
 where ev_prio = 4
 /* Set Disturbance Alarms to Priority 4 */
update #working
set ev_prio = 4
 where ev_prio = 6

/* Calculate total alarms for calcs */
set @total = (select count(*) from #working where ev_prio <> 4)

/* Get priority distribution into a table */
select ev_prio, cast(count(*) as decimal(10,3)) as priopercent
 into #prioritydistribution
 from #working
 where ev_prio<>4
 group by ev_prio
 order by ev_prio
update #prioritydistribution
 set priopercent = priopercent / @total

/* Get Top Alarms into a table */
/* Priority 1, 2, 3 and Maintnenance alarms */
select top 20 tag_name, tag_description, tag_shortdescription, tag_status, ev_prio, COUNT(*) as total
,COUNT(*) / @total as alarm_percent
 into #topalarms
 from #working
 where ev_prio <> 4
 group by tag_name, tag_description, tag_shortdescription, tag_status, ev_prio
 order by total desc

/* Get Top Maintenance Alarms into a table */
select top 10 tag_name, tag_description, tag_shortdescription, tag_status,  ev_prio, COUNT(*) as
total, COUNT(*) / @total as alarm_percent
 into #topmaintenance
 from #working
 where ev_prio = 0
```

```
 group by tag_name, tag_description, tag_shortdescription, tag_status, ev_prio
 order by total desc


/* Get Top Disturbance Alarms into a table */
set @total = (select count(*) from #working where ev_prio = 4)

select top 10 tag_name, tag_description, tag_shortdescription, tag_status,  ev_prio, COUNT(*) as
total, COUNT(*) / @total as alarm_percent
 into #topdisturbance
 from #working
 where ev_prio = 4
 group by tag_name, tag_description, tag_shortdescription, tag_status, ev_prio
 order by total desc

/* Get the daily alarm rates into a table */
SELECT DATEADD(dd, DATEDIFF(dd, 0, ts_subsystem), 0) as Date, COUNT(*) as Rate
 into #dailyrate
 FROM  #working
 where ev_prio <> 4
 group by DATEADD(dd, DATEDIFF(dd, 0, ts_subsystem), 0)
 order by Date

 /* Output results */
select * from #prioritydistribution order by ev_prio
select * from #topalarms order by total desc
select * from #topmaintenance order by total desc
select * from #topdisturbance order by total desc
select * from #dailyrate order by Date

/* Clean up temp tables */
IF OBJECT_ID('tempdb..#working') IS NOT NULL
    DROP TABLE #working
IF OBJECT_ID('tempdb..#topalarms') IS NOT NULL
    DROP TABLE #topalarms
IF OBJECT_ID('tempdb..#topmaintenance') IS NOT NULL
    DROP TABLE #topmaintenance
IF OBJECT_ID('tempdb..#topdisturbance') IS NOT NULL
    DROP TABLE #topdisturbance
IF OBJECT_ID('tempdb..#prioritydisturbance') IS NOT NULL
    DROP TABLE #prioritydistribution
IF OBJECT_ID('tempdb..#dailyrate') IS NOT NULL
    DROP TABLE #dailyrate
```

Appendix C.2. SQL Subroutine Code Listing

```
Sub SQL(ByVal startdate As String, ByVal enddate As String)

' Declare the objects and variables
Dim Cnn As New ADODB.Connection
Dim Rst As New ADODB.Recordset
Dim ConnectionString, SqlTextFile, SqlStatement As String

' Read connection string of configuration sheet
ConnectionString = Worksheets("SQL").Cells(2, 1).Value

' Execute the 'Open' method using the connection string
Cnn.Open ConnectionString
Cnn.CommandTimeout = 900

' Initialise the row index
r = 4

' Main program loop - while the cell at RrC1 is no blank there are more SQL commands to process
While Worksheets("SQL").Cells(r, 1).Value <> ""

    sqlstr = Worksheets("SQL").Cells(r, 1).Value
    sqlstr = Replace(sqlstr, "STARTDATE", startdate)
    sqlstr = Replace(sqlstr, "ENDDATE", enddate)

    ' Determine with object ot use to process the SQL commands
    If Worksheets("SQL").Cells(r, 2).Value = "" Then

        ' Execute SQL commands using connection object - no record set will be returned
        Cnn.Execute sqlstr

    Else

        ' Execute SQL command using the recordset object
        Rst.Open sqlstr, Cnn
        ' Put the record set at the row and column referecne as per SQL configuration sheet
        Range(Chr(64 + Worksheets("SQL").Cells(r, 3).Value) & Worksheets("SQL").Cells(r,
2).Value).CopyFromRecordset Rst
        Rst.Close

    End If

    ' Increase the row index
    r = r + 1

Wend

' Close the connection to the SQL server and release memory for objects
Cnn.Close
Set Cnn = Nothing
Set Rst = Nothing

End Sub
```

Appendix C.3. ReportGenerator Code Listing

```
Sub ReportGenerator()

' Declare the variables
Dim strStartDate, strEndDate As String

' Get the report date from the date picker object on the user interface worksheet
strDate = Worksheets("Main").ReportDatePicker.Value

' Determine the reporting period from the radio button selection - weekly or monthly
If Worksheets("Main").WeeklyButton.Value = True Then

    ' Weekly Report
    ' Determine the start date
    ReportDate = strDate - Weekday(strDate, vbMonday) + 1
    ReportYear = Year(ReportDate)
    ReportMonth = Month(ReportDate)
    If ReportMonth < 10 Then ReportMonth = "0" & ReportMonth
    ReportDay = Day(ReportDate)
    If ReportDay < 10 Then ReportDay = "0" & ReportDay
    ' Start date for weekly report that will be passed to the SQL subroutine
    strStartDate = ReportMonth & "-" & ReportDay & "-" & ReportYear

    ' Built strings for report titles and subtitles
    strReportName = "Weekly " & ReportYear & ReportMonth & ReportDay
    strReportTitle = "Weekly Alarm Report"
    strReportPeriod = "Monday, " & MonthName(ReportMonth) & " " & ReportDay & ", " & ReportYear

    ' Determine the end date
    ReportDate = ReportDate + 7
    ReportMonth = Month(ReportDate)
    ReportYear = Year(ReportDate)
    ReportDay = Day(ReportDate)
    ' End date for weekly report that will be passed to the SQL subroutine
    strEndDate = ReportMonth & "-" & ReportDay & "-" & ReportYear

Else

    ' Monthly Report
    ' Determince the start date
    ReportDate = strDate
    ReportYear = Year(ReportDate)
    ReportMonth = Month(ReportDate)
    If ReportMonth < 10 Then ReportMonth = "0" & ReportMonth
    ' Start date for monthly report that will be passed to the SQL subroutine
    strStartDate = ReportMonth & "-1-" & ReportYear

    ' Built strings for report titles and subtitles
    strReportName = "Monthly " & ReportYear & ReportMonth & "01"
    strReportTitle = "Monthly Alarm Report"
    strReportPeriod = MonthName(ReportMonth) & ", " & ReportYear

    ' Determine the end date
    ReportMonth = ReportMonth + 1
    If ReportMonth > 12 Then
        ReportMonth = 1
        ReportYear = ReportYear + 1
    End If
    ' End date for monthly report that will be passed to the SQL subroutine
    strEndDate = ReportMonth & "-1-" & ReportYear

End If

' Create a copy of the report template and name it appropriately
Sheets("Report").Visible = -1
Sheets("Report").Copy after:=Sheets("SQL")
ActiveSheet.Name = strReportName
Sheets("Report").Visible = 2
Sheets(strReportName).Activate

' Call the SQL subroutine with the appropriate start and end dates
Call SQL(strStartDate, strEndDate)

' Update the report title and subtitle appropriately
Cells(1, 1).Value = strReportTitle
Cells(2, 1).Value = strReportPeriod

' Trim the unused rows in the Daily Alarm Rate table
LastRow = Range("B150").End(xlUp).row + 1
Range("B" & LastRow & ":E144").Delete
```

```
' Move the alarm report to a new Excel file
Sheets(strReportName).Move

End Sub
```

Appendix C.4. Weekly Alarm Report Example

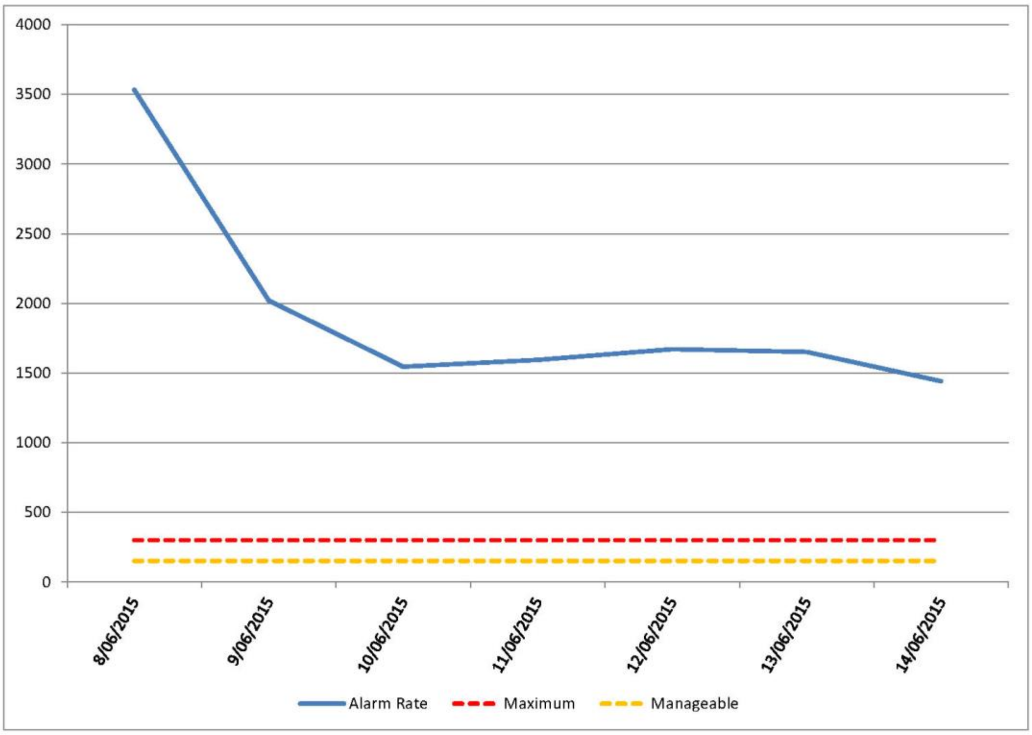
Weekly Alarm Report

Monday, June 08, 2015

Alarm Distribution

Prio	%
Maintenance	8%
1	7%
2	71%
3	14%

Daily Alarm Rate



Top Alarms

Rank	KKS Tag	Description	Status	Desc	Prio	Count	%	Cum %
1	11HFW31CP010 XG11	P SEALG AIR COAL FEED 30	State 1 alarm		2	898	6.7%	6.7%
2	11QEA30CM010 XQ50	DEW POINT DRYER 3 OUTLET	Limit H	>HIGH	2	689	5.1%	11.8%
3	11ETJ00EA800 XU02	VACUUM ECO HOPPERS	State 1 alarm		2	681	5.1%	16.9%
4	11HFH50CL010 XG11	L PYRITE BOX PULV 50	State 1 alarm		2	662	4.9%	21.8%
5	11QCD00EA111 XU01	CONDUCTIVITY > SP	State 1 alarm		2	655	4.9%	26.7%
6	11HFH30CL010 XG11	L PYRITE BOX PULV 30	State 1 alarm		2	538	4.0%	30.7%
7	11CJA00DU002 XU04	FREQUENCY DEVIATION	State 1 alarm		2	388	2.9%	33.5%
8	11HYA00EY801 XU12	T GAS AH OUTLET DIFF	State 1 alarm		1	377	2.8%	36.3%
9	11HFH40CL010 XG11	L PYRITE BOX PULV 40	State 1 alarm		2	328	2.4%	38.8%
10	11HFC30EA800 XU01	PULVERIZER 30 RATIO	State 1 alarm		2	264	2.0%	40.7%
11	11QEA30CM010 XQ50	DEW POINT DRYER 3 OUTLET	Limit HH	>MAX	1	261	1.9%	42.7%
12	90GNK35CQ010 XU13	SALINE WTP OUTLET pH	State 1 alarm		3	188	1.4%	44.1%
13	11LAC30AP013 XU01	BFP3 UNLOADING	State 1 alarm		2	181	1.3%	45.4%
14	90GNK35CQ010 XQ50	PH SALINE BSTR PP RECIRC	Limit H	>HIGH	2	155	1.2%	46.6%
15	90GNK35CQ010 XQ50	PH SALINE BSTR PP RECIRC	Limit L	<LOW	2	146	1.1%	47.7%
16	90GND10CQ010 XU13	pH OXIDATION TANK	State 1 alarm		3	134	1.0%	48.7%
17	90GNK35CQ010 XQ50	PH SALINE BSTR PP RECIRC	Limit HH	>MAX	2	134	1.0%	49.7%
18	90GNQ31AS010	CAUSTIC PP 1 STROKE CNTR	Discr., Prot <-		0	134	1.0%	50.7%
19	90GNK35CQ010 XQ50	PH SALINE BSTR PP RECIRC	Limit LL	<MIN	2	130	1.0%	51.6%
20	90SGA40AP010 XG11	FPSTN PRESS MAINT RUN	State 1 alarm		3	128	1.0%	52.6%

Top Maintenance Alarms

Rank	KKS Tag	Description	Status	Desc	Prio	Count	%	Cum %
1	90GNQ31AS010	CAUSTIC PP 1 STROKE CNTR	Discr., Prot <-		0	134	1.0%	1.0%
2	11HCB00EA100	GROUP CONTROL	Time mon. On		0	84	0.6%	1.6%
3	11HFE84AA001	PULV 20 COLD AIR DAMPER	Discr. int. pos.		0	76	0.6%	2.2%
4	11HFE84AA001	PULV 20 COLD AIR DAMPER	Discr., Off/Cl.		0	57	0.4%	2.6%
5	11HFE74AA001	PULV 20 HOT AIR DAMPER	Discr. int. pos.		0	40	0.3%	2.9%
6	11GHA50EA100	GROUP CONTROL	Time mon. On		0	26	0.2%	3.1%
7	11HFC21EA100	GROUP CONTROL	Time mon. On		0	17	0.1%	3.2%
8	11GHA30EA100	GROUP CONTROL	Time mon. On		0	15	0.1%	3.3%
9	11GHA40EA100	GROUP CONTROL	Time mon. On		0	15	0.1%	3.4%
10	11GHE31AA020	SLURRY MIX TNK WTR IN VV	Discr., Off/Cl.		0	13	0.1%	3.5%

Top Disturbance Alarms

Rank	KKS Tag	Description	Status	Desc	Prio	Count	%	Cum %
1	90GCF42CF140 XQ50	FLOW RO TRAIN 2 REJECT	Error L		4	69699	48.8%	48.8%
2	90GCF42CF140 XQ50	FLOW RO TRAIN 2 REJECT	Error AV		4	69427	48.6%	97.3%
3	11HFE74AA001	PULV 20 HOT AIR DAMPER	Electr. disturb.		4	212	0.1%	97.5%
4	11HFE84AA001	PULV 20 COLD AIR DAMPER	Electr. disturb.		4	212	0.1%	97.6%
5	90GNK25AA010	SALINE WTP INLET CTRL V	Error AV		4	163	0.1%	97.7%
6	90GNK25AA010	SALINE WTP INLET CTRL V	Error L		4	163	0.1%	97.9%
7	90GNK25CF010 XQ50	FLOW SALINE FD OXIDN TNK	Error AV		4	163	0.1%	98.0%
8	90GNK25CF010 XQ50	FLOW SALINE FD OXIDN TNK	Error L		4	163	0.1%	98.1%
9	11ETK41DS010	SLURRY PUMP 1 SPEED CNTR	Error AV		4	132	0.1%	98.2%
10	11ETK41DS010	SLURRY PUMP 1 SPEED CNTR	Error L		4	132	0.1%	98.3%

Daily Alarm Rate

8/06/2015	3533
9/06/2015	2019
10/06/2015	1545
11/06/2015	1593
12/06/2015	1670
13/06/2015	1651
14/06/2015	1440

Appendix C.5. Monthly Alarm Reports

The following pages show the monthly alarm reports for January 2015 to September 2015

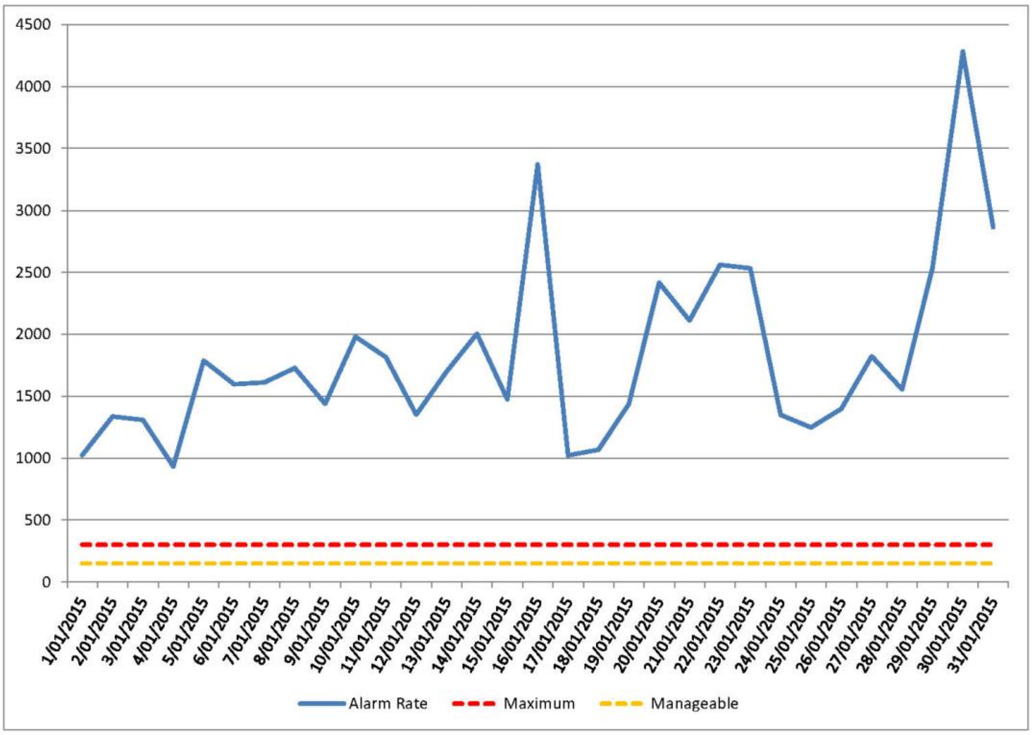
Monthly Alarm Report

January, 2015

Alarm Distribution

Prio	%
Maintenance	9%
1	1%
2	70%
3	20%

Daily Alarm Rate



Top Alarms

Rank	KKS Tag	Description	Status	Desc	Prio	Count	%	Cum %
1	11PGC10CE101 XQ50	3300V CCW PP CURR	Limit H	>HIGH	2	4104	7.2%	7.2%
2	11ETJ00EA800 XU02	VACUUM ECO HOPPERS	State 1 alarm		2	3076	5.4%	12.7%
3	11GNA70CL001 XQ50	L BOILER BLOWDOWN PIT	Limit HH	>MAX	2	2472	4.4%	17.0%
4	11HFH30CL010 XG11	L PYRITE BOX PULV 30	State 1 alarm		2	1918	3.4%	20.4%
5	90SGA40AP010 XG11	FPSTN PRESS MAINT RUN	State 1 alarm		3	1716	3.0%	23.5%
6	90SGA40AP010 XG12	FPSTN PRESS MAINT FLT	State 1 alarm		2	1716	3.0%	26.5%
7	11ETK20CL020 XQ50	L ASH SLURRY TANK	Limit L	<LOW	2	1659	2.9%	29.4%
8	11HFH40CL010 XG11	L PYRITE BOX PULV 40	State 1 alarm		2	1654	2.9%	32.3%
9	90ECJ20CW010 XQ50	WEIGHTOMETER T2C	Limit H	>HIGH	2	1628	2.9%	35.2%
10	11HFH20CL010 XG11	L PYRITE BOX PULV 20	State 1 alarm		2	1621	2.9%	38.1%
11	90GNK35CQ010 XU13	SALINE WTP OUTLET pH	State 1 alarm		3	1549	2.7%	40.8%
12	11HFH10CL010 XG11	L PYRITE BOX PULV 10	State 1 alarm		2	1382	2.4%	43.2%
13	90GNK35CQ010 XQ50	PH SALINE BSTR PP RECIRC	Limit L	<LOW	2	1246	2.2%	45.4%
14	11HCB10EA100 XU02	T SOOTBLOWERS DRAINS	State 1 alarm		2	1089	1.9%	47.4%
15	11GNA00EA111 XU03	L BLR BLWDN PIT (MANUAL)	State 1 alarm		2	1053	1.9%	49.2%
16	90GNN30CL010 XH64	L DEWATER POLYMR MIX TNK	State 1 alarm		3	1046	1.8%	51.1%
17	90GNN30CL010 XQ50	L DEWATER POLYMR MIX TNK	Limit LL	<MIN	3	1046	1.8%	52.9%
18	90GNK35CQ010 XQ50	PH SALINE BSTR PP RECIRC	Limit LL	<MIN	2	905	1.6%	54.5%
19	11QUA10CQ075 XQ50	DOWNCOMER WATER OXYGEN	Limit H	>HIGH	2	873	1.5%	56.1%
20	90GNN30CL010 XH13	L DEWATER POLYMR MIX TNK	State 1 alarm		3	851	1.5%	57.6%

Top Maintenance Alarms

Rank	KKS Tag	Description	Status	Desc	Prio	Count	%	Cum %
1	11HCB00EA100	GROUP CONTROL	Time mon. On		0	451	0.8%	0.8%
2	11HFH40AA010	PYRITE BOX 40 INLET GATE	Time monit.		0	189	0.3%	1.1%
3	90GNQ34AS010	CAUSTIC PP 4 STROKE CNTR	Discr., Prot <-		0	169	0.3%	1.4%
4	11HFH30AA020	PULV 30 REJECT OUTLET VV	Discr. int. pos.		0	136	0.2%	1.7%
5	11GHA40EA100	GROUP CONTROL	Time mon. On		0	130	0.2%	1.9%
6	11HFH30AA020	PULV 30 REJECT OUTLET VV	Discr., Off/Cl.		0	119	0.2%	2.1%
7	11GHE31AA020	SLURRY MIX TNK WTR IN VV	Discr., Off/Cl.		0	103	0.2%	2.3%
8	11LAA10AA212	FEEDWATER TANK VENT VLV	Discr., On/Op.		0	103	0.2%	2.5%
9	11GHE40AA020	ASH PUG MILL INL CTRL V	Discr., Off/Cl.		0	101	0.2%	2.6%
10	90GNR02EA100	GROUP CONTROL	Time mon. On		0	100	0.2%	2.8%

Top Disturbance Alarms

Rank	KKS Tag	Description	Status	Desc	Prio	Count	%	Cum %
1	90GCF42CF140 XQ50	FLOW RO TRAIN 2 REJECT	Error L		4	3626	12.0%	12.0%
2	90GCF42CF140 XQ50	FLOW RO TRAIN 2 REJECT	Error AV		4	3623	12.0%	24.1%
3	90GNK25AA010	SALINE WTP INLET CTRL V	Error AV		4	1881	6.2%	30.3%
4	90GNK25AA010	SALINE WTP INLET CTRL V	Error L		4	1881	6.2%	36.5%
5	90GNK25CF010 XQ50	FLOW SALINE FD OXIDN TNK	Error AV		4	1881	6.2%	42.8%
6	90GNK25CF010 XQ50	FLOW SALINE FD OXIDN TNK	Error L		4	1881	6.2%	49.0%
7	11ETK41DS010	SLURRY PUMP 1 SPEED CNTR	Error AV		4	1269	4.2%	53.2%
8	11ETK41DS010	SLURRY PUMP 1 SPEED CNTR	Error L		4	1269	4.2%	57.4%
9	11ETK42DS010	SLURRY PUMP 2 SPEED CNTR	Error AV		4	1269	4.2%	61.7%
10	11ETK42DS010	SLURRY PUMP 2 SPEED CNTR	Error L		4	1269	4.2%	65.9%

Daily Alarm Rate

1/01/2015	1023
2/01/2015	1336
3/01/2015	1308
4/01/2015	931
5/01/2015	1788
6/01/2015	1596
7/01/2015	1611
8/01/2015	1726
9/01/2015	1439
10/01/2015	1981
11/01/2015	1814
12/01/2015	1351
13/01/2015	1699
14/01/2015	2004
15/01/2015	1473
16/01/2015	3372
17/01/2015	1022
18/01/2015	1067
19/01/2015	1436
20/01/2015	2416
21/01/2015	2111
22/01/2015	2561
23/01/2015	2532
24/01/2015	1348
25/01/2015	1247
26/01/2015	1398
27/01/2015	1822
28/01/2015	1555
29/01/2015	2534
30/01/2015	4282
31/01/2015	2863

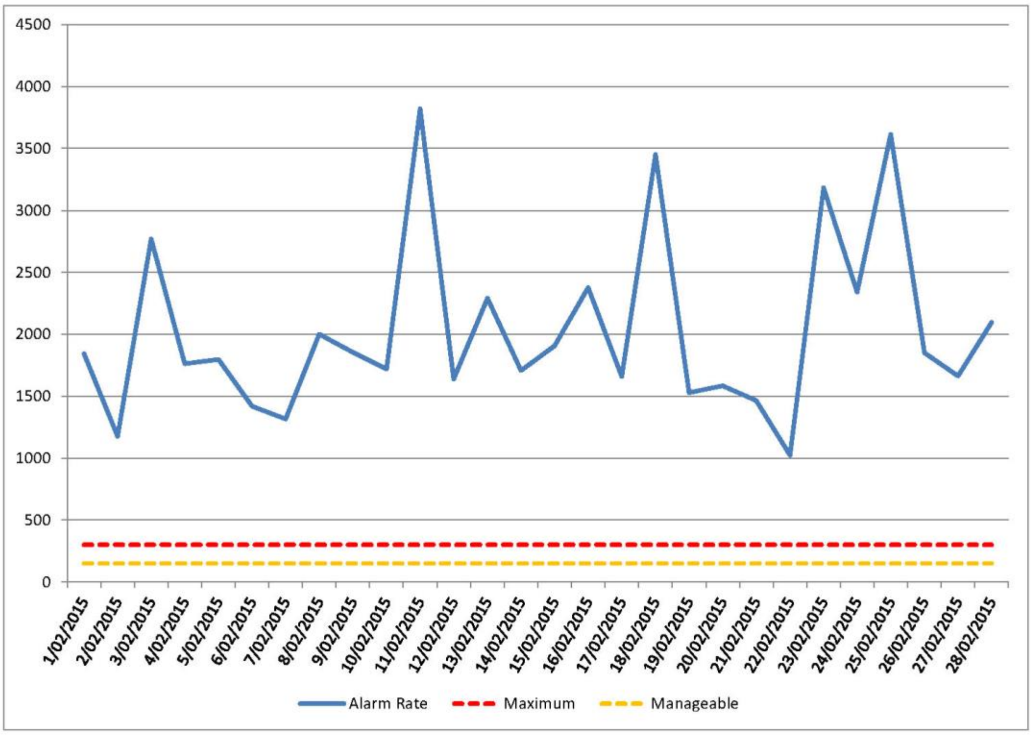
Monthly Alarm Report

February, 2015

Alarm Distribution

Prio	%
Maintenance	10%
1	2%
2	69%
3	19%

Daily Alarm Rate



Top Alarms

Rank	KKS Tag	Description	Status	Desc	Prio	Count	%	Cum %
1	11HDA01CP003 XG11	DP SDCC HYDR OIL FILTER	State 0 alarm		2	4193	7.4%	7.4%
2	11ETJ00EA800 XU02	VACUUM ECO HOPPERS	State 1 alarm		2	2816	5.0%	12.3%
3	11HFH30CL010 XG11	L PYRITE BOX PULV 30	State 1 alarm		2	2418	4.3%	16.6%
4	11PGC20CE101 XQ50	3300V CCW PP CURR	Limit H	>HIGH	2	2253	4.0%	20.5%
5	11HFH40CL010 XG11	L PYRITE BOX PULV 40	State 1 alarm		2	1875	3.3%	23.8%
6	90GNK35CQ010 XU13	SALINE WTP OUTLET pH	State 1 alarm		3	1514	2.7%	26.5%
7	90ECJ20CW010 XQ50	WEIGHTOMETER T2C	Limit H	>HIGH	2	1457	2.6%	29.1%
8	11HFH20CL010 XG11	L PYRITE BOX PULV 20	State 1 alarm		2	1399	2.5%	31.5%
9	90SGA40AP010 XG11	FPSTN PRESS MAINT RUN	State 1 alarm		3	1283	2.3%	33.8%
10	90SGA40AP010 XG12	FPSTN PRESS MAINT FLT	State 1 alarm		2	1283	2.3%	36.0%
11	11HFH10CL010 XG11	L PYRITE BOX PULV 10	State 1 alarm		2	1121	2.0%	38.0%
12	11GNA00EA111 XU03	L BLR BLWDN PIT (MANUAL)	State 1 alarm		2	1114	2.0%	40.0%
13	11HCB10EA100 XU02	T SOOTBLOWERS DRAINS	State 1 alarm		2	1001	1.8%	41.7%
14	90GNN30CL010 XH64	L DEWATER POLYMR MIX TNK	State 1 alarm		3	979	1.7%	43.5%
15	90GNN30CL010 XQ50	L DEWATER POLYMR MIX TNK	Limit LL	<MIN	3	979	1.7%	45.2%
16	90GNK35CQ010 XQ50	PH SALINE BSTR PP RECIRC	Limit L	<LOW	2	938	1.7%	46.8%
17	90GNN30CL010 XH13	L DEWATER POLYMR MIX TNK	State 1 alarm		3	861	1.5%	48.4%
18	90GNN30CL010 XQ50	L DEWATER POLYMR MIX TNK	Limit HH	>MAX	3	861	1.5%	49.9%
19	90GNK35CQ010 XQ50	PH SALINE BSTR PP RECIRC	Limit H	>HIGH	2	836	1.5%	51.3%
20	90GNK35CQ010 XQ50	PH SALINE BSTR PP RECIRC	Limit LL	<MIN	2	828	1.5%	52.8%

Top Maintenance Alarms

Rank	KKS Tag	Description	Status	Desc	Prio	Count	%	Cum %
1	11HCB00EA100	GROUP CONTROL	Time mon. On		0	368	0.6%	0.6%
2	90GNQ31AS010	CAUSTIC PP 1 STROKE CNTR	Discr., Prot <-		0	326	0.6%	1.2%
3	11HFH30AA020	PULV 30 REJECT OUTLET VV	Discr. int. pos.		0	202	0.4%	1.6%
4	11HFH30AA020	PULV 30 REJECT OUTLET VV	Discr., Off/Cl.		0	149	0.3%	1.8%
5	11HJA35AA210	PULSE IGN 35 CYLINDER	Time monit.		0	103	0.2%	2.0%
6	11LAA10AA212	FEEDWATER TANK VENT VLV	Discr., Prot ->		0	91	0.2%	2.2%
7	90GNQ33AS010	CAUSTIC PP 3 STROKE CNTR	Discr., Prot <-		0	90	0.2%	2.3%
8	11LAA10AA212	FEEDWATER TANK VENT VLV	Discr., Off/Cl.		0	85	0.1%	2.5%
9	11ETN70EA100	GROUP CONTROL	Discrep.		0	83	0.1%	2.6%
10	90ETN10EA100	GROUP CONTROL	Time mon. Off		0	82	0.1%	2.8%

Top Disturbance Alarms

Rank	KKS Tag	Description	Status	Desc	Prio	Count	%	Cum %
1	11BRU10CE403 XG11	INVERTER ALT AC SUPPLY	Error		4	2426	9.5%	9.5%
2	90GCF42CF140 XQ50	FLOW RO TRAIN 2 REJECT	Error AV		4	1977	7.8%	17.3%
3	90GCF42CF140 XQ50	FLOW RO TRAIN 2 REJECT	Error L		4	1977	7.8%	25.1%
4	90GNK25AA010	SALINE WTP INLET CTRL V	Error AV		4	1692	6.6%	31.7%
5	90GNK25AA010	SALINE WTP INLET CTRL V	Error L		4	1692	6.6%	38.3%
6	90GNK25CF010 XQ50	FLOW SALINE FD OXIDN TNK	Error AV		4	1692	6.6%	45.0%
7	90GNK25CF010 XQ50	FLOW SALINE FD OXIDN TNK	Error L		4	1692	6.6%	51.6%
8	11ETK41DS010	SLURRY PUMP 1 SPEED CNTR	Error AV		4	628	2.5%	54.1%
9	11ETK41DS010	SLURRY PUMP 1 SPEED CNTR	Error L		4	628	2.5%	56.6%
10	11ETK42DS010	SLURRY PUMP 2 SPEED CNTR	Error AV		4	628	2.5%	59.0%

Daily Alarm Rate

1/02/2015	1842
2/02/2015	1176
3/02/2015	2769
4/02/2015	1762
5/02/2015	1796
6/02/2015	1418
7/02/2015	1315
8/02/2015	2001
9/02/2015	1854
10/02/2015	1719
11/02/2015	3820
12/02/2015	1639
13/02/2015	2290
14/02/2015	1707
15/02/2015	1906
16/02/2015	2376
17/02/2015	1659
18/02/2015	3451
19/02/2015	1529
20/02/2015	1583
21/02/2015	1464
22/02/2015	1023
23/02/2015	3182
24/02/2015	2340
25/02/2015	3614
26/02/2015	1849
27/02/2015	1662
28/02/2015	2095

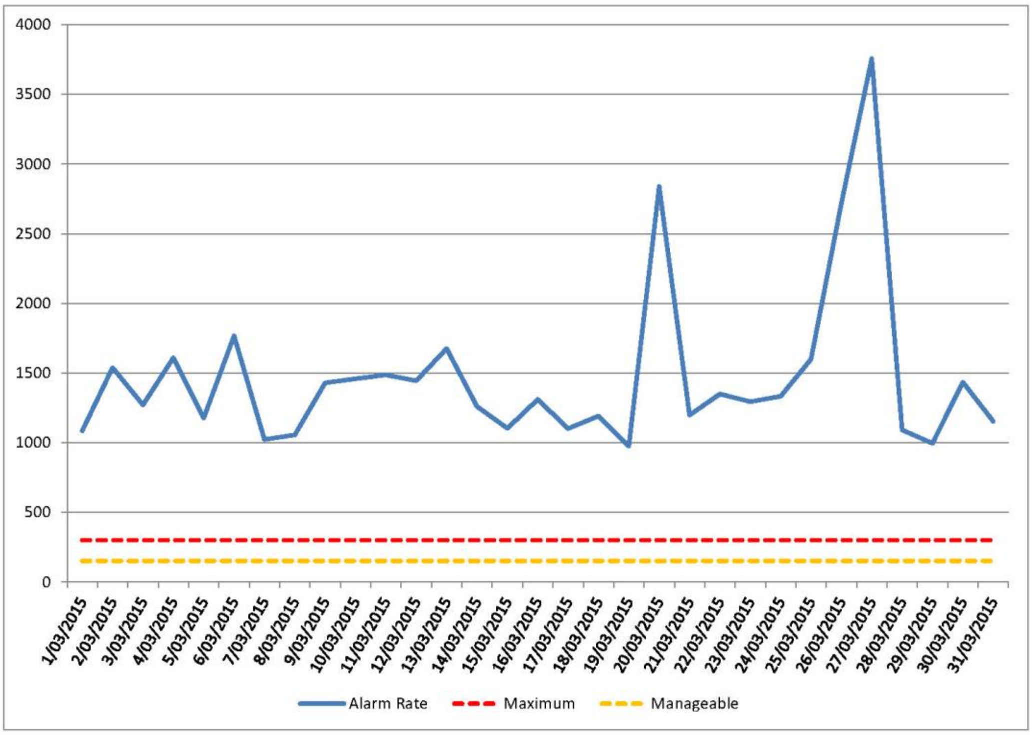
Monthly Alarm Report

March, 2015

Alarm Distribution

Prio	%
Maintenance	14%
1	2%
2	71%
3	13%

Daily Alarm Rate



Top Alarms

Rank	KKS Tag	Description	Status	Desc	Prio	Count	%	Cum %
1	11ETJ00EA800 XU02	VACUUM ECO HOPPERS	State 1 alarm		2	3100	6.8%	6.8%
2	11HFH50CL010 XG11	L PYRITE BOX PULV 50	State 1 alarm		2	2782	6.1%	12.9%
3	11PGC20CE101 XQ50	3300V CCW PP CURR	Limit H	>HIGH	2	2310	5.1%	17.9%
4	11HFH30CL010 XG11	L PYRITE BOX PULV 30	State 1 alarm		2	1997	4.4%	22.3%
5	11HFH20CL010 XG11	L PYRITE BOX PULV 20	State 1 alarm		2	1589	3.5%	25.8%
6	11HFH40CL010 XG11	L PYRITE BOX PULV 40	State 1 alarm		2	1491	3.3%	29.0%
7	11HFC20CG030 XG11	G GRIND ROLLER 2 PULV 20	State 0 alarm		2	1336	2.9%	32.0%
8	90GNK35CQ010 XU13	SALINE WTP OUTLET pH	State 1 alarm		3	1261	2.8%	34.7%
9	11BFF10CE400 XG11	CAS 2 INSULATOR HEATERS	State 1 alarm		2	1171	2.6%	37.3%
10	11HCB10EA100 XU02	T SOOTBLOWERS DRAINS	State 1 alarm		2	1083	2.4%	39.6%
11	90GNK35CQ010 XQ50	PH SALINE BSTR PP RECIRC	Limit L	<LOW	2	1018	2.2%	41.9%
12	90GNK35CQ010 XQ50	PH SALINE BSTR PP RECIRC	Limit LL	<MIN	2	859	1.9%	43.8%
13	90SGA40AP010 XG11	FPSTN PRESS MAINT RUN	State 1 alarm		3	800	1.8%	45.5%
14	90SGA40AP010 XG12	FPSTN PRESS MAINT FLT	State 1 alarm		2	800	1.8%	47.3%
15	11CJA00DU002 XU04	FREQUENCY DEVIATION	State 1 alarm		2	636	1.4%	48.6%
16	90GNK35CQ010 XQ50	PH SALINE BSTR PP RECIRC	Limit H	>HIGH	2	595	1.3%	50.0%
17	11HFC50EA800 XU01	PULVERISER 50 RATIO	State 1 alarm		2	512	1.1%	51.1%
18	11QUA10CQ075 XQ50	DOWNCOMER WATER OXYGEN	Limit H	>HIGH	2	511	1.1%	52.2%
19	11HFC30EA800 XU01	PULVERIZER 30 RATIO	State 1 alarm		2	437	1.0%	53.1%
20	11HCB00EA100	GROUP CONTROL	Time mon. On		0	435	1.0%	54.1%

Top Maintenance Alarms

Rank	KKS Tag	Description	Status	Desc	Prio	Count	%	Cum %
1	11HCB00EA100	GROUP CONTROL	Time mon. On		0	435	1.0%	1.0%
2	90GNQ31AS010	CAUSTIC PP 1 STROKE CNTR	Discr., Prot <-		0	424	0.9%	1.9%
3	90GNQ34AS010	CAUSTIC PP 4 STROKE CNTR	Discr., Prot <-		0	244	0.5%	2.4%
4	11HFH30AA020	PULV 30 REJECT OUTLET VV	Discr. int. pos.		0	218	0.5%	2.9%
5	11HFH30AA020	PULV 30 REJECT OUTLET VV	Discr., Off/Cl.		0	160	0.4%	3.2%
6	11HFH50AA020	PULV 50 REJECT OUTLET VV	Discr. int. pos.		0	145	0.3%	3.6%
7	11HFH50AA020	PULV 50 REJECT OUTLET VV	Discr., Off/Cl.		0	111	0.2%	3.8%
8	11HJA35AA210	PULSE IGN 35 CYLINDER	Time monit.		0	91	0.2%	4.0%
9	11LAA10AA212	FEEDWATER TANK VENT VLV	Discr., Prot ->		0	89	0.2%	4.2%
10	11LAA10AA212	FEEDWATER TANK VENT VLV	Discr., Off/Cl.		0	86	0.2%	4.4%

Top Disturbance Alarms

Rank	KKS Tag	Description	Status	Desc	Prio	Count	%	Cum %
1	11BRU10CE403 XG11	INVERTER ALT AC SUPPLY	Error		4	21021	54.4%	54.4%
2	90GCF42CF140 XQ50	FLOW RO TRAIN 2 REJECT	Error AV		4	3068	7.9%	62.3%
3	90GCF42CF140 XQ50	FLOW RO TRAIN 2 REJECT	Error L		4	3066	7.9%	70.2%
4	11HFC20CG030 XG11	G GRIND ROLLER 2 PULV 20	Error		4	1332	3.4%	73.7%
5	11ETK41DS010	SLURRY PUMP 1 SPEED CNTR	Error AV		4	520	1.3%	75.0%
6	11ETK42DS010	SLURRY PUMP 2 SPEED CNTR	Error AV		4	520	1.3%	76.3%
7	11ETK50CF020 XQ50	F SLURRY PUMPS OUTL	Error AV		4	520	1.3%	77.7%
8	11ETK50DF100	SLURRY DISCHARGE FLOW SP	Error AV		4	520	1.3%	79.0%
9	11ETK41DS010	SLURRY PUMP 1 SPEED CNTR	Error L		4	516	1.3%	80.4%
10	11ETK42DS010	SLURRY PUMP 2 SPEED CNTR	Error L		4	516	1.3%	81.7%

Daily Alarm Rate

1/03/2015	1084
2/03/2015	1538
3/03/2015	1271
4/03/2015	1609
5/03/2015	1175
6/03/2015	1766
7/03/2015	1022
8/03/2015	1055
9/03/2015	1429
10/03/2015	1458
11/03/2015	1486
12/03/2015	1444
13/03/2015	1675
14/03/2015	1259
15/03/2015	1102
16/03/2015	1310
17/03/2015	1100
18/03/2015	1191
19/03/2015	975
20/03/2015	2837
21/03/2015	1197
22/03/2015	1348
23/03/2015	1293
24/03/2015	1332
25/03/2015	1598
26/03/2015	2719
27/03/2015	3757
28/03/2015	1091
29/03/2015	994
30/03/2015	1433
31/03/2015	1153

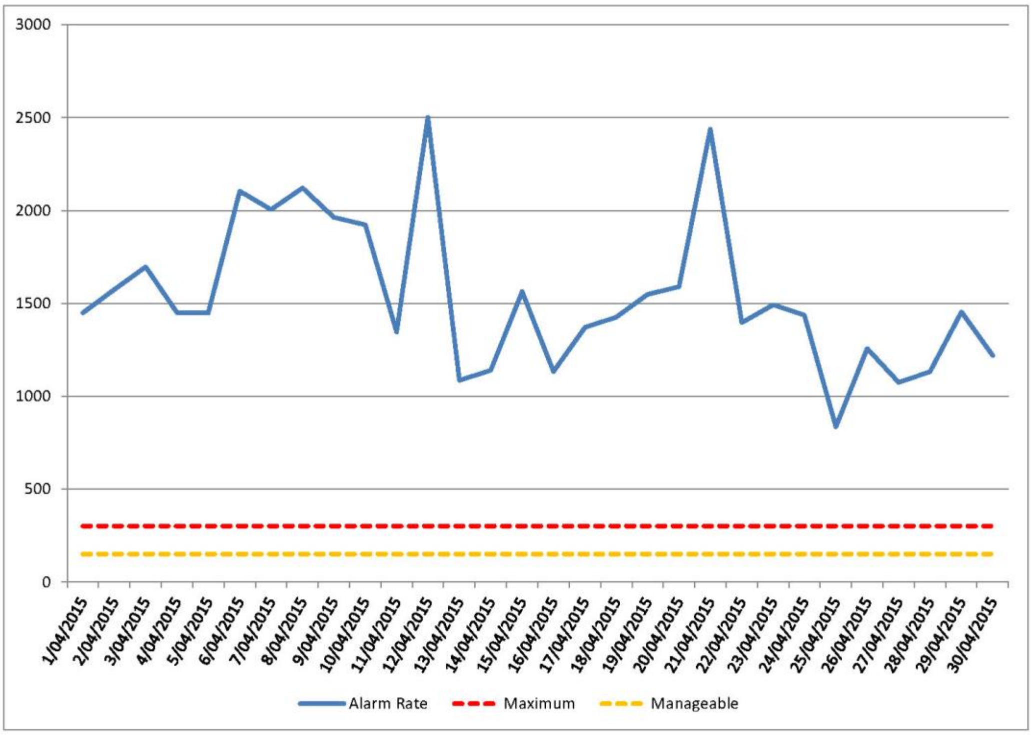
Monthly Alarm Report

April, 2015

Alarm Distribution

Prio	%
Maintenance	13%
1	3%
2	68%
3	16%

Daily Alarm Rate



Top Alarms

Rank	KKS Tag	Description	Status	Desc	Prio	Count	%	Cum %
1	11ETJ00EA800 XU02	VACUUM ECO HOPPERS	State 1 alarm		2	2913	6.3%	6.3%
2	11PGC20CE101 XQ50	3300V CCW PP CURR	Limit H	>HIGH	2	2268	4.9%	11.2%
3	11HFH30CL010 XG11	L PYRITE BOX PULV 30	State 1 alarm		2	2220	4.8%	16.0%
4	11HFH50CL010 XG11	L PYRITE BOX PULV 50	State 1 alarm		2	1849	4.0%	20.0%
5	90GNK35CQ010 XU13	SALINE WTP OUTLET pH	State 1 alarm		3	1484	3.2%	23.3%
6	90GNK35CQ010 XQ50	PH SALINE BSTR PP RECIRC	Limit H	>HIGH	2	1329	2.9%	26.1%
7	90SGA40AP010 XG11	FPSTN PRESS MAINT RUN	State 1 alarm		3	1158	2.5%	28.6%
8	90SGA40AP010 XG12	FPSTN PRESS MAINT FLT	State 1 alarm		2	1158	2.5%	31.1%
9	90GNK35CQ010 XQ50	PH SALINE BSTR PP RECIRC	Limit L	<LOW	2	1151	2.5%	33.6%
10	11HFC50EA800 XU01	PULVERISER 50 RATIO	State 1 alarm		2	1123	2.4%	36.1%
11	11QUA10CQ075 XQ50	DOWNCOMER WATER OXYGEN	Limit H	>HIGH	2	1096	2.4%	38.4%
12	90EAF20CP010 XG11	CHARGE PRESS R1 FEEDER	State 0 alarm		3	890	1.9%	40.4%
13	11CJA00DU002 XU04	FREQUENCY DEVIATION	State 1 alarm		2	883	1.9%	42.3%
14	90GNK35CQ010 XQ50	PH SALINE BSTR PP RECIRC	Limit LL	<MIN	2	841	1.8%	44.1%
15	11HCB10EA100 XU02	T SOOTBLOWERS DRAINS	State 1 alarm		2	810	1.8%	45.9%
16	11HFH40CL010 XG11	L PYRITE BOX PULV 40	State 1 alarm		2	755	1.6%	47.5%
17	11HFH10CL010 XG11	L PYRITE BOX PULV 10	State 1 alarm		2	736	1.6%	49.1%
18	11HFH20CL010 XG11	L PYRITE BOX PULV 20	State 1 alarm		2	733	1.6%	50.7%
19	90GNK35CQ010 XQ50	PH SALINE BSTR PP RECIRC	Limit HH	>MAX	2	658	1.4%	52.1%
20	11HFC30EA800 XU01	PULVERIZER 30 RATIO	State 1 alarm		2	507	1.1%	53.2%

Top Maintenance Alarms

Rank	KKS Tag	Description	Status	Desc	Prio	Count	%	Cum %
1	11HCB00EA100	GROUP CONTROL	Time mon. On		0	348	0.8%	0.8%
2	90GNQ31AS010	CAUSTIC PP 1 STROKE CNTR	Discr., Prot <-		0	298	0.6%	1.4%
3	11ETG80AF020	ESP DUST BUCKET ELEVATOR	Discr., Off/Cl.		0	174	0.4%	1.8%
4	11LAA10AA212	FEEDWATER TANK VENT VLV	Discr., Prot ->		0	173	0.4%	2.2%
5	11LAA10AA212	FEEDWATER TANK VENT VLV	Discr., Off/Cl.		0	167	0.4%	2.5%
6	11ETG80AF010	ESP DUST COLL CONVEYOR	Discr., Prot <-		0	161	0.3%	2.9%
7	11ETG80AF010	ESP DUST COLL CONVEYOR	Discr., Off/Cl.		0	160	0.3%	3.2%
8	11ETG10AF010	ESP DUST CONVEYOR 1	Discr., Off/Cl.		0	158	0.3%	3.6%
9	11ETG40AF010	ESP DUST CONVEYOR 4	Discr., Off/Cl.		0	158	0.3%	3.9%
10	11ETG30AF010	ESP DUST CONVEYOR 3	Discr., Off/Cl.		0	157	0.3%	4.2%

Top Disturbance Alarms

Rank	KKS Tag	Description	Status	Desc	Prio	Count	%	Cum %
1	90GCF42CF140 XQ50	FLOW RO TRAIN 2 REJECT	Error L		4	8347	15.2%	15.2%
2	90GCF42CF140 XQ50	FLOW RO TRAIN 2 REJECT	Error AV		4	8328	15.1%	30.3%
3	90GNK25AA010	SALINE WTP INLET CTRL V	Error L		4	6115	11.1%	41.4%
4	90GNK25CF010 XQ50	FLOW SALINE FD OXIDN TNK	Error L		4	6115	11.1%	52.5%
5	90GNK25AA010	SALINE WTP INLET CTRL V	Error AV		4	6111	11.1%	63.6%
6	90GNK25CF010 XQ50	FLOW SALINE FD OXIDN TNK	Error AV		4	6111	11.1%	74.7%
7	11BRU10CE403 XG11	INVERTER ALT AC SUPPLY	Error		4	2425	4.4%	79.1%
8	11PAH15CP007 XG11	CONDR A-SIDE OLCS DP	Error		4	1469	2.7%	81.7%
9	11HNA30CT019 XQ50	T GAS AIR HEATER OUTLET	Error AV		4	1133	2.1%	83.8%
10	11HLD01CT902 XJ51	T AH SECOND COLD END AV	Error L		4	733	1.3%	85.1%

Daily Alarm Rate

1/04/2015	1449
2/04/2015	1573
3/04/2015	1696
4/04/2015	1450
5/04/2015	1449
6/04/2015	2104
7/04/2015	2005
8/04/2015	2121
9/04/2015	1963
10/04/2015	1923
11/04/2015	1346
12/04/2015	2502
13/04/2015	1085
14/04/2015	1139
15/04/2015	1563
16/04/2015	1133
17/04/2015	1370
18/04/2015	1425
19/04/2015	1548
20/04/2015	1590
21/04/2015	2438
22/04/2015	1396
23/04/2015	1491
24/04/2015	1436
25/04/2015	835
26/04/2015	1256
27/04/2015	1074
28/04/2015	1132
29/04/2015	1453
30/04/2015	1218

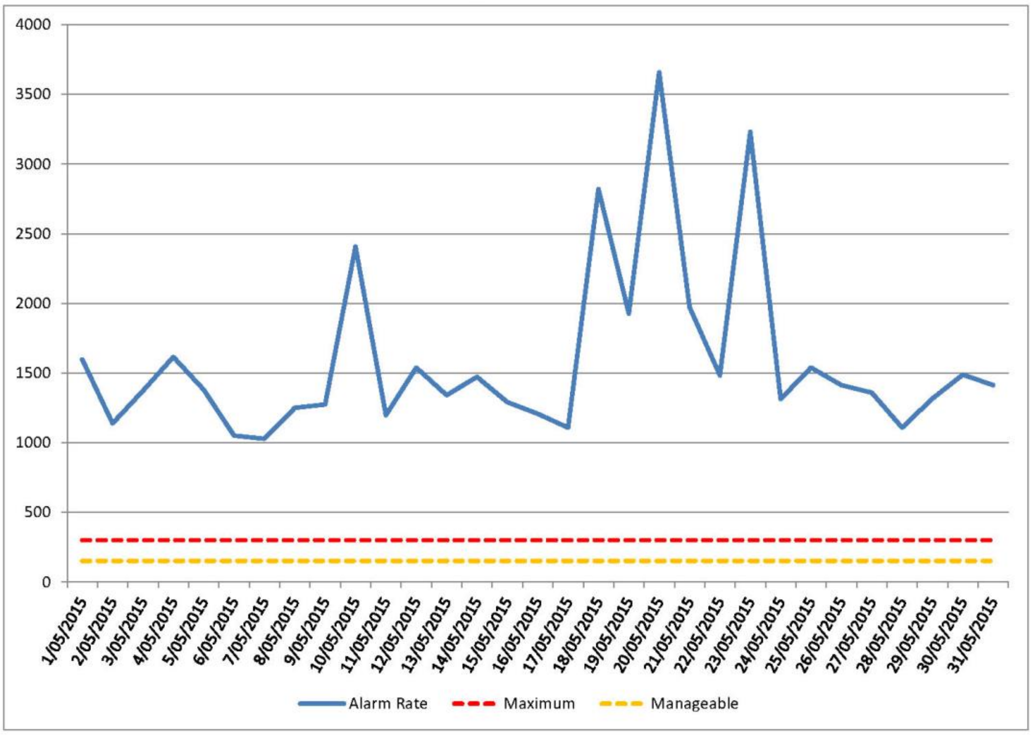
Monthly Alarm Report

May, 2015

Alarm Distribution

Prio	%
Maintenance	16%
1	2%
2	69%
3	13%

Daily Alarm Rate



Top Alarms

Rank	KKS Tag	Description	Status	Desc	Prio	Count	%	Cum %
1	11ETJ00EA800 XU02	VACUUM ECO HOPPERS	State 1 alarm		2	3020	6.1%	6.1%
2	11HFH30CL010 XG11	L PYRITE BOX PULV 30	State 1 alarm		2	2952	6.0%	12.1%
3	11HFH50CL010 XG11	L PYRITE BOX PULV 50	State 1 alarm		2	2131	4.3%	16.4%
4	11HFH10CL010 XG11	L PYRITE BOX PULV 10	State 1 alarm		2	1793	3.6%	20.1%
5	11HFH40CL010 XG11	L PYRITE BOX PULV 40	State 1 alarm		2	1579	3.2%	23.3%
6	90GNK35CQ010 XU13	SALINE WTP OUTLET pH	State 1 alarm		3	1078	2.2%	25.5%
7	11CJA00DU002 XU04	FREQUENCY DEVIATION	State 1 alarm		2	1009	2.0%	27.5%
8	90GNK35CQ010 XQ50	PH SALINE BSTR PP RECIRC	Limit H	>HIGH	2	988	2.0%	29.5%
9	11QUC30CQ902 XJ51	COND BFR DEA PH FNCT GEN	Limit H	>HIGH	2	916	1.9%	31.4%
10	11HFW31CP010 XG11	P SEALG AIR COAL FEED 30	State 1 alarm		2	860	1.7%	33.1%
11	90GNK35CQ010 XQ50	PH SALINE BSTR PP RECIRC	Limit L	<LOW	2	777	1.6%	34.7%
12	11HCB10EA100 XU02	T SOOTBLOWERS DRAINS	State 1 alarm		2	677	1.4%	36.1%
13	90GNK35CQ010 XQ50	PH SALINE BSTR PP RECIRC	Limit LL	<MIN	2	626	1.3%	37.3%
14	11QUA10CQ075 XQ50	DOWNCOMER WATER OXYGEN	Limit H	>HIGH	2	579	1.2%	38.5%
15	11HFC30EA800 XU01	PULVERIZER 30 RATIO	State 1 alarm		2	548	1.1%	39.6%
16	90ECJ20CW010 XQ50	WEIGHTOMETER T2C	Limit H	>HIGH	2	533	1.1%	40.7%
17	11QCB10CF010 XQ50	F CAUSTIC DOSING PUMPS	Limit L	<MIN	3	524	1.1%	41.8%
18	11HFC50EA800 XU01	PULVERISER 50 RATIO	State 1 alarm		2	501	1.0%	42.8%
19	90GNK35CQ010 XQ50	PH SALINE BSTR PP RECIRC	Limit HH	>MAX	2	493	1.0%	43.8%
20	90GND10CQ010 XU13	pH OXIDATION TANK	State 1 alarm		3	465	0.9%	44.7%

Top Maintenance Alarms

Rank	KKS Tag	Description	Status	Desc	Prio	Count	%	Cum %
1	90GNQ31AS010	CAUSTIC PP 1 STROKE CNTR	Discr., Prot <-		0	464	0.9%	0.9%
2	11LBG30AA010	AUX ST COLD RH PRESS CV	Discr., Off/Cl.		0	422	0.9%	1.8%
3	11HCB00EA100	GROUP CONTROL	Time mon. On		0	399	0.8%	2.6%
4	11LBG30AA010	AUX ST COLD RH PRESS CV	Discr. int. pos.		0	376	0.8%	3.4%
5	11LBG30AA010	AUX ST COLD RH PRESS CV	Discr., On/Op.		0	293	0.6%	4.0%
6	90EAC10AA110	CNVR T1A OUTL FLAP GATE	Discr. int. pos.		0	224	0.5%	4.4%
7	11HFH40AA010	PYRITE BOX 40 INLET GATE	Time monit.		0	150	0.3%	4.7%
8	11HFH50AA020	PULV 50 REJECT OUTLET VV	Discr. int. pos.		0	149	0.3%	5.0%
9	11LAA10AA212	FEEDWATER TANK VENT VLV	Discr., Prot ->		0	144	0.3%	5.3%
10	11HFH50AA020	PULV 50 REJECT OUTLET VV	Discr., Off/Cl.		0	140	0.3%	5.6%

Top Disturbance Alarms

Rank	KKS Tag	Description	Status	Desc	Prio	Count	%	Cum %
1	90GCF42CF140 XQ50	FLOW RO TRAIN 2 REJECT	Error L		4	76302	39.0%	39.0%
2	90GCF42CF140 XQ50	FLOW RO TRAIN 2 REJECT	Error AV		4	75962	38.8%	77.8%
3	11LBG30AA010	AUX ST COLD RH PRESS CV	Electr. disturb.		4	10576	5.4%	83.2%
4	11LBG50AA020	FEEDWATER TANK PRESS CV	Electr. disturb.		4	10576	5.4%	88.6%
5	11BRU10CE403 XG11	INVERTER ALT AC SUPPLY	Error		4	2667	1.4%	90.0%
6	11HLD01CT902 XJ51	T AH SECOND COLD END AV	Error L		4	2021	1.0%	91.0%
7	90GNK25AA010	SALINE WTP INLET CTRL V	Error AV		4	1259	0.6%	91.6%
8	90GNK25AA010	SALINE WTP INLET CTRL V	Error L		4	1259	0.6%	92.3%
9	90GNK25CF010 XQ50	FLOW SALINE FD OXIDN TNK	Error AV		4	1259	0.6%	92.9%
10	90GNK25CF010 XQ50	FLOW SALINE FD OXIDN TNK	Error L		4	1259	0.6%	93.6%

Daily Alarm Rate

1/05/2015	1597
2/05/2015	1139
3/05/2015	1371
4/05/2015	1615
5/05/2015	1380
6/05/2015	1050
7/05/2015	1027
8/05/2015	1250
9/05/2015	1274
10/05/2015	2407
11/05/2015	1197
12/05/2015	1538
13/05/2015	1340
14/05/2015	1472
15/05/2015	1290
16/05/2015	1207
17/05/2015	1107
18/05/2015	2820
19/05/2015	1927
20/05/2015	3658
21/05/2015	1973
22/05/2015	1483
23/05/2015	3231
24/05/2015	1313
25/05/2015	1538
26/05/2015	1413
27/05/2015	1359
28/05/2015	1108
29/05/2015	1316
30/05/2015	1488
31/05/2015	1413

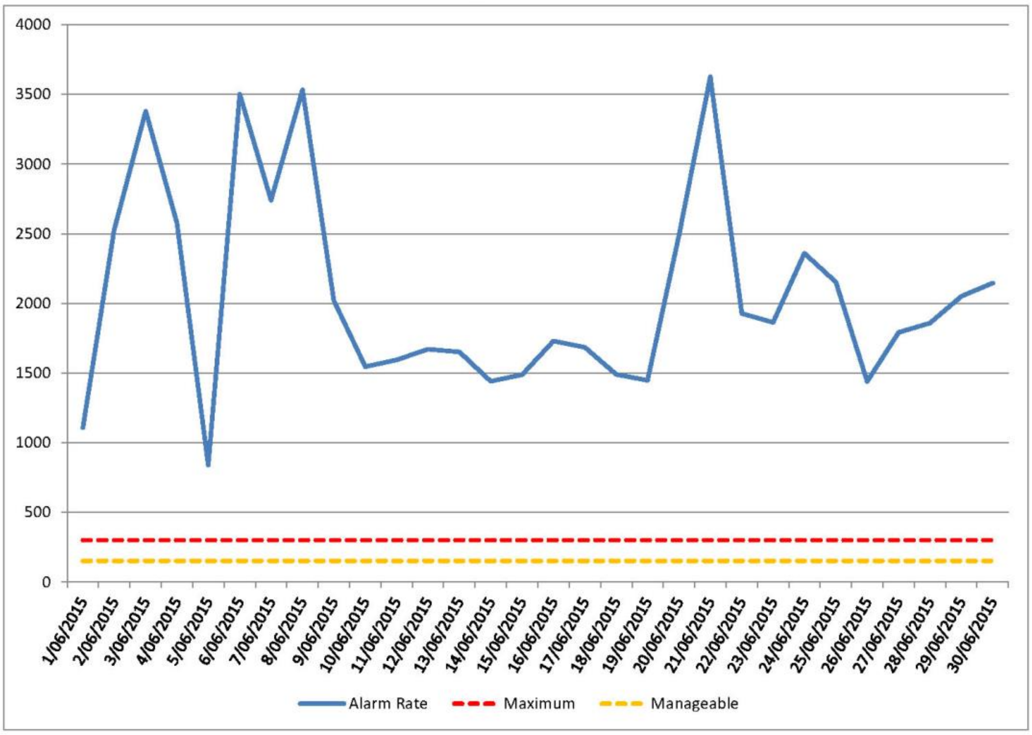
Monthly Alarm Report

June, 2015

Alarm Distribution

Prio	%
Maintenance	13%
1	7%
2	63%
3	17%

Daily Alarm Rate



Top Alarms

Rank	KKS Tag	Description	Status	Desc	Prio	Count	%	Cum %
1	11QEA30CM010 XQ50	DEW POINT DRYER 3 OUTLET	Limit H	>HIGH	2	2882	4.7%	4.7%
2	11ETJ00EA800 XU02	VACUUM ECO HOPPERS	State 1 alarm		2	2616	4.2%	8.9%
3	11HFH50CL010 XG11	L PYRITE BOX PULV 50	State 1 alarm		2	2515	4.1%	13.0%
4	11HFH30CL010 XG11	L PYRITE BOX PULV 30	State 1 alarm		2	2157	3.5%	16.5%
5	11HFW31CP010 XG11	P SEALG AIR COAL FEED 30	State 1 alarm		2	2027	3.3%	19.8%
6	11HYA00EY801 XU12	T GAS AH OUTLET DIFF	State 1 alarm		1	1496	2.4%	22.2%
7	11LAD60CL902 XJ51	HP6 CTRL LEVEL TX (2oo3)	Limit L	<LOW	2	1368	2.2%	24.4%
8	11LAD60CL902 XU63	HP6 CTRL LEVEL TX (2oo3)	State 1 alarm		3	1367	2.2%	26.6%
9	11HFH40CL010 XG11	L PYRITE BOX PULV 40	State 1 alarm		2	1307	2.1%	28.8%
10	90GBQ10CG010 XG11	LIME DOSING TANK COVER	State 0 alarm		2	1255	2.0%	30.8%
11	90GNK35CQ010 XU13	SALINE WTP OUTLET pH	State 1 alarm		3	1238	2.0%	32.8%
12	90ETM10EA800 XU02	ASH DAM MODBUS COMMS	State 1 alarm		2	1232	2.0%	34.8%
13	11PGC20CE101 XQ50	3300V CCW PP CURR	Limit H	>HIGH	2	1141	1.9%	36.7%
14	90ETM12AP010 XG13	UNDER DRAIN SUMP PUMP	State 1 alarm		3	1122	1.8%	38.5%
15	90GNK35CQ010 XQ50	PH SALINE BSTR PP RECIRC	Limit H	>HIGH	2	1118	1.8%	40.3%
16	11QEA30CM010 XQ50	DEW POINT DRYER 3 OUTLET	Limit HH	>MAX	1	1102	1.8%	42.1%
17	11HAD01DP100 XU01	F FEEDWATER DEVIATION	State 1 alarm		2	1068	1.7%	43.8%
18	90ETM13AP010 XG13	CENTRAL DECANT SUMP PUMP	State 1 alarm		3	1055	1.7%	45.5%
19	11CJA00DU002 XU04	FREQUENCY DEVIATION	State 1 alarm		2	1035	1.7%	47.2%
20	11HFH20CL010 XG11	L PYRITE BOX PULV 20	State 1 alarm		2	997	1.6%	48.8%

Top Maintenance Alarms

Rank	KKS Tag	Description	Status	Desc	Prio	Count	%	Cum %
1	90ETM13AP010	CENTRAL DECANT SUMP PUMP	Discr., Off/Cl.		0	952	1.5%	1.5%
2	90ETM13AP010	CENTRAL DECANT SUMP PUMP	Discr., On/Op.		0	772	1.3%	2.8%
3	90ETM12AP010	UNDER DRAIN SUMP PUMP	Discr., Off/Cl.		0	629	1.0%	3.8%
4	90GNQ31AS010	CAUSTIC PP 1 STROKE CNTR	Discr., Prot <-		0	597	1.0%	4.8%
5	90ETM12AP010	UNDER DRAIN SUMP PUMP	Discr., On/Op.		0	582	0.9%	5.7%
6	11HCB00EA100	GROUP CONTROL	Time mon. On		0	383	0.6%	6.4%
7	90GNQ33AS010	CAUSTIC PP 3 STROKE CNTR	Discr., Prot <-		0	102	0.2%	6.5%
8	11GHA30EA100	GROUP CONTROL	Time mon. On		0	99	0.2%	6.7%
9	11GHA50EA100	GROUP CONTROL	Time mon. On		0	93	0.2%	6.8%
10	11HFE84AA001	PULV 20 COLD AIR DAMPER	Discr. int. pos.		0	86	0.1%	7.0%

Top Disturbance Alarms

Rank	KKS Tag	Description	Status	Desc	Prio	Count	%	Cum %
1	90GCF42CF140 XQ50	FLOW RO TRAIN 2 REJECT	Error L		4	323264	48.2%	48.2%
2	90GCF42CF140 XQ50	FLOW RO TRAIN 2 REJECT	Error AV		4	322180	48.0%	96.2%
3	11HLD01CT902 XJ51	T AH SECOND COLD END AV	Error L		4	4671	0.7%	96.9%
4	11LAD60CL902 XJ51	HP6 CTRL LEVEL TX (2oo3)	Error H		4	1367	0.2%	97.1%
5	11LAD60CL902 XJ51	HP6 CTRL LEVEL TX (2oo3)	Error HH		4	1367	0.2%	97.3%
6	11LAD60CL902 XJ51	HP6 CTRL LEVEL TX (2oo3)	Error L		4	1367	0.2%	97.5%
7	90GNK25AA010	SALINE WTP INLET CTRL V	Error AV		4	1052	0.2%	97.7%
8	90GNK25AA010	SALINE WTP INLET CTRL V	Error L		4	1052	0.2%	97.8%
9	90GNK25CF010 XQ50	FLOW SALINE FD OXIDN TNK	Error AV		4	1052	0.2%	98.0%
10	90GNK25CF010 XQ50	FLOW SALINE FD OXIDN TNK	Error L		4	1052	0.2%	98.1%

Daily Alarm Rate

1/06/2015	1107
2/06/2015	2528
3/06/2015	3380
4/06/2015	2576
5/06/2015	838
6/06/2015	3501
7/06/2015	2740
8/06/2015	3533
9/06/2015	2019
10/06/2015	1545
11/06/2015	1593
12/06/2015	1670
13/06/2015	1651
14/06/2015	1440
15/06/2015	1487
16/06/2015	1729
17/06/2015	1683
18/06/2015	1489
19/06/2015	1447
20/06/2015	2489
21/06/2015	3625
22/06/2015	1926
23/06/2015	1863
24/06/2015	2359
25/06/2015	2152
26/06/2015	1438
27/06/2015	1791
28/06/2015	1858
29/06/2015	2050
30/06/2015	2146

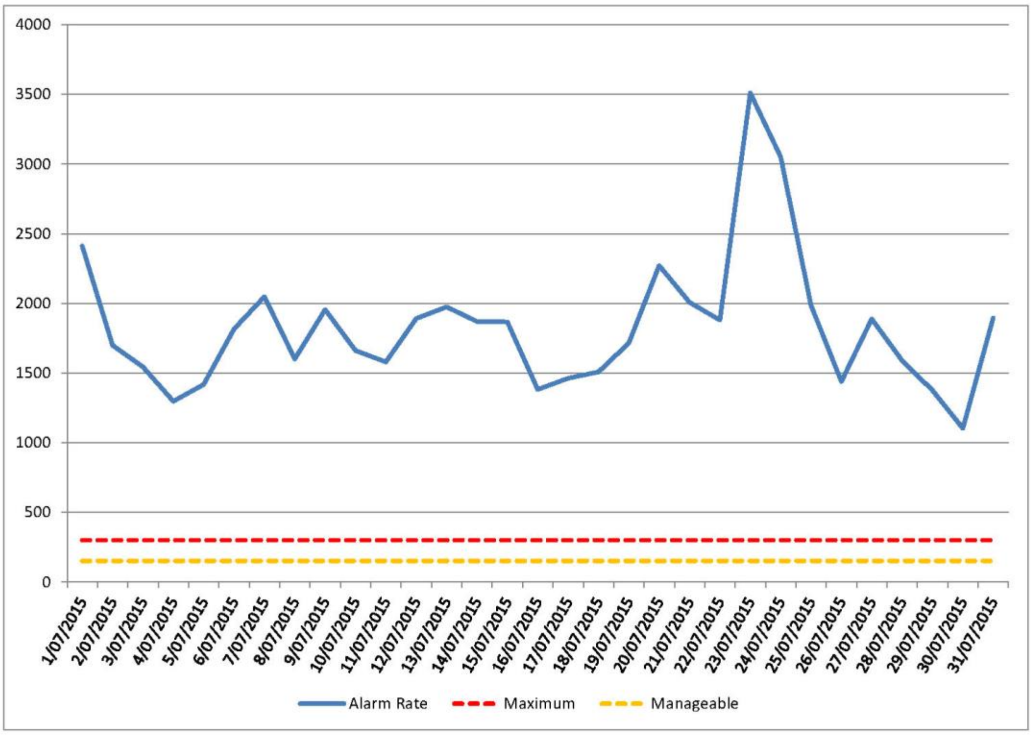
Monthly Alarm Report

July, 2015

Alarm Distribution

Prio	%
Maintenance	19%
1	7%
2	58%
3	16%

Daily Alarm Rate



Top Alarms

Rank	KKS Tag	Description	Status	Desc	Prio	Count	%	Cum %
1	11HFH50CL010 XG11	L PYRITE BOX PULV 50	State 1 alarm		2	3817	6.7%	6.7%
2	90EAF10EA123 XU02	RCLMR CHAIN TENSION DEVI	State 1 alarm		2	3201	5.6%	12.4%
3	11HFH40CL010 XG11	L PYRITE BOX PULV 40	State 1 alarm		2	2946	5.2%	17.6%
4	11ETJ00EA800 XU02	VACUUM ECO HOPPERS	State 1 alarm		2	2923	5.2%	22.7%
5	11HYA00EY801 XU12	T GAS AH OUTLET DIFF	State 1 alarm		1	2484	4.4%	27.1%
6	11HFH30CL010 XG11	L PYRITE BOX PULV 30	State 1 alarm		2	1988	3.5%	30.6%
7	11HFH20CL010 XG11	L PYRITE BOX PULV 20	State 1 alarm		2	1822	3.2%	33.8%
8	11QEA30CM010 XQ50	DEW POINT DRYER 3 OUTLET	Limit H	>HIGH	2	1728	3.0%	36.9%
9	90GND10CQ010 XU13	pH OXIDATION TANK	State 1 alarm		3	1342	2.4%	39.3%
10	90ETM12AP010	UNDER DRAIN SUMP PUMP	Discr., Off/Cl.		0	1265	2.2%	41.5%
11	11ETK40AE010	DISCHARGE VLVS HYD PACK	Discr., Off/Cl.		0	1259	2.2%	43.7%
12	11ETK40AE010 XU03	SLURRY PP DISCH VLV HYD	State 1 alarm		3	1252	2.2%	45.9%
13	90ETM12AP010	UNDER DRAIN SUMP PUMP	Discr., On/Op.		0	1251	2.2%	48.1%
14	11CJA00DU002 XU04	FREQUENCY DEVIATION	State 1 alarm		2	956	1.7%	49.8%
15	90ETM13AP010	CENTRAL DECANT SUMP PUMP	Discr., Off/Cl.		0	898	1.6%	51.4%
16	11HCB10EA100 XU02	T SOOTBLOWERS DRAINS	State 1 alarm		2	894	1.6%	53.0%
17	90ETM13AP010	CENTRAL DECANT SUMP PUMP	Discr., On/Op.		0	860	1.5%	54.5%
18	90ECJ20CW010 XQ50	WEIGHTOMETER T2C	Limit H	>HIGH	2	819	1.4%	55.9%
19	11QEA30CM010 XQ50	DEW POINT DRYER 3 OUTLET	Limit HH	>MAX	1	785	1.4%	57.3%
20	11HFC30EA800 XU01	PULVERIZER 30 RATIO	State 1 alarm		2	763	1.3%	58.7%

Top Maintenance Alarms

Rank	KKS Tag	Description	Status	Desc	Prio	Count	%	Cum %
1	90ETM12AP010	UNDER DRAIN SUMP PUMP	Discr., Off/Cl.		0	1265	2.2%	2.2%
2	11ETK40AE010	DISCHARGE VLVS HYD PACK	Discr., Off/Cl.		0	1259	2.2%	4.5%
3	90ETM12AP010	UNDER DRAIN SUMP PUMP	Discr., On/Op.		0	1251	2.2%	6.7%
4	90ETM13AP010	CENTRAL DECANT SUMP PUMP	Discr., Off/Cl.		0	898	1.6%	8.2%
5	90ETM13AP010	CENTRAL DECANT SUMP PUMP	Discr., On/Op.		0	860	1.5%	9.8%
6	90GNQ31AS010	CAUSTIC PP 1 STROKE CNTR	Discr., Prot <-		0	709	1.3%	11.0%
7	11HCB00EA100	GROUP CONTROL	Time mon. On		0	415	0.7%	11.7%
8	90GNQ33AS010	CAUSTIC PP 3 STROKE CNTR	Discr., Prot <-		0	316	0.6%	12.3%
9	90EAC10AA110	CNVR T1A OUTL FLAP GATE	Discr. int. pos.		0	227	0.4%	12.7%
10	90GCN20AA110	DILUTION WATER VALVE	Discr. int. pos.		0	106	0.2%	12.9%

Top Disturbance Alarms

Rank	KKS Tag	Description	Status	Desc	Prio	Count	%	Cum %
1	90GCF42CF140 XQ50	FLOW RO TRAIN 2 REJECT	Error L		4	302161	41.2%	41.2%
2	90GCF42CF140 XQ50	FLOW RO TRAIN 2 REJECT	Error AV		4	300725	41.0%	82.2%
3	11BRU10CE403 XG11	INVERTER ALT AC SUPPLY	Error		4	47752	6.5%	88.7%
4	11HNA30CT023 XQ50	T GAS AIR HEATER OUTLET	Error AV		4	40148	5.5%	94.2%
5	11HLD01CT901 XJ51	T AH PRIMARY COLD END AV	Error L		4	33479	4.6%	98.7%
6	90GNK25AA010	SALINE WTP INLET CTRL V	Error AV		4	443	0.1%	98.8%
7	90GNK25AA010	SALINE WTP INLET CTRL V	Error L		4	443	0.1%	98.9%
8	90GNK25CF010 XQ50	FLOW SALINE FD OXIDN TNK	Error AV		4	443	0.1%	98.9%
9	90GNK25CF010 XQ50	FLOW SALINE FD OXIDN TNK	Error L		4	443	0.1%	99.0%
10	11ETK42CG010 XG11	OUTL VLV 2 OPEN LIMIT 1	Error		4	240	0.0%	99.0%

Daily Alarm Rate

1/07/2015	2412
2/07/2015	1698
3/07/2015	1543
4/07/2015	1297
5/07/2015	1418
6/07/2015	1816
7/07/2015	2047
8/07/2015	1600
9/07/2015	1954
10/07/2015	1660
11/07/2015	1579
12/07/2015	1891
13/07/2015	1974
14/07/2015	1870
15/07/2015	1866
16/07/2015	1382
17/07/2015	1461
18/07/2015	1507
19/07/2015	1715
20/07/2015	2271
21/07/2015	2007
22/07/2015	1879
23/07/2015	3510
24/07/2015	3052
25/07/2015	1985
26/07/2015	1439
27/07/2015	1887
28/07/2015	1588
29/07/2015	1375
30/07/2015	1102
31/07/2015	1895

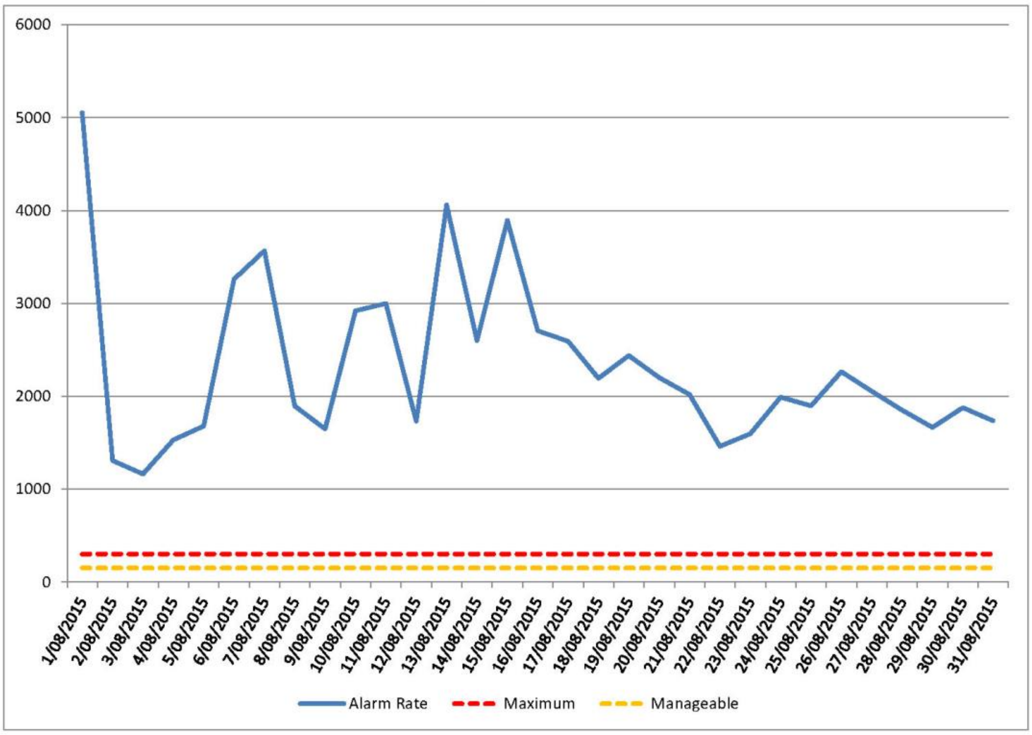
Monthly Alarm Report

August, 2015

Alarm Distribution

Prio	%
Maintenance	22%
1	4%
2	61%
3	13%

Daily Alarm Rate



Top Alarms

Rank	KKS Tag	Description	Status	Desc	Prio	Count	%	Cum %
1	11PGC20CE101 XQ50	3300V CCW PP CURR	Limit H	>HIGH	2	9622	13.4%	13.4%
2	90GCF31CF010 XU62	FLOW RO TRAIN 1 FEED PMP	State 1 alarm		2	4933	6.9%	20.3%
3	90ETM12AP010	UNDER DRAIN SUMP PUMP	Discr., Off/Cl.		0	2048	2.9%	23.1%
4	90ETM13AP010	CENTRAL DECANT SUMP PUMP	Discr., Off/Cl.		0	2041	2.8%	26.0%
5	90ETM12AP010	UNDER DRAIN SUMP PUMP	Discr., On/Op.		0	2036	2.8%	28.8%
6	90ETM13AP010	CENTRAL DECANT SUMP PUMP	Discr., On/Op.		0	2024	2.8%	31.6%
7	90GND10CQ010 XU13	pH OXIDATION TANK	State 1 alarm		3	2001	2.8%	34.4%
8	11HFH50CL010 XG11	L PYRITE BOX PULV 50	State 1 alarm		2	1965	2.7%	37.1%
9	11ETJ00EA800 XU02	VACUUM ECO HOPPERS	State 1 alarm		2	1856	2.6%	39.7%
10	11HFH30CL010 XG11	L PYRITE BOX PULV 30	State 1 alarm		2	1518	2.1%	41.8%
11	11HFH20CL010 XG11	L PYRITE BOX PULV 20	State 1 alarm		2	1135	1.6%	43.4%
12	11QEA10CM010 XQ50	DRYER 1 OUTLET DEW POINT	Limit HH	>MAX	1	1108	1.5%	45.0%
13	11HFW31CP010 XG11	P SEALG AIR COAL FEED 30	State 1 alarm		2	1070	1.5%	46.4%
14	11CJA00DU002 XU04	FREQUENCY DEVIATION	State 1 alarm		2	1005	1.4%	47.8%
15	90GNQ31AS010	CAUSTIC PP 1 STROKE CNTR	Discr., Prot <-		0	926	1.3%	49.1%
16	11HFH40CL010 XG11	L PYRITE BOX PULV 40	State 1 alarm		2	893	1.2%	50.4%
17	11HYA00EY801 XU19	P WTR BLR DRM DIFF	State 1 alarm		2	889	1.2%	51.6%
18	11QEA10CM010 XQ50	DRYER 1 OUTLET DEW POINT	Limit H	>HIGH	2	827	1.2%	52.8%
19	11QUA10CQ075 XQ50	DOWNCOMER WATER OXYGEN	Limit H	>HIGH	2	790	1.1%	53.9%
20	11QEA20CM010 XQ50	DEW POINT DRYER 2 OUTLET	Limit H	>HIGH	2	676	0.9%	54.8%

Top Maintenance Alarms

Rank	KKS Tag	Description	Status	Desc	Prio	Count	%	Cum %
1	90ETM12AP010	UNDER DRAIN SUMP PUMP	Discr., Off/Cl.		0	2048	2.9%	2.9%
2	90ETM13AP010	CENTRAL DECANT SUMP PUMP	Discr., Off/Cl.		0	2041	2.8%	5.7%
3	90ETM12AP010	UNDER DRAIN SUMP PUMP	Discr., On/Op.		0	2036	2.8%	8.5%
4	90ETM13AP010	CENTRAL DECANT SUMP PUMP	Discr., On/Op.		0	2024	2.8%	11.3%
5	90GNQ31AS010	CAUSTIC PP 1 STROKE CNTR	Discr., Prot <-		0	926	1.3%	12.6%
6	90EAC10AA110	CNVR T1A OUTL FLAP GATE	Discr., On/Op.		0	386	0.5%	13.2%
7	90EAC10AA110	CNVR T1A OUTL FLAP GATE	Discr. int. pos.		0	342	0.5%	13.7%
8	11HCB00EA100	GROUP CONTROL	Time mon. On		0	251	0.3%	14.0%
9	90GNQ34AS010	CAUSTIC PP 4 STROKE CNTR	Discr., Prot <-		0	182	0.3%	14.3%
10	11LAA10AA212	FEEDWATER TANK VENT VLV	Discr., Prot ->		0	180	0.3%	14.5%

Top Disturbance Alarms

Rank	KKS Tag	Description	Status	Desc	Prio	Count	%	Cum %
1	90GCF42CF140 XQ50	FLOW RO TRAIN 2 REJECT	Error L		4	249793	47.1%	47.1%
2	90GCF42CF140 XQ50	FLOW RO TRAIN 2 REJECT	Error AV		4	248594	46.8%	93.9%
3	11BRU10CE403 XG11	INVERTER ALT AC SUPPLY	Error		4	6399	1.2%	95.1%
4	11HLD01CT901 XJ51	T AH PRIMARY COLD END AV	Error L		4	4576	0.9%	96.0%
5	11HNA30CT023 XQ50	T GAS AIR HEATER OUTLET	Error AV		4	4548	0.9%	96.8%
6	90GNK25AA010	SALINE WTP INLET CTRL V	Error AV		4	1105	0.2%	97.1%
7	90GNK25AA010	SALINE WTP INLET CTRL V	Error L		4	1105	0.2%	97.3%
8	90GNK25CF010 XQ50	FLOW SALINE FD OXIDN TNK	Error AV		4	1105	0.2%	97.5%
9	90GNK25CF010 XQ50	FLOW SALINE FD OXIDN TNK	Error L		4	1105	0.2%	97.7%
10	11HLD01CT110 XQ50	T AH BRG CLG FAN BRG DE	Error H		4	1048	0.2%	97.9%

Daily Alarm Rate

1/08/2015	5053
2/08/2015	1307
3/08/2015	1161
4/08/2015	1528
5/08/2015	1679
6/08/2015	3259
7/08/2015	3566
8/08/2015	1893
9/08/2015	1645
10/08/2015	2920
11/08/2015	2997
12/08/2015	1730
13/08/2015	4060
14/08/2015	2599
15/08/2015	3893
16/08/2015	2704
17/08/2015	2592
18/08/2015	2193
19/08/2015	2437
20/08/2015	2199
21/08/2015	2019
22/08/2015	1461
23/08/2015	1595
24/08/2015	1988
25/08/2015	1897
26/08/2015	2263
27/08/2015	2053
28/08/2015	1850
29/08/2015	1663
30/08/2015	1877
31/08/2015	1735

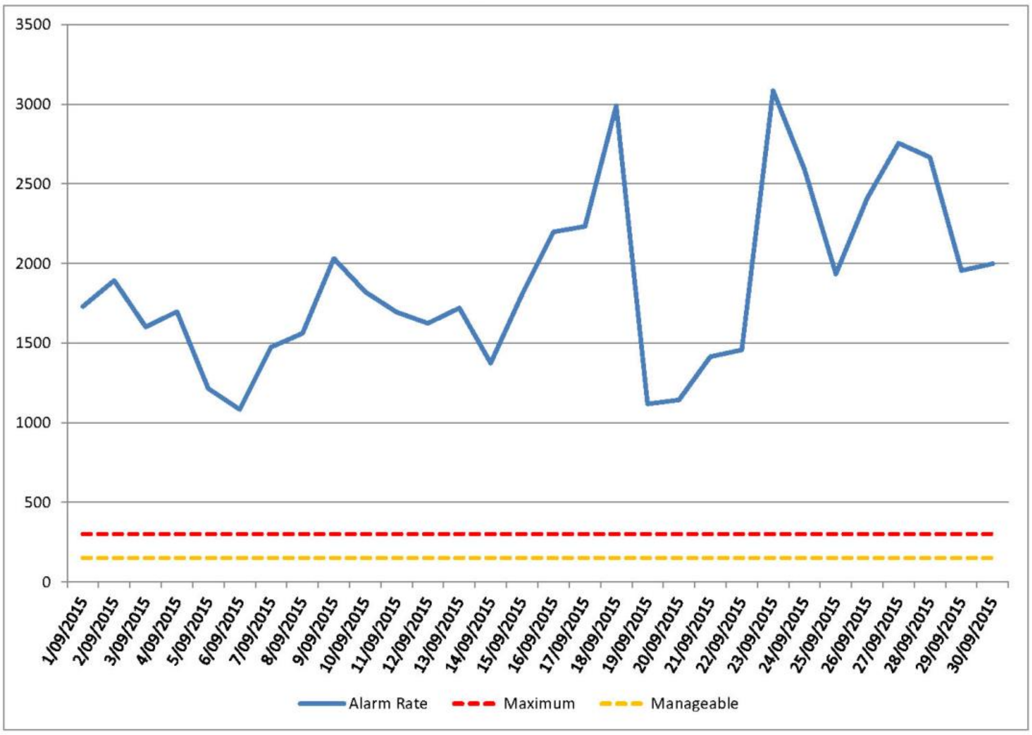
Monthly Alarm Report

September, 2015

Alarm Distribution

Prio	%
Maintenance	24%
1	10%
2	54%
3	12%

Daily Alarm Rate



Top Alarms

Rank	KKS Tag	Description	Status	Desc	Prio	Count	%	Cum %
1	90GND10CQ010 XU13	pH OXIDATION TANK	State 1 alarm		3	2713	4.8%	4.8%
2	11ETJ00EA800 XU02	VACUUM ECO HOPPERS	State 1 alarm		2	2578	4.6%	9.4%
3	90ETM12AP010	UNDER DRAIN SUMP PUMP	Discr., Off/Cl.		0	2275	4.0%	13.4%
4	90ETM12AP010	UNDER DRAIN SUMP PUMP	Discr., On/Op.		0	2274	4.0%	17.5%
5	11QEA20CM010 XQ50	DEW POINT DRYER 2 OUTLET	Limit HH	>MAX	1	2233	4.0%	21.5%
6	11QEA20CM010 XQ50	DEW POINT DRYER 2 OUTLET	Limit H	>HIGH	2	2146	3.8%	25.3%
7	11HFH20CL010 XG11	L PYRITE BOX PULV 20	State 1 alarm		2	1894	3.4%	28.6%
8	11HFH40CL010 XG11	L PYRITE BOX PULV 40	State 1 alarm		2	1827	3.2%	31.9%
9	11HFH50CL010 XG11	L PYRITE BOX PULV 50	State 1 alarm		2	1762	3.1%	35.0%
10	11HFH30CL010 XG11	L PYRITE BOX PULV 30	State 1 alarm		2	1604	2.8%	37.9%
11	11CJA00DU002 XU04	FREQUENCY DEVIATION	State 1 alarm		2	1589	2.8%	40.7%
12	90ETM13AP010	CENTRAL DECANT SUMP PUMP	Discr., Off/Cl.		0	1589	2.8%	43.5%
13	90ETM13AP010	CENTRAL DECANT SUMP PUMP	Discr., On/Op.		0	1588	2.8%	46.3%
14	11HYA00EY801 XU12	T GAS AH OUTLET DIFF	State 1 alarm		1	1566	2.8%	49.1%
15	11QUA10CQ075 XQ50	DOWNCOMER WATER OXYGEN	Limit H	>HIGH	2	1455	2.6%	51.7%
16	11HFC40EA800 XU01	PULVERISER 40 RATIO	State 1 alarm		2	1067	1.9%	53.6%
17	90GND10CQ010SXJ51	PH OXIDATION TANK	Limit L	<LOW	2	983	1.7%	55.3%
18	11QEA10CM010 XQ50	DRYER 1 OUTLET DEW POINT	Limit HH	>MAX	1	861	1.5%	56.9%
19	90GCF31CF010 XU62	FLOW RO TRAIN 1 FEED PMP	State 1 alarm		2	631	1.1%	58.0%
20	11QEA10CM010 XQ50	DRYER 1 OUTLET DEW POINT	Limit H	>HIGH	2	527	0.9%	58.9%

Top Maintenance Alarms

Rank	KKS Tag	Description	Status	Desc	Prio	Count	%	Cum %
1	90ETM12AP010	UNDER DRAIN SUMP PUMP	Discr., Off/Cl.		0	2275	4.0%	4.0%
2	90ETM12AP010	UNDER DRAIN SUMP PUMP	Discr., On/Op.		0	2274	4.0%	8.1%
3	90ETM13AP010	CENTRAL DECANT SUMP PUMP	Discr., Off/Cl.		0	1589	2.8%	10.9%
4	90ETM13AP010	CENTRAL DECANT SUMP PUMP	Discr., On/Op.		0	1588	2.8%	13.7%
5	90EAC10AA110	CNVR T1A OUTL FLAP GATE	Discr. int. pos.		0	383	0.7%	14.4%
6	11HCB00EA100	GROUP CONTROL	Time mon. On		0	369	0.7%	15.1%
7	90GNQ31AS010	CAUSTIC PP 1 STROKE CNTR	Discr., Prot <-		0	344	0.6%	15.7%
8	11LAA10AA212	FEEDWATER TANK VENT VLV	Discr., Prot ->		0	302	0.5%	16.2%
9	11LAA10AA212	FEEDWATER TANK VENT VLV	Discr., Off/Cl.		0	260	0.5%	16.7%
10	11LAA10AA212	FEEDWATER TANK VENT VLV	Discr. int. pos.		0	215	0.4%	17.1%

Top Disturbance Alarms

Rank	KKS Tag	Description	Status	Desc	Prio	Count	%	Cum %
1	90GCF42CF140 XQ50	FLOW RO TRAIN 2 REJECT	Error L		4	69401	44.1%	44.1%
2	90GCF42CF140 XQ50	FLOW RO TRAIN 2 REJECT	Error AV		4	68936	43.8%	87.9%
3	90GNK25AA010	SALINE WTP INLET CTRL V	Error L		4	1922	1.2%	89.1%
4	90GNK25CF010 XQ50	FLOW SALINE FD OXIDN TNK	Error L		4	1922	1.2%	90.3%
5	90GNK25AA010	SALINE WTP INLET CTRL V	Error AV		4	1921	1.2%	91.5%
6	90GNK25CF010 XQ50	FLOW SALINE FD OXIDN TNK	Error AV		4	1921	1.2%	92.8%
7	11BRU10CE403 XG11	INVERTER ALT AC SUPPLY	Error		4	1586	1.0%	93.8%
8	11HLD01CT110 XQ50	T AH BRG CLG FAN BRG DE	Error H		4	355	0.2%	94.0%
9	11HLD01CT110 XQ50	T AH BRG CLG FAN BRG DE	Error HH		4	355	0.2%	94.2%
10	11HLD01CT110 XQ50	T AH BRG CLG FAN BRG DE	Error AV		4	350	0.2%	94.4%

Daily Alarm Rate

1/09/2015	1730
2/09/2015	1893
3/09/2015	1601
4/09/2015	1697
5/09/2015	1214
6/09/2015	1083
7/09/2015	1475
8/09/2015	1562
9/09/2015	2032
10/09/2015	1821
11/09/2015	1695
12/09/2015	1625
13/09/2015	1720
14/09/2015	1374
15/09/2015	1807
16/09/2015	2198
17/09/2015	2233
18/09/2015	2991
19/09/2015	1118
20/09/2015	1143
21/09/2015	1414
22/09/2015	1457
23/09/2015	3085
24/09/2015	2593
25/09/2015	1934
26/09/2015	2410
27/09/2015	2755
28/09/2015	2667
29/09/2015	1956
30/09/2015	1999

Appendix D – Alarm Philosophy

The following pages are the alarm philosophy developed for project site. Note the numbering of pages, figures and tables is separate and does not coincide with this document.

Alarm Philosophy

Contents

List of Figures

List of Tables

1. Introduction

1.1. Purpose

The purpose of the Alarm Philosophy is to define the management systems, procedures and activities to ensure the management of the *Alarm System*, where practical, is consistent with both ISA-18.2-2009 – Management of Alarm Systems for the Process Industries and Engineering Directive – Alarm Management in Process Control Systems. This Alarm Philosophy will evolve as the journey of Alarm Management moves forward.

1.2. Scope

The scope of the *Alarm System* is:

- The *DCS* logic configuration which results in both *User Alarms* and *System alarms*
- The *HMI* system which is used to display alarms and provide the means for *Operators* to respond to alarms
- The Master Alarm Database
- The historical data collection of activated alarms and events
- The reporting tools used to generate alarm performance reports

1.3. Definitions

Table 1 – Definitions

Alarm	"An audible and/or visual means of indicating to the operator an equipment malfunction, process deviation, or an abnormal condition requiring a response." ISA-18.2-2009 definition
User Alarm	An alarm which the user has complete control over which conditions will cause it to activate
System Alarm	An alarm which the system generates based on its interaction with the equipment connected to the *DCS*. These alarms are usually diagnostic in nature and the user has no control over the configuration of these alarms
DCS	Distributed Control System - the site's process control system
HMI	Human Machine Interface used to control and operate the plant via the *DCS*
Operator	Panel operator in who operates the plant via the *HMI*
Bad Actors	Alarms that cause the alarm performance to exceed predefined metrics
Alarm Masking	Programmatically (in the *DCS* configuration) preventing alarms from activating based on equipment conditions – e.g. preventing a low discharge pressure alarm on a pump when it is shutdown

2. Alarm Management Roles

2.1. Site Management Team

The Site Management Team shall ensure the necessary resources, including people, systems and equipment, are available to adequately implement and execute the Alarm Philosophy.

2.2. Alarm Champion

The Alarm Champion is the lead Alarm Management role on the site. This role is responsible for ensuring that alarm management is executed in accordance with this Alarm Philosophy. The Alarm Champion should be an Instrument and Control / Electrical Asset Engineer as they have the skills and system knowledge to support the Alarm Philosophy.

2.3. Asset Engineering

Asset Engineering shall provide the technical knowledge and skills to support the Alarm Philosophy where required. As the A*larm System* is also used to improve asset and risk management of equipment Asset Engineering also act as a key stakeholder in the *Alarm System*.

2.4. Production

Production represent the end user of the *Alarm System*. Production shall hold the Alarm Champion to account for the performance of the *Alarm System* as well its use to improve the operability of the process. Production shall also provide technical knowledge to support the Alarm Philosophy where required.

2.5. Maintenance

Maintenance shall provide the technical knowledge and skills to support the Alarm Philosophy where required. Maintenance shall also rectify defects that affect the performance of the *Alarm System* in a timely manner.

3. Alarm Management Model

The Alarm Management Model describes the systematic manner in which the *Alarm System* will be managed. As the site has an existing *Alarm System* a combined approach will be taken to ensure:

- New alarms or are designed and implemented as per this alarm philosophy
- *Bad Actors* are quickly identified, rectified if caused by alarm maintenance issue, otherwise re-designed and implemented as per this alarm philosophy
- There is a method to rationalise all of the remaining installed alarms

To support these goals three distinct workflow entry points to the Alarm Management Model will be used. Appendix A depicts a visual representation of the Alarm Management Model and workflow entry points.

3.1. Core Model

3.1.1. Rationalisation

Rationalisation is the process where new or existing alarms are scrutinised to ensure that they meet the requirement to be an alarm and are designed consistent with this Alarm Philosophy.

Refer to Section 0 for details of the Rationalisation Process.

3.1.2. Master Alarm Database

All configured *User Alarms* are to be documented in a Master Alarm Database. The Master Alarm Database shall also document all alarm information identified during the Rationalisation process.

The Master Alarm Database is to be administered by the Alarm Champion. It is the master data for control system personnel when installing or maintaining an alarm. It should also be available to *Operators* for the purpose of determining the correct response to alarms.

3.1.3. Management of Change

To ensure alarms are correctly implemented, the appropriate people know about the alarms, and any follow-up documentation or actions are completed, all changes to the *Alarm System* must be managed using the site's management of change process. No changes to may be made to the *Alarm System* without authorization via the management of change process.

Refer to the sites Management of Chance Process for details.

3.1.4. DCS Configuration

The way in with alarms are generated are a result of the DCS Configuration. *User Alarms* are configured to activate when specific conditions are present, while *System Alarms* are a consequence of how equipment connected to the *DCS* behaves. When configuring *User Alarms* they must be implemented as specified in the Master Alarm Database. When installing or modifying equipment is important that the control system personnel understand how the equipment will generate *System Alarms.*

The DCS Configuration is administered by the Asset Engineering group.

3.1.5. Real-time Control

Real-Time Control is the operation of the process. Alarms are generated due to the operation of the process and how equipment is connected to the *DCS* responds. In an ideal situation the there are three layers to prevent undesirable consequences – the process control layer, the alarm layer, and the shutdown/trip layer.

The process control layer consists of the plant automation which keeps the process in normal operating parameters. If there is an abnormal situation that the process control layer cannot prevent an Alarm is presented the *Operator* via the *HMI*. The *Operator* will make an adjustment to the process via the *HMI* and return the process to normal operation. If no action or incorrect action is taken then shutdown/trip layer will shut down equipment to prevent consequences such as harm to people, equipment damage and environmental damage. Although the shutdown itself is likely to be an undesirable consequence, it is more favourable than consequences such as harm to people, equipment damage and environmental damage.

3.1.6. Alarm and Event History Collection

Chronological data on the activation of alarms and events is collected and stored for historical purposes. This data is used for both review of plant operation and alarm performance reporting.

The Alarm and Event History Collection is administered by the Asset Engineering.

3.1.7. Alarm Performance Reporting

The performance of the *Alarm System* is measured through regularly schedule reports that analyse chronological alarm activation data and compare against pre-defined metrics.

Refer to Section 6 for details of Alarm Performance Reporting.

3.2. Alarm Management Workflow Entry Points

The following Alarm Management workflow entry points have been identified:

3.2.1. Workflow Entry 1 – New Alarm

Whenever a new alarm is proposed it shall progress through the core of the Alarm Management Model. Proposed alarms are rationalised, entered into the Master Alarm Database. From there the management of change process should guide the implementation of the alarm into the *DCS* Configuration and then into Real-time Control. Once implemented the alarm may be reviewed in the future if is progresses through the other workflow entry points

3.2.2. Workflow Entry 2 – Alarm Performance Improvement

The Alarm Performance Improvement workflow is a result of Alarm Performance Reporting. Weekly and Monthly reports shall be used to identify *Bad Actors*. The Alarm Champion shall determine if the cause of the *Bad Actor* is an alarm maintenance issue or a poorly designed alarm.

Alarm maintenance issues include faulty equipment, mal-operation or insufficient protection offered by the process control layer. The Alarm Champion may require support from Asset Engineering, Maintenance and/or Production personnel to rectify maintenance issues. Responsibility for rectification may be passed to other departments but the Alarm Champion shall ensure they are completed. If the *Bad Actor* has never been rationalised then is shall also be put forward for rationalisation. Note that *System Alarms* cannot be rationalised and should be treated as alarm maintenance issues.

If the *Bad Actor* cannot be rectified by alarm maintenance the alarm should be put forward for rationalisation. In some circumstances it may be more appropriate to group the *Bad Actor* with all other alarms that are part of the same sub-system or plant area and re-design the alarming strategy for the sub-system or plant area.

Note: Where an equipment defect or equipment malfunction produces a fleeting that is overshadowing all other alarms then it should be rectified immediately. These alarms may undermine the effectiveness of the whole *Alarm System*.

3.2.3. Workflow Entry 3 – Existing Alarm

Due to the high number of installed alarms (1000's) it is not practical to provide the time and human resource required to rationalise all existing *User Alarms*. The drivers for selection may be to improve asset and risk management of equipment, or to improve the alarming strategy for a sub-system or plant area. The scheduling and criteria for selecting alarms for Scheduled Rationalisation shall be determined by the Alarm Champion in consultation with Asset Engineering and/or Production.

4. Alarm System Description

The *HMI* provides the means the present alarms to the *Operator*. The alarm functionality is fixed within the *HMI* in that it provides three priorities for *User Alarms* and two priorities for *System Alarms*.

The *HMI* provides three distinct states for Alarms, they are:

- Normal
- Active Un-acknowledged
- Active Acknowledged

Figure 1 shows a state transition diagram for the alarm states. The *HMI* provides a method to implement Alarm Masking. The alarm masking provided only prevents the alarm from making an audible sound and flashing, i.e. it will progress straight to the Active and Acknowledged state. The alarm will still appear in the Alarm List, in an alarm state on graphical displays and also be recorded in the Historian. This is not consistent with the ISA18.2-2009 definition of "Suppressed by Design". It is not recommended that this feature be used. Instead alarm masking should be configured in the application software loaded into the DCS controllers.

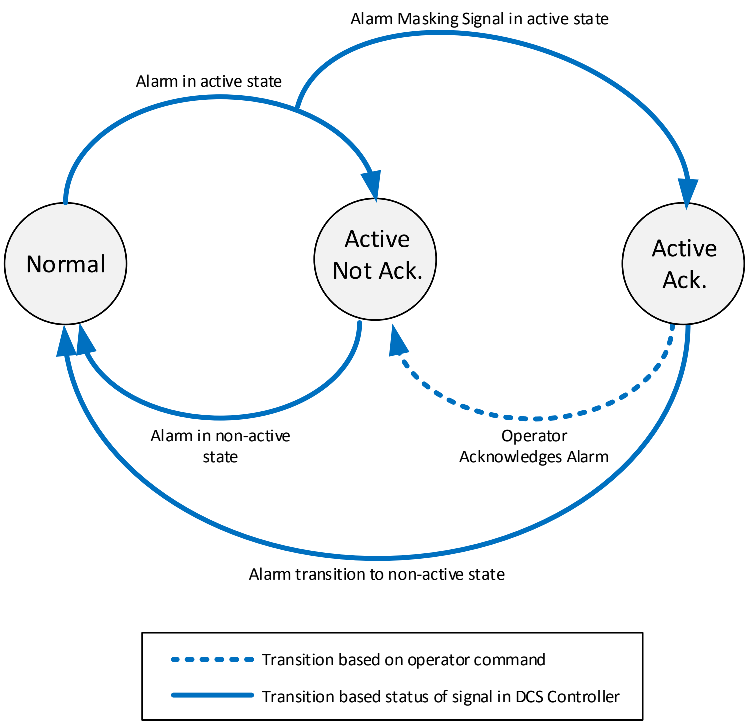


Figure 1 - Alarm Handling transition diagram (note HMI alarm masking not to be used)

Table 2 describes the priorities of *User Alarms*, how they are visually indicated, whether there is an audible indication, and the manner in which the O*perator* should respond. *Table 3* describes the priorities *System Alarms*, how they are visually indicated, the types of situations that can cause the alarm to activate, and manner in which the O*perator* should respond.

During normal operation alarm displays should be set to only present activations requiring an operator response – this is Priority 1, 2, 3 and Maintenance alarms. Priority S (Disturbance) alarms should filtered out so they are not presented to *Operators*. These are diagnostic alarms where the *Operator* response would be to relay information to maintenance personnel.

Table 2 – Alarm System Priorities for User Alarms

Priority	Visual Indication	Audible Annunciation	*Operator* Response
1	High-lighted Red with White text (Flashing until Acknowledged)	Yes	Cease all current tasks and activities and respond to the alarm
2	High-lighted Orange with White text (Flashing until Acknowledged)	Yes	Close off any current tasks or activities and then respond to the alarm
3	High-lighted Yellow with Black text (Flashing until Acknowledged)	No	Timely (within 10 to 30 minutes) response to the alarm is required – lowest priority of both *User Alarms* and *System Alarms*
Event	White or Green text	No	Alarm displays should be filtered to prevent these alarms from being presented to operators

Table 3 – Alarm System Priorities for System Alarms

Priority	Visual Indication	Possible Source of Alarm	*Operator* Response
Maintenance	Blue (Flashing until Acknowledged)	A Drive or Sequence is not at its expected position – there has been an unexpected change of state, the monitoring time to transition to an expected state has been exceeded, or the has been an interlock protection trip	Response as per Priority 2 Alarm (refer to Table 2)
S (Disturbance)	High-lighted Grey with Yellow text (Flashing until Acknowledged)	System diagnostics has determined, or a device is reporting an error which is or will prevent it from operating correctly	Alarm displays should be filtered to prevent these alarms from being presented to operators

5. Alarm Rationalisation

Apart from the process as identified in this section the most important part of Alarm Rationalisation is the documentation of alarms. All outcomes of the Alarm Rationalisation process shall be documented in the Master Alarm Database.

5.1. Rationalisation Team

Alarm Rationalisation shall be performed using a cross functional team. The Rationalisation Team shall consist of the following roles:

- The Alarm Champion
- Instrument and Control Asset Engineer
- Electrical Asset Engineer
- Mechanical Asset Engineer
- Production Coordinator
- Senior Production Operator
- Instrument and Control / Electrical Maintenance Analyst (as required)
- Mechanical Maintenance Analyst (as required)
- Environmental (as required)
- Safety and Health (as required)

The Rationalisation Team shall meet in the context of a design review meeting. The Alarm Champion shall lead the Rationalisation Team. Prior to meeting the Alarm Champion shall:

- Compile the list of alarms to be rationalised, identified via one of the Alarm Management Workflows (refer to section 3.2)
- Pre-populate the *DCS* configuration (as intended for new alarms or as installed for exiting alarms) for the list of alarms for the alarms to be rationalised
- Ensuring the correct team members attend the meeting
- Ensure any required supporting documentation is available to the team.

5.2. Rationalisation Guidance

The following guidance is provided to ensure rationalisation in performed in the correct context:

- Alarms should indicate to the *Operator* an equipment malfunction, process deviation, or an abnormal condition requiring a response
- The Alarm System should not be used as protection layers to prevent harm to people. Alarms with a consequence category of Safety should only be activated after to alert the *Operator* to that an emergency response maybe required. Examples of safety consequence alarms are Fire System alarms, safety shower initiation alarms and area gas detection alarms. Alarms with a consequence category of Safety should always be configured as Priority 1. Process equipment should have protection layers for Safety designed into equipment.
- Alarms should not be used as the first protection layer to prevent undesirable consequences – alarms should be used indicate that process control layer has become ineffective
- Alarms should not be used as the last layer of protection to prevent undesirable consequences – the shutdown/trip layer should be used where there has been no action or incorrect action in response to an alarm.

- Base on the previous two points it is likely that the for the bulk of alarms the consequences of no action or incorrect action will be assigned to the consequence category of Business Interruption due to the shutdown/trip layer
- Alarms should not activate to provide information only – particular attention is directed to the alarming of logic conditions used for automated operation of the processes. If the process control layer is working as required no alarms should be activated.
- Alarms requiring the same response should be grouped to a single alarm
    - Where these alarms are generated from external subsystems the use of a group or summary alarm is recommended. An example of this may be a group of trip indications from an external subsystem. The response to each of the individual trip alarms is likely the same for all. The best implementation may be to use one common alarm to indicate that a trip has occurred, while the individual alarms are reconfigured as events and their status used as an indication on a *HMI* graphic display.
    - Where there are multiple or many measurements a single alarm can be implemented. An example of this is generator winding alarms where could be several dozens of measurements, each with an alarm. The response to each of the individual trip alarms is likely the same for all. The best implementation may be to use one common alarm to indicate a temperature problem. The *Operator* response could be to review all of the measurements, confirm that there is an abnormal situation and then decide on the correct cause of action.

5.3. Rationalised Alarm Definition

During the alarm rationalisation the following items are to be defined for each alarm:

5.3.1. DCS Configuration

Table 4 provides a list of the information required to implement an alarm in the *DCS*.

Table 4 – DCS Configuration

Attribute	Guidance
KKS Tag	Dependant on how the alarm in configured – this may need to be updated once the alarm has been implemented in the *DCS* Configuration.
Descriptor	System limits this to 24 characters – this should be as intuitive as possible to help the *Operator* identify the abnormal situation.
Text for Alarm State	System limits this to 7 characters – this should be used in conjunction with the Descriptor to help the *Operator* identify the abnormal situation.
Text for Normal State	System limits this to 7 characters.
Functional Description	The functional description is the *DCS* configuration required to implement the alarm. This is the alarm set point or logic conditions that will activate the alarm. *See text below table for guidance in determining the function description.

Attribute	Guidance
Time Delay	Time delay can precent fleeting alarms, though overuse may reduce the maximum time to respond. ISA-18.2-2009 Time Delay Recommendations: • Flow Rate: ~15 seconds • Level: ~60 seconds • Pressure: ~15 seconds • Temperature: ~60 seconds
Hysteresis	Hysteresis can be used to prevent fleeting alarms, though overuse can create standing alarms. ISA-18.2-2009 Hysteresis Recommendations: • Flow Rate: ~5% • Level: ~ 5% • Pressure: ~2% • Temperature: ~1%
Alarm Masking Conditions	Identity any logic conditions in the DCS which can be used to prevent the alarm from activating unnecessarily, i.e. sub-system or equipment shutdown which may generate an alarm that is unnecessary.

The Instrument and Control / Electrical Asset Engineer should provide guidance to the Rationalisation Team when determining the functional description of the alarm to ensure what is specified is within the capabilities of the *DCS*.

The following guidance is provided when designing the Functional description of the alarm:

- Limit values of measured analog signals – these types of alarms are not recommended as there is no means to apply time delays or masking conditions.
- Measured binary signals – the types of alarms are not recommended for process measurements as there is no means to apply time delays or masking conditions.
- Calculations on measure values – these types of alarms are recommended as they can be tailored to best identify abnormal situations. It is also easier to apply *Alarm Masking* to these types of alarms
- Logic Base Alarm – these types of alarms are recommended as they can be tailored to best identify abnormal situations. It is also easier to apply *Alarm Masking* to these types of alarms

5.3.2. Consequence of No Action or Incorrect Action

For each alarm to be rationalised the Rationalisation Team shall access the consequence if there is no action or incorrect action to the abnormal situation the alarm has identified. The consequence shall be considered for the categories of Safety, Environmental, Asset Damage or Loss, Asset Integrity and Business Interruption. For each of these consequence categories the consequence shall be classed as Minor, Major or Severe according the guidelines in Table 5. It should be assumed that any shutdown layers will operate if there is no action or incorrect action to the alarm

Note that it may be useful to determine the corrective actions first if the consequence is not easily determined

The Rationalisation Team should document the rationale of the selections from the consequence matrix for inclusion in the Master Alarm Database. This will aid future alarm rationalisation of the alarm.

Table 5 – Consequence Matrix

Consequence Category	Consequence		
	Minor	**Major**	**Severe**
Safety	Any alarm that prevents harm to personnel shall be Priority 1. *Alarms shall not be used as the primary layer of protection to prevent harm to personnel		
Environment	Local clean up required	Major clean up required Incident report to corporate level	Offsite clean up required Breech of License conditions or incident report to regulator
Assets Damage or Loss	Damage or loss <$10K	Damage or loss >$10K	Damage or loss >$100K
Business Interruption	Loss of availability of redundant equipment	Temporary loss of generating capacity <24 hours	Unit Trip or Shutdown Temporary loss of generating capacity >24 hours
Asset Integrity	Any Alarm that protects Asset Integrity shall be Priority 2. *Asset Integrity is related to consequences of continued operation outside of safe operating windows where consequences may be reduced asset life or a scheduled plant shutdown to make repairs.		

5.3.3. Maximum Time for Operator to Respond

For each alarm to be rationalised the Rationalisation Team shall determine the maximum time for an *Operator* to respond to the alarm in order to prevent the abnormal situation from escalating to the consequence.

The times should be classified as either:

- Less than three minutes
- Three to ten minutes
- Ten minutes to 30 minutes
- Greater than 30 minutes

Note that the maximum time for an *Operator* to respond is not required for consequence categories of Safety and Asset Integrity.

5.3.4. Potential Causes

For each alarm to be rationalised the Rationalisation Team shall identify potential causes of the abnormal situation the alarm has identified. The context for the potential cause is to provide guidance to an *Operator* in real time to confirm abnormal situation. This will also assist the *Operator* in making an assessment of the appropriate corrective action.

5.3.5. Corrective Actions

For each alarm to be rationalised the Rationalisation Team shall identify the possible corrective action(s) required to return the process to normal operation. The context for the corrective action(s) is to provide guidance to an *Operator* in real time as to what correct action(s) to take to return the process to normal operation.

5.3.6. Priority Determination

Alarms are prioritised according to the Consequences of No Action or Incorrect Action and Maximum Time for the *Operator* to Responded. Table 6 shows how alarms are to be prioritised using these two attributes.

Table 6 – Priority Determination Matrix

Maximum Time for operator to respond	**Consequence**		
	Minor	**Major**	**Severe**
>30 minutes	Event	Event	Event
10 to 30 minutes	3	3	2
3 to 10 minutes	3	2	2
<3 minutes	2	1	1

Note that the Priority for consequence categories of Safety and Asset Integrity are not related to the maximum time for an *Operator* to respond, they are fixed as per Table 5.

6. Alarm Performance Monitoring

The purpose of Alarm Performance Monitoring is to provide a continuous improvement loop in the alarm management. Initially Alarm Performance Monitoring will focus on basic alarm performance metrics. As the sites alarm management journey continues and alarm performance improves the Alarm Performance Monitoring more sophisticated metrics will be assessed.

6.1. Alarms Reports

All alarm reports are to be based on the total alarms each operating positon will receive in the reporting period. This includes all plant areas within the span of control of the *Operator*. Priority S (Disturbance) alarms will not be included in the alarm rate reporting metrics. These are diagnostic alarms where the *Operator* response would be to relay information to maintenance personnel.

The reporting periods to be used will be calendar month and week – Monday to Monday. For each reporting period the report the follow items will be reported:

6.2. Alarm Performance Measures

The following Alarm Performance Measures will drive Alarm Performance Improvement:

6.2.1. Alarm Priority Distribution

Definition:

> All alarm activations requiring an operator response (Priority 1, 2, 3 and Maintenance alarms) in the reporting period are grouped into priority. The total count of alarm activations for each group is expressed as a percentage of the total number of alarm activations.

For an *Alarm System* with three priorities ISA-18.2-2009 identifies an Alarm Priority Distribution of ≈80% for Priority 3, ≈15% for Priority 2, and ≈5% for Priority 1. Poor priority distribution can undermine the intent of priorities. ISA-18.2-2009 provides not guidance for Maintenance alarms, but these should be less than 5%

Exceedances of the Alarm Priority Distribution metric should drive scheduled rationalisation – e.g. overuse of a priority may mean that the focus of scheduled rationalisation should focus on a particular priority ahead of others. I may also be used to determine it the rationalisation methodology is effective – e.g. if the priority distribution of alarms that have been rationalised exceeds the metric then a review of the rationalisation methodology may be required.

6.2.2. Top Alarms

Definition:

> All alarm activations in the reporting period requiring an operator response (Priority 1, 2, 3 and Maintenance alarms). The top 20 alarms based on total number of activations is listed. Further processing of the list will include:
>
> - The alarm count percentage – i.e. the total count for each alarm expressed as a percentage of the total alarm activations for the reporting period
> - The alarm count cumulative percentage – i.e. the cumulative percentage of the alarms working down the list from highest count to lowest count.

The Top Alarms for alarms requiring an operator response (Priority 1, 2, 3 and Maintenance alarms) should are used to determine *Bad Actors*. The *Bad Actors* should progress through the

Alarm Performance Improvement workflow entry (refer to Section 3.2.2). The Top Alarms can be used to identify both frequently occurring alarms and fleeting alarms.

6.2.3. Top Maintenance Alarms

Definition:

All Maintenance alarm activations in the reporting period. The top 10 alarms based on total number of activations is listed. Further processing of the list will include:

- The alarm count percentage – i.e. the total count for each alarm expressed as a percentage of the total alarm activations for the reporting period
- The alarm count cumulative percentage – i.e. the cumulative percentage of the alarms working down the list from highest count to lowest count

The Top Maintenance Alarms should be used to identify equipment that requires maintenance intervention.

6.2.4. Top Disturbance Alarms

Definition:

All Disturbance alarm activations in the reporting period. The top 10 alarms based on total number of activations is listed. Further processing of the list will include:

- The alarm count percentage – i.e. the total count for each alarm expressed as a percentage of the total alarm activations for the reporting period
- The alarm count cumulative percentage – i.e. the cumulative percentage of the alarms working down the list from highest count to lowest count.

The Top Disturbance Alarms should be used to identify equipment that requires maintenance investigation.

6.2.5. Daily Alarm Total

Definition:

The total alarm activations requiring an operator response (Priority 1, 2, 3 and Maintenance alarms) for each day in the reporting period are totalled and listed.

The Daily Alarm Total is the key performance metric that drives Alarm System Monitoring. ISA-18.2-2009 identifies two metrics for the Daily Alarm Total. The first is 'Very Likely to Be Acceptable' at 150 alarms per day, the second is 'Maximum Manageable' at 300 alarms per day. The Daily Alarm Total should be below 150 alarms per day, though some exceedances up to 300 alarms per day can accepted.

The alarm management response to the exceedance of the Daily Alarm Total is not directed at individual alarms, but it should be used are an overall indicator of the health of the *Alarm System*. Focus on alarm management should intensify when the 'Very Likely to Be Acceptable' metric is regularly exceeded.

6.2.6. Future Alarm Performance Metrics

Although not currently used as reporting metrics, the following will be considered into the future:

- Standing Alarms (alarm active for more than one shift/24 hours)

- Top 10 Alarm Percentage (the percentage of the alarm count made up by the top 10 alarms)
- Fleeting Alarms (direct analysis)
- Alarm Flooding (based on 10 minute intervals)
- Peak Alarm Rates (based on 10 minute intervals)

Appendix A Alarm Management Model with Workflows