OPG WESTERN WASTE MANAGEMENT FACILITY

WVRB CONTROL ROOM UPGRADES LESSONS LEARNED

Justin Julian P. Eng.
Ontario Power Generation, Western Waste Management Facility
Tiverton, Ontario, Canada

ABSTRACT

The Ontario Power Generation (OPG) Western Waste Management Facility (WWMF) uses a computer based Supervisory Control and Data Acquisition (SCADA) system to monitor its facility, and control essential equipment. In 2007 the WWMF Low and Intermediate Level Waste (L&ILW) technical support section conducted a review of outstanding corrective maintenance work. Technical support divided all work on a system by system basis. One system under review was the Waste Volume Reduction Building (WVRB) control room SCADA system.

Technical support worked with control maintenance staff to assess all outstanding work orders on the SCADA system. The assessment identified several deficiencies in the SCADA system. Technical support developed a corrective action plan for the SCADA system deficiencies, and in February of 2008 developed an engineering change package to correct the observed deficiencies. OPG Nuclear Waste Engineering approved the change package and the WVRB Control Room Upgrades construction project started in January of 2009. The WVRB control room upgrades construction work was completed in February of 2009.

This paper provides the following information regarding the WWMF SCADA system and the 2009 WVRB Control Room Upgrades Project:

- A high-level explanation of SCADA system technology, and the various SCADA system components installed in the WVRB.
- A description of the state of the WVRB SCADA system during the work order assessment, identifying all deficiencies.
- A description of the new design package.
- A description of the construction project.
- A list of lessons learned during construction and commissioning, and a path forward for future upgrades.

1. BACKGROUND

1.1 Supervisory Control and Data Acquisition (SCADA)

A SCADA or Supervisory Control and Data Acquisition system is a computer-based control system for industrial process control[1] that consists of three major components:

1. The "Supervisory Control" component,
2. The "Data Acquisition" component and,
3. The Programmable Logic Controller (PLC) component[2].

Refer to Figure 1 for a diagram of a typical SCADA system.

1.1.1 Supervisory Component

The Supervisory component provides an operator with a graphical user interface for all processes within an industrial facility. The Supervisory Component hardware is typically a computer with a monitor, keyboard, and mouse. The Supervisory Component software monitors process data from the PLCs in real time and presents the user with a graphical interface. The graphical interface has the following functionality:

- A real-time display of all process parameters such as pressure, temperature, levels, positions, and statistical data (running totals, min, max, and average). The real-time display is usually a collection of numeric or animated objects displayed over top of a graphical abstraction of the process, usually in the form of a Piping and Instrumentation (P&ID) drawing or process flow chart.
- Process setpoint change screens to adjust high-level operating parameters such as auto start / stop levels, controller setpoint or reference values, and manual override values.
- Supervisory control features such as Auto start / stop commands, auto / manual mode transitions, and alarm acknowledge commands.
- Historical trending screens showing the variation of process parameters and alarms over time.
- Active alarm annunciation and acknowledgement screens.

1.1.2 Data Acquisition Component

The "Data Acquisition" component consists of one or more computers with a Relational Database Management System (RDBMS). The Data Acquisition component continuously reads process data from the PLCs and maintains a historical log of all process values. The Data Acquisition component makes historical data available to third-party reporting software on the SCADA network.

---

[1] Practical SCADA for Industry, David Bailey B.Eng, Edwin Wright MIPENZ BSc (hon), Newnes September 17 2003, Chapter 1, Section 1.1 (see reference 1)

[2] The terms PLC (Programmable Logic Controller) and RTU (Remote Terminal Unit) are often used interchangeably in various industries. There are subtle differences between the two technologies; however for the purpose of this paper, it is safe to consider the two as equivalent.

1.1.3 Programmable Logic Controller Component

SCADA systems communicate with Programmable Logic Controllers (PLCs) in the field over an industrial Ethernet network[3]. A PLC provides real-time control of equipment. The PLC communicates with the equipment using hardwired analog and digital input and output signals. A custom program inside the PLC processor memory processes the input signals and generates output signals to control equipment.

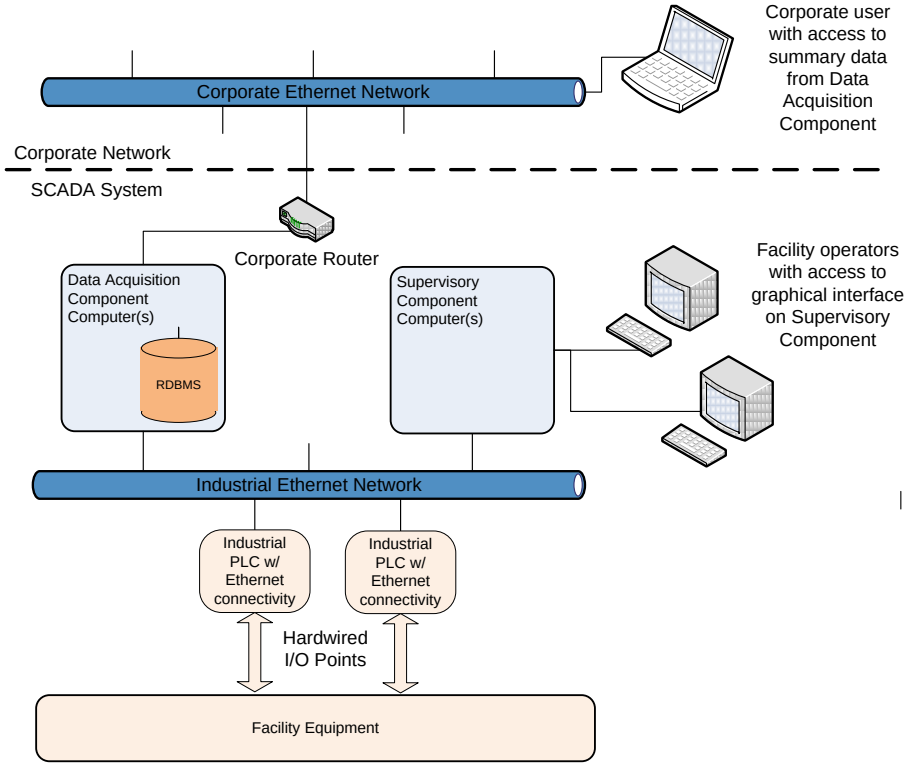

Figure 1 Typical SCADA System

2. WWMF SCADA SYSTEM

2.1 WWMF Facility

The WWMF SCADA system monitors and controls facility equipment in three main areas:

- the Western Used Fuel Dry Storage Facility (WUFDSF),
- the Transportation Package and Maintenance Building (TPMB), and
- the Low and Intermediate Level Waste Facility Waste Volume Reduction Building (WVRB).

Refer to Figure 2 for a diagram of the WWMF buildings and all equipment controlled by the SCADA system.

[3] SCADA system design using a PLC processor over an industrial Ethernet network represents one of several possible variations. For the purpose of this paper, the Ethernet / PLC design demonstrates the core components of a SCADA system. For a more information on SCADA system architecture refer to Practical SCADA for Industry, David Bailey B.Eng, Edwin Wright MIPENZ BSc (hon), Newnes September 17 2003.

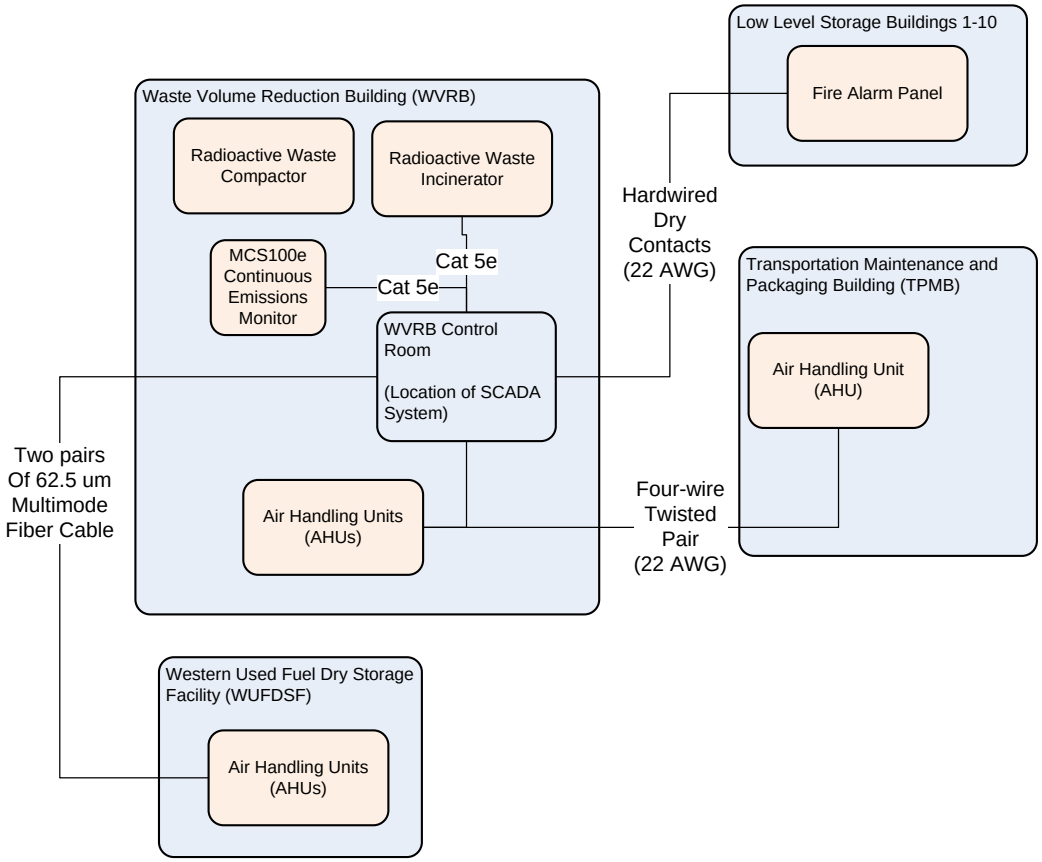

Figure 2 WWMF Facility Equipment Monitored by the SCADA System

2.1.1 WUFDSF Equipment

High level nuclear waste (spent fuel from the Bruce A and Bruce B reactors) is placed into dry storage containers at the spent fuel pools in the stations. The dry storage containers are transported to the WUFDSF for interim storage. The WWMF uses various Air Handling Units (AHUs) and ventilation fans to control air quality and temperature in the WUFSDF processing area. The WWMF SCADA system monitors and controls the building ventilation system at the WUFDSF.

2.1.2 TPMB Equipment

Low and Intermediate level waste packages are maintained in the TPMB building. The TPMB building also houses maintenance shop facilities for mechanics and control technicians working at the TPMB and the WVRB. The TPMB uses one Air Handling Unit to control air temperature and quality. The WWMF SCADA system monitors and controls the AHU at the TPMB.

2.1.3 WVRB Equipment

Low level waste packages are received and off-loaded at the WVRB receiving dock. OPG uses two major technologies to reduce the volume of low level nuclear waste:

- One Anderson 2000 Radioactive Waste Incinerator and;
- One 200 Ton Supercompactor (Container Products Corporation)

The incinerator and compactor are located in the Waste Volume Reduction Building (WVRB). The WWMF SCADA system monitors and / or controls the following equipment at the WVRB:

- the Radioactive Waste Incinerator and all ancillary systems,
- building heating, cooling and ventilation systems,
- various facility alarms (sump levels, transformer alarms, CO2 fire suppression system trouble), and
- Secondary fire alarm monitoring from the low level storage buildings.[4]

After all low level waste is incinerated or compacted; the waste is stored in metal bins inside ten Low Level Storage Buildings on site[5].

2.2 WVRB Control Room

The WWMF SCADA system is located in the WVRB control room. All computer hardware for the WWMF SCADA system is located on the control room desk. The control room desk has four parts that form an "h" shape. The four parts of the desk are called the north, south, east and west side of the control room desk. Refer to Figure 3 for a basic layout diagram of the WVRB control room, showing the desks, computers, and various control panels.

WVRB facility operators use the WWMF SCADA system to monitor and control all equipment at the WVRB and the TPMB 24 hours a day, seven days a week. The WVRB facility operators provide monitoring and emergency response services to the WUFDSF outside normal working hours. The day shift operators at the WUFDSF control the building ventilation system using a local operator interface panel.

2.3 WWMF SCADA System Prior to Upgrades

Prior to the control room upgrades work, the WWMF SCADA system used six computers on four different networks to control all equipment.

2.3.1 Johnson Computer

The WVRB building management system used a Johnson Controls[6] NCM (Network Control Module) to monitor and control the building heating, cooling, and ventilation systems at the WVRB. The NCM was located in a panel inside the WVRB control room (see the panel in Figure 3 labeled "COMPT1"). The NCM communicated with four DX-9100 modules installed in the field and remote I/O modules inside the "Johnson I/O Panel" in the WVRB control room. The Johnson system used an N2 communications bus to communicate with all devices. The DX-9100 modules controlled two air handling units in the WVRB and one air handling unit in the TPMB. The I/O blocks in the Johnson I/O Panel monitored miscellaneous equipment in the WVRB as well as three discrete contacts from the Low Level Storage building fire alarm panels. The NCM exchanged information with the Johnson Computer on the north side of the control

[4] "Secondary" fire alarm monitoring refers to the fact that the fire alarm system has its own National Fire Code complaint detection and annunciation hardware. The WWMF SCADA system receives duplicate signals from the fire alarm system for historical logging and redundant annunciation.

[5]. By the time this document was completed, the WWMF box compactor and conveyor systems were not yet connected to the WWMF SCADA system See 7.2 System Integration (Master Plan).

[6] NCM, NAE, DX-9100, and Metasys are all registered trademarks of Johnson Controls Inc. (JCI)

room desk over a direct Ethernet connection. The Johnson computer was a Dell[7] Pentium[8] III Windows XP based PC. The Johnson Computer ran Johnson Controls Inc. (JCI) Metasys software package to provide a graphical user interface for the heating, cooling and ventilation systems at the WVRB and the TPMB. Refer to Figure 4 for a diagram of the existing Johnson Computer and the facility equipment that it monitored and controlled.

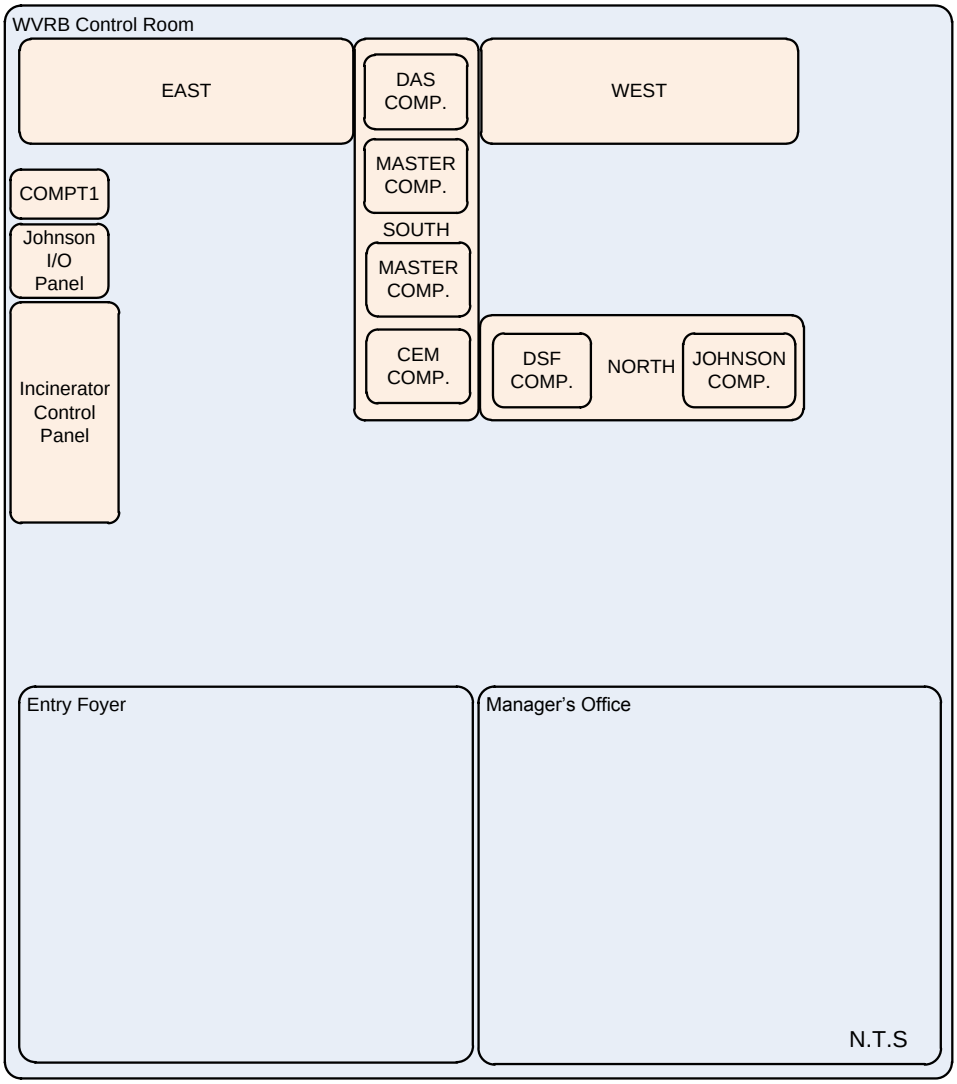

Figure 3 WVRB Control Room Layout (before upgrades)

[7] Dell is a registered trademark of Dell Corporation.

[8] Pentium is a registered trademark of Intel Corporation.

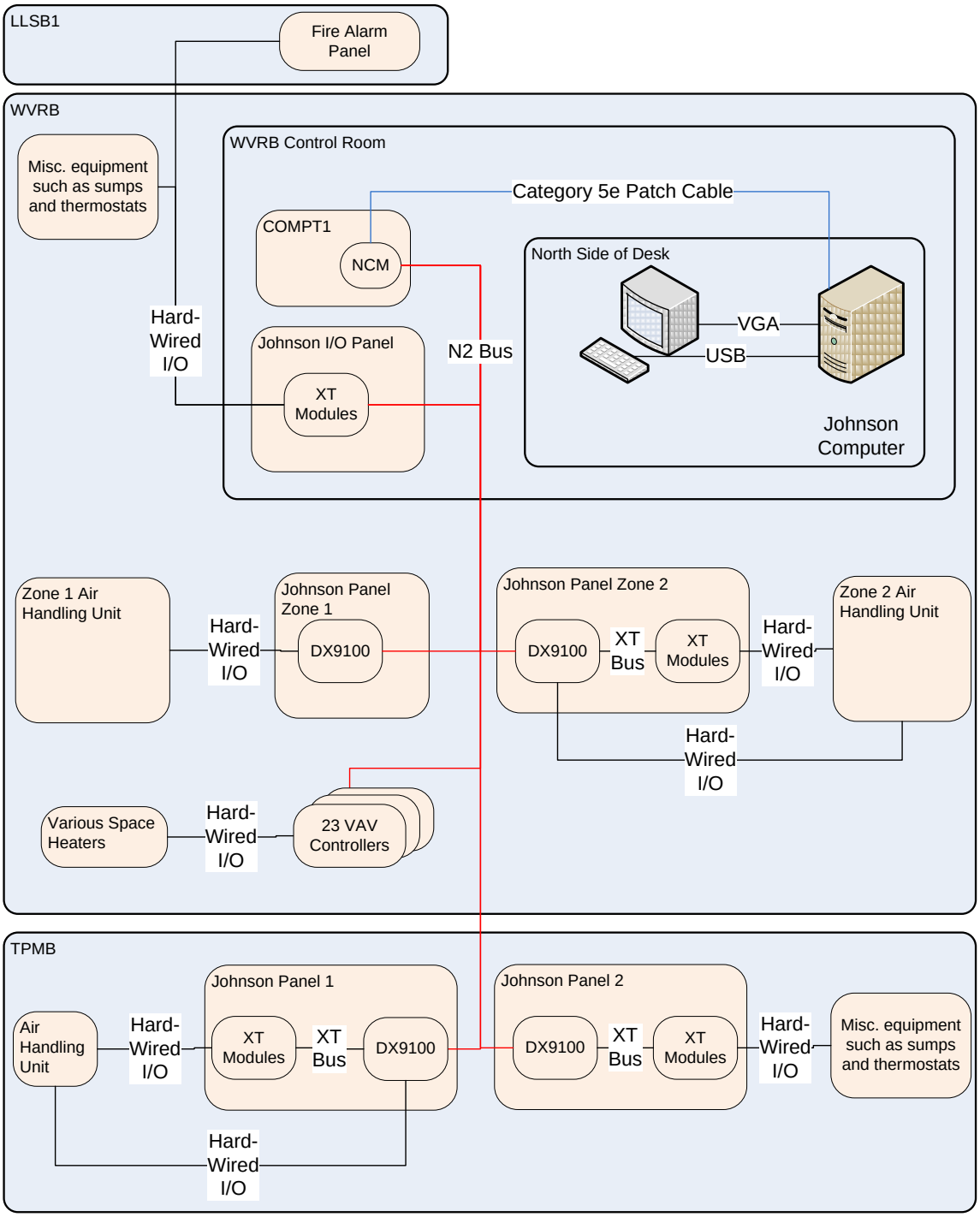

Figure 4 Existing SCADA System - Johnson Computer

2.3.2 Master and Slave Computers

The WVRB incinerator uses a GE Fanuc 90/70[9] PLC to perform all real-time control functions. A second smaller GE Fanuc 90/30 PLC controls the flue gas cooling system. An Allen-Bradley SLC 5/04 PLC[10] controls the incinerator solid waste conveyor feed system and solid waste scales. The conveyor system PLC exchanges information with the incinerator GE 90/70 PLC over hardwired I/O points connected directly from PLC to PLC.

The GE 90/70 and 90/30 PLCs were connected to two Dell Pentium III PCs on the WVRB control room desk via a small 10Base-T Ethernet hub. The Dell PCs were called the Master and Slave computer.

GE Cimplicity HMI Server was installed on the Master computer. Cimplicity HMI Viewer was installed on the Slave computer. The Master PC obtained real-time data from the incinerator PLC and the flue gas treatment PLC over the Ethernet hub. The Master PC logged historical data in its local database, and provided a graphical user interface for the control room operator. The Slave PC provided a second copy of the incinerator user interface, obtaining all real-time data from the Master PC over the Ethernet hub. Refer to Figure 5 for a diagram of the existing Master, Slave, DAS, and CEM computers, and the facility equipment connected to each computer.

A small dedicated user interface panel was installed in the incinerator room. The user interface panel (Eaton Panelmate Pro[11]) provided limited control and monitoring functions for the operator in the field. The Panelmate Pro was connected to the incinerator PLC by a dedicated serial cable.

2.3.3 Data Acquisition System (DAS) Computer

A Pentium III clone PC was connected to the 10Base-T Ethernet hub on the same LAN as the Master and Slave computers. The third PC was called the Data Acquisition System or DAS computer. The DAS computer used a GE Cimplicity HMI SCADA application to obtain real-time stack emission data from the incinerator PC. The DAS computer logged historical emission data in its local database, and provided real-time and historical display screens for the control room operator. The DAS computer had a 56k external modem that allowed third party vendors to dial into the incinerator DAS PC for remote service calls.

2.3.4 Continuous Emissions Monitoring (CEM) Computer

The Ontario Ministry of Environment requires the WWMF to continuously monitor stack emissions, ensuring that concentrations remain within limits set out by Certificate of Authorization (Air) 8376-5SMRWL. The WWMF uses a SICK MAIHAK MCS 100E[12] multi-component I/R photometer to measure stack emissions in real-time. The CEM system extracts hot stack gasses from the incinerator stack, and analyzes CO, CO2, HCl, SO2, NOX, and H20 concentrations using single-beam dual-wavelength and gas filter correlation methods. The CEM uses a zirconium-oxide sensor to measure oxygen concentration. The MCS100e uses a custom

[9] GE and Fanuc are registered trademarks of General Electric Company.

[10] Allen-Bradley and SLC 5/04 are registered trademarks of Rockwell Corporation.

[11] PanelMate Pro is a registered trademark of Eaton Corporation.

[12] MCS100e is a registered trademark of SICK MAIHAK inc.

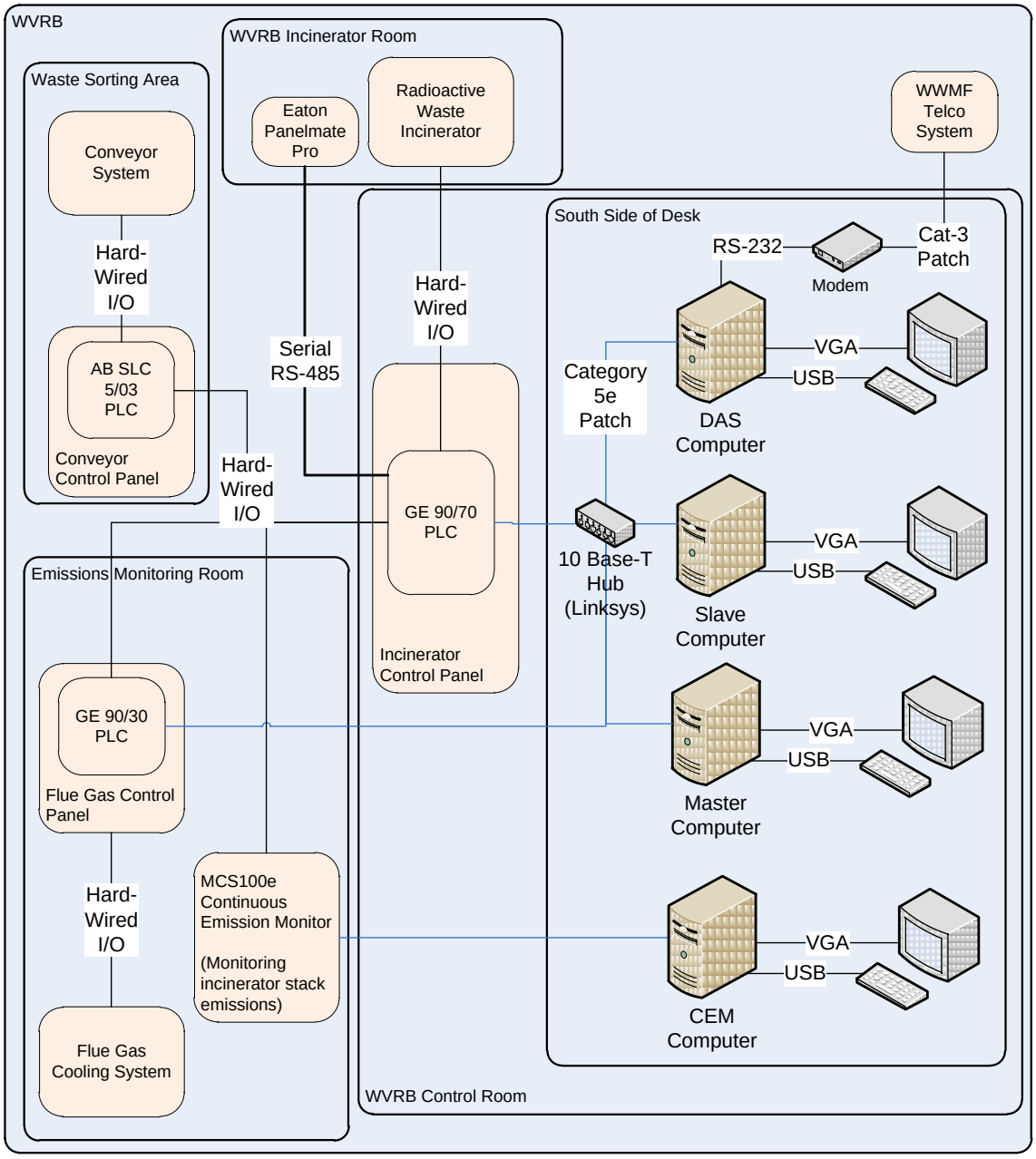

Figure 5 Existing SCADA System - Master, Slave, DAS, and CEM Computers

program running on a solid-state computer with an 80386 processor to control all of its functions. The MCS 100E operating system is MS-DOS[13].

The MCS 100E transmits real time CO, HCL, SO2, NOX, O2, and H20 concentrations directly to the incinerator GE 90/70 PLC using 4-20 mA analog loops. The incinerator PLC uses these readings to shut down waste feeds before emission values go out of compliance with the CofA.

[13] MS-DOS, Windows, and Windows XP are registered trademarks of Microsoft Corporation.

The MCS 100e was connected to a Windows XP based Pentium 4 IBM clone PC on the control room desk via a direct Ethernet connection (no hubs or switches). The clone PC was called the CEM computer. The CEM (Continuous Emissions Monitor) computer ran a program called CEMView[14] server. CEMView server collected real-time data from the MCS 100e and logged the historical data to its local database. CEMView performed calculations on the real-time data, generating all reports and summaries required to demonstrate compliance with the CofA. The CEMView user interface provided the control room operator with a real-time display of all regulatory emissions, warnings to alert the operator that emission levels approached the CofA limits, and alarms to indicate exceedance conditions and equipment malfunctions.

2.3.5 The Dry Storage Facility (DSF) Computer

The WUFDSF building management system uses eleven Allen-Bradley FlexLogix[15] PLCs to control the building air handling units, heaters, chillers, and ventilation fans. All eleven PLCs communicate with each other using the ControlNet protocol over a dedicated trunk line tri-axial cable network.

A media converter panel located in the WUFDSF electrical room converted and transmitted the ControlNet signal over two pairs of 62.5 multimode fibers inside an inter-building cable that runs from the WUFDSF electrical room to the WVRB control room. A similar media converter panel in the WVRB control room converted the optical signal back into a ControlNet signal on a tri-axial cable. The tri-axial cable connected directly to a ControlNet bus interface card (1784-PCIC) in the back of a Pentium III computer on the WVRB control room desk. The Pentium III computer was referred to as the DSF (Dry Storage Facility) computer.

The DSF computer ran Allen-Bradley RS-View 32 SCADA software. The custom RSView 32 software monitored all alarms from the WUFDSF building management system, providing visual and audio notifications of all alarms. Refer to Figure 6 for a diagram of the existing DSF computer, and the equipment that it monitored and controlled.

3. SYSTEM DEFICIENCIES

3.1 Background

In 2007 the WWMF Low and Intermediate Level Waste (L&ILW) technical support section conducted a review of outstanding corrective maintenance work. Technical support divided all work on a system by system basis. One system under review was the WWMF SCADA system. While working with the control maintenance group to assess all outstanding maintenance items, technical support identified numerous SCADA system deficiencies.

3.2 Existing system deficiencies

3.2.1 Segmented system

The existing control room SCADA system had six computers connected to four different networks. The Johnson, DSF, and CEM computers were on their own individual networks. The Master, Slave and DAS computers were connected to a fourth network. The existing SCADA system design did not take full advantage of the fact that all six computers could have co-existed

[14] CEMView is a registered trademark of Nexus Solutions Inc.

[15] FlexLogix, RS-View 32, and ControlNet are registered trademarks of Rockwell Corporation.

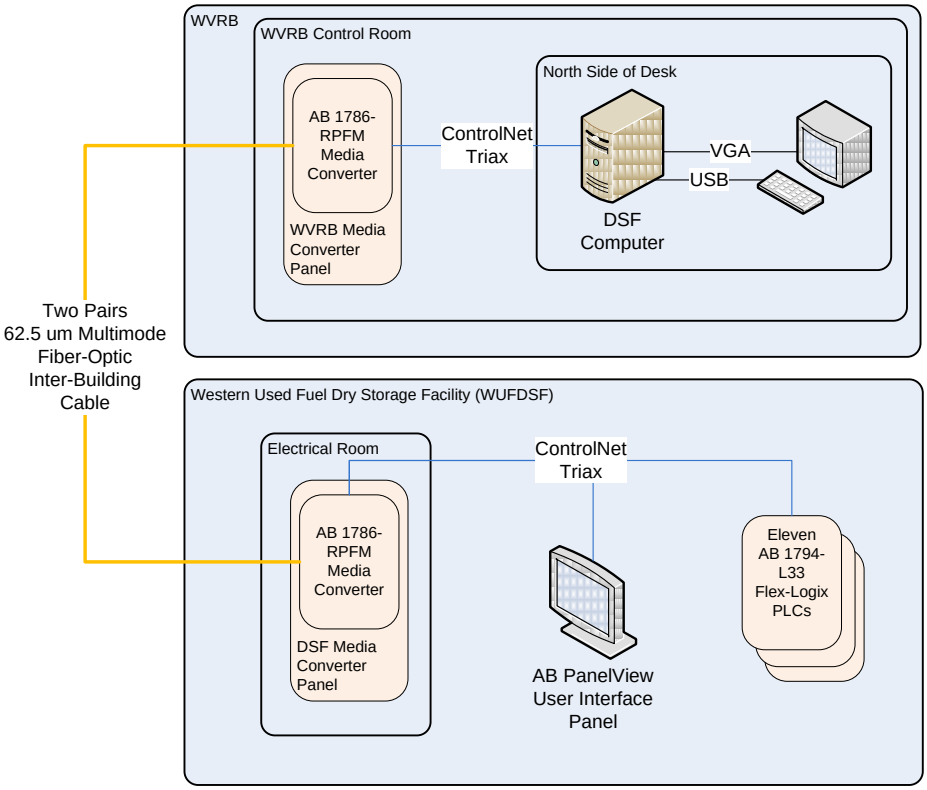

Figure 6 Existing SCADA System - DSF Computer

on the same Ethernet network. The design did not take advantage of the fact that the Master, Slave, DSF, and DAS computer applications could have been merged into a single unified SCADA application. The existing SCADA system was a segmented system, spread across four networks and multiple programs.

The Incinerator SCADA system stored all historical data for the incinerator systems on two computers. The Master computer sampled all incinerator process data once every minute, and stored the resulting records in a single Microsoft MSDE[16] database instance. Every week, the

Master computer would remove all one-minute records that were older than one week from its MSDE database, and export them to a CSV (Comma Separated Value) file on the local hard drive. The DAS computer performed the same function with incinerator stack emission data only.

The historical data on the Johnson computer was stored in proprietary format, with no software installed to export the data to a common file format (text file, Excel spreadsheet, etc.)

All historical data on the DSF computer was stored in memory, and then exported to text files on a daily basis.

The CEM computer would generate average values for each real-time emission value (1-minute, 30-minute, 1 day, etc.) and store them in a local instance of a Microsoft MSDE database. The only way to access historical data was to generate custom reports using the CEMView Reporting software, and to export the report to CSV or Excel format. All data older than 2 years would be

[16] MSDE is a registered trademark of Microsoft Corporation

archived to proprietary files, and could be temporarily re-imported into the MSDE database using the CEMView software.

All four systems stored data in various formats on completely different networks. This configuration hindered any attempt to review historical data in the following ways:

- Historical data files could be removed from the Master, Slave, CEM and DAS computers by USB key. The DSF computer USB ports no longer functioned properly. The CDRom bay on the DSF computer was used to house a cold-standby backup disk drive. The only way to get files off the DSF computer was to use a temporary Ethernet switch and patch-in to the computer using a laptop computer. Historical data could not be extracted from the Johnson computer at all.
- All historical data from the Master and DAS computers were available one week after the event. The historical data was stored in CSV files that contained every single process point for the entire system, sampled every minute. The only tool available to Technical Support to review the data was MS Access running on corporate workstations. Basic queries would take anywhere from 3 hours to several days to complete.
- The only way to compare historical data from the Master computer with data from the CEM computer was to extract the data separately from each system. Technical support had to use MS Access to correlate the data offline as both systems were not connected to each other.
- All historical data on the DSF computer was only available one day after the event. Any events that took place during the day were only available for viewing using RSView 32.
- The Johnson computer did not have any tools installed on it to retrieve historical data from its proprietary database.

Refer to Figure 7 for a diagram of all separate data sources.

3.2.2 Single points of failure

In 2006 L&ILW operations reported that the Johnson computer failed to reboot after a power failure. The error message on screen stated that the computer's primary hard drive failed. The hard drive resumed operation when the operators cycled power to the computer a second time. The operator reported the failure by issuing a work request.

3.2.2.1 Johnson Computer

The Johnson computer diagnostic work order was on the maintenance backlog for the SCADA system, and was identified as a priority item by technical support. Technical support decided to replace the hard drive on the computer, and transfer the contents from the old drive to the new one. During the hard drive replacement work, the hard drive imaging software failed in mid operation and all data on the original drive was lost. Technical support had to restore all factory installed software on the Johnson computer from scratch. Over four years of historical data on the building management system was lost, as were numerous corrections and small changes applied to the user interface over the lifetime of the system.

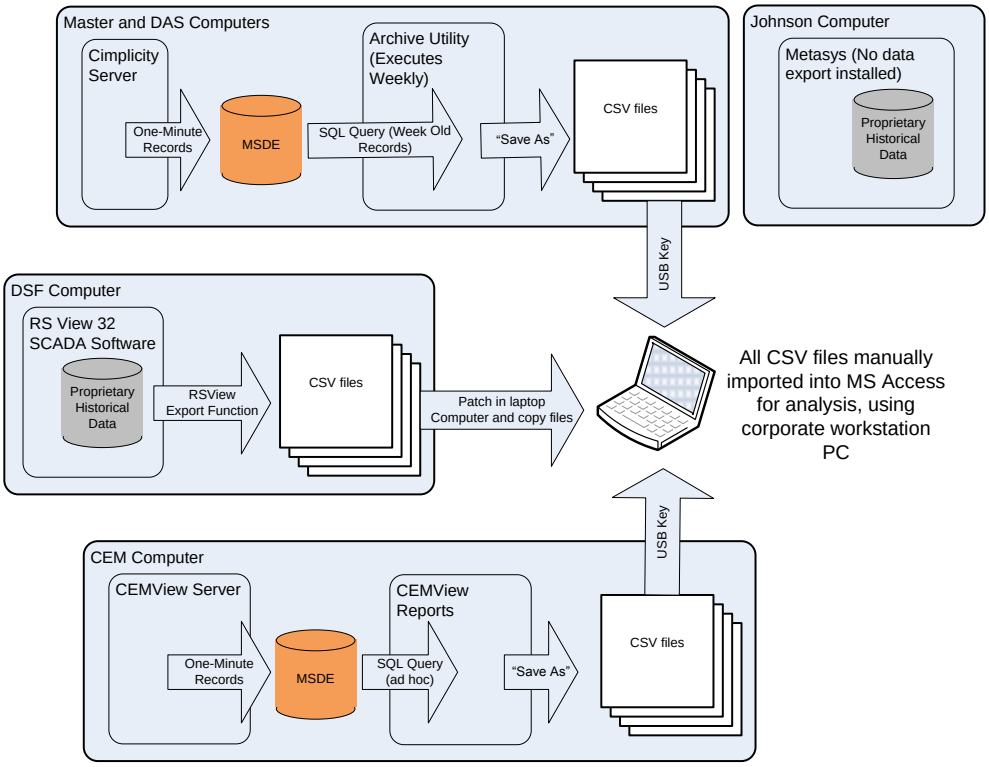

Figure 7 Existing SCADA System - Separate Data Sources

While the Johnson computer was out of service, the WVRB operators had to start an unplanned fire-watch of the low level storage buildings. All heating and ventilation systems in the WVRB and in the TPMB could only run in the last known state. The software restoration work on the Johnson computer took approximately 6 hours to complete. The failure of a single computer disabled monitoring and control of the building ventilation systems in two buildings, added unplanned work to the schedule, created a substantial loss of historical data, and restored legacy software errors. The Johnson computer failure prompted technical support to investigate the possibility of similar problems on all other SCADA system computers.

3.2.2.2 DSF Computer

The DSF computer was the only computer in the WWMF SCADA system that monitored alarms from the Dry Fuel Storage Facility. The CDROM drive was removed and replaced with a cold standby hard disk drive. The cold standby drive contained a version of the operating system and the RSView32 SCADA software that was 3 years old. Control maintenance did not have any periodic maintenance tasks to re-copy the active drive to the backup drive.

The DSF computer was in a similar same state as the Johnson computer. Failure of the computer operating system would require a restoration of the hard drive contents from the cold standby drive. The restoration would take 4 to 6 hours to complete with no alarm monitoring function available during that time. The restoration would eliminate all historical data and would leave the system with a legacy version of the user interface software.

3.2.2.3 Master Slave and DAS computers

The Master computer sent a copy of all of its process data to the Slave computer. The Slave computer would use the data from the Master computer to display a second set of user interface screens for the operator.

Any failure of the Master computer would result in the following:

- a complete loss of monitoring and control functions on both the Master and Slave computers, resulting in a forced shutdown of the incinerator (using the PanelMate Pro in the incinerator room),
- a complete loss of all historical data, and
- The restoration of all legacy user interface problems, as the application would have to be restored from the vendor's backups.

Any failure of the DAS computer would leave the operator unable to prevent waste lockout conditions before they happened. This would leave the facility at increased risk for MOE reportable excess emission events. Similar to the Master and Slave computers, the DAS computer would suffer a complete loss of all historical data and the restoration of legacy user interface errors.

3.2.2.4 CEM Computer

The CEM computer used a Redundant Array of Independent Disks (RAID) array consisting of two 100 GB hard drives. The RAID array held a duplicate copy of all of the computer software and historical data in real-time on two hard drives. A failure of one of the hard drives would leave the system functioning on one drive until the faulty drive was replaced.

The RAID array protected the CEM computer against physical failure. The CEM computer did not have any measures in place to protect against a software failure. If the operating system was corrupted for any reason, the software error would be instantly copied to both RAID drives leaving the computer inoperable.

The CofA requires 95% quarterly availability on all measured components from the CEM. The CEM computer (or any component of the emission monitoring system including the MCS100e) can be out of service for a maximum of 70 hours per calendar quarter. The incinerator takes at least 24 hours to bring cool down to an "out of service" status (secondary chamber temperature less than 500 degrees Celsius). Any failure of the CEMView software or computer operating system would leave the incinerator system in non-compliance with the CofA in less than 46 hours.

The failure of a single computer on any of the four SCADA systems would shut down or disable a key system in the WWMF. Refer to Figure 8 for a diagram of the four single points of failure, and their impact on WWMF systems.

3.2.3 Lack of routine maintenance

When control maintenance staff opened the Johnson computer to install the new hard drive, they observed that the inside of the computer was covered in a thick layer of dust. A follow-up inspection of all of the other SCADA system computers revealed the same situation.

Technical support conducted a review of the routine maintenance tasks in the WVRB control room. The maintenance tasks did not include a task to clean dust out the control room computers, or to back up the operating system files, and historical data.

3.2.4 Little consideration for future expansion

All six computers were very slow to reboot with very little room for future expansion. The DAS computer was constantly running at near 100% CPU utilization and took approximately 10 minutes to shut down and reboot. The Master computer hard drive was 75% filled. The weekly CSV files had to be removed quarterly to prevent the hard drive from filling up and locking up the entire incinerator SCADA system. The Johnson and DSF computer hard drives were more than 80 percent filled and also took approximately 8 minutes to shutdown and reboot.

Any new program in the WWMF SCADA system would require a new computer[17].

[17] The CEM computer was dedicated to the CEMView software due to the regulatory reporting requirement function that it carried out.

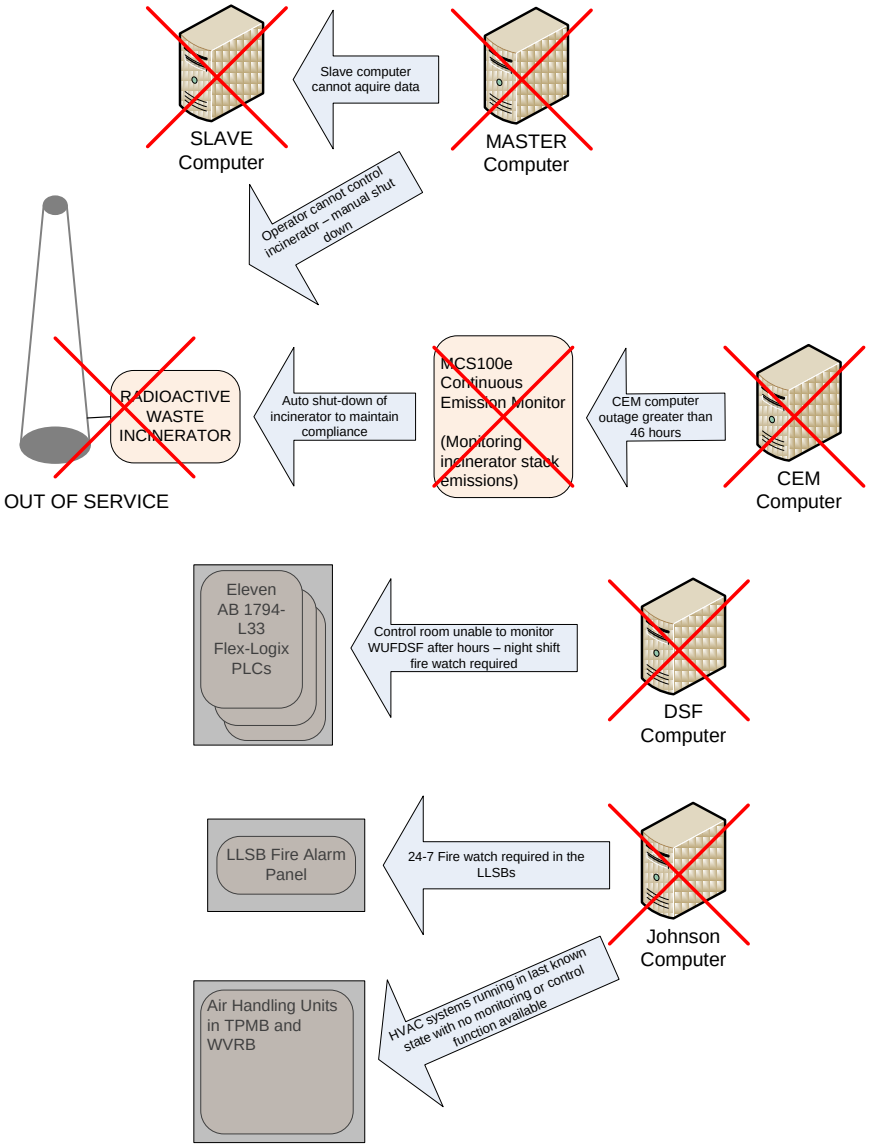

Figure 8 Existing SCADA System - Four Single Points of Failure

3.2.5 Control room desk clutter

The WVRB Control Room SCADA system used six computers, each with their own CRT style monitors, and with their own keyboard and mouse. Six keyboards, mice, and CRT style monitors occupied more than half of the control room desk. The Johnson, DAS, and DSF computers rarely needed operator use, showing the same screen all of the time. The DSF and DAS computer monitors exhibited "phosphor burn-in".

The six SCADA computers were attached to the control room desk using small metal shelves attached to the underside of the desktop. The computers occupied a large quantity of the leg room under the desk for the operator. On two occasions, operators accidentally switched off a computer with their knee while they were seated at the desk. The computers could not be placed

on top of the desk due to the large amount of space already taken by the monitors, keyboards and mice.

The underside of the desk only had two receptacles (on the same 15A circuit) for plugging in all six computers. The underside of the desk was cluttered with communications cables, extension cables, power bars, and two desktop style UPS units sitting on the floor.

4. DESIGN

In June of 2007 technical support developed a detailed design for the WVRB Control Room Upgrades project. The overall design included modifications to the control room with the goal of reducing or eliminating all of the deficiencies identified in the current system. A description of the design is as follows:

4.1 Control Room Desk Upgrades

Remove all computer equipment, power cables, extension cords, data cables, and UPSs from the control room desk.

Run four new 20A 120VAC circuits to the control room desk. Two circuits will be fed from facility UPS (Class II) power, and will provide two receptacles per circuit under the north side of the control room desk. Two circuits will be fed from facility main (Class IV) power and will provide 2 receptacles per circuit on the south side of the control room desk. Provide one additional Class IV receptacle on each circuit under the east of the control room desk, and a second receptacle on each circuit on the west side. Run all power circuits under the desk in aluminum conduit, painted flat black.

Install a new Category 6 Ethernet structured cabling system in the WVRB control room, compliant with the Telecommunications Industry Association / Electronic Industries Alliance TIA/EIA568 cabling standard. Install 4-port office Ethernet jacks to service laptop computer connections on the north, south, east, and west side of the control room desk. Run two 62.5 multimode fiber patch cables (with ST style connectors) from the location of panel P1000 (see section 4.2 PL1000) to a breakout box underneath the control room desk on the north side.

4.2 PL1000

Install a new APC NetShelter AR3150[18] network enclosure in the WVRB control room (referred to as PL1000). PL1000 is an EIA-310-E compliant 750mm network rack enclosure (1070mm deep) with 42 U height. PL1000 will be the Main Cross-Connect cabinet for the WWMF SCADA system. Refer to Figure 9 for a diagram of PL1000 and its internal components.

[18] Netshelter is a registered trademark of American Power Corporation (APC).

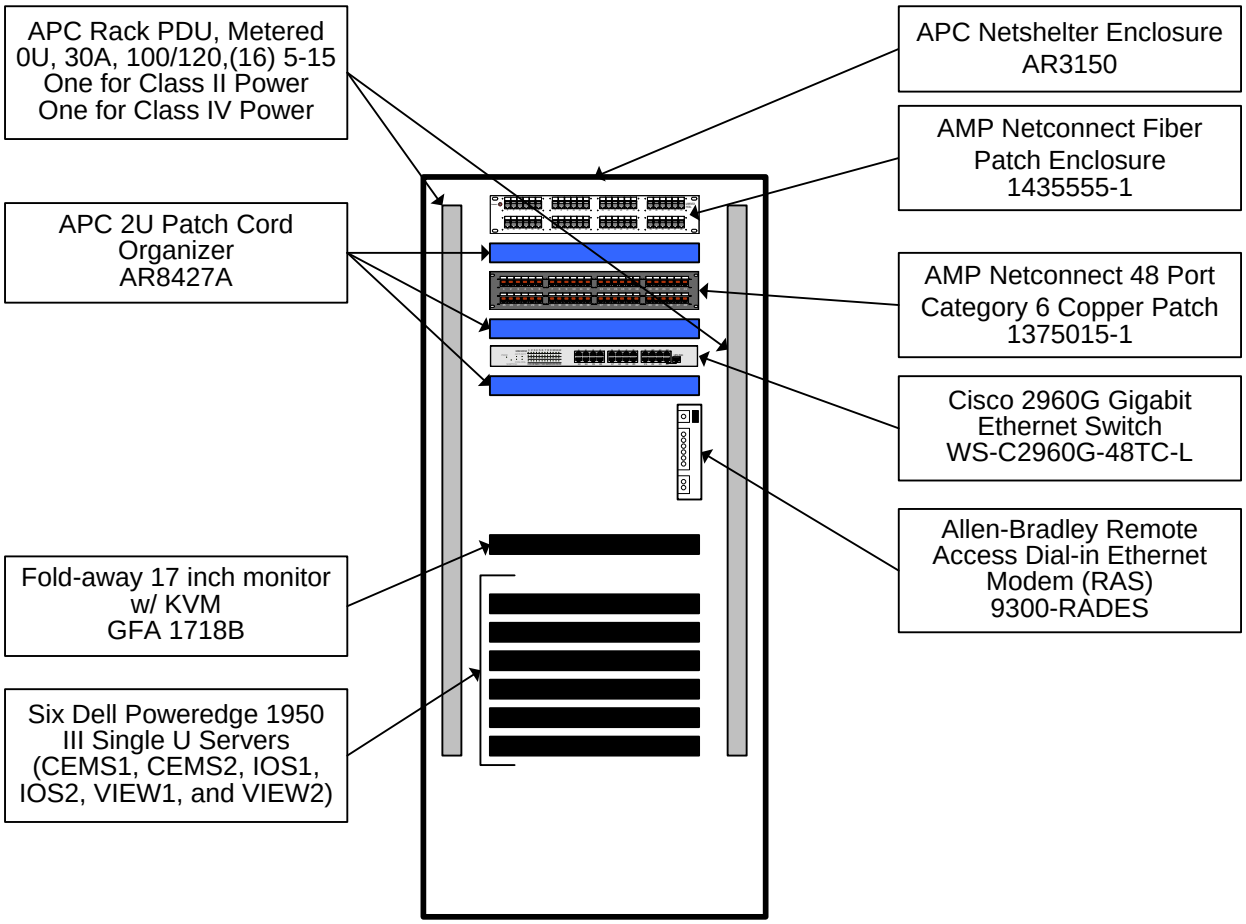

Figure 9 PL1000 Layout

4.2.1 Power

Provide two dedicated 20A 120VAC power circuits to PL1000. Once circuit must be fed from UPS-backed Class II power and one circuit must be fed from facility Class IV power. Install two Power Distribution Units (PDUs) in the back of PL1000, one for Class II power, and one for Class IV power. Each PDU provides eight 15A plug-in receptacles for the 20A circuit feed.

4.2.2 Terminations

Install one 48-port copper patch panel in PL1000. Terminate all Category-6 Ethernet cables from the control room desk at the patch panel. Install one 1-U fiber patch panel in PL1000 with six ST-style pass-through bulkheads, and spare space for 18 more bulkheads. Terminate the two patch cords from the control room desk in the patch panel.

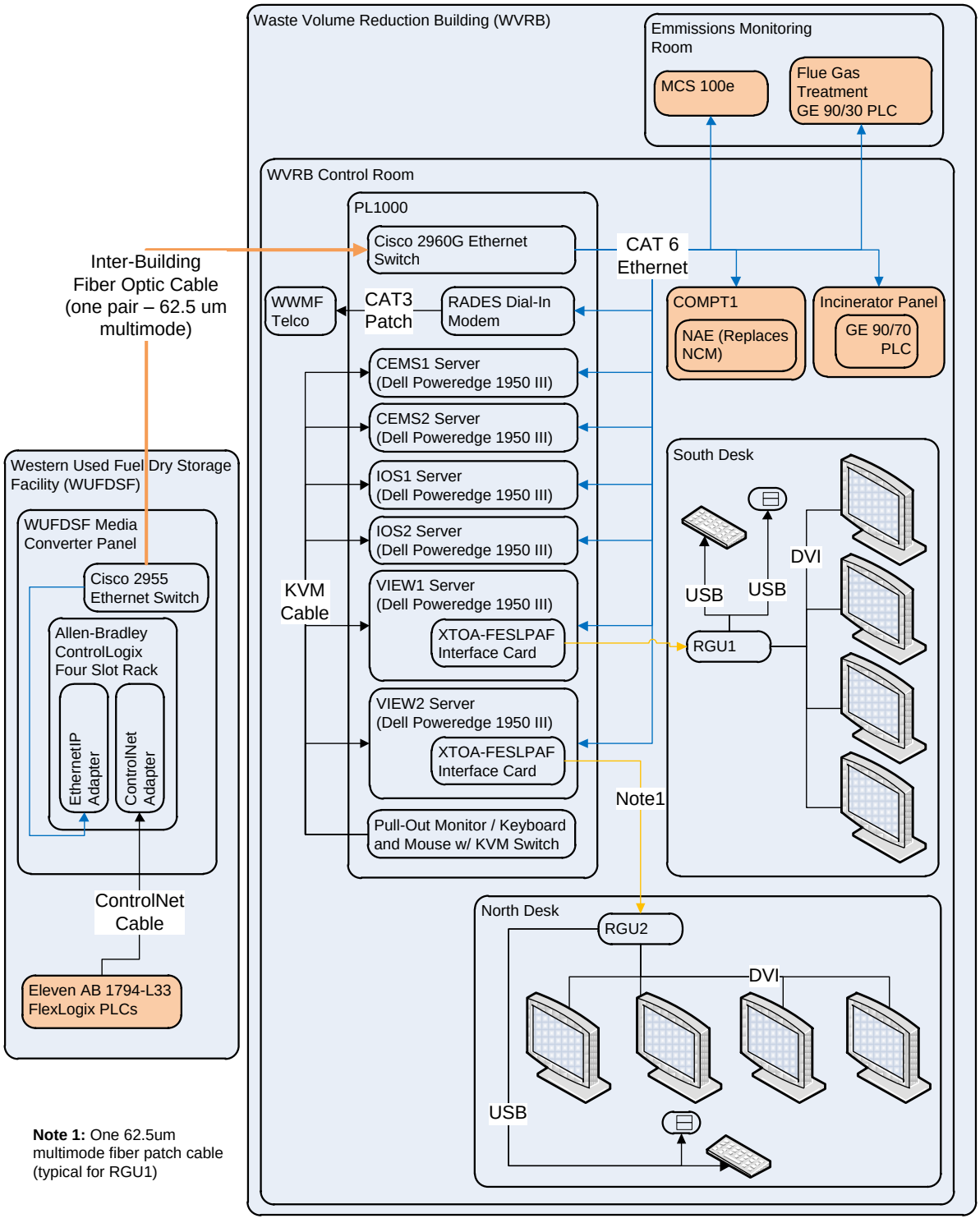

Figure 10 New SCADA System - Hardware Architecture

4.2.3 Switchgear

Install one Cisco Catalyst 2960G[19] copper Ethernet switch in PL1000. The Ethernet switch is a layer 3 switch with 44 copper gigabit ports, and four multi-purpose gigabit fiber uplink ports. The Ethernet switch is the core switch for the WWMF SCADA system. The MCS100e, incinerator PLC, Johnson System NAE, DSF switch and all six new servers will connect to the Cisco Switch in PL1000.

4.2.4 Dial-In

Install one Allen-Bradley Remote Access Server (RAS) dial-in modem in PL1000. Use a copper patch cable to connect the Ethernet port on the RAS in PL1000 to the Ethernet switch. Run one category 3 patch cable from the telephone jack on the RAS in PL1000 to the telephone jack on the north side of the control room. Refer to Figure 10 for a diagram of the new SCADA system hardware layout.

4.2.5 Servers

Install six new Dell Poweredge[20] 1950-III severs in PL1000. Each server comes with Microsoft Windows Server[21] 2003 factory-installed. Install and configure all software to perform the following functions on each server:

4.2.5.1 CEMS1 - WVRB CEM SERVER PRIMARY

CEMS1 is the primary CEMView server, responsible for continuously monitoring the MCS100e, historically logging all emission values, and generating all reports to document compliance with the CofA. Provide 120 VAC power to CEMS1 from UPS-backed Class II power. Install and configure the following software on this server:

- CEMView Server High Availability Primary: Performs all CEMView functions and synchronizes with the Backup node in real time.
- Microsoft SQL Server Standard 2005: The database back-end for CEMView server.
- Diskeeper[22] 2010: Hard drive optimization software
- Acronis Driveimage[23]: Automated hard drive imaging software

Upgrade the current CEMView configuration on the CEM computer and import it into the CEMView Server installation on CEMS1. Export all historical data from the CEM computer, and import it into the database on CEMS1.

[19] Catalyst is a registered trademark of Cisco Systems Inc.

[20] Poweredge is a registered trademark of Dell Corporation.

[21] Windows Server and SQL Server are registered trademarks of Microsoft Corporation.

[22] Diskeeper is a registered trademark of Diskeeper Corporation.

[23] Driveimage is a registered trademark of Acronis Inc.

4.2.5.2 CEMS2 - WVRB CEM SERVER BACKUP

CEMS2 is the backup CEMView server, responsible for continuously monitoring the MCS100e, historically logging all emission values, and generating all reports to document compliance with the CofA when the primary server has failed. Provide 120 VAC power to CEMS2 from facility Class IV power. Install and configure the following software on this server:

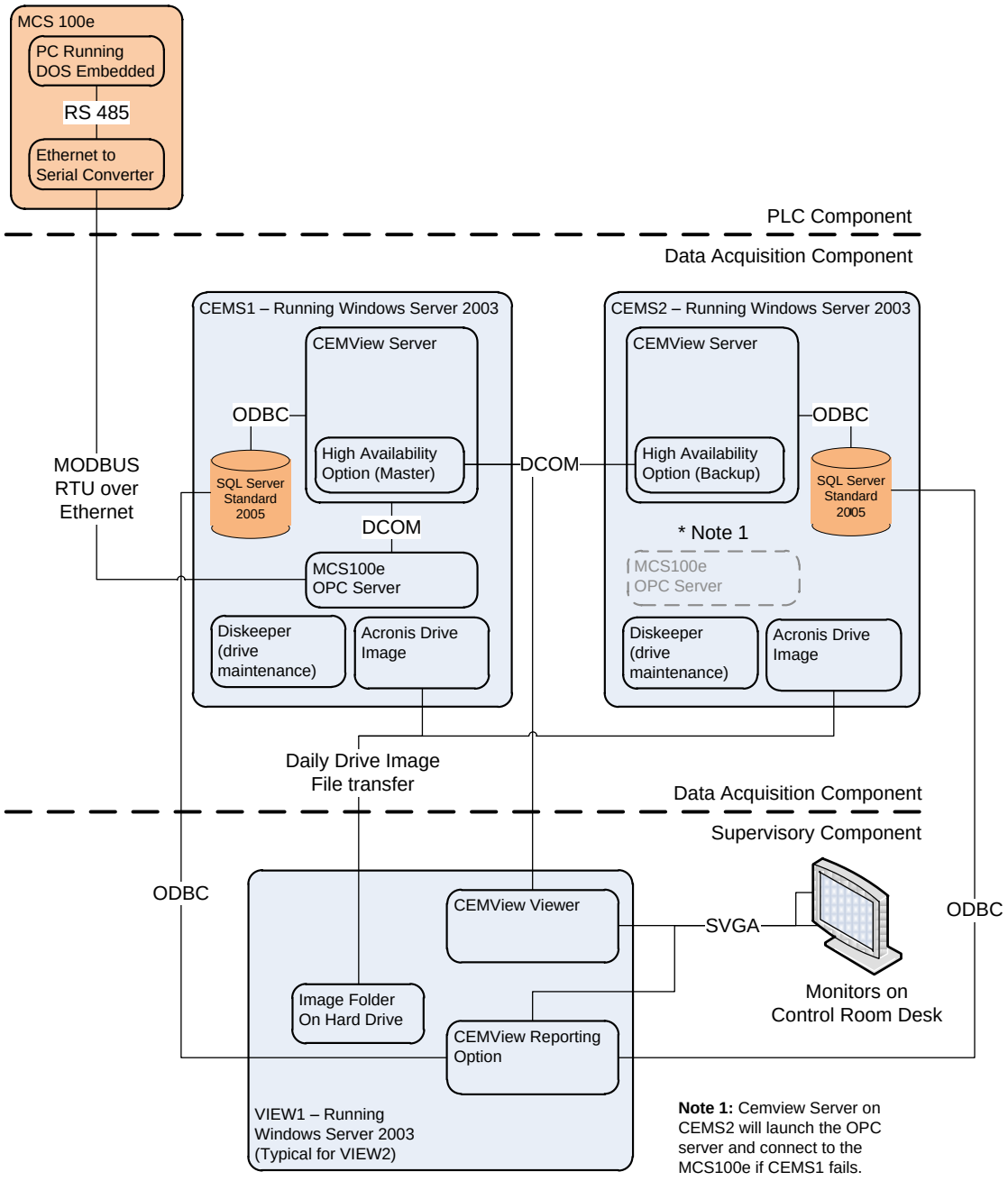

Figure 11 New SCADA System – CEMS Server Software Architecture

- CEMView Server High Availability Backup: Performs all CEMView functions when the primary server has failed.
- Microsoft SQL Server Standard 2005: The database back-end for CEMView server.
- Diskeeper 2010: Hard drive optimization software
- Acronis Driveimage: Automated hard drive imaging software

Install a duplicate copy of the configuration stored in CEMS1 on the CEMS2. Import a copy of all historical data from CEMS1 into CEMS2.

Refer to Figure 11 for a diagram of the CEMS and VIEW SCADA server software architecture.

4.2.5.3 IOS1 – WVRB IO SERVER 1 (PRIMARY)

IOS1 provides the main SCADA server for the WVRB incinerator, and all auxiliary systems. Provide 120 VAC power to IOS1 from UPS-backed Class II power. Install and configure the following software on this server:

- Cimplicity HMI Server Redundant Master: SCADA server software for the WWMF facility
- Metasys SCT and Archive Utility: Facility management software for Johnson Controls NAE
- Microsoft SQL Server Standard 2005: The database back-end for CEMView server and Metasys SCT
- RSLinx[24] Professional: Communications gateway server for the Flexlogix PLCs in the WUFSDF
- Diskeeper 2010: Hard drive optimization software
- Acronis Driveimage: Automated hard drive imaging software

Move the custom SCADA application running on the Master and Slave computer to the Cimplicity HMI Server program running on IOS1. Take the custom Cimplicity HMI SCADA application running on the DAS computer and integrate it into the program running on IOS1.

4.2.5.4 IOS2 – WVRB IO SERVER 2 (BACKUP)

IOS2 provides the main SCADA server for the WVRB incinerator, and all auxiliary systems when the primary server has failed. Provide 120 VAC power to IOS2 from facility Class IV power. Install and configure the following software on this server:

- Cimplicity HMI Server Redundant Backup: SCADA server software for the WWMF facility.
- Microsoft SQL Server Standard 2005: The database back-end for CEMView server
- RSLinx Professional: Communications gateway server for the Flexlogix PLCs in the WUFSDF
- Diskeeper 2010: Hard drive optimization software

[24] RSLinx, ControlNet, and EthernetIP are registered trademarks of Rockwell Corporation.

- Acronis Driveimage: Automated hard drive imaging software

4.2.5.5 VIEW1 – WVRB VIEW NODE1

VIEW1 provides the user interface for the monitors on the north side of the control room desk. Provide 120 VAC power to VIEW1 from UPS-backed Class II power. Install and configure the following software on this server:

- Cimplicity CimView: SCADA Viewer software for the WWMF facility
- CEMView: User interface for the CEMView Server software (monitoring the MCS100e)
- Diskeeper 2010: Hard drive optimization software
- Acronis Driveimage: Automated hard drive imaging software

4.2.5.6 VIEW2 – WVRB VIEW NODE2

VIEW2 provides the user interface for the monitors on the south side of the control room desk. Provide 120 VAC power to VIEW2 from facility Class IV power. Install and configure the following software on this server:

- Cimplicity CimView: SCADA Viewer software for the WWMF facility
- CEMView: User interface for the CEMView Server software (monitoring the MCS100e)
- Diskeeper 2010: Hard drive optimization software
- Acronis Driveimage: Automated hard drive imaging software

Refer to Figure 12 for a diagram of the IOS and VIEW SCADA server software architecture.

4.3 User Interface Upgrades

Replace the existing control room monitors with eight 20" flat panel monitors with native resolution of 1280x1024 pixels. Locate four monitors on the south side of the control room desk (Monitor1, 2, 3, and 4). Locate four monitors on the north side of the control room desk (Monitor 5, 6, 7, and 8). Mount all eight monitors on swivel mounts providing three axes of motion.

Install one four-port Matrox Extio[25] F1400 RGU (Remote Graphics Unit) on the south side of the control room desk (RGU1), and one on the north side of the control room desk (RGU2). Each RGU must be mounted on the underside of the desk, set half way to the back of the desk. Run one 62.5 multimode fiber patch cable from the back of each RGU to the fiber break-out box under the control room desk. Install one Matrox XTOA-FESLPAF interface card in the first available PCI slot in the back each VIEW server. Run one 62.5 multimode fiber patch cable from the interface card on VIEW1 to the fiber patch port in PL1000 that is connected to RGU1. Run a second patch cable for VIEW2 and RGU2.

Connect one standard 101 key USB keyboard and one optical USB mouse in each RGU.

Configure the operating system on the VIEW1 and VIEW2 server to use the four monitors connected to the RGU for the consol desktop. Spread the desktop horizontally across all four monitors. Create one "Operator" user on VIEW1 and VIEW2 with a locked-down desktop. The desktop will only allow the user to run all operator interface programs and log out the current

[25] Extio is a registered trademark of Matrox Corporation.

user. The Operator user desktop will ignore all new hardware plugged into the USB port (no auto-run).

Create one user on all six servers for control maintenance. The control maintenance user will have all of the privileges of the operator user and read-only access to all configuration files. The control maintenance user will not have a locked-down desktop. Control maintenance will not be able to change any operating system settings.

The administrator user on each server will have full access to the operating system.

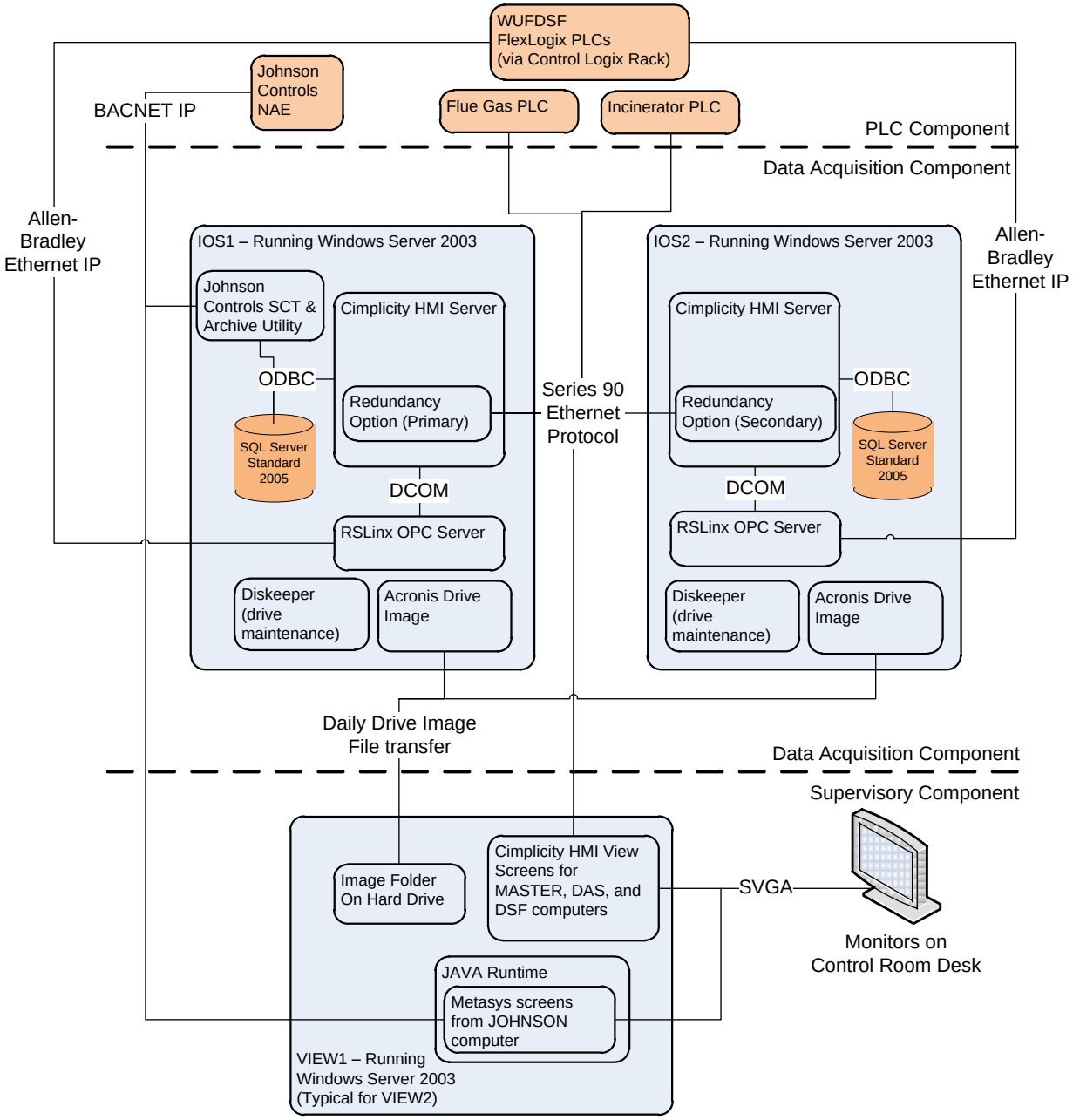

Figure 12 New SCADA System – IOS Server Software Architecture

4.4 Johnson System Upgrade

Remove the Johnson Controls Network Control Module (NCM) from panel COMPT1 in the WVRB control room. Replace the NCM with a new Network Automation Engine (NAE) controller. Upload the Metasys application installed on the Johnson computer to the processor on the NAE. Configure the web browser on VIEW1 and VIEW2 to launch the JAVA[26] Runtime Engine and run the Johnson Controls user interface directly from the NAE. Install the Metasys Archive utility on the IOS1 server. Configure the archive utility to remove all historical alarm, trend and audit records from the NAE memory, and archive the records to the SQL server instance on IOS1.

4.5 WUFDSF Upgrade

Remove the fiber media converter panel on each end of the WUFDSF inter-building fiber cable. Terminate the two fiber pairs in the WVRB control room to the patch panel in PL1000. Run one 62.5 um multimode patch cable from the patch panel port to one of the fiber uplink ports on the Ethernet switch in PL1000.

Replace the media converter panel in the WUFDSF with a new panel consisting of the following hardware:

- one Allen-Bradley ControlLogix four slot rack and power supply,
- one Allen-Bradley ControlNet adapter card mounted in the four slot rack,
- one Allen-Bradley EthernetIP adapter card mounted in the four slot rack, and
- one Cisco Catalyst 2955 Layer 3 Ethernet switch with 12 copper gigabit ports and two 62.5 um multimode fiber uplink ports.

Connect the WUFDSF ControlNet network to the ControlNet card. Run one copper patch cable from the EthernetIP card to the Cisco switch. Configure the MAC Address security on the Ethernet switch in PL1000 to communicate exclusively with the EthernetIP card at WUFDSF.

Convert the SCADA application running on the DSF computer into a Cimplicity HMI application, and integrate the new application into the Cimplicity HMI application installed on IOS1.

Configure RSLinx running on IOS1 to route all information from the WUFDSF building management system to the local Cimplicity HMI instance. Duplicate the configuration on IOS2.

4.6 Routine maintenance

Technical support developed a routine maintenance plan for the new WWMF SCADA system. The maintenance plan was designed to address two main concerns for system reliability:

1. Software and data archival
2. Hardware preventative maintenance

Technical support configured Acronis DriveImage on each server to take a daily image of the entire RAID image and store two copies of the image file. One image file is stored on the VIEW1 server, and the other image file is stored on the VIEW2 server. If a server image file

[26] JAVA is a registered trademark of Sun Microsystems.

cannot fit onto a single layer DVD (4.7 Gb), Acronis splits the image into multiple files. Each daily image file overwrites the previous image file. The maintenance plan calls for control maintenance staff to burn all of the images to DVD every month.

The maintenance plan includes a quarterly inspection task. The inspection task calls for control maintenance to perform the following on each server in PL1000:

1. Shut down the server, and remove it from PL1000.
2. Take the server from the control room, into the control shop and place the server onto a static free mat under an exhaust hood.
3. Remove the server cover and inspect the server for any signs of electrical burns or damage.
4. Use CO2 to blow off any dust from the server internals. Remove the power supply, ventilation fans, and hard drive. Remove any dust from the server components.
5. Re-assemble the server and return it to PL1000.
6. Power up the server and confirm that all communications alarms for that server have been reset.

PL1000 contains six servers in three groups of two redundant pairs (IOS1/2, CEMS1/2, and VIEW1/2). Operations can continue to monitor and operate the facility while the inspection and dust removal work is in progress.

5. PROJECT EXECUTION

At the start of the upgrade project control maintenance re-located the Master, DSF, and Johnson computers to a temporary desk in the entry foyer of the control room[27]. Control maintenance moved all other computers from the control room to a temporary storage area (offline). Once the control room desk was cleared, the contractor performed the following work:

- Install all power and data receptacles in and around the control room desk.
- Install and assemble PL1000, complete with network terminations, six Dell Poweredge servers, and Ethernet switchgear.
- Install the new media converter in the WUFDSF electrical room and re-terminate the WVRB-DSF inter-building fiber optic cable.
- Remove the NCM from the COMPT1 panel and replace it with the NAE controller.
- Install the new flat-panel monitors on the control room desk
- Install the RGUs under the control room desk and terminate the fiber-optic connections to the VIEW1 and VIEW2 servers.

Refer to Figure 13 of a diagram of the temporary control room setup.

[27] The control room upgrades work took place during a planned incinerator outage. The DAS and CEM computers were not required during the outage. The Slave computer was redundant in the original configuration; hence the temporary configuration did not include it.

Once the contractor completed all power and data system continuity tests, OPG control maintenance staff relocated the old computers to the south side of the control room desk. The old computers were temporarily connected to the new monitors, and all building communications took place via the new control room LAN. Tehnical support performed minor changes to the old computers to allow the old computers to use the new LAN.

The contractor connected the four flat panel monitors on the north side of the control room desk to RGU2. Technical support powered up and configured all operator interface software on the VIEW1 and VIEW2 servers (CEMView and Cimview). Technical support configured the four-monitor display on the north side of the control room desk to "stretch" the VIEW2 console desktop horizontally across all four monitors. Finally, technical support staff installed and configured all software on CEMS1, CEMS2, IOS1, and IOS2. Technical support transferred the application running on the Johnson computer to the NAE, and configured the Java Runtime Engine on the DSF computer to run the Johnson computer application. Refer to Figure 14 for a diagram of the control room commissioning setup.

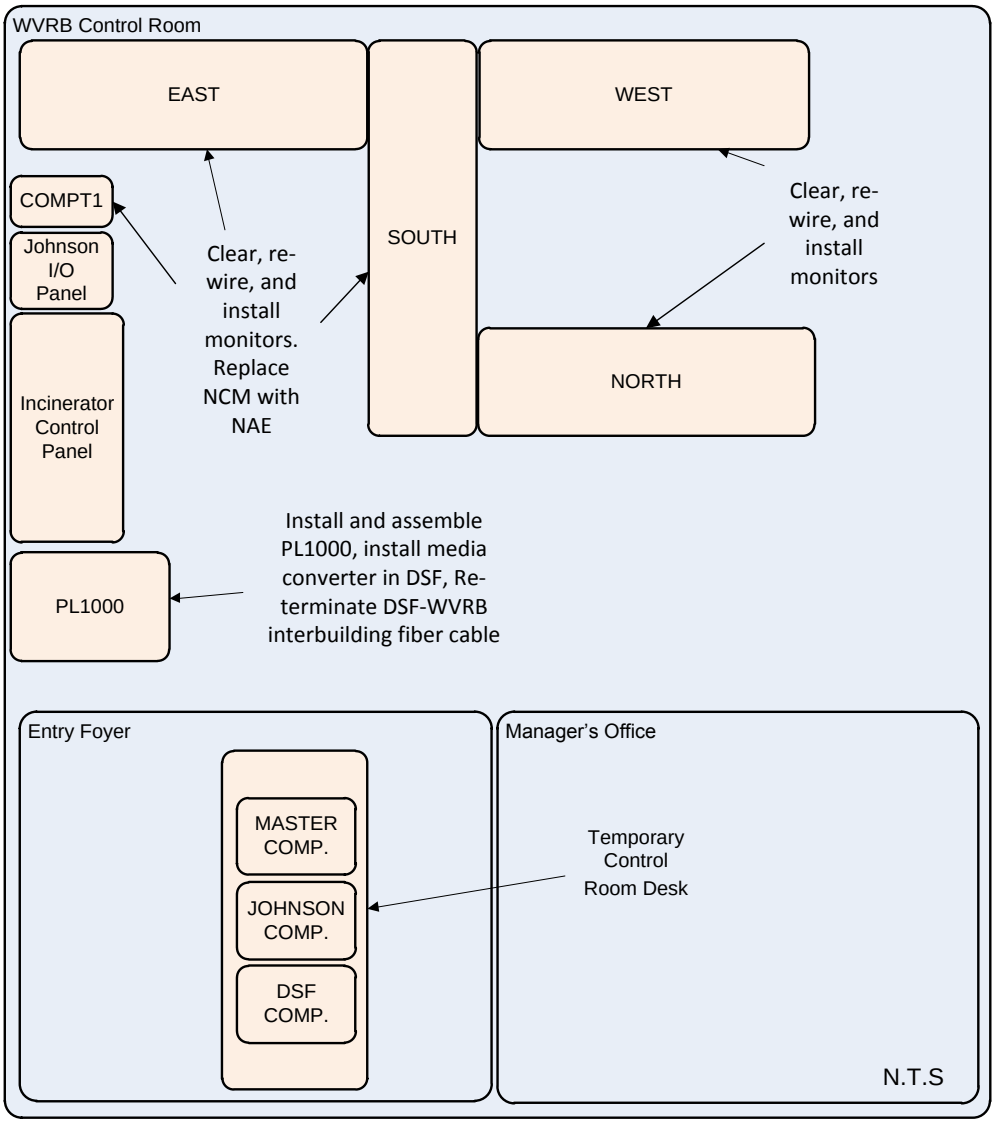

Figure 13 Installation - Temporary Control Room

During the routine incinerator outage in Q1 2009, technical support staff scheduled and carried out the commissioning of the six new servers using the monitors connected to VIEW2. The commissioning started with the CEMView servers (CEMS1 and CEMS2). Operations staff shut down the old CEMView application. Technical support transferred all historical records over to CEMView Server running on the CEMS1 and CEMS2 servers. Technical support launched the new CEMView application and operations staff commissioned the new CEMView installation by performing the following tasks:

1. Operations: Power up the MCS100e, and allow the system to run with ambient air.
2. Technical Support: Confirm that the CEMView system can communicate with the MCS100e, and confirm that the readings on the server screens match those on the MCS100e front panel.
3. Operations: Use the CEMView software to initiate an auto calibration sequence on the MCS100e.
4. Technical Support: Confirm that the results from the calibration report match those found on the MCS100e display screen.
5. Operations: At the end of the incinerator outage, bring the incinerator up to operating temperature using propane only
6. Technical Support: Confirm that the secondary chamber temperature readings on CEMView match those on the MCS100e display screen.
7. Technical Support: Confirm that all real-time gas emissions match the MCS100e display screen.
8. Operations: Initiate incinerator liquid waste feeds
9. Technical Support: Confirm that all real-time gas emissions match the MCS100e display screen.
10. Operations: Initiate incinerator solid waste feeds
11. Technical Support: Confirm that all real-time gas emissions match the MCS100e display screen.

At the end of the Q1 2009 incinerator outage, technical support issued an operating procedure for the new SCADA system. The procedure provided operations with the following:

1. Instructions for opening and closing all applications on the new four-panel display.
2. Detailed instructions for allowing third-party access to the LAN using the remote dial-in equipment.
3. Instructions for non-standard operating conditions (power failures, error messages, screen failures etc).

The MCS100e allows only one client to connect to it at a time. During the trial period, the old CEMView computer was left in the control room powered down and disconnected on cold-

standby. Technical support provided operations a temporary instruction document that showed operations how to bring the old CEM computer back on line if the new system fails.

The new SCADA application on the north side of the control room desk was left running alongside the old system on the south side of the control room desk for four months. During this time, operations could monitor and control all equipment using both systems (old and new). Operations notified technical support of any functionality present in the old system (running on the south side of the control room desk) that was not carried over to the new system on the north side of the control room desk. Technical support restored system control functionality that was missing in the new system.

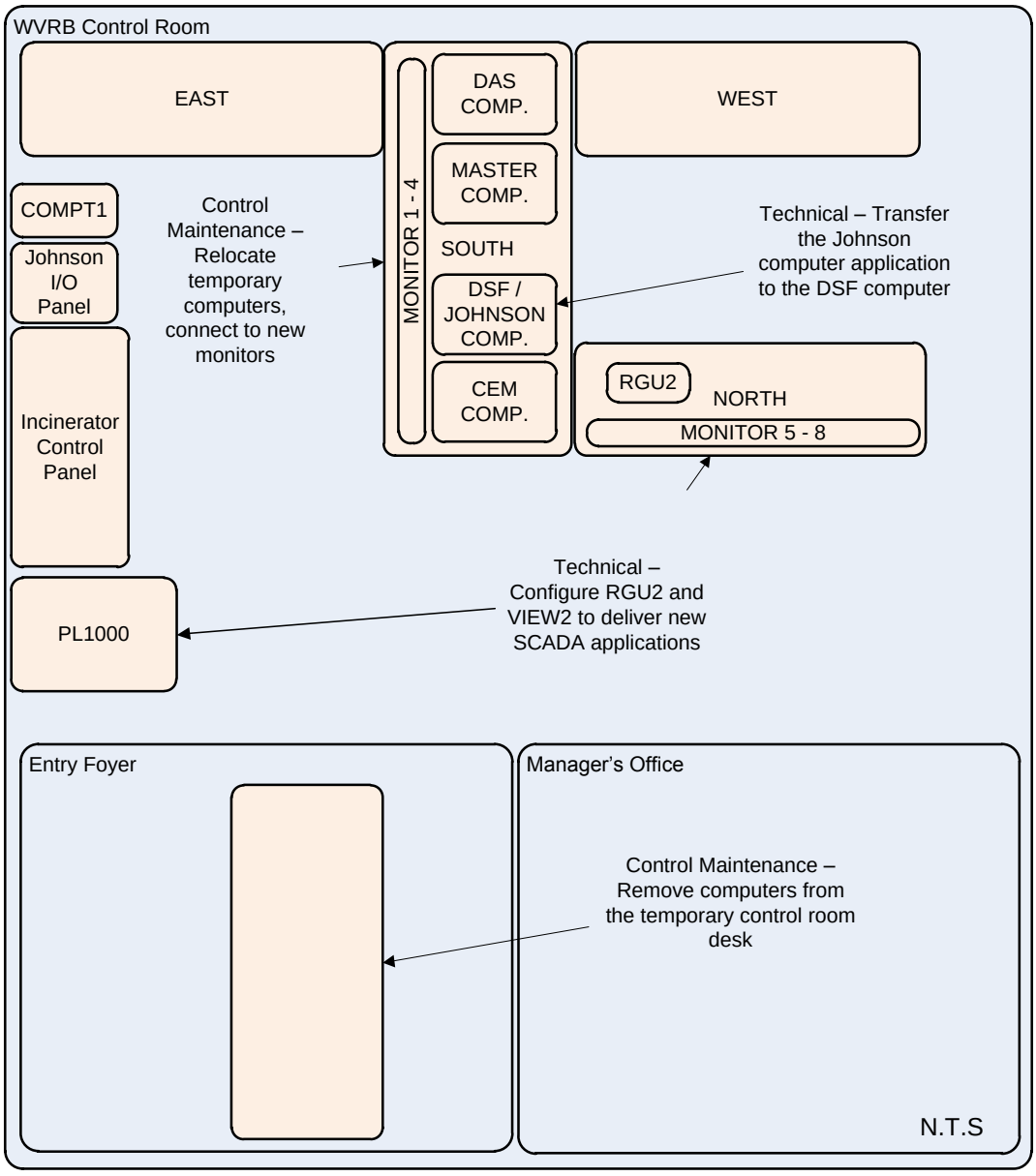

Figure 14 Installation - Commissioning Setup

After the four month test period and during a subsequent outage, control maintenance shut down and removed the old computers from the control room desk. Control maintenance connected the four remaining flat panel monitors to RGU1. Technical support configured the four-monitor display on the north side of the control room desk to "stretch" the VIEW1 console session desktop horizontally across all four monitors. At this point the new SCADA application was running on all eight control room monitors. Technical support issued a control maintenance procedure with instructions for carrying out the system routine maintenance plan.

6. ACHIEVEMENTS

6.1 Unified Ethernet Network

All six servers, the remote dial-in modem, all PLCs, and the MCS100e are now connected on a single unified gigabit (1000 megabit) Ethernet Local Area Network (LAN). All components in the WWMF SCADA system have access to each other (as permitted by the security settings on the switch in PL1000). Technical support can connect a laptop computer anywhere on the control room desk and provide support for the entire system. The remote access server (RAS) provides dial-in connectivity for third-party support[28].

6.2 Fault tolerant redundant system

All control room functions are carried out on three groups of two redundant servers.

CEMS1 and CEMS2 run the CEMView Server software, each with a redundant SQL Server 2005 Standard instance. If one server fails, the redundant server takes over the continuous emissions monitoring task. CEMView automatically updates the failed server with all missing data once it has powered back up.

IOS1 and IOS2 run the Cimplicity HMI SCADA application for the incinerator and all supporting systems. Each server has a redundant SQL Server 2005 Standard instance. If one of the servers shut down, the other server maintains supervisory control of all systems. Cimplicity HMI does not automatically back-fill missing data. The data is re-synchronized manually using the Cimplicity HMI DB-Synch application.

IOS1 periodically uploads the entire Metasys application that is running on the NAE every day, and sends a copy to IOS2. In the event of a failure of the NAE, the most recent application can be re-installed from IOS1 or IOS2. IOS1 periodically downloads all trend, alarm, and audit information from the NAE. IOS1 sends a duplicate copy of all records to IOS1. If IOS1 and IOS2 are not available, the NAE can temporarily hold historical data for up to one month.

The VIEW1 and VIEW2 servers are duplicates of each other. The two servers run all operator interface software. Each VIEW server provides the operator with a four flat-panel monitor display, with one keyboard and one mouse. In the event that one VIEW server fails, one bank of four monitors will go dark. The second server will continue to provide all operator interface software until the failed server has been restored.

Each functional pair of servers is fed from two different power sources. CEMS1, IOS1, and VIEW1 are fed from the facility UPS power. CEMS2, IOS2, and VIEW2 are fed from normal

[28] The RAS modem remains disconnected from the WWMF telephone system at all times. Operators connect the modem to the telephone system only when instructed to do so by technical support.

plant power. In the event of a power failure, only half of the control room computers will shut down. Operations can continue to monitor the facility for at least 30 minutes after a power failure.

Although there are a total of eight flat panel monitors in the WVRB control room, operations can maintain critical monitoring and control functions with only a single monitor. If up to seven flat panel monitors fail, operations can still operate and monitor the facility.

Each server has two physical hard drives presenting themselves to the server as a single logical drive in what is known as a Redundant Array of Independent Drives or RAID-1 configuration. The server RAID controller duplicates all hard drive data in real time across both disks. If a single drive fails, the server continues to operate on the functional drive. The failed drive can be removed on-line, and re-synchronized with the failed drive the next time the server is restarted.

The facility Ethernet switch is the last remaining single point of failure. A standby spare switch is available in the OPG WWMF warehouse. A replacement switch will operate out-of-the-box with minimal functionality until technical support restores all Ethernet switch settings.

Single points of failure are nearly eliminated, with SCADA system functionality distributed across three pairs of two servers. Eight monitors provide a high level of protection against monitor failure. Each server is protected against drive failure using a RAID-1 (mirror) drive array.

6.3 Effective use of inter-building fiber optics

Prior to the WVRB control room upgrades project, the SCADA system used two pairs of 62.5um multimode fiber optic cable to monitor the building management system at the WUFDSF. Both fiber pairs were used for a dedicated proprietary network (ControlNet). The control room upgrades project introduced updated media converters and an Ethernet switch at the WUFDSF. The Ethernet switch uses only one pair of fiber for the SCADA system Ethernet network, while freeing up the other pair as a spare for future applications.

6.4 Regular maintenance program

Prior to the upgrades project, the WVRB control room SCADA system did not have a regular maintenance program. This left the SCADA system venerable to equipment failure. Equipment failure coupled with the lack of redundancy set the facility up for unplanned outages and data loss.

The control room upgrades project addressed two key areas of routine maintenance for computer based systems; software and hardware maintenance.

Periodic hardware inspection, and dust removal act as a barrier against CPU overheating. A build-up of dust can act as a layer of insulation for computer hardware, increasing board temperatures. In addition, dust can enter the moving components inside the computer case, further inhibiting ventilation, and increasing server temperatures.

Periodic software archival provides a recovery path for events such as hard drive failures, and operating system corruption. Storing the data in redundant locations ensures that data can be retrieved should one archive fail. The current maintenance program will allow a maximum loss of 24 hours of data, with monthly historical archives available should a previous configuration need to be restored.

6.5 Capacity for future upgrades

6.5.1 Spare capacity in existing hardware

The upgraded WVRB SCADA system uses a small fraction of server resources to operate and monitor the facility. Refer to Table 1 for spot measurements of control room server usage.

System	Resource	Usage
IOS1 and IOS2	Hard Drive Space	20%
	CPU Usage	5%
CEMS1 and CEMS2	Hard Drive Space	30%
	CPU Usage	10%
VIEW1 and VIEW2	Hard Drive Space	15%
	CPU Usage	3%

Table 1 New SCADA System - Server Resource Utilization

Since commissioning in Q3 2009, resource usage has been climbing very slowly. CPU usage has remained the same, with hard drive usage up 2-3%. The current software installation can double in size, leaving at least 50% of the hard drive capacity for historical data and archival. CPU usage is very low, however this value is best kept as low as possible as CPU utilization tends to be very erratic, particularly when multiple processes operate at the same time. This usually takes place during the off-shift (between 00:00 hrs and 06:00) during hard drive imaging operations.

6.5.2 Spare capacity for new hardware

As software complexity increases with time, resource usage will increase. Each server in PL1000 has spare capacity for hardware upgrades. Refer to Table 2 for server hardware utilization at commissioning.

Component	Current capacity	Total capacity
Hard Drive Space	300 GB	750 GB
Memory	4GB	16GB
CPU	One quad core Intel Xeon processor at 2.5 GHz	Two quad core Intel Xeon processors at 3.16 GHz

Table 2 New SCADA System - Server Hardware Utilization

Given the rapid pace of computer hardware obsolescence, as well as price trends in the computer industry, any subsequent upgrade project must consider current industry prices and available technology. A complete analysis of computer industry price trends is outside the scope of this paper. Any plan to upgrade the WVRB control room server hardware must be carefully weighed against the costs associated with a complete replacement.

PL1000 is an EIA (310) standard 19" form factor network enclosure. The existing servers can be removed from PL1000 and replaced with computer hardware from any manufacturer that makes 19" enclosure mounted hardware. Dell, HP, and IBM all manufacture a wide variety of products that fit inside PL1000.

The core Ethernet switch supports 44 copper gigabit Ethernet connections, and 4 fiber-optic uplink ports. The current installation uses 22 copper ports, and one fiber uplink port. Fifty percent of the copper ports are available for future connections. Seventy five percent of the fiber uplink ports are also available for future upgrades.

6.6 Reduced control room footprint

The new WVRB control room desk monitors, keyboards and mice reduce the amount of space taken up on the control room desk.

The previous installation consisted of two 20" CRT style monitors (for the CEMView and DAS computers), two 14" CRT monitors (for the WUFDSF application and the Metasys application), and two 15" flat panel monitors (for the incinerator SCADA). All six monitors used up half of the control room desk space alone. All six computers had their own individual keyboard and mouse, creating excessive desktop clutter.

The new WVRB control room desk user interface consists of eight 20" flat panel monitors, four on the north side, and four on the south side. Each bank of four flat panel monitors consists of two groups of two monitors, swivel mounted and adjustable in three dimensions. The swivel mounts keep the monitors above the control room desk, with the mounts at the very back of the desk. Each group of four monitors is connected to a single RGU unit, with one keyboard and one mouse (as opposed to six mice and six keyboards previously).

The pull-out console on PL1000 allows technical support to perform administrative functions on the SCADA system, without entering the control room desk area. This helps to keep the control room desk area clear for operators.

6.7 Tools for debugging and forensics

6.7.1 New SCADA System

The new WWMF SCADA system provides four instances of Microsoft SQL Server Standard 2005, running on the IOS1, IOS2, CEMS1 and CEMS2 servers.

Cimplicity HMI (running on IOS1) stores all one minute data to its local instance of SQL Server. IOS2 stores a redundant copy to its own database as well. CEMView Server (running on CEMS1) stores all regulatory historical data to its local instance of SQL server. CEMS1 interacts with the CEMView installation on CEMS2 to ensure that it has a duplicate record in the CEMS2 SQL Server instance at all times.

The IOS1 server runs an archival tool to extract all historical records saved in the non-volatile memory space of the Jonson Controls NAE. All historical records are stored in the SQL Server instance running on IOS1, and then duplicated on the IOS2 database as well.

SQL Server Standard 2005 provides three very powerful tools to manipulate and analyze historical data from all data sources at the WWMF.

6.7.1.1 SQL Server Integration Services (SSIS)

SSIS provides a graphical user interface that allows the user to import data from various sources, perform transformations on that data, and to export the data to a wide variety of destinations. SSIS can pull records directly from the CEMView, Cimplicity HMI, and Metasys historical databases, relate the data based on key columns, and then export the results either back into a SQL server database instance, MS Access mdb file, or to a flat text file. The entire process can be stored as a single project, and then re-executed manually, or even scheduled on a periodic basis as needed. Refer to Figure 15 for an example of an SSIS program. The two data sources are at the top of the diagram. Data flows through the various transformation blocks to the data destinations at the bottom.

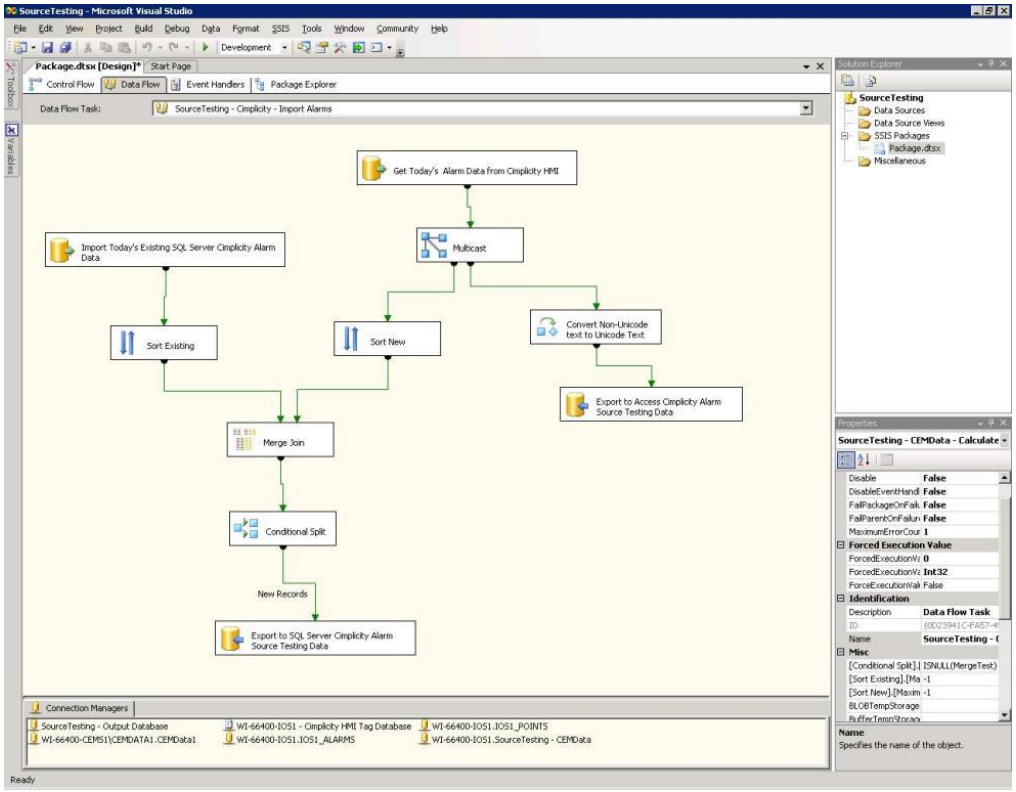

Figure 15 Installation - SSIS Example

6.7.1.2 Transact Structured Query Language (TSQL)

TSQL is a powerful database query language that allows the user to design custom queries to retrieve large amounts of data from a database instance. Basic operations such as Select, Delete, Update, and Insert are supported. Complex operations such as sub-queries, recursion, and triggers are also available. TSQL in combination with SSIS allow the user to extract and relate large amounts of information with a single instruction.

6.7.1.3 SQL Server Analysis Services (SSAS)

SSAS expedites common data mining activities by allowing the user to create data "cubes". Each cube contains a collection of tables from various sources with their relationships pre-defined. The user can view summary data from the cube quickly and easily using drag-and-drop operations in a graphical user interface.

6.7.1.4 Unified Presentation of Data

The large amount of spare processing capacity of each server, combined with the powerful database query and relational tools provided by Microsoft SQL Server 2005, allow Technical support staff to compare millions of records of historical data from multiple sources using a single software package. Technical support now has the ability to query and compare historical data from all data sources in the WWMF over a period of several years (instead of only several weeks). Technical support can develop the queries on the pull-out console in PL1000, or from a development laptop PC located anywhere in the WVRB control room.

6.7.2 Remote Desktop Protocol (RDP)

Microsoft Windows Server 2003 is installed on all six servers in PL1000. RDP is a service provided by Windows Server that allows a computer to open up a desktop instance from the server on a computer anywhere on the LAN. Technical support can connect a laptop computer to the WVRB control room LAN, and open up a desktop session on IOS1, IOS2, CEMS1, CEMS2, VIEW1, or the VIEW2 servers. RDP also allows technical support to open up multiple desktop sessions simultaneously on the four different monitors running on VEIW1 or VIEW2.

For example, control room operators may request technical support assistance when using the WWMF SCADA system. Operators can monitor and control the facility with the four monitors connected to VIEW1, while technical support logs into the VIEW2 server, and runs desktop sessions on IOS1, IOS2, CEMS1, and CEM2, using the monitors connected to VIEW2. The operator can use the SCADA software to control the facility, and technical support can observe the response on the servers at the same time.

6.8 Security

The new WWMF SCADA system uses several layers of security to protect against malicious users, and to reduce the probability of unplanned equipment outage.

6.8.1 Desktop Level Security

The VIEW1 and VIEW2 servers are configured to automatically log in the "operator" user. The VEIW Servers run a script on startup that modifies the windows registry to "lock down" the operator desktop. The locked-down operator desktop has the following features:

- No icons are present on the desktop
- The user cannot right-click on anything on the desktop
- Everything from the start menu is removed, except shortcuts to the control room SCADA applications and a button to logout the current user
- The CTRL-ALT-DEL key sequence is disabled
- All shortcuts using the windows key are disabled
- Auto-run for the CDRROM and USB ports are deactivated

The desktop is restricted to control room functions only, reducing the ability for a user in the control room to install unauthorized software on the SCADA system.

6.8.2 Operating System Level Security

Each server has a collection of users that strictly limit access to the operating system based on the user's role. Users from technical support have complete access to the operating system. Control maintenance has access to an unlocked desktop; however they cannot modify the operating system configuration, or install any software. The operator user has access to the locked-down desktop on the VIEW servers.

6.8.3 Hardware Level Security

The core Ethernet switch in PL1000 carefully controls what devices can connect to the WWMF SCADA LAN. Equipment is identified by Media Access Control Address (MAC Address). Access rights are then granted based on the equipment's function in the SCADA system.

For instance, laptop computer users connected at the WUFDSF can only access the BMS system in their own facility. The WUFDSF users do not have any access to the servers installed in PL1000 in the WVRB control room (and vice-versa). The only exception to the previous rule is the protocol converter that sends monitoring information up to the WVRB control room from the WUFDSF.

7. LESSONS LEARNED

7.1 Summary

Engineering design for an industrial facility must pay adequate attention to the SCADA system. Failure to do so will have a negative impact on system reliability and usability. The existing WWMF SCADA system design had three major problems. Inadequate system integration resulted in a complex system that was difficult to maintain and introduced substantial risk to the facility. The absence of routine maintenance on the system compounded that risk, increasing the likelihood of a failure and the loss of historical data. The facility historical data was not easily accessible and was not stored in redundant easy to access locations.

7.2 System Integration (Master Plan)

The original WVRB control room used four different software packages to provide a user interface for the operator:

1. Cimplicity HMI: For the Incinerator monitoring and control functions.
2. RSView 32: To monitor alarms from the WUFDSF.
3. CEMView: For continuous monitoring of the MCS100e Continuous Emissions Monitor.
4. Metasys: To monitor and control the building ventilation systems in the WVRB and TPMB.

The DSF computer required a separate software package, on a separate computer, with its own network to monitor 47 alarm points from the WUFDSF. The control room upgrades project exported these points from the RSView32 application and imported them into the existing Incinerator SCADA application.

The Johnson computer used a separate software package and network exclusively for one sub-system in the facility. The control room upgrades project work involved converting the Metasys application to run on a solid state computer controller (NAE), connected to the industrial LAN.

The upgrade work made the Metasys application available on all computers connected to the LAN.

The DAS computer provided the operator with real-time incinerator emission values from the MCS100e[29]. The DAS computer used a completely separate instance of Cimplicity HMI with its own screens, trends, and historical data. The control room upgrades project imported the DAS computer application into the SCADA application running on the Master and Slave computers.

The Master and Slave computers ran duplicate copies of all incinerator control screens. The Slave computer would refer to the Master computer for the status of all points in the system. A failure of the Master computer would leave both the Master and Slave computers inoperable. The control room upgrades project introduced a redundant SCADA system on two separate servers. As long as one server is running, operators are able to monitor and control the Incinerator.

Three of the old control room SCADA computers were connected to a small Ethernet LAN using a 10 BASE-T hub, located underneath the control room desk. The control room upgrades project includes an enterprise grade Layer3 Gigabit Ethernet switch inside PL1000. The new switch provides a unified Ethernet LAN for all control room computers.

Design work that includes the SCADA system prevents complex upgrade work in the future. A SCADA master plan provides the engineer with the following information:

1. Details about the existing industrial network (or Ethernet LAN) with instructions for future expansion.
2. Existing SCADA software with instructions for adding new systems.
3. Historical data logging and reporting requirements.
4. PLC hardware specifications and programming standards.

This list of master plan contents is by no means complete. A detailed description of a SCADA master plan is outside the scope of this paper. The Regional Municipality of Peel public works department has a complete SCADA system master plan entitled Process Automation Instrumentation Design Standards or PAIDS[30]. The PAIDS standard provides engineers with details of the existing SCADA system at the Region of Peel, along with expansion requirements for future work.

The master plan ensures that design work considers existing technologies when adding new facilities or expanding current facilities. Isolated and incompatible systems are not possible, eliminating single points of failure and segmented systems.

The WWMF has specification standards for the SCADA system. The new standard was created as a corrective action in response to the WVRB control room upgrades work.

7.3 Routine Maintenance

The WWMF did not have a routine maintenance program in place for the existing SCADA system. The Master, DSF, Johnson, and CEM computers were single points of failure in the

[29] Refer to Figure 5 for an illustration of the MCS100e, DAS, and CEM computer connections.

[30] Visit www.paids.ca for more information on the PAIDS standard. Click on the Documentation/Software link to complete a PAIDS request form, or request the standard by sending an e-mail to peelscada@peelregion.ca.

SCADA system. None of the existing computers were routinely inspected for potential failure. The software and data on each of the computers were not protected against hard drive failure. The SCADA system did not support routine maintenance work without interrupting monitoring and control functions in the WVRB control room.

The WVRB control room upgrades work introduces a routine maintenance program for the WWMF SCADA system. Each server is cleaned and inspected for signs of electrical failure. Each server backs up its contents to a single drive image on a daily basis to two redundant locations (VIEW1 and VIEW2). Image files are backed up on a monthly basis to DVD disks. Every function in the SCADA system is duplicated to ensure that shutting down one server will not interrupt monitoring and control functions in the control room.

A routine maintenance program guards against SCADA system failures and helps to protect against data loss in the event of a failure. Routine maintenance must be considered at design time to ensure that the system can be maintained without interrupting control room functionality.

7.4 Access to Historical Data

The existing SCADA system stored historical data in various formats across six different computers. In order to relate historical data across more than one system (data on the Master computer against data on the CEM computer), historical records had to be extracted from each SCADA computer manually in the operator's area at the control room desk. The records had to be removed from the control room and then processed using low-powered corporate workstation PCs outside the WVRB control room.

The control room upgrades introduces a unified Ethernet network and four instances of SQL Server 2005 Standard running on enterprise level server hardware. SQL Server includes powerful utilities such as SSIS, SSAS, and TSQL that allow the user to mine all historical data from any server on the network. Each server has excess capacity available to perform the query without removing control room functionality. The user can perform the query from the pull-out console on PL1000, or by using a laptop computer plugged into a receptacle anywhere on the control room desk.

7.5 Unresolved Issues

Correcting SCADA system design problems after construction are very difficult. The control room upgrades project attempted to correct three major problems (segmented system, routine maintenance, and access to historical data), however more problems exist that are not easily solved.

7.5.1 Air Handling Systems

The DSF air handling system uses a network of Allen-Bradley PLCs running custom programs to control the facility. The WVRB air handling system has a Johnson Controls system, using DX9100 modules to control the facility. The SCADA application that was running on the DSF computer was very small and was easy to integrate into the incinerator Cimplicity HMI application. The graphical user interface running on the Johnson Controls NCM was substantially larger, and could not be easily integrated into the Cimplicity SCADA. As a result the WVRB air handling system still has its own user interface running on the NAE. This problem could have been averted if the facility design requirements documentation stated that all user

interfaces must be compatible with Cimplicity HMI (or a unified SCADA software program from any other vendor).

7.5.2 Corporate WAN

The entire WWMF SCADA system is connected to an Ethernet LAN separate from the OPG corporate network. Integration with the corporate network has the obvious advantage of increased corporate connectivity. Information from the plant floor can be made available to all levels of the corporation. Making the move to corporate connectivity requires substantial planning and cooperation between multiple groups. Every new system added to a corporate network must undergo rigorous testing to minimize risks to the entire network. Internet access also adds substantial security risks to the system which must be addressed at design time.

When technical support developed the control room upgrades scope of work, they had to focus on eliminating the imminent risks to the facility. Although corporate connectivity would increase system accessibility, it did not address facility risks, and was hence dropped from the scope of work. The control room upgrades work specified a Layer-3 managed Ethernet switch for the SCADA system Ethernet network. This switch will fully support corporate connectivity should the WWMF decide to connect the SCADA system LAN to the corporate network in the future.

8. LOOKING FORWARD

8.1 Advanced Data Mining and Reporting

The WVRB control room upgrades work introduced new data mining software (SSIS, SSAS, and TSQL). Technical support is developing training qualifications for current and future technical employees that will allow the WWMF to unlock the full potential of this software. Technical support plans to use the reporting functionality of SQL Server 2005 (SQL Server Reporting Services or SSRS) to replace manual reporting tasks in the WVRB control room. The new reports will obtain the historical totals from the incinerator PLC, and from the MCS100e using SSIS. The consolidated totals and average values will be published to a web site on the IOS1 and IOS2 servers. The daily reports will be accessible to the operators through a web browser, or by using Cimplicity HMI. Refer to Figure 16 for a software architecture diagram of the proposed SSRS solution.

8.2 Server Virtualization

The WVRB control room upgrades project introduces six new enterprise grade servers (Dell Poweredge 1950 III). Each server runs a single operating system with all software for that server running on the single operating system. Server virtualization software allows a single server to run multiple operating systems at the same time. The virtualization server runs as a top-level operating system, with all host operating systems running below it. The host operating systems run completely unaware of the virtualization server. The host operating systems behave as though if they were installed on their own independent server.

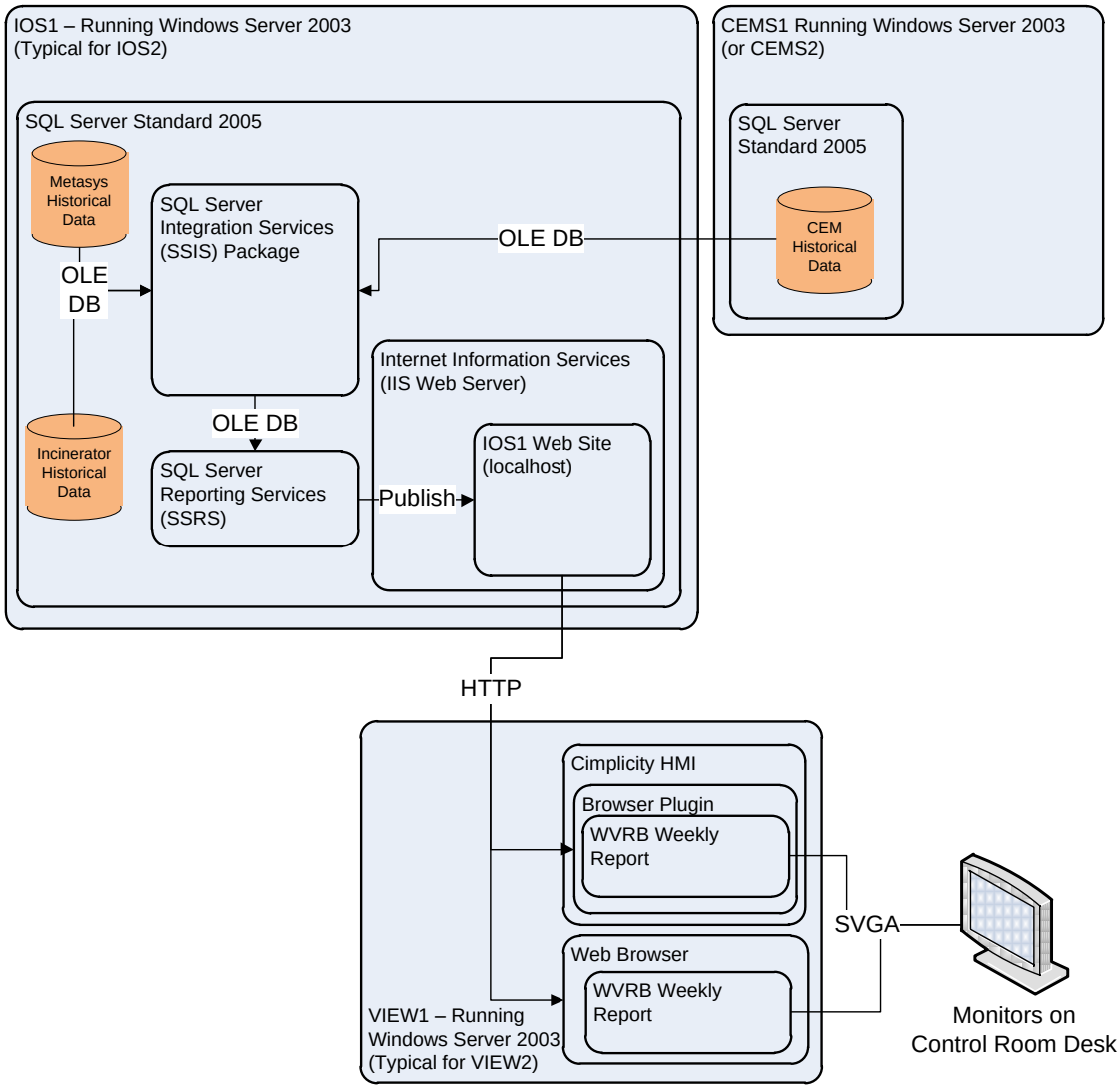

Figure 16 Future SCADA System - SSRS Architecture

8.2.1 Benefits

The CEMView redundant software packages run on their own independent server (CEMS1 and CEMS2). This configuration avoids inter-vendor software conflicts on a server that has a direct impact on regulatory compliance.

Virtualization would allow a single server to run a separate instance of Windows Server 2003 for the CEMView software alone. Additional host operating systems allow each software package to run in their own operating system to resolve situations where two software packages cannot co-exist on the same server.

8.2.2 Challenges

The WVRB control room servers are currently under-utilized. Technical support would be challenged to make sure that the servers have the capacity to handle multiple host operating systems, and to set a conservative limit on resource utilization.

With virtualization, it is possible to run all of the WVRB control room software on a single server. This configuration eliminates server redundancy in the control room. Routine maintenance would be very difficult as control maintenance would have to shut down the entire control room to perform the quarterly maintenance tasks.

Technical support is currently investigating options for implementing redundant virtualization across multiple servers. Refer to Figure 17 for a diagram of the server virtualization option.

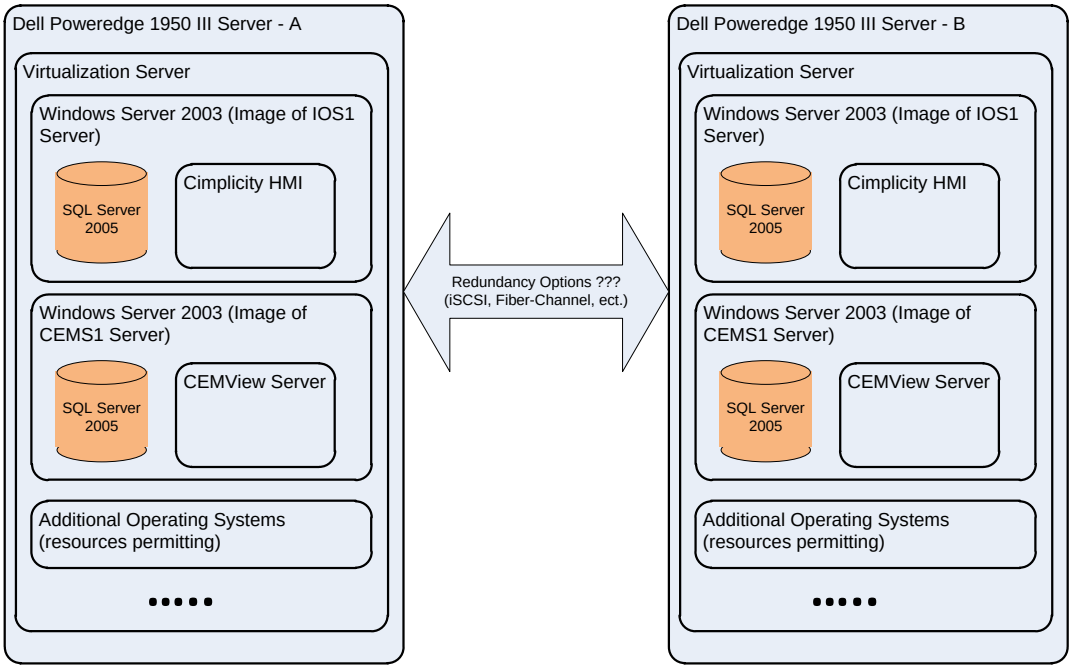

Figure 17 Future SCADA System – Redundant Virtualization

8.3 Solid State Computers

The routine maintenance program includes a dust removal task. The dust removal task prolongs the lifetime of components in the server.

Solid state computers have no moving parts. All components in the server are in a sealed unit protected from the environment. Heat sink fins on the outside of the solid state computer provide the required cooling via convection and conduction.

Solid state computers would eliminate the need for the quarterly maintenance tasks on the control room servers as the sealed units would eliminate the ingress of dust. Technical support is currently investigating the use of solid state servers for a future upgrade.

8.4 Planned Obsolescence

The Microsoft distribution lifecycle program[31] indicates the extended support date for Windows Server 2003 R2 (currently installed on all six servers) will expire on July 14th 2015. Technical

[31] According to Microsoft's support lifecycle website: http://support.microsoft.com/lifecycle/. When the software support lifecycle expires, Microsoft no longer provides path fixes to correct bugs and address security issues.

support is currently considering options for upgrading to the next operating system by 2014 (Windows Server 2012).

Technical support is currently working to develop an aging management plan to address all WWMF facility PLC and SCADA obsolescence by 2015. The plan will provide details for a facility wide upgrade of all obsolete PLC and SCADA technology in the form of a unified SCADA master plan.

REFERENCES

[1.] David Bailey B.Eng, Edwin Wright MIPENZ BSc (hon) "Practical SCADA for Industry", Newnes September 17 2003, Chapter 1, Section 1.1