Automation Infrastructure Upgrades at an Oil Storage Terminal

By Richard Caouette, P.Eng., Letico Inc.

KEYWORDS

Automation, Infrastructure, Upgrades, Oil Storage Terminal, SIS, PLC, HMI, API-2350, Project Management

ABSTRACT

This paper discusses the approach taken to upgrade the automation infrastructure at an existing oil storage terminal comprising pipeline reception as well as truck and tank car loading bays. The project aimed at replacing obsolete components and subsystems with newer technology equipment, while improving site safety and security. A description of the various control subsystems involved and their interaction with the process equipment is provided. The project included the relocation of the main control room as well as upgrades of the power distribution and control systems. Compliance review with various standards and regulations is also discussed.

The HMI software and PLC hardware were both obsolete. The article describes their modernization and implementation based on a Programmable Automation Controller (PAC) combined with a standard library of faceplates and standard routines for pumps, valves and process instruments.

In addition, the paper discusses the implementation of a redundant overfill protection system as per API-2350, as well as a Safety Instrumented System (SIS) as per ISA-84/IEC 61511, integrated with the basic process control system (BPCS PLC) and HMI.

The paper discusses the various measures taken by the team to reduce downtime associated with the project execution, taking into account the dynamic product demand and equipment availability. This included planning and communication on multiple fronts throughout the project. The conclusion summarizes what made the project a success.

1 INTRODUCTION

1.1 HISTORY

The facility was built in the early 1960s. As is often the case with older sites, a number of upgrades and plant additions had taken place over the years, resulting in a mix of technologies of various vintage. The installation conformed to the standards in effect at the time. However, as technology advanced and changes within the industry's regulatory environment took place, some of the

installation no longer complied with the newer standards. Some of the equipment had inherent incompatibilities, resulting in islands of automation with significant limitations.

Following the Buncefield accident in the UK in 2005, the owner wanted to implement redundant overfill protection per API-2350, as well as a Safety Instrumented System (SIS) as per ISA-84/ IEC 61511-1 Mod, integrated with the Basic Process Control System (BPCS PLC) and HMI. A siting review had recently determined that the existing control room was too close to the process equipment and that it should be relocated to a safer location.

In addition, as with many aging facilities, the electrical power distribution infrastructure was also due for an upgrade, including the main transformer, the 600V power distribution network and equipment, as well as some motor control centers (MCCs).

Some components of the controls and communication infrastructure were also obsolete, spare parts were becoming increasingly difficult to procure, with some software no longer supported.

2 PROCESS OVERVIEW

2.1 PROCESS DESCRIPTION

The site is a storage and distribution terminal, receiving distillates and gasoline products via pipeline, as well as Ethanol and various additives via tank trucks and/or tankcars. From the storage tanks, the product is then loaded onto tank trucks or tankcars, with blending at the load racks.

Tank trucks are filled by the truck drivers with the help of an automated system. Tankcars are filled manually by terminal operators.

Instrument air is not available at the site. Therefore, automatic valves are typically motor-operated valves (MOV), driven by either electric or electro-hydraulic actuators.

The majority of the equipment is on-off, following the demands of product receipt and sales. Analog instrumentation is present mostly for the purpose of inventory management, comprising of level and temperature transmitters at the tanks, as well as custody metering (flow, density and temperature) at the pipeline receipt manifold and at the load racks. As the plant is responsible only for storage and distribution, there is little need for analog controls such as PID loops, except for regulating the pipeline pressure. Some product pumps include VFDs and soft-starters to reduce fluid hammers effects as well as compensate for fluctuating demands at the load racks.

2.2 PROCESS FLOW DIAGRAM

Figure 2.1 presents a simplified process flow diagram (PFD) of the facility.

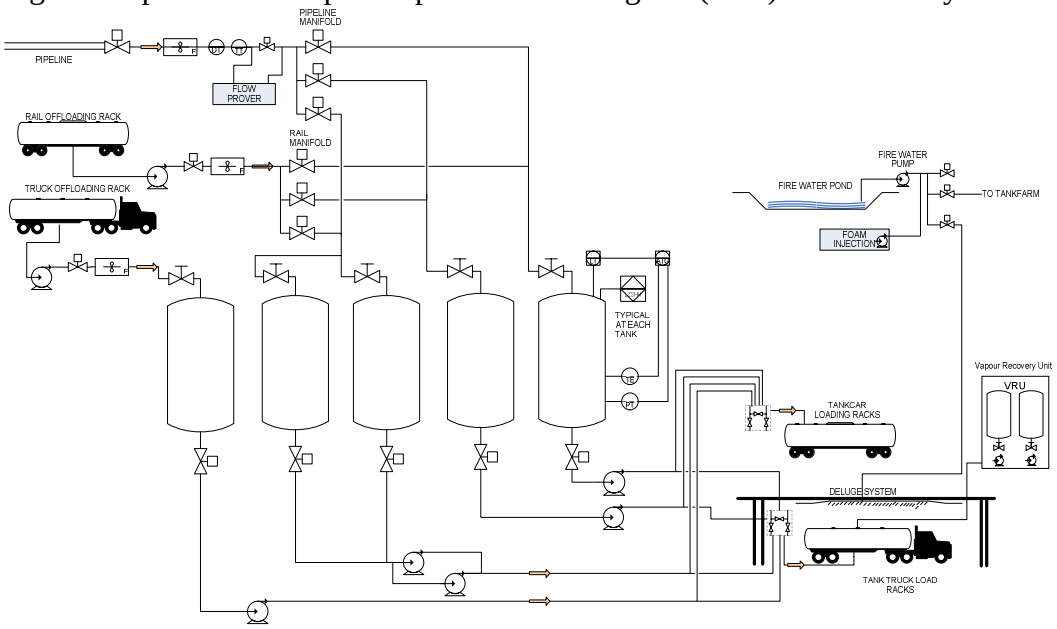

Figure 2.1 Simplified Process Flow Diagram

3 CONTROL SYSTEMS

3.1 INFRASTRUCTURE OVERVIEW – BEFORE THE UPGRADE

Several automation subsystems interact to support the operation of the terminal.

Due to the physical size of the terminal, the process control equipment is distributed. The PLCs have remote I/O chassis interconnected via a fiber optics communication backbone.

Figure 3.1 presents a simplified overview of the control systems before the project started.

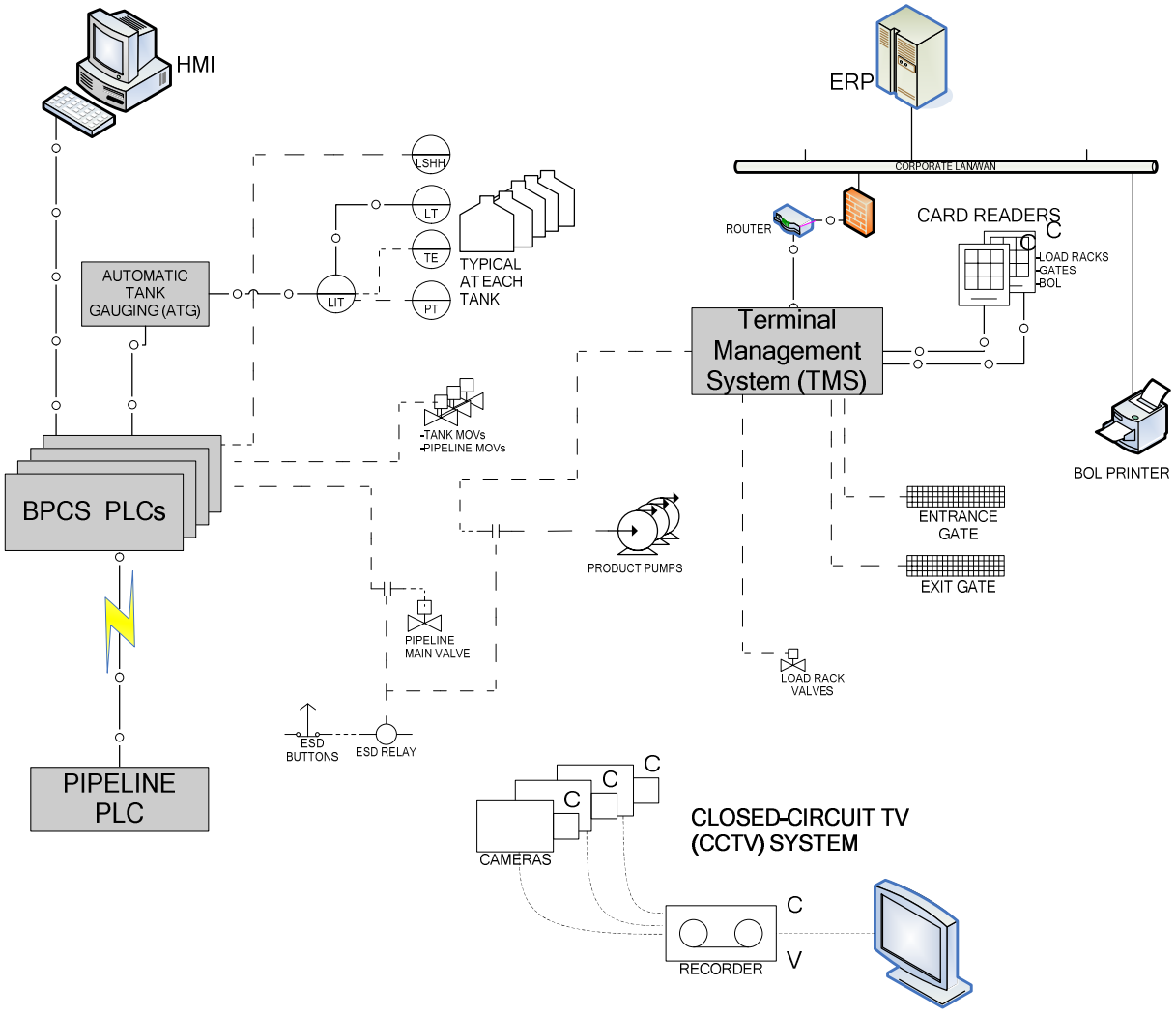

Figure 3.1 Control systems block diagram – Before the project

3.2 PROJECT SCOPE

Before the upgrade project, the team performed an assessment of each of the automation subsystems, identifying the functions they were responsible for and how they interacted together. Each subsystem was evaluated in terms of its relevance (it is still required?), its performance, its potential obsolescence, as well as its compliance with the applicable local and industry standards.

Following this analysis, the various improvements identified were evaluated and a capital project request was submitted for approval. Section 3.2.1 presents a summary of this analysis.

Figure 3.2 shows an overview of the controls systems after project completion. To the operator, the most visible changes were the new control room location and the new HMI software. However, the most significant architecture changes were the addition of the SIS PLC (see section 3.2.4) and the associated modifications to the overfill protection system (see section 3.2.5).

Several other subsystems needed modifications and had significant impact on project execution, including the CCTV and Terminal Management System (TMS).

3.2.1 ASSESSMENT OF THE SUBSYSTEMS

The team evaluated alternative options for each of the improvements proposed. Cost justifications were considered, based particularly upon:
- □ Return on investment (ROI)
- □ Obsolescence and potential lost revenue in the event of failure
- □ Regulatory compliance

In the oil and gas industry, the storage and distribution segment of the business usually has a more limited investment budget than the “upstream” segment of exploration and production. Trade-offs are often necessary. “Best in class” is nice, but not always justified. Therefore, consideration was given to how critical each system is and whether we should spend more efforts and funds in other areas.

For instance, redundant communication paths and processing power can improve uptime and reduce spurious trips. However, given the physical size of a distribution terminal, it can be very expensive to build a ring topology for a network backbone. We considered the historical failure rate at the site and other similar ones, as well as what would be the impact of an outage, given the mean time to repair (MTTR). Shutting down a pipeline is a more serious consequence than interrupting loading at the truck racks. Instead of installing redundancy, we rather focused on trying to avoid pipeline-related signals from being dependent on remote I/Os.

This assessment was formalized into a User Requirements Specifications (URS) document, which was reviewed by the customer’s stakeholders:
- □ Technical subject-matter experts (SMEs)
- □ Operations representatives
- □ Project management

The following table lists the various subsystems present and summarizes the evaluation that was done prior to preparing the scope of the project.

Subsystem	Functions	Improvements proposed
BPCS PLC	□ Monitor and control various instruments and valves around the tank farm. □ Interface with the Automatic Tank Gauging (ATG) system. □ Track products and detect interface when receiving via pipeline, switch destination tanks.	□ Replace obsolete CPU and I/O racks for which spares were no longer readily available. □ Combine multiple CPUs and programs into a single one. □ Separate safety from basic process control functions. □ Control the product pumps based on requests from the TMS. □ Expand the remote I/O network to the new buildings. □ Use standardized process control object library routines for ease of troubleshooting and commissioning.
HMI	□ Provide a graphical view of the instrumentation around the tank farm. □ Present tank farm inventory summary (from the ATG via the PLC). □ Accept operator entries and generate reports for pipeline receipts. □ Display and log alarm messages.	□ Upgrade the obsolete software package and operating system. □ Use multiple monitors to avoid constantly switching displays. □ Use a process control object library with standardized faceplates. □ Conform to the latest HMI design standards for display navigation and style conventions.[1] □ Install an historian database. □ Improve alarm management.[2] □ Virtualized environment with terminal services and thin clients.

[1] At the time of executing the project, the recently published ISA-101 "Human Machine Interfaces for Process Automation Systems" standard was not yet available. However, other standards, such as the ASM® Consortium Guidelines were available and utilized.
[2] We used the standard ISA-18.2 "Management of Alarm Systems for the Process Industries" to review the list of alarms and try to avoid alarm floods during abnormal situations.

Subsystem	Functions	Improvements proposed
TMS	□ Authentication of truck drivers. □ Control access to the terminal via vehicle gates. □ Metering and blending of products at the load racks. □ Metering of product at offload racks. □ Printing Bill of Lading (BOL) □ Send transactions to the corporate ERP. □ Stock reconciliation.	□ Relocate the server to the main office building, away from the load racks. □ Upgrade to newer software version. □ Send product requests to the BPCS PLC via communication, instead of directly starting the pumps.
Automatic Tank Gauging (ATG)	□ Interface the level instrumentation at each product tank. □ Calculate product density in each tank. □ Calculate gross and net volumes per individual tank strapping tables and API-54 tables.	□ Add unexpected movement alarms via the PLC and HMI. □ Implement level alarms at the PLC level, to enhance visibility and diagnostics. Thresholds under strict Management of Change (MOC) policy.
Tank Overfill Protection System (AOPS)	□ Protect against tank overfills by detecting high-high level conditions and interlocking the pipeline and offloading operations.	□ Make the system completely independent from the ATG and BPCS PLC. □ Connect the High-High level switches to a SIS PLC, which would be responsible for the interlocking. □ Interlock the main pipeline valve. □ Install an emergency siren, audible throughout the site.
Closed-Circuit TV (CCTV)	□ Monitor surveillance cameras distributed around the site. □ Record images from each camera for potential event investigations.	□ Convert to an IP-based system to facilitate its relocation to the new control room relocation. □ Provide access for the supervisor via a separate client computer for event investigations. □ Add cameras at strategic locations to better monitor some areas. □ Install a wide-screen monitor to provide a mosaic of multiple camera images simultaneously.

Subsystem	Functions	Improvements proposed
Communication Infrastructure	□ Link various process control equipment, including the BPCS PLC and HMI.	□ Extend the fiber optics network to new buildings. □ Replace unmanaged switches with new managed switches. □ Separate with VLANs and router/firewalls to improve security.
Electrical Power distribution	□ Provide electrical power to the various process equipment and buildings.	□ Replace the main substation, transformer and 600V switchgear. □ Replace an obsolete MCC with a new unit. □ Take into account voltage drops across the power distribution system. □ Improve selective coordination, with arc-flash reduction. □ Add metering and diagnostics capabilities, with trends available on the new HMI.

3.2.2 UPGRADED INFRASTRUCTURE BLOCK DIAGRAM

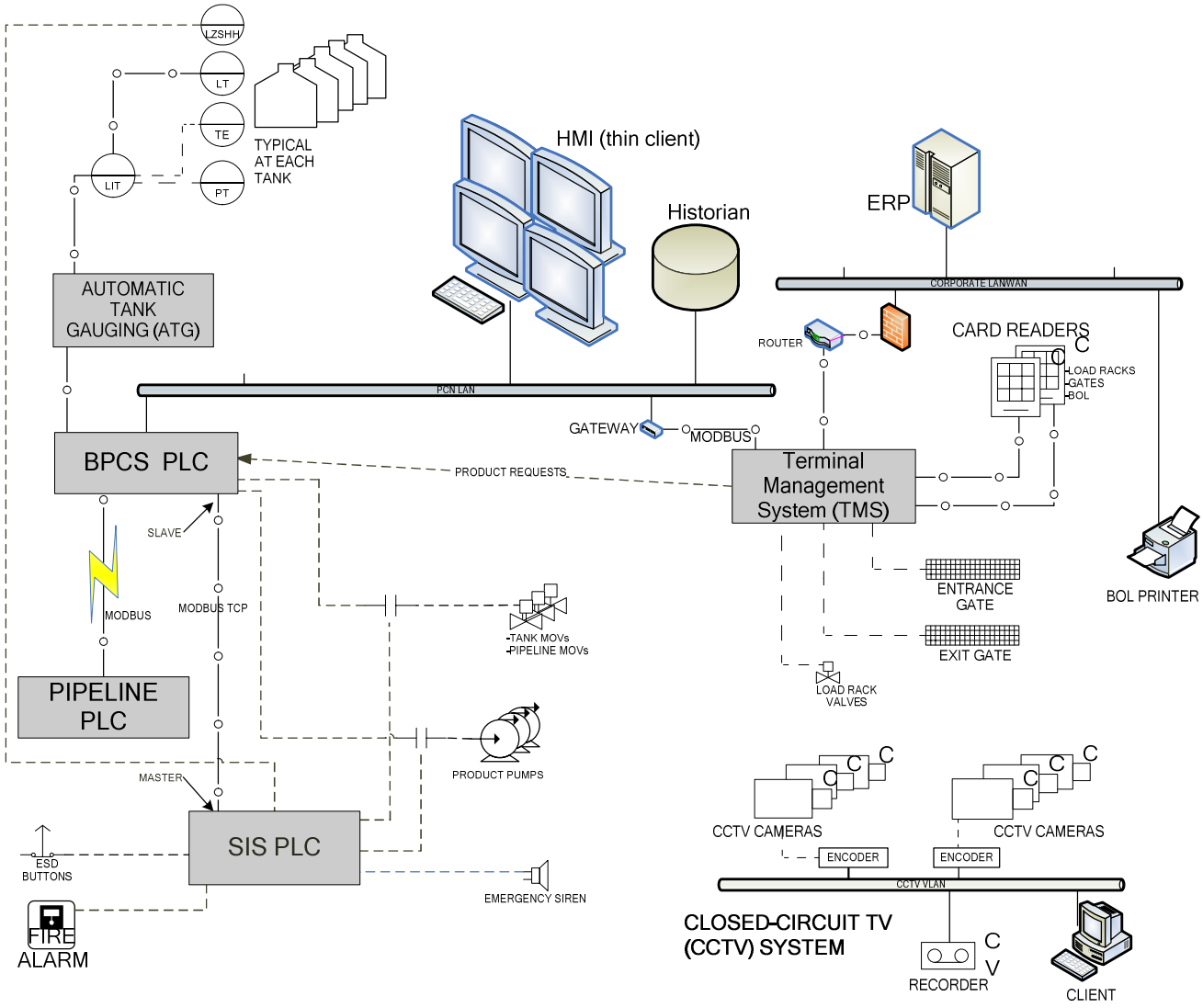

Figure 3.2 Control systems block diagram – After the upgrades

3.2.3 BPCS PLC AND HMI UPGRADE

The plant originally comprised four independent PLCs, each covering a specific physical area within the terminal. They had been installed by various systems integrators as they executed different projects. Historically, there had been reluctance from each party involved to integrating new equipment into existing PLC. Each integrator preferred to add his own new design, network it with the other PLCs, and avoid modifying the existing systems. The PLC programs had inconsistent programming styles and naming conventions.

In a distribution terminal, related process equipment is often located at significant distances from one another. As the PLCs architecture had been structured more from a geographical rather than functional perspective, the communication between each CPU was more complex.

The most important shortcoming was that the CPUs and some of the I/O racks had become obsolete. Used spare parts were still available globally via sites such as EBay™, but no longer directly from the manufacturer or its distributors. There was little option but to replace those I/O racks.

The evaluation concluded that having multiple CPUs did not contribute to the plant's reliability. While a single CPU would create a single point of failure, the operation of the plant required several PLCs to interact in order to allow loading of specific products. Depending upon the destination tanks, even pipeline receipts sometimes needed two PLCs to properly control and interlock the equipment, as well as provide data for the HMI.

The roles of the PLC system and the TMS were reviewed, taking into account their strengths and weaknesses. The TMS is a well-established system for controlling the loading and offloading operations, custody metering and blending equipment. However, its configuration (fill-in-the-blank style), does not lend itself well to managing equipment availability, starting priorities and exception handling. We adopted the principle that the TMS was going to be responsible for requesting products to the PLC and then deliver them to the load racks. The PLC would take care of starting the selected pump with the required interlocking, opening the associated tank outlet valve and managing fail-to-start errors and run priorities together with the HMI. The derived benefits are a greater level of flexibility, diagnostics and equipment protection.

The HMI software was obsolete and no longer supported by its vendor. It was hosted on an old tower PC running an obsolete operating system. The original vendor had proposed a migration path, but it involved a complete re-engineering of the displays and database.

It was decided to base the new system on a Programmable Automation Controller (PAC), making extensive use of a process control library of faceplates and standard routines for pumps, valves and process instruments. The new HMI is from the same vendor, and the tag database is linked to the PLC database. The HMI and historian were implemented in a virtualized environment, which isolates the hardware and software platforms. Software backups are now automated. The operator interfaces with a diskless thin client computer. These features greatly facilitated the upgrade, as well as the commissioning, troubleshooting and software maintenance. The use of software libraries and a single CPU made the program more uniform and easier to understand.

3.2.4 SIS PLC

A SIL evaluation was performed, as per ISA-84/ IEC 61511-1 "Functional Safety: Safety Instrumented Systems for the Process Industry Sector", and included the main potential hazards within the terminal. Taking into account the layers of protection available at the site, the analysis concluded that overfill protection of the main product tanks required a SIL-1 level. As a result, SIL-rated high-high level detectors were wired to the SIS PLC. The main pipeline shutoff valve is a SIL-rated MOV, with its ESD signal controlled by the SIS PLC. See also section 3.2.5 for more details.

A safety requirements specifications (SRS) document, coupled with a Cause & Effect matrix (C&E) were written and approved for implementation.

Although they require human intervention and as such cannot meet the SIL-1 level[3], emergency-stop buttons were integrated into the SIS PLC. In addition, fire alarm signals from various points around the terminal (buildings, fire water pump controller, manual stations), were also linked to the SIS PLC. This allowed the SIS to combine various signals to shutdown equipment according to a controlled and documented scheme. Final elements were interlocked with safety relays driven by outputs from the SIS PLC. Of course, including more signals into the SIS implies that those additional devices need to be tested with the same rigour as the rest of the SIS system, following the SIFs lifecycle. Those life-safety elements were considered critical enough that their testing needed to be documented and that they adhere to strict maintenance procedures. Since the highest integrity rating required was only SIL-1, it was decided that to facilitate maintenance and reduce spare parts, the CPU would be the same type as for the BPCS PLC. This equipment is rated for applications up to SIL-2. Additional features were specified for the SIS PLC components, in order to improve on its reliability and provide additional diagnostics:

- □ Redundant power supplies (UPS and normal) for PLC chassis power supplies and communication components.
- □ Redundant power supplies for 24VDC field power.
- □ Diagnostic input and output modules, to detect open wiring, loss of field power, etc.
- □ Interlocking of process equipment such as pumps and valves via SIL-rated safety relays.

While there is a need to provide the status and diagnostics of the SIS to the HMI, as well as communicate ESD signals to the BPCS for some software interlocking, the integrity of the SIS system must be maintained at all times. Good engineering practices and corporate standards suggest that a peer-to-peer network may create vulnerabilities. For example, another device or someone could potentially modify setpoints and interlocks, jeopardizing safety. A firewall can certainly restrict the traffic, but not necessarily filter safety-related from non-safety-related data. Our solution was to implement a master-slave network, based on Modbus TCP/IP, with the master being the SIS PLC, and the BPCS PLC acting as a slave. Special interface modules at each end are interconnected directly, without going through a network switch. The data exchanged is limited to the mapping programmed in the SIS. The BPCS cannot write data outside of the assigned memory range. The HMI can access SIS information through the BPCS PLC, but not directly.

A separate network port is available on the SIS, but it is used only when software changes are required, or for troubleshooting when the diagnostics provided on the HMI are not sufficient. It is physically disconnected the rest of the time. Software changes are restricted and subject to Management of Change (MOC) procedures. The memory protect key on the PLC is set to “Run”, further restricting online program changes.

[3] Per IEC61511-3, appendix F.7, the performance of a trained operator responding to alarms has a PFD of 1.0x10-1, which amounts to a risk reduction factor of 10 (the minimum for SIL1). However, the human performance under stress drops to a PFD of 0.5 to 1.0, which is far below what is required for SIL1. In addition, we have to assume the operator's location allows him to detect the hazard, which is not the always the case.
In addition, IEC61511-2, section 8.2.1 states that "Care is also needed where credit is taken for reduction in demand frequency due to operator action. The credit that can be taken will need to be limited by human factor issues such as how quickly action needs to be taken and the complexity of the tasks involved. Where an operator, as a result of an alarm, takes action and the risk reduction claimed is greater than a factor of 10, then the overall system will need to be designed according to IEC 61511-1 ANSI/ISA-84.00.01-2004 Part 1 (IEC 61511-1 Mod)." This includes periodic "proof-testing".

3.2.5 OVERFILL PROTECTION

In the aftermath of the Buncefield incident, various safety standards were updated, and in particular, API standard 2350 “Overfill Protection for Storage Tanks in Petroleum Facilities”, which includes key requirements.

This independent system consists of the following elements:

- □ High-high level switches (LZSHH)[4] at each tank. Their trip points were calculated to take into account the maximum fill rates, as well as the demonstrated response time for each tank, transposed into the individual strapping tables. The switches are connected to the SIS PLC (see section 3.2.4).
- □ A fail-close main pipeline valve, forced to close by the SIS in case of high-high level, with a closing time that takes into account the hydraulic characteristics of the pipeline, to avoid fluid hammer and provide for enough time for the pipeline pressure controls to react.
- □ Communication with the pipeline PLC to allow it to perform an orderly shutdown.
- □ Audible annunciation via a siren that can be heard throughout the site.
- □ Visible indication at the console via an independent annunciator as well as alarms on the HMI.

3.2.6 CCTV SYSTEM UPGRADE

The existing system was analog-based, each camera connected via a coaxial cable to an individual channel at the back of the recorder. The recorder was still supported, but would probably be obsolete within a few years. Due to the geographical size of the facility and limitations with transmission of video signals over long distances via coaxial cables, the system was already using fiber optics. This was accomplished by converting analog signals via coax to optical signals via individual strands of fiber in the vicinity of the camera, patching along the way and bringing them all to the control room for converting back to coax into the recorder.

Since the control room was being relocated, consideration was given to relocating the recorder and all the associated converters at the same time. That effort was estimated to take several days, including a complete redesign of the fiber optics interconnections. During that time, most of the CCTV system would not be usable and the security of the site would be affected.

The decision taken was to replace the recorder with an IP-based system. Conversion to IP is done at each building where coax-to-fiber media converters were installed. As fiber was already present at those locations, we connected the coax cables to IP encoders, which in turn are connected to the local network switch. Some switches were added at locations that did not have Process Control Network (PCN) switches. A dedicated VLAN was configured into the managed switches for added security.

The main advantage of this configuration is that the recorder can be located anywhere a network switch is present. This provided the ability to install the new recorder at its final location, while the client computer was temporarily installed next to the old system in the old control room.

[4] The “Z” in LZSHH is to conform to the notation recommended by ISA 5.1-2009 “Instrumentation Symbols and Identification” for functions that are part of a SIS.

4 PROJECT EXECUTION

4.1 PROJECT MANAGEMENT

4.1.1 PROJECT RISKS AND CONCERNS

As with most brownfield sites, particular attention had to be paid to reducing downtime associated with the project execution. Extended, plantwide outages were not practical and the preference was given to having numerous, short-duration, localized outages instead.

Also of concern was the fact that due to the complexity of the project and some of the equipment lead times, the project would be spread over two years. One of the risks identified was that some key personnel might not remain available during the entire project. While we assigned people who had been with the firm for several years, we also made efforts to keep more than one person informed of the decisions being made and challenges encountered in each area, thereby providing backup for vacation periods or unplanned absences. We also demanded similar safeguards from the electrical contractor.

When the project was being evaluated, the project team considered splitting the relocation of the control room and the infrastructure upgrade into two separate projects. The purpose was to reduce some perceived risks. However, it was demonstrated that combining these two aspects into a single project would create synergies, resulting in significant cost savings, as well as shorten the execution. We had confidence from previous projects that the added risks could be managed by adequate planning, reviews and strong management.

4.1.2 SCHEDULING

The schedule was developed using the following principles (not necessarily in order of importance):

- □ Obtain seed money to perform some high-level pre-engineering, define the scope as well as prepare the budget for the project. Develop a User Requirements Specification (URS) and obtain sign-off from operations and management before submitting the investment proposal.
- □ Conduct formal design reviews at 30%, 60% and 90% completion, involving representatives from operations, maintenance, management and corporate subject-matter experts (SMEs) when applicable. Make sure to cover topics that directly affect operations and maintenance.
- □ Dedicate time and resources for properly documenting the existing installation prior to starting the work. Identify cabling, markup schematics as needed. Involve maintenance electricians. This effort can significantly reduce risks.
- □ Verify that existing instrumentation is actually functional prior to touching it.
- □ Agree on naming and numbering conventions at the beginning of the detailed design phase.
- □ Manage product inventories and deliveries. Notify the supply department and customers in advance of planned outages.
- □ Build, commission and burn-in the new infrastructure first, before transferring any equipment.

- □ Transfer the most complex and critical instruments and components only after the project team has built experience and confidence with other “simpler” transfers.
- □ Group equipment transfers according to their impact on the plant operation. If multiple components affect the same operation, combining them into a single shutdown leads to less disruption.
- □ Minimize risk by taking into account equipment complexity and what can reasonably be transferred and retested in the time allowed.
- □ Take advantage of equipment redundancy, for instance multiple tanks with the same product or a set of parallel pumps. The plant can continue running at reduced capacity, with little visible impact on customers.
- □ Take advantage of the physical size of the facility. Multiple work crews can perform work simultaneously without interference.
- □ Take into account the burden on operations and HSSE for supporting multiple work areas and non-routine work.
- □ Carefully assign resources. Dedicate a core of experienced and competent personnel to the project. Assist them with less experienced but fast learning workers.
- □ Start with a larger crew and execute a large portion of the work early on. Reduce to a smaller crew composed of a few select instrumentation technicians and electricians for the final stretch.
- □ Keep a reasonable amount of non-critical tasks as filler work for those days when equipment is not available or if weather conditions do not permit work.
- □ Have a pool of readily available “extra hands” that can be called-in when some larger equipment transfers and shutdowns are taking place.
- □ Allocate sufficient time and resources to complete a software Factory Acceptance Test (FAT) with a simulation environment before installation on site. While the main purpose of the FAT is to fix deficiencies and make improvements to the control system without affecting actual operation, it is an important opportunity to train the operators on the new system and help them take ownership.
- □ Have daily informal meetings involving only a few key people: contractor site supervisor, project operator and project engineer. Plan the day’s activities and challenges. Re-address throughout the day as needed.
- □ Have weekly meetings involving all the stakeholders, produce detailed minutes of meeting and keep each party accountable with action items.
- □ Carefully plan each plant outage, identifying the work crews and tasks timeline, as well as lock-out/tag-out locations.

With dynamic product demand, equipment availability could not always be predicted. Emphasis was given on preparing the work on multiple fronts, with the goal of being able to adapt to the availability of the equipment, keeping the project team (both engineering and electrical contractor) busy at all times, and the schedule on track in regards to project milestones. This was accomplished by careful planning of the execution, identifying dependencies between various pieces of equipment and the impact on plant operation. Through frequent communication with the site operation personnel, continuous onsite presence by the project engineering team and a flexible electrical/instrumentation contractor team, the installation schedule was adjusted daily and tasks reassigned as needed.

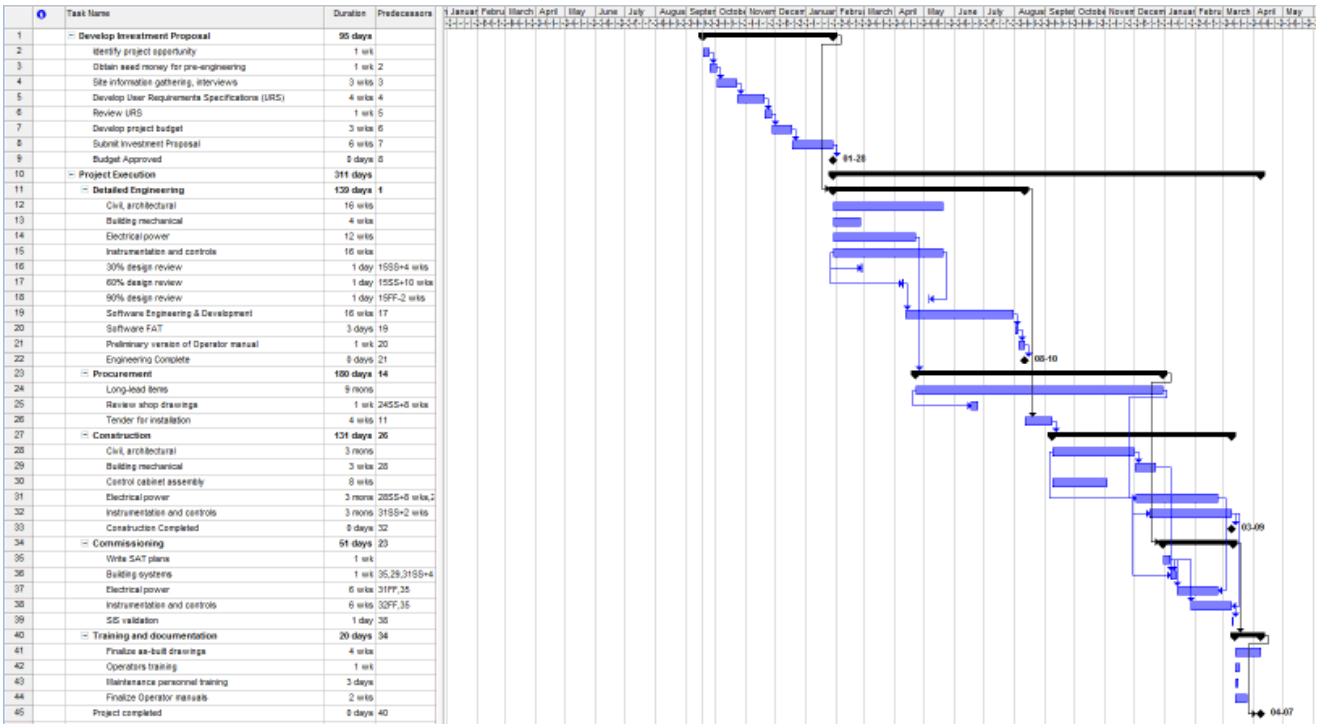

Figure 4.1 Summarized project schedule

4.1.3 OTHER SAFEGUARDS

Involve plant operators and maintenance personnel when developing the project scope. Listen to their opinions and use their experience to identify hardware and software issues, improvement opportunities. Bounce ideas off them during preliminary and detailed design. Keep them informed during construction and commissioning.

For continuity and avoid losing track of some of the early discussions and decisions, the same engineering personnel involved in the design remained assigned to the project during the construction and commissioning phases. The lead project engineer setup office at the terminal during most of the project, in order to be more readily available during construction and resolve any issues as they occurred. This facilitated communication with the other parties and reduced potential cost and schedule overruns.

Record keeping and organization was enforced by the project team. In particular minutes of meeting can be invaluable in avoiding scope creep.

In order to facilitate the project execution, one of the senior operators was assigned to coordinate projects at the site and acted as the focal person for planning the outages and identifying potential risks to operations.

At the beginning of the detailed engineering phase, obtain copies of all relevant existing documentation. Identify drawings that show obsolete information, those that appear in conflict or redundant, those that will require updates, and those that will be completely superseded by the project. A careful study can point to areas that require field surveys to validate the accuracy of the documents.

A relatively small number of hours spent at this stage can save much more later in the project, including potential schedule and cost overruns. Given the scope of the project and its duration, as well as the large number of drawings involved, we deemed essential to continuously maintain a master set of drawings with markups reflecting all changes made during construction and commissioning, instead of waiting until the end. While this speeds up the production of as-built documentation, another purpose is to provide accurate information to the maintenance team at any time during the project. As the equipment was being turned over one piece at a time, maintenance could be required on things that may or may not have been transferred yet.

A register was maintained and made available to maintenance and operations personnel, so that they knew what was still in the old system or had already been commissioned. While the official record was our detailed SAT document, a more visual “running tab” was kept up to date, by highlighting equipment on a set of single-line diagrams and P&IDs available to all for consultation.

During construction, electricians often wait until the end to start labelling cables. We insisted that each cable had at least some temporary labelling, in case troubleshooting was needed after the initial tests.

We reserved a budget to purchase commissioning spare parts. They constitute an insurance policy when you need to get production back in operation. They can be also be used for system development and simulations.

4.2 CONSTRUCTION

4.2.1 NEW ELECTRICAL SUBSTATION

An independent evaluation had identified a number of issues with the current equipment, including the main transformer and 600V switchgear and some of the MCCs at the site. Some decaying underground conduits as well as deteriorating overhead power lines were also present. The project built a new electrical substation at a convenient location, at a sufficient distance from the main hazards, primarily the load racks and the tank farm. New power feeders were installed, via armored cables in cable trays. A new MCC was installed in a new building at a convenient distance from the loads.

The new transformer and switchgear were commissioned first. The commissioning of the new MCC followed. After a “burn-in” period, individual loads were transferred from the old to the new distribution in groups. Grouping the transfers minimized the number of shutdowns required. A single shutdown to transfer all loads at once was judged too risky and would have required a longer outage, and therefore more impact on customers.

Once the new infrastructure was functional, the old power feeders and substation were dismantled.

4.2.2 CONTROL ROOM RELOCATION

A siting review conducted by corporate experts had found that the existing control room was located too close to some of the hazards, namely the pipeline manifold and some storage tanks. They recommended its relocation to a safer area.

A suitable existing building was available, but required some renovations and upgrades before we could use it. Once the required basic building work was completed (power, HVAC, lighting and telecommunication), we installed a new operator console, as well as the new controls and networking equipment. Everything was then tested in preparation for the move date.

The HMI server was installed in the new location right from the start. The thin-client was initially installed in the old control room. The day of the move, we only needed to relocate the HMI thin-client, effectively causing a very short downtime.

4.2.3 PLC AND EQUIPMENT TRANSFERS

Replacing the I/O racks was considered to be the highest risk. With enough simulation and testing, we figured the software could be validated well enough prior to deployment, with some relatively minor adjustments afterwards once in production. However, rewiring I/O racks involves significant downtime and potential errors, and cannot be simulated.

Attempting to simultaneously upgrading both the main PLC, the HMI and at the same time rewiring new I/Os was out of the question. The approach we took to reduce the risk was to first install some communication adapters between the new CPU and the existing I/O racks. This allowed us to first transfer the PLC CPU with its new software, along with the new HMI, but conserving the old I/Os temporarily. This provided for the “peace of mind” of not having to worry about hardware problems in addition to having to deal with the software issues that are normally expected at the beginning.

As the existing MCC was also obsolete, we installed a new I/O rack in a new building. The new cabinet was pre-tested at the shop. We then pre-wired and tested all the interconnections between the PLC and the MCC prior to transferring the power wiring to the motors. The risk would then be small, as the electrician only had to worry about 3 wires for each motor!

Field instrumentation required complete re-wiring to the new I/O modules, and the best we could do was to pre-test the input and output modules prior to transfers.

The PLC program incorporated a dedicated I/O mapping routine in which we had prepared two sets of addresses for the equipment: old and new. After a brief transition period, we started rewiring individual instruments to the new I/Os and motors to the new MCCs. While electricians were busy in the field, a programmer would modify the mapping routine for the specific devices affected that day and remove the old mapping.

Once every I/O point had been transferred, the old I/O racks and remote I/O links were dismantled.

The software library used has built-in simulation functionalities. This allowed conducting a thorough software FAT, test all HMI animations, validate the pipeline transfer sequences, as well as the reporting and alarming capabilities. We also used the test environment to do some early operator training, solicitate their input and suggestions, and most importantly, get their "buy-in" into the new system.

4.2.4 CCTV SYSTEM

Before the move into the new control room, individual cameras were migrated one-by-one to the new system until the old system could be completely decommissioned. Since we had already located the new recorder at its final location inside the new building, it did not need any work. The day of the move, we simply had to take the client computer, relocate it to the new building, and hook it up to UPS power and the network switch. The downtime for visualization was approximately one hour, but the recording was never actually interrupted.

4.3 COMMISSIONING

As the buildings and power distribution systems provide a basic support for the automation systems and components, they inevitably had to be commissioned first.

A single site acceptance test (SAT) plan was created for the project, but it was structured into multiple sub-sections, each covering separate geographical and functional areas.

As virtually all the equipment controlled by the PLCs was rewired and reprogrammed, the commissioning consisted of several verifications. These verifications had to be staged as each task in the schedule was completed, such that the equipment affected could immediately be put back into operation. We could not wait until everything was complete before doing a sign-off. Therefore, the commissioning was an on-going effort, happening in parallel with construction in other areas. This is also reflected in the summarized schedule (Figure 4.1).

As we transferred individual equipment, we had to also include testing of the SIS interlocking immediately. This implied that the SIS functions were activated and tested one at a time, while construction was still ongoing. There was a concern that functions and cabling that had previously been tested may be later jeopardized by construction activities taking place nearby. We judged that a full functional test of the SIS system was warranted after the end of construction, so that we could confirm that the integrity of the system had not been compromised.

We made sure to involve operations and maintenance personnel in the commissioning effort. This is a great training opportunity for them, and it helps them taking ownership of the system. In addition, their insights can make for a safer and more efficient start-up.

The following is a summary of the commissioning sequence used:
- □ Power and building infrastructure
- □ BPCS PLC, SIS PLC, HMI FAT
- □ Pre-test BPCS PLC and new MCC I/Os

- □ Transfer overfill protection and other SIS inputs
- □ BPCS PLC and HMI SAT, using old I/Os
- □ Transfer various equipment and instruments
- □ Control room relocation
- □ Full SIS test

5 CONCLUSION

It is possible to upgrade most of the power distribution and automation infrastructure in a single project. This can create synergies in terms of cost and time required. However, the scope must be established following a thorough assessment of the existing systems.

Careful planning and scheduling, coupled with the experience and sustained dedication from the execution team are then essential to bring the project to a successful completion.

Continuous cooperation and communication between all the parties involved (project management, engineering, plant operations and electrical contractor) are also key to success.