

The Afghanistan Engineering Support Program assembled this deliverable. It is an approved, official USAID document. Budget information contained herein is for illustrative purposes. All policy, personal, financial, and procurement sensitive information has been removed. Additional information on the report can be obtained from Firouz Rooyani, Tetra Tech Sr. VP International Operations, (703) 387-2151.

MEMO

To: [REDACTED]

Cc: [REDACTED]

From: [REDACTED] E
[REDACTED] E, BCEE, AESP Chief of Party

Date: November 30, 2014

Subject: LT-WO-70 Amendment 4 Task 1 & 2 Tarakhil SCADA Decision Memorandum

This memorandum is presented for the fulfillment LT-WO-70 Amendment 4 task 1 & 2. Notice to proceed (NTP) was received for this task on 27 July 2014.

SUMMARY

There are multiple issues with the Supervisory Control and Data Acquisition (SCADA) automatic operating software for the Tarakhil Thermal Power Plant (TTPP). The scope of this work is to determine a solution for the issues and reduce the complexity of the software control system. After the completion of Task 1 of this scope of work, a face-to-face meeting was held in Kabul, Afghanistan to discuss coordination details with the new Commercialization 2 contractor Phoenix. This meeting included USAID, Phoenix's TTPP engineering team and Tetra Tech's field install team. This meeting was to facilitate a working relationship between Phoenix's engineering team and Tetra Tech's field install team. The meeting utilized to finalize the decision that was needed as a result of Task 1 completion and to develop an interim operation plan. The decision to completely replace and upgrade the SCADA software was agreed by all parties involved.

INITIAL CONDITIONS

On-site inspection by Tetra Tech's field team during March 2014 determined several deficiencies in the plant related to the SCADA/HMI systems. These deficiencies require action in order to fully restore plant operations to as-built specifications and accommodate long-term longevity of the plant and continued operations. The Tarakhil SCADA Decision Memorandum created by POWER Engineers defines the existing problems at both a brief level and more detailed level, and presents options to resolve each problem (Appendix A). A diagram representative of the current network configuration is attached (Appendix B).

CONCLUSION

During the meetings held at the Tetra Tech villa on 10 September 2014, the group decided to proceed with Option 2. Option 2 was selected because the entire SCADA software control system needs to be upgraded and its complexity needs to be reduced. Diagrams that represent the future network based on the Option 2 are attached (Appendix C and D). Resulting from the decision to pursue Option 2, it was also decided that the facility will utilize two of the three power blocks through the winter operating season. This limited operation requirement will allow the idle power block to be upgraded. Based on the limited operation detail, the SCADA upgrade process should not affect the total power production need of the facility.

END MEMO

LIST OF APPENDICES

Appendix A POWER Engineers Tarakhil SCADA Decision Memorandum

Appendix B Old Architecture

Appendix C New Architecture

Appendix D New Architecture Network Diagram

APPENDIX A
POWER ENGINEERS TARAKHIL SCADA DECISION MEMORANDUM



MEMORANDUM

DATE: September 26, 2014

TO: Tetra Tech (Kabul Office)

C: [REDACTED]

FROM: [REDACTED]

SUBJECT: Outbrief Memorandum for LT-70 (Tarakhil Power Plant Site Visit and Power Block "B" Control Assessment) Amendment 4 (SCADA Site Visit and Brief of Options)

MESSAGE

This memorandum will briefly describe what the team accomplished during the week-long visit at Tarakhil, and what was decided during the outbrief. Per Task 2 of LT-0070, Amendment 4, "The deliverables for this task will [include] an Outbrief Memo that includes the Task 1 decision and a brief executive summary of the discussion held in the meetings. Interim operational plan courses of action (COA) will be delivered to provide guidelines that should allow the power plant to produce power over the winter running season."

SUMMARY:

The team spent one week in Kabul, visiting the Tarakhil Power Plant twice. While at the site, the team was able to resolve a problem with faulty cylinder exhaust temperature indication. The team also observed additional deficiencies at the site, but did not have sufficient time to resolve them. The team outbriefed USAID and DABS/Tarakhil staff before departing, and during that brief USAID indicated a desire to proceed with an update of the existing SCADA software and hardware.

DESCRIPTION OF MEETING DISCUSSIONS:

The POWER team presented a PowerPoint brief (Enclosure 1) and a decisional memo (Enclosure 2) to USAID and DABS on September 10, 2014. The brief presented two options for resolving the SCADA problems; a "restore to as-designed" option and a "re-design" option. USAID indicated a preference for the "re-design" option, and requested a statement of work and rough-order-of-magnitude cost estimate from Tetra Tech for that work.

INTERIM COURSES OF ACTION FOR WINTER POWER PRODUCTION:

During the outbrief, DABS personnel stated that the Tarakhil plant was expected to produce less than 60MW of production at any given time during the winter months. Because this is within the capability of 2 of the 3 power blocks to deliver, the SCADA upgrade will be planned to affect only one block at a time, leaving 70MW of generation capability in reserve at all times.

Attachments:

- (1) PowerPoint Brief delivered September 10, 2014.
- (2) SCADA decision memo, updated September 26, 2014.
- (3) Revised network diagram including a second Ethernet backbone.

Tarakhil SCADA Decision Brief

September 10, 2014



Trip Report (brief)

- Two 1-day visits
- Analyzed PLC network & HMI network
- Repaired Genset A1 faulty exhaust gas indication
- Noted some additional problems
 - Block C hardware
 - Block A droop (possibly fixed, needs op-test)
 - Block A PLC network fault condition
 - Only 1 PLC programming laptop (“PG”)
 - Breaker coil failed in Block C

Status: System/SCADA/PLC

- System:
 - UPS inoperable, causes hardware and software faults
- SCADA:
 - Complex: 3 individual (but interconnected) SCADA systems (1 per block)
 - Parent/child SCADA in each block, block-specific & unique control seats
 - Multiple points of interconnection
 - Multiple points of hardware failure (Block C)
 - See network diagram for details
 - SCADA misconfigured on Block B (prevents remote block operation)
 - Insufficient number of software licenses
 - SCADA software obsolete and incompatible with any new hardware
 - Genset HMIs combine monitor and PC...single point of failure
 - Hardware old, obsolete, and failing (e.g. Block C)
 - Poor alarm and error handling
- PLC's
 - PLC code stored on volatile RAM, requires frequent restoration
 - PLC code not readable (inhibits troubleshooting)

PROBLEM RESOLUTION: TWO OPTIONS

Repair/Upgrade Options

- Both Options:
 - Upgraded central (“clustered”) UPS
 - HMI replacement with separate monitor and PC
 - SCADA software update and full licensing
 - Hardware replacement
 - Furnish 3ea new PLC programming computers
 - Block B SCADA restoration
 - Installed with no impact on existing operations
- Option 1: “Restore old architecture”
 - Refreshes hardware and software, connects and tests operability only (details to follow)
- Option 2: “Update old architecture”
 - Replace SCADA architecture with centralized servers, virtualized for easier maintenance and reliability and less complexity (details to follow)

Option 1 Technical Description

- Option 1: “Restore old architecture”
 - Refreshes hardware and software
 - Connects and tests operability only
 - No improvements to the system
 - Retains existing system complexity (Parent/child SCADA, block-specific control seats)

Option 1 Cost/Schedule

- Assume all equipment purchased and on site
- Equipment: [REDACTED]
- Labor ~ [REDACTED]:
 - RB SCADA analysis: 4w (1 person)
 - On-site installation: 3-4w (2 person)
 - On-site testing: 3-9w (2 person) (varies based on problems discovered)
 - Total: ~<17 calendar weeks

Option 2 Technical Description

- Option 2: “Update old architecture”
 - Replace SCADA architecture with centralized servers
 - Eliminates complex parent/child SCADA; all control seats support all functions
 - Single software build running on “virtual machine”...de-couples hardware and software
 - Restoration is easy, remotely or locally
 - Facilitates troubleshooting and support

Option 2 Cost/Schedule

- Assume all equipment purchased and on site
- Equipment: [REDACTED]
- Labor [REDACTED]:
 - RB SCADA analysis: 4w (1 person)
 - RB SCADA build: 5w (2 person)
 - RB SCADA test & install rehearsal: 3w (2 person)
 - On-site installation: 3-4w (2 person)
 - On-site testing: 3-5w (2 person) (varies based on problems discovered)
 - Total: ~<17 calendar weeks (less on-site time)

Option 1 & 2 Comparison

	Option 1	Option 2
Improved Power Protection	✓	✓
Mitigated Software/Hardware Obsolescence	✓	✓
Repaired SCADA Mis-configuration	✓	✓
Risk of Additional On-Site Troubleshooting	✓	
Reduced Complexity		✓
Simplified Maintenance & SCADA/PLC Crash Recovery		✓
Increased Operational Flexibility		✓
Improved Error Handling and Alarm Reporting		✓

Path Forward

- Decisions:
 - Option 1 or 2?
 - When to begin?
- Commitments:
 - Procurement (DABS concurrence)
- Further Discussion?

Tarakhil SCADA Decision Memorandum

Introduction

This is a description of solutions to SCADA/HMI-related problems at Tarakhil power plant in Kabul, Afghanistan. On-site inspection during March of 2014 determined several deficiencies in the plant related to the SCADA/HMI systems that require action in order to fully restore plant operations to as-built specifications and accommodate long-term longevity of the plant and continued operations. The following sections define the existing problems at both a brief level and more detailed level, and present options to resolve each problem.

Summary of Existing Problems

The following SCADA/HMI-related problems were discovered during the Tetra Tech March 2014 assist visit. A detailed description of each problem follows in subsequent sections.

- **Power Protection:** Existing power protection system does not function as designed. This failure to properly function had led to damage of software and hardware systems.
- **Wonderware & Windows Obsolescence:** Existing systems are all based on the Microsoft Windows XP operating system, which Microsoft has discontinued support for. SCADA is based on InTouch 9.5, which WonderWare has discontinued support for. Software and hardware upgrades will be necessary when equipment fails.
- **Hardware Obsolescence:** Existing systems run on outdated hardware, making replacement parts difficult to find.
- **SCADA Misconfiguration:** The SCADA deployment for block B was lost due to computer crash, and no backup exists. The master SCADA application for block B must be rebuilt in order to restore stable Block B control and remote control of all other blocks.
- **SCADA Alarm Condition & Error Reporting:** SCADA on all power blocks does not currently handle error conditions properly.
- **Complexity:** Existing architecture is overly complex and has an unnecessarily large number of failure points. This complexity makes it difficult to maintain.
- **Poor Documentation:** Existing system is poorly documented, inhibiting plant maintenance and repair.
- **Setpoints & Calibration:** Over time, existing SCADA and HMI applications have been mismatched to correct hardware failure. As a consequence, individual system setpoints/calibration may be wrong, which could cause the plant to run inefficiently.
- **Crash Recovery:** No system currently in place to restore SCADA or HMI software properly after a crash. Restoration is difficult.

Detailed Problem Description

This section provides a more detailed description of all problems.

Power Protection

Because of voltage instability on the main grid, under-voltage protection relays often trip, opening the breakers and cutting power to the power plant. This is a regular occurrence, observed almost daily during the team's March visit. When the plant loses power, suboptimal system design forces a hard shutdown of the PLC, HMI, and SCADA systems.

There are two main problems with the existing power protection system.

1. Systems currently have UPS protection, but the batteries for these systems are dead and cannot be obtained locally in Afghanistan.
2. Existing UPS does not interface with HMI or SCADA. Systems do not shut down gracefully when batteries are depleted (or dead).

In the case of the HMI and SCADA, which are Windows-based industrial computers, this is especially bad. Hard shutdowns can cause the software image to become corrupt, and can damage the hardware itself. To date, multiple HMI hardware systems have been destroyed. Moreover, after repeated hard shutdowns, software images on the individual HMI's become corrupt. This causes software crashing and requires a complete reinstallation to restore generator operation. Additionally, the HMI itself lacks an on/off switch or a means to manually shut it down properly, or turn it back on after an outage.

Wonderware & Windows Obsolescence

Currently the SCADA and HMI systems are based on Wonderware InTouch 9.5, which is no longer supported. InTouch 9.5 requires Windows XP or 2003 and is incompatible with newer versions of Windows such as Windows 7, 8, or 2012 Server. In addition to this, Microsoft has terminated support for Windows XP, which also means hardware manufacturers no longer develop drivers for Windows XP.

This means current SCADA and HMI software will not run on new hardware. When current hardware fails, which is inevitable (and has already happened to some equipment), replacement hardware will not be able to run the existing SCADA or HMI software.

Hardware Obsolescence

Hardware on existing servers is outdated and replacement parts are difficult to find. Monitors are non-standard resolutions. Servers require outdated memory and operating systems to run.

SCADA Misconfiguration

As a result of hardware failure, critical copies of existing HMI & SCADA software applications and their configurations have been lost. This most severely affects power block B, where the master SCADA application was lost and replaced with the application from block A. Block B's data is received and interpreted as though it is from Block A. This results in communication errors between power blocks and prevents remote control functionality from working.

SCADA Alarm Condition & Error Reporting

The existing SCADA application does a poor job of reporting alarm and error conditions. Currently alarm reporting in the system does not provide a way to acknowledge alarms, and it does not make it clear whether a reported alarm is currently active or left over from a previous state. Moreover, SCADA coding allows the operators to accidentally rename errors, making it difficult to identify specific plant error conditions. As a result, operators cannot tell whether a problem currently exists or whether corrective action was successful.

Complexity

The current SCADA system is overly complicated, see appendix B. The existing architecture has many points of failure, any one of which can cause power block or plant operation to go down.

Poor Documentation

When warnings, alarms, and fault conditions arise in the existing system, the reason is not clearly apparent. The SCADA supplies error codes to the operator which are not useful or intuitive. Moreover, some error conditions have multiple causes, and plant operators are familiar with one cause but not others.

In addition to this, the SCADA system has configuration parameters which can be modified by users. As with the error codes, there is no documentation for these configuration parameters. Although understanding all the configuration options is not necessary for current daily operation, it is important when troubleshooting problems or making adjustments to plant operation.

Set Points & Calibration

Over time, as HMI and SCADA systems have crashed and been restored, configuration settings may have been inadvertently mismatched between power blocks. This is a consequence of plant operator restoration without a proper crash recovery process in place. An analysis of individual power block setpoints should be performed to ensure that individual systems have the proper localized set points and calibrations in place.

Crash Recovery

A procedure for crash recovery does not currently exist. If a node of the SCADA network fails, it will bring down an entire power block, and there is no defined procedure in place which allows plant operators to restore the plant to operational status.

Summary of Proposed Solutions

Two options are summarized below for solving the above-described problems. A detailed description will be presented in subsequent sections.

Option 1 -Restore Old Architecture

Old distributed architecture will be preserved and restored to original as-built operation. New hardware and software will be provided, and an improved uninterruptible power supply (UPS) will be provided. Problems directly related to flaws in the designed architecture will not be fixed. This option will save some cost in engineering labor.

Option 2 -Update Old Architecture

The old architecture will be updated and replaced with a new modern architecture, which is much simpler in design. This simplicity makes the system both more reliable and easier to maintain. New hardware and software will also be provided.

Problem Checklist

This is a quick checklist of the problems addressed by each option.

	Option 1	Option 2
Power Protection	✓	✓
Wonderware & Windows Obsolescence	✓	✓
Hardware Obsolescence	✓	✓
SCADA Misconfiguration	✓	✓
SCADA Alarm Condition & Error Reporting		✓
Complexity		✓
Poor Documentation		✓
Set Points Calibration		✓
Crash Recovery		✓

Detailed Description of Proposed Solutions

This section provides a more detailed description of each solution.

Both Options: Update and Redesign Power Protection

Both options include a redesign of the existing power protection system for all SCADA, HMI, and PLC systems. The existing distributed power protection system will be replaced with a single large and centralized UPS in each power block capable of powering all PLC/control cabinets, as well as HMI and SCADA computer systems, in the power block. The system will be designed to operate with standard 12V automotive batteries, which are easy to procure locally in Afghanistan, simplifying maintenance. This will require electrical work (within the capabilities of the plant electricians) to wire a distribution circuit from the UPS to all the control cabinets in the power block. The central UPS will monitor the state of the battery bank and notify plant operators when batteries require replacement.

A Windows-service-based software application will be developed to monitor the status of the UPS over the network. If power is lost to the facility, computers will shut down automatically to prevent damage to the operating system and SCADA or HMI software deployments. Normally-closed contact switches will be installed in the HMI cabinets so that they may be power cycled and turned back on after a self-shutdown occurs.

Both Options: Update Wonderware & Windows Licenses

All systems will be updated to InTouch 2014 and Windows 8.1 or Windows Server 2012. This is a straightforward process, and is simply a matter of updating the requisite licenses. In the case of the SCADA and HMI, the deployed application also needs to be converted to the updated version of InTouch, which is a mostly point-and-click process, without requiring substantial additional development work. This cost is similar for both Option 1 and Option 2, but with some slight differences. Specifically, Option 2 requires the purchase of two additional Wonderware server licenses to support the simplified architecture.

Both Options: Update System Hardware

Hardware on HMI and SCADA systems will be replaced with current hardware equivalents. The HMI's will be replaced with a two-piece solution that separates the touch-screen interface/monitor from the computer/CPU. The existing system integrates the two, which means that a single highly specialized and expensive piece of equipment must be replaced if any component fails. By separating the two we will increase the reliability and maintainability of the system. In a worst-case scenario, the HMI computer can be replaced with any standard desktop or laptop computer. Likewise the touch-screen monitor can be replaced with a regular monitor. This would be a suitable temporary solution to keep the plant operational while industrial components are shipped from outside of the country.

Monitors on the control room SCADA systems will be replaced with modern wide-screen aspect ratio screens, which are easy to replace through local sources. This will require minor changes to the SCADA applications to accommodate the changed resolution.

Requirements for the updated hardware are similar for both Option 1 and Option 2, but with some slight differences that are detailed below.

Both Options: Repair SCADA Misconfiguration

The master SCADA application for power block B has been reconstructed by taking a copy of the application from power block A and changing hard-coded addresses and other configurations. The Block B master SCADA will be restored to original functionality.

Option 1 -Restore Old Architecture

This option involves repairing the SCADA misconfiguration, as well as updating all the system hardware and requisite software licenses. This will restore the system to as-built design.

Appendices B contain diagrams of the old architecture. As shown in Appendix B, the old architecture is complicated in terms of communication channels. Every single SCADA and HMI system operates as both a servers and access client. In order to operate, the SCADA depends on two-way communication with every node on the network, including all PLCs and HMIs, and the network is broken up into many independent LANs (as shown in Appendix B). This is a very brittle architecture, which is highly impacted by failures at any point in the network. With Option 1, no changes would be made to this network architecture.

In order for remote control (operation of the entire plant from a single control room) to function, the master controller in each power block must be operational. A failure at any one block will prevent the plant from operating from a central location. In this case, however, the plant could still be operated locally at each power block.

There are three different SCADA applications, master, child, and HMI, and varying set/calibration points for each. In the event of a crash recovery, a complicated manual installation and configuration procedure is required in order to restore software to any system that fails. In Option 1, no user interface or feature changes will be made to the existing SCADA application.

Option 2 -Update Old Architecture

In Option 2, the old architecture will be updated and replaced with a new modern architecture, which is much simpler in design. Appendices C and D contain drawings of the architecture and network. This simplicity makes the system both more reliable and easier to maintain. The network architecture will be simplified by bridging LANs that are currently independent in order to create a single SCADA network, as shown in Appendix D.

The current distributed SCADA servers will be replaced with two virtualized servers that import PLC data for the entire plant, rather than just a single power block. The first server is a primary, with the secondary server as a hot redundant installed spare. A cold server backup will also be provided to be stored as spare parts located in the warehouse. All control I/O will go through this central server. Because these systems will run virtualized, they are extremely easy to restore in the event of a crash. Rather than having to manually rebuild and configure the software installation for the entire SCADA system, an operator would only need to restore a copy of virtual image, for which the procedure will be well defined. Standard hardware will be used for the servers, allowing virtual images to be restored to any common hardware, which could be obtained locally.

Six virtualized terminals will then connect to the SCADA servers. These are dumb terminals that simply connect to the server and load a virtual instance of the SCADA client. Consequently, hardware or software failures with the access terminals will not impact plant operations. Each SCADA terminal will also be the same, rather than two different types of terminals as currently exists. Each terminal will have 4 monitors rather than some having only 2 and some having 4. Because the servers are virtualized, they can also be interconnected, allowing a single keyboard and mouse to control both terminals and all 8 monitors in each power block. This enables easier plant operation, since operators will no longer squeeze all control windows onto a few monitors; they can use 4 monitors for each power block, controlling all three at once.

Pricing

Detailed pricing spreadsheets are provided separately, but bottom line amounts are listed below.

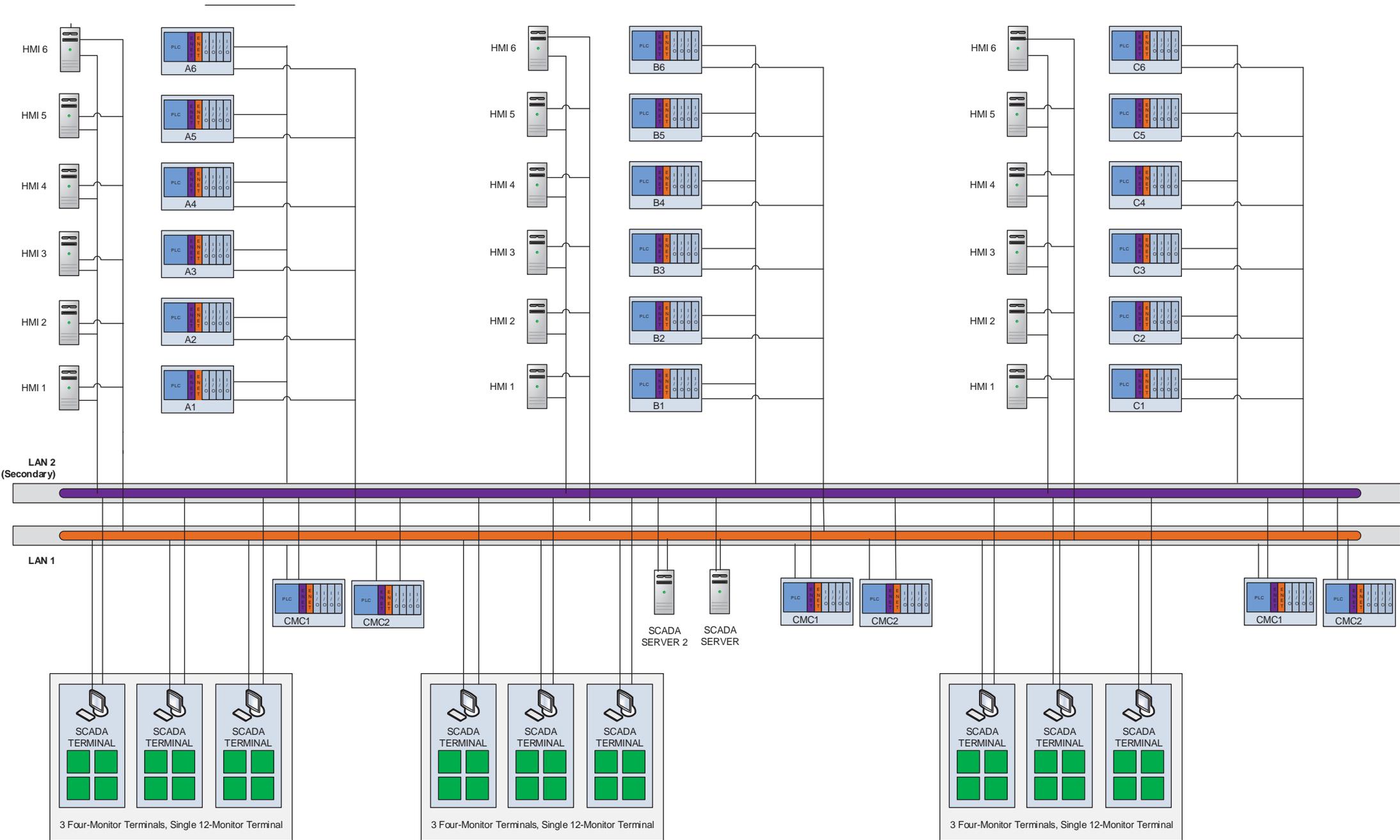
Option 1

Option 1's total material cost is estimated at [REDACTED]

Option 2

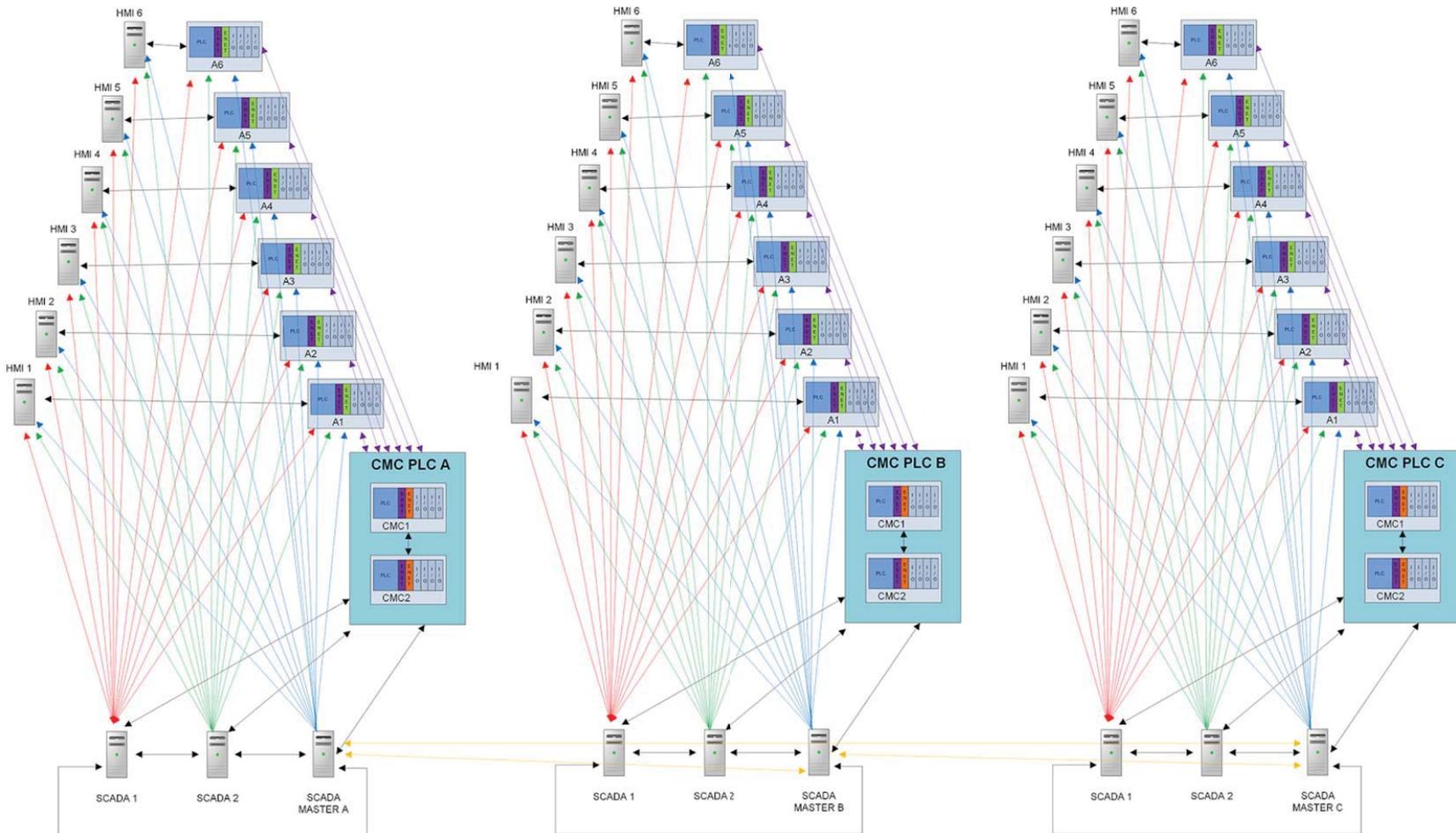
Option 2's total material cost is estimated at [REDACTED]

Option 2: New Architecture Network Diagram



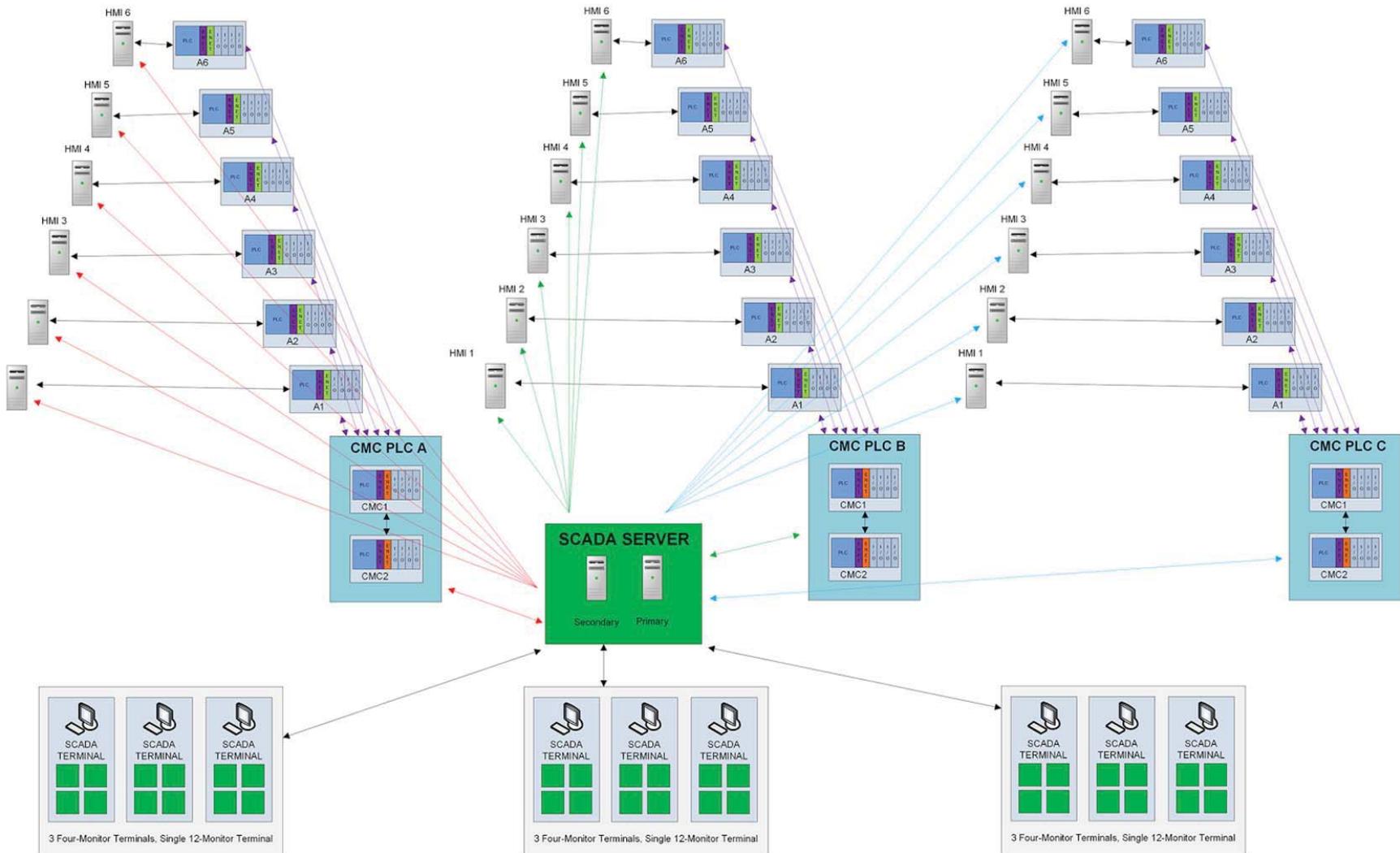
APPENDIX B
OLD ARCHITECTURE

Appendix A: Old Architecture



APPENDIX C
NEW ARCHITECTURE

Appendix C: New Architecture



APPENDIX D
NEW ARCHITECTURE NETWORK DIAGRAM

Option 2: New Architecture Network Diagram

