xxx Location **- SCADA System Deficiencies**

Revised 10/17/2007

Greetings,

As a consultant working for Electrical Solutions Corporation, I have worked at *company* location in various capacities since 1998. Over the years, I have noticed certain deficiencies in the SCADA system. Taken individually, each deficiency might be tolerated as simply a nuisance; however, assessed together, they indicate the need for a major overhaul of the system.

Some of these deficiencies reduce production and increase operating costs; some compromise worker safety or increase the risk of environmental noncompliance; and some place *company* at an increased risk of litigation.

I have attached my recommendations for improving the existing SCADA system, along with my assessment of the problems, as well as a few examples.

Please feel free to contact me to discuss this further.

Sincerely,

Rick Hurdle
Electrical Solutions Corporation

SCADA System Deficiencies – PLC Documentation and Programming

Recommended Action	Reason for Concern	Examples
• Review PLC ladder logic for all (12) PLCs, rung by rung, adding comments and descriptions where appropriate and deleting logic that is no longer being used. • Cross reference PLC database with the WW database and the P&IDs so tagname descriptions are consistent throughout the plant. • Resolve addressing conflicts so each PLC address is referenced by only one WW tagname. • Create WW-based troubleshooting guide for all equipment which has a complicated set of run permissives. This guide should visually show all conditions that could "lock-out" the equipment and the state that each of those conditions are in.	• Poor PLC documentation does not identify obsolete PLC ladder logic, which makes it extremely difficult to understand how the PLCs operate. • Poor PLC documentation increases the need to have a programmer on site to answer questions relating to process operations. • Poor PLC documentation increases the need to have a programmer on site to assist the plant electrician to troubleshoot simple problems.	• Operators and Foremen repeatedly ask for clarification of how ammonia injection compliance for the turbine Cogen is calculated. • Operators repeatedly ask for clarification of what the Thermal Oxidizer Hi and Lo Fire Rate shutdowns are. • Trends in WW show the incoming oil flow rate and the FWKO pressure exactly matching. From a process standpoint, there is no reason why this should be so. • The incoming gas pressure and the Water Tank Vapor Pressure in WW both reference the same data point in the PLC. It is unclear which is correct. • There is no copy of the ladder logic documentation for the new Micro Turbine PLC. Without proper documentation, it is unclear how the micro turbine safeties work. • When starting the Amine pumps, WW might display that the pump is "locked-out." The operator is then expected to know the 9 conditions that might be responsible for the lock out, and check each one of these.

SCADA System Deficiencies – WW Documentation and Programming

Recommended Action	Reason for Concern	Examples
• Review WW database for accuracy and consistency. Items to be checked would include: scaling of analog tagnames, min/max values, PLC addresses, tagname descriptions, alarm priorities, value fields, alarm states, logging frequencies, access names, and alarm groups. • Cross reference all WW tagnames to make sure the I/O points in the PLC are correctly identified. • Modify alarm comments to make sure the comments are meaningful to the operators and provide the information they need. • Modify tagnames as needed to adopt the standardized plant naming conventions per API RP 14C. • Redesign the WW screens, using standard symbols and colors, to make them easier for people with color deficiencies to read. • Review all scripting to make sure the scripting has been programmed correctly and all obsolete scripting has been deleted.	• Obsolete WW tagnames still reference valid PLC addresses. When these PLC addresses are reused with new instrumentation, network traffic increases which slows down computer response to process upsets. • Some WW tagnames are incorrectly identified. This causes erratic – and sometimes dangerous – process conditions. • Incorrect WW tagnames create confusion during troubleshooting. • Many screens in WW contain color combinations that cannot be easily distinguished by somebody with a color deficiency.	• The "Stop Lubricator Pump" button shuts down the CM6 compressor instead of the lubricator. • The "Reset" button on the compressor detail page does not reset the shutdown conditions. This causes frustration for some operators who cannot seem to start the compressor (because it is still locked out). • When trying to recreate the First-In shutdown conditions for a compressor, multiple tagnames are listed which are, in fact, identical events. The alarm comments are ambiguous, which causes confusion over what happened when and what the proper response should be. • When an alarm condition is created for a PID loop, the alarm colors make the PV "disappear" into the background, making it impossible for an operator with a color deficiency to read what the process variable is.

SCADA System Deficiencies – PLC Panel Wiring and Documentation

Recommended Action	Reason for Concern	Examples
• Inspect all control panel wiring, with the aim of producing PLC and motor control drawings for all (12) PLCs and all motors at *company*. • Label all individual conductors at the PLC and in the field according to the drawings created in item #1, so that future electricians will be able to identify the source of power for any device in the plant simply by consulting the instrumentation drawings. • Maintain field copies of PLC drawings at each PLC, and a Master, red-lined, set in the main control room. Send these red-lines out for drafting as needed. • Purchase and maintain spare PLC I/O cards, bases, power supplies, CPUs, radios, network switches, fuses, and terminal blocks.	• Without detailed PLC drawings, it is difficult to know the full extent of the control system. During maintenance or capital projects process control is often changed unintentionally... These errors are only caught when operators notice abnormal operating conditions. • Lack of detailed PLC drawings means that work is often done without properly isolating and locking-out 120 VAC control circuits during testing and maintenance. This can lead to fuses being inadvertently blown, which in turn, can cause essential equipment to stop functioning. • Without detailed drawings, even simple troubleshooting often requires the assistance of the programmer to figure out the problem and recommend a solution. • Lack of drawings and isolation fuses necessitates that instruments often be disconnected in the field instead of at a PLC panel. Inadvertently shorting out control wires can cause a high-impedance electrical fault, which in turn, can cause an electrical surge large enough to damage sensitive electrical components.	• The hard-safety string for CM5 and CM6 does not shut down the compressors anymore. When the switchgear was rebuilt in 2006, it was not understood how the safety string worked, so it was not re-installed. • Wiring diagrams for CM5 and CM6 have been updated but do not correctly show the interconnection between the PLC and the high voltage starters. • WW shows the position of the Maxon valves for fuel, tail gas and vent. But only one of these valves has feedback position switches which are working. The position of the other valves is inferred from the command to open or close the valves. This could lead to an undetected leak-by condition which could cause an explosion. • While working on 120 VAC control circuits during the past week, the *company* electrician managed to blow 4 fuses. Each of these incidents could have had very serious consequences. In one incident, an IC compressor had to be run because the fuse which controlled the ESD stations for the electric compressors could not be located. The fuse was found after 3 hours of tugging on wires to find out where they came from. • An intermittent fault in the Fire and Gas panel caused all electric compressors to shut down while a pig was coming in from offshore. It took 5 hours for the programmer to bypass the system, trace out the wires to find the fault, and repair the connections. • Erratic reading from a temperature transmitter were eventually traced to a bad I/O point on an analog input module to a PLC. But it took 4 hours to trace out these wire and identify the correct module.

SCADA System Deficiencies – Data Accuracy and Reliability		
Recommended Action	**Reason for Concern**	**Examples**
• Purchase a server with RAID-3 hard-drives and redundant network cards. • Change the network architecture from a peer-to-peer system to a server-client system. • Modify WW so instead of running (5) redundant machines, there will be a Master application and (4) Slave applications. Since the slave applications would get their data from the Master, all (5) computers would have exactly the same data. The update time for critical information would drop from 12 seconds to less than 2 seconds. • Setup the server as a time master. All the other SCADA machines would then sync their clocks to the master, so each computer would always show the same time and have the same time stamp for alarm events. • Create a "Communications" screen in WW to monitor the status of communications to all the PLCs. This will require modification of the PLC ladder logic in each PLC so the clock time can be read by WW and modified as needed.	• Data accuracy and reliability are seriously lacking at *company*. Because operators cannot trust the data they view in WW, production becomes less efficient, safety may be compromised, and environmental compliance can be uncertain.	• Different computers nearly always show different data for the same process conditions. Operators are unable to decide which data are correct and so choose whatever data they want to believe. • The time between hitting a button to stop a motor in the Amine Plant and seeing confirmation that it has stopped can be as long as 12 seconds. This is far too long in an emergency situation. • The counter which shows how many seconds before a gas compressor starts, sometimes does not change until after the compressor has started. This makes it difficult to know when to stop the currently running compressor to allow for a smooth shift between compressors. • WW sometimes shows a zero volume of gas heading to flare... even when the operators can see a flame at the flare stack. (Currently, there are plans to install a new flare meter to resolve this issue.) • Periodically, an alarm will be generated at one machine and clear before it is received by the other machines. This drives the operators nuts with "phantom" alarms because the PA system keeps going off all night long, but there are no alarms on the local machine that the operators are monitoring.

SCADA System Deficiencies – Historical Logging		
Recommended Action	**Reason for Concern**	**Examples**
• Install Microsoft's SQL Server and Wonderware's InSQL Server on the new SCADA server to archive and time stamp all historical and alarm data. • Arrange for the IT department to back up the server at regular intervals to an off-site location. The on-site programmer would be responsible for placing any data or backup ladder logic files onto this server. • Eliminate the alarm printers. (With all alarm events and historical data saved to a dual-hard drive computer with off-site backups, the existing alarm printers are no longer needed.) • Purchase and install a new color printer for the main control room. This will allow the operators to print important historical trends and reports. • Program InSQL scripting to calculate daily totals and print reports at the server level to free up PLC processing power. • Create alarm priorities for all WW tagnames. • Modify the Historical and Summary alarm screens to take advantage of the alarm priorities... showing only the most important alarms during process upset conditions.	• Because the time stamp of each computer is different, and the update time for data coming in from the field is so slow, historical and alarm data are sometimes worthless. • APCD requires that ammonia injection data for the turbine be kept for many years and forwarded to them on demand. For various reasons this data is often not available to be forwarded when it is required. • Because obsolete tagnames in WW are rarely deleted (due to lack of documentation), events can trigger alarms for equipment that is no longer in service. This causes the Alarm Log to fill with junk and makes it harder for the operators to identify real alarms that require action. • No backups of PLC hardware, software, ladder logic, Alarm Logs, or historical data are currently being kept by *company*.	• The alarm printer in Cogen room has not recorded any alarms since Nov 2006. (Replacing the printer could resolve this issue, but a better approach would be to go paperless and eliminate the printer altogether.) • The alarm printer in the office has reams of paper spilling all over the floor. The papers become damaged and are sometimes inadvertently thrown away. • The backup printer for the APCD-required daily report, has not functioned for 6 months. So on days when the primary printer is off-line (out of paper, empty ink cartridge, power switch accidentally bumped to the OFF position), no report is generated for the APCD. (Replacing the printer would be a short-term fix, but installing a data historian, e.g., InSQL, would be a better solution.) • At one time, Excel was being used to archive APCD-required data relating to NH3 injection. Visual Basic scripting was used to log the data into a separate file for each day. This scripting is broken, so these data are no longer archived. • The time stamps for events on each machine are different. So on one machine, event A precedes event B, but on another, the order is swapped. This makes it difficult to analyze the historical logs to find the cause of adverse events. • Recently, the programming terminal for the main plant PLC crashed. *company* did not have a spare computer, a copy of the programming software, or the ladder logic. Fortunately, Rick Hurdle had a copy of the programming software on his laptop and had made backups of the ladder logic just the week before.

SCADA System Deficiencies – Legal Compliance		
Recommended Action	**Reason for Concern**	**Examples**
• Purchase copies of drivers and software necessary to fully comply with the software licenses. • Upgrade WW 7.0 to WW 9.5 (WW 7.0 has not been supported by Wonderware for the last 5 years). • Purchase (5) copies of KepDirect to replace DSData. (DSData is not compatible with WW 9.5). • Purchase (5) new SCADA PCs running the WindowsXP operating system. (WW 9.5 and KepDirect are not compatible with Windows NT, and the existing PCs do not have enough memory and speed to handle the newer versions of the software that need to be installed.	• *company* has installed non-licensed copies of software on its SCADA computers in an effort to reduce costs. This places the *company* at increased risk of litigation.	• There are only (2) InTouch (Wonderware) licenses at *company*, but there are (5) instances of the application running. • *company* has (1) copy of DSData. but there are (5) instances of this driver running. • *company* has (1) copy of CTI2572, but there are (5) instances of this driver running. • *company* has (2) copies of ABTCP, but there are (5) instances of this driver running. • The copy of the programming software that *company* uses to program the Amine Plant and Thermal Oxidizer PLCs (RSLogix500) is the personal property of Rick Hurdle.

SCADA System Deficiencies – Safety and Training		
Recommended Action	**Reason for Concern**	**Examples**
• Eliminate all PLC bypasses. (This requires that the PLC and WW database cleanups have already taken place.) • Add bypasses in WW that can be accessed only with the proper user name and password. • Log all bypass actions with the date and time that a safety was bypassed, along with the name of the person who was logged on at the time. (This requires that the WW upgrade to 9.5 has already taken place and that the network architecture has been changed.)	• Many instruments and shutdown conditions are not tested per the requirements of API RP 14C, because the devices cannot be tested without shutting down important processes. • In the past, when a field instrument failed, it was sometimes "bypassed" in the PLC with hard-code. Later, this "bypass" was forgotten... even after the instrument had been replaced. The safety could be bypassed for years without anybody realizing it: there was rarely any record of when the bypass was installed or who installed it.	• CM6 compressor vibration had been bypassed in the PLC and would not shut down compressor. When the compressor threw a rod, it took several minutes for the operator to drive to the compressor building and press the ESD button. • CM6 motor vibration has been bypassed in WW and does not shut down motor. There is no visual indication that the motor vibration has been bypassed and many operators do not realize that the compressor lacks this important safety device. (This item has been resolved: the motor vibration safety is now functional... but there may be other safeties which are bypassed in the PLC of which we are unaware.) • Many Thermal Oxidizer safeties have never been tested while the unit is running because the instruments cannot be placed in a testing mode.