Olympic Pipe Line Company
Pipeline Control Methodology & SCADA System Assessment
Byron Coy PE, 07-02-99

Olympic Pipeline (OPL) has an pipeline control operating philosophy like many other liquid pipeline operators, in that individual stations are designed to operate within safety limits; without depending on a perpetual connection to a headquarter-based SCADA system. This "station interlock" approach incorporates discharge pressure control, mechanical fault sensors, over pressure protection, and a variety of other operating parameters within station control panels, that have been designed to constrain or shutdown station equipment should any number of parameters breach preset threshold values. This technique extends protection to adjacent line pipe by limiting discharge pressure or incorporating pressure relief systems. The most basic example of this approach is the application of a discharge pressure control valve on remote station pumps. A Controller at headquarters may start, increment pressure or stop the pump; but its discharge pressure is limited by station equipment safety settings. These setting will override inappropriate Controller commands, and will react to operational anomalies should they occur. The station interlock technique is designed such that a central SCADA or communications failure will result in the station continuing to operate in the mode last commanded from the SCADA system. If an upset condition occurs during a SCADA outage, the station interlocks may(if thresholds are breached) interject operating restrictions or station shutdown.

OPL operates their SCADA system like most other liquid pipeline operators. The SCADA system is used to track system operations from a global perspective, and to transition the pipeline from one operating mode to another. Typical actions performed by headquarters-based controllers via the SCADA system include:

- monitoring pipeline operating data
- changing the direction of flow from one lateral to another
- starting or stopping pumps
- initiating or changing deliveries
- switching tanks
- reacting to abnormal conditions

Centralized SCADA operations are used to create efficiency in manpower and power consumption; track and control the movement of material across the system; and provide a vehicle for Controllers to identify and resolve hydraulic anomalies. The Controllers' global view of system operations should allow them to react to abnormal conditions before the narrow view of any one set of station interlock equipment could detect a problem. In essence, the Controller uses the SCADA system as a tool to create a "system interlock", where key data from a number of stations is routinely used by the Controller to identify operating problems in advance of alarm thresholds that may eventually occur at individual stations. Although the industry has an interest in adapting computer programs to automatically detect abnormal hydraulic anomalies as system interlock alarms, the numerous and complex permutations of normal operating parameters make it extremely difficult for computers to differentiate between normal from abnormal. As a result, a well-trained human Controller remain the best resource to identify developing operational anomalies.

The current OPL SCADA System was installed in 1990-91. The base product is titled Vector, provided by Teledyne Control Applications. This system was preceded by an earlier Teledyne product, and several other computer-oriented control systems before them. The 1990-91 project included the installation of two Digital Equipment Corp.(DEC) 4300 series computers in a primary/back-up configuration under the VMS operating system. This type configuration places one machine in operation, which periodically conveys data to the backup in order to keep it up-to-date with system operations. The backup is primed and ready to presume operation in light of a failure in the primary. OPL triggers a weekly fail-over to exercise the machines. Although additional memory and disk storage have been added recently, the base computers remain in service as originally installed in 1990-91. The currently installed 3.6-1 version of the Vector SCADA software is the most current revision of the product available for the existing computer platforms. This version was installed in Aug-98. The Vector product has continued to evolve as computer technology has advanced, with the current release of Vector at 4.0-2. It is unlikely that Teledyne will release any further revisions of Vector for the aging 4300 series platforms.

Recent history of changes in the SCADA System Environment			
Date	Operating System(1)	SCADA Application(2)	Physical Equipment Changes
Jul-98	VMS 5.4	Vector 3.5	Unchanged
Aug-98	VMS 6.2	Vector 3.6	Unchanged
Nov-98	VMS 7.1	Vector 3.6	Unchanged
Jan-99	VMS 7.1	Vector 3.6-1	Unchanged
Jan-99	VMS 7.1	Vector 3.6-1	Bayview Station Added
Mar-99	VMS 7.1	Vector 3.6-1	SCADA Memory & Disk Space Added

(1) *7.2 released by DEC earlier in 1999*

(2) *Current version of Vector is 4.0-2, but only available on Alpha platforms*

There were no active or planned projects to make changes or enhancements to the SCADA computer system prior to the accident. Another notable change to the SCADA environment was the addition of Bayview Station at the beginning of 1999. The table below shows that Bayview represents approximately a 15% increase in system data points.

Field Data Points			
Data Type	Typical Application	Bayview Station	OPL Total
Analog	Pressure, Temperature and Gravity Values	158	1034
Digital	Valve Status, Pressure Switch, Winding Temp. Alarms	290	2180
Control	Open/Close Valves, Start/Stop Pumps	121	839
Accumulators	Meters for Line Balance and Custody Transfer	12	125
Tanks	Level Readings for Volume Tracking	7	42
Historical	Defined Virtual Point for Trending and Archive	43	356
Total		759	4576

The SCADA System polls remote locations to collect field data points on a continuous basis, usually collecting fresh data every 5-7 seconds. Communications links from headquarters to field locations is achieved either by conventional leased telephone lines, or through more advance frame relay service, both of which are provided by local utilities. There are no dial back-up facilities to temporally restore field connections during communications failures. In the event of a communications failure at one station, the controller uses his discretion to decide if it is necessary to dispatch field personnel to monitor operations. There is no written guidance to help the controller make the decision. Some of the decision criteria include the expected duration of outage and actions occurring or scheduled for that location.

OPL had experienced some recurring incidents of SCADA system slow-downs, as characterized by the Controllers as "sluggish" only during the daily ticket accounting process that occurs for 5-10 minutes each midnight. During these periods, the system had been slower than normal to gather and display field data, and slow to respond when Controllers entered commands. These periods were noted as beginning after a systems upgrade of the computer operating system and SCADA software in Aug-98. OPL's computer systems support person responded to these situations by adding memory and increasing disk space in 1Q99. The systems support person did not receive any more comments about sluggishness after the computer hardware was added.

The computer systems support person is formerly a full-time pipeline controller, and still fills in as a relief pipeline controller during vacation periods and sickness. Although appearing well-versed in SCADA technology, he has not received any formal training in the operating system or SCADA Applications.

Equilon became affiliated with OPL in Mar-99 as a result of the merger between Shell and Texaco. Shortly after the Equilon affiliation was established, a SCADA systems meeting was planned to compare SCADA operating practices between Equilon, Texaco and OPL. Conflicts in schedules and ongoing project work delayed the target for this meeting until 4Q99. Inquiring about system similarities and differences during this meeting may have been disclosed differences in the historical process configuration.

Shell/Equilon, now majority owners of OPL, also have a Vector SCADA system. They have sent several SCADA analysts to OPL in order to review the configuration and operation of the OPL SCADA System. Their initial assessment was that the current processor load (a measure of computer performance load) was in the 65% range. The configuration had all processes and sub-systems on the primary computer, holding the back-up computer in reserve with no operational load. They also analyzed the apparent SCADA failure to determine that the historical process had encountered a database error in the form of corrupted records. These errors caused the historical process to repeatedly attempt to clear the problem, at the expense of other processes that were critical to controller operations. The Shell/Equilon analysts suggested that the database error had been encountered by other Vector Users. In fact, Shell made changes to their Vector system in about Nov-97 to address a similar problem. Although OPL has participated in User Group meetings sponsored by Teledyne, it is unclear at this time if OPL personnel were aware of the problem or had a plan to address it.

Shell/Equilon analysts believe that the sluggishness reported and resolved with the midnight processing earlier this year may not have been associated with the problem encountered with the historical process during the accident. The corrupted record problem was identified as an error in the historical process and not a problem with field data. When the historical sub-system is called to process a field data element, it performs some manipulation and places the results in its database. A part of that process checks to insure a valid result. If found in error, repeated attempts are made to resolve the corrupted value. The number of retries is defined in the process configuration, after which an error is logged and the process is ended. If there are other field data elements to be handled, the process begins all over again; potentially aggrevating the imposed load on the computer. The corrupted file propagated from one machine to the other, as part of the normal transfer of critical data from the primary to the back-up. The combination of an ailing historical process and dynamic changes in pipeline operations, could have magnified the imposed load on the computer, making it difficult for the Controllers to see and react to the development of an abnormal situation. Ongoing discussions between Teledyne, Equilon and OPL should lead to a better understanding of the problem.

Shell had applied some effort to isolate and permanently solve the ailing historical database problem. Shell's effort to identify the problem was performed on a development machine, independent of their online SCADA system. During that analysis, the configuration of the historical process was modified to minimize the effect of the recurring problem, by reducing retry attempts. According to Equilon analysts, the robust processing power of Shell's SCADA computers, in conjunction with the reformed configuration of the historical process, reduced the problem to a nuisance issue. Their efforts were then redirected to more pressing needs.The current configuration of OPL's SCADA system does not have an independent development machine, making it inappropriate to conduct similar testing at OPL.

The Shell/Equilon analytical work continues, but they have already made two changes to the SCADA system. First, several sub-systems have been moved to the back-up computer to distribute the load, reducing the primary processor load to the 35-40% range. The performance monitor was witnessed on-line at 38% at 16:47 on June-30. Second, they reformed the historical data sub-system by reducing the retry count, so that future database errors are not as severe to processor performance. Changes this week to help enhance processing power was mainly achieved by transferring a few processes to the back-up computer, which was formerly setting idle in the back-up mode. Placing active processes on a back-up computer does not compromise the redundant architecture. Other less-significant fine-tuning was also performed, but of much less value than the process transfer to the back-up computer. As an interim measure, new computer CPU's are being acquired to provide approximately a 500% increase in CPU power, further insulating SCADA system performance from loads imposed by repetitious historical processing. New computer systems will likely be pursued as a long term project effort.

A preliminary SCADA assessment report from Equilon is targeted for delivery to OPS on July-02, but will also be included (perhaps revised) in the complete response to the current version of the OPS Corrective Action Order due in early July.

Findings...

1. The SCADA failure may have occurred during the transition of pipeline operations from one mode to another, requiring a change in pump configuration. The SCADA failure may have prohibited the Controller from completing the transition, leaving the pipeline in an abnormal set-up.

2. The Controllers may have surmissed a developing problem, but were unable to react and control the situation in a timely manner through the failing SCADA system.

3. Although OPL does not have dial back-up for SCADA communications failures, the nature of this particular SCADA failure could not have avoided with dial back-up.

4. The station interlock design applied in OPL should have provided control or shutdown of the pipeline as pressures reached safety limits. Calculation and/or simulation to determine the actual pressures on the pipeline at the time of the accident will help determine if design parameters or field equipment failures were contributing factors to the accident.

5. Portions of the OPL pipeline are now shutdown during investigation, clean-up and restoration. This, in effect, has lessened the operating load of the SCADA system, thereby potentially cloaking any continuing SCADA problems.

6. The inability to interview the Controllers who were on shift during the accident is delaying the analysis of the problem, and is inhibiting the development of a broader understanding of the chain of events that lead to the accident.

7. The inability to interview the Controllers who were on shift during the accident inhibits our ability to determine what impact the SCADA problems may have had on the severity of the accident.

8. The actions already taken to reduce the load on the SCADA primary computer mimics the impact of actions taken within the Shell SCADA system in 1997. This warrants the actions taken as viable.

9. The SCADA systems support person has not received any formal training in computer platforms, operation system, or SCADA applications

10. It appears that the SCADA problems encountered during the accident may have inhibited the routine collection of key events, which may include field alarms, status conditions, as well as logging commands attempted by Controller.

Recommendations...

1. An exerted effort should be applied to piece together an exact sequence of events through the period just before, during and after the accident.

2. The Corrective Action Order should require OPL to report all SCADA fail-overs, errors related to the historical process, or system "sluggishness" to the OPS for consideration in refining the the Corrective Action Order.

3. OPL should be encouraged to continue the dialog with both Equilon and Teledyne, regarding the analysis of the SCADA fault and its resolution.

4. Teledyne analysis of SCADA is critical component of unfinished work

5. Although appearing well-versed, the SCADA systems support person should receive formal training in computer platforms, operation system, and SCADA applications.

6. OPL should be encouraged to establish written guidelines for handling computer and communications failures, including personnel call-out parameters and pipeline shutdown considerations.

7. The Corrective Action Order should be revised when the full details of the events leading to the accident become available.

8. Encourage Teledyne to explain the potential of the historical process problem to their User community.

9. Consider generating an alert notice to inform hazardous liquid pipeline operators that SCADA systems may become overwhelmed during upset conditions, and that measures should be taken to insure that SCADA systems have sufficient capacity to handle worse-case scenanio's.