TABLED DOCUMENT NO. 91 15(3) TABLED ON FEB 9 2005

EMD Plant Day Tank Fill System

Overfill Incident Investigation

Probable Causes

Preventive Recommendations

Prepared by:

Tim Farrell, P.Eng.
October 26, 2004

Jackfish Lake EMD Plant Fuel Overfill

General

An overfill incident at the EMD Plant which resulted in the spilling of a quantity of diesel fuel prompted an investigation into the circumstances surrounding the overfill. The goal of the investigation was to determine the probable cause of the overfill in order to determine measures required to prevent a reoccurrence.

The overfill incident occurred over a period of time starting at around 17:30 September 21 until it was discovered at approximately 08:30 September 22. A rigorous account of fuel held, transferred, and consumed during the period of 16:00, September 21 to 10:00 September 22 resulted in an estimate for the quantity of fuel spilled of 13,000 litres +/- 1,400 litres. At the time of discovery, the day tanks on the two non-running engines, G8 and G5, were filled to overflow.

Summary and Conclusions

The sequence of known events leading up to the spill, together with observations and operating history, rule out all causes for the overfill with the exception of gravity bypass through one of the manual bypass valves, either on G5 or G8. It is possible that one of these valves was either left improperly closed, or bumped, causing it to open slightly, allowing a small flow through the valve for the period from around 16:45 on September 21, until discovery of the spill at around 08:30 on September 22. Estimates of the flow leading up to the activation of the High Level Alarms on Unit G5, together with the final estimate of total quantity spilled over the period, are consistent with a slight opening of the gravity bypass valve on Unit G5.

Several measures are being taken to prevent a re-occurrence of this incident. These measures are outlined below under the heading "Fuel Systems Upgrade Recommendations". The physical modification to the vent manifold has been completed, and lockable valve guards have been placed on all manual bypass valves as an interim safeguard against inadvertent opening of the valves. As an additional interim measure, a security firm has been contracted to carry out a visual inspection of the property every 2 hours during unattended periods, looking for any signs of fuel leakage or spillage. All other recommendations will be completed within the next 90 days.

EMD Day Tank Fill System – General Description

The EMD Plant is fitted with one 275 US gallon day tank for each engine. The day tanks are integral with the engine bases. Each day tank has a dedicated fuel transfer pump which automatically fills the day tank from main Jackfish Lake fuel storage tank. The automatic fuel transfer is controlled by a series of level control switches and pump timers in each day tank.

The level control and overfill protection system for each day tank comprises five independent level control switches plus a timing relay. All power for the control system is provided through the control circuit of the Motor Control Centre (MCC) cell associated with the pump. Switch locations are described as L1 to L5, with L1 being the lowest level and L5 the highest. The control system works as follows:

Normal operation is between L2 and L3. At L2, the pump is started. At L3, the pump is stopped by shutting off power to the motor. If the fuel level continues to rise, the circuit is again interrupted at L4. Activation of L4 is accompanied by a latching alarm (alarm must be reset by operator – doesn't go away with de-activation of L4) indicating change in state of the second high level switch. If the level continues to rise, at L5 power circuit to the pump is again interrupted, with a latching alarm indicating activation of the third high level switch.

The pump is also operated through a timing relay, which is activated by L2 level switch or by setting of MCC selector to Manual. This timing relay allows the pump to operate for a specified length of time. Power to the pump is shut off after this time period, and a latching alarm is activated, indicating pump time-out has occurred. Timer must be manually reset at panel for operation to be restored. The timing relay is normally reset on activation of L3 level switch.

The main supply tank, when full, can provide sufficient head to gravity fill day tanks in the EMD Plant. Available head is sufficient to cause complete filling of vent stack, and subsequent spilling of fuel. Each engine fuel delivery system is fitted with a solenoid valve which opens on call for fuel, allowing the pump to fill the day tank, and then closing to prevent siphoning from the main supply tank. The solenoid valve also provides protection from overfill in the event that the pump motor starter contacts do not open when pump control stops the pump. A solenoid bypass valve allows manual bypass of the solenoid valve for maintenance purposes.

The plant is also equipped with a bypass manifold, allowing each individual fill system to be gravity fed from the main tank. Each bypass is operated by a single 1" gate valve. This valve is

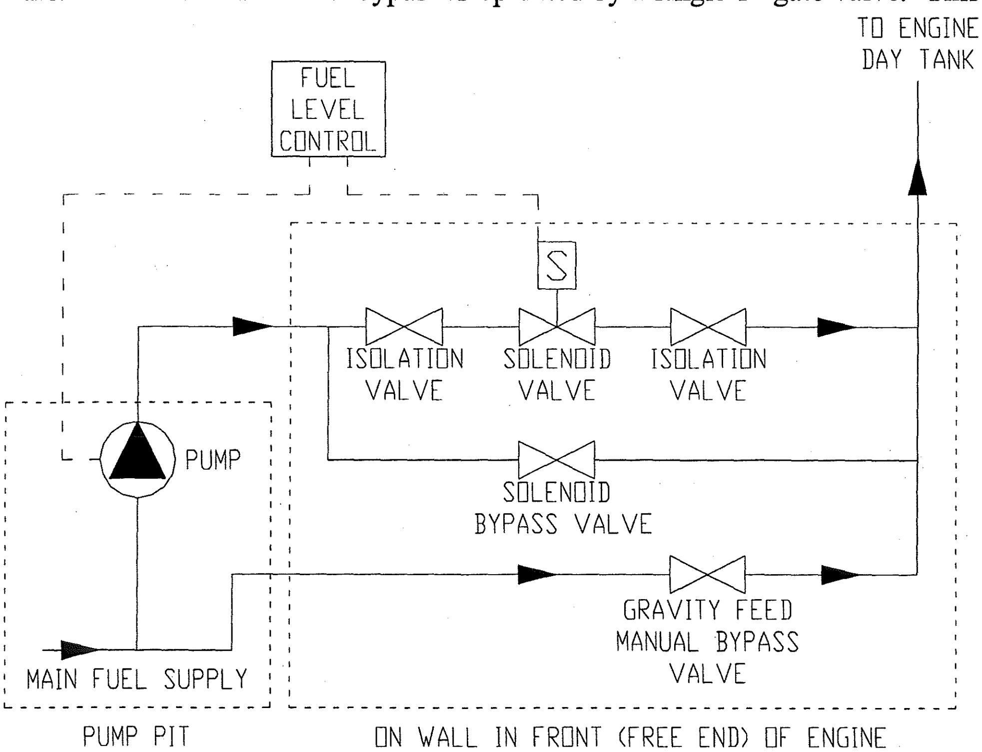

Figure 1 - Day Tank Pump and Bypass System

unlocked, and no procedures are apparent for the manual fill operation. See Figure 1 above. Also see photos 1 and 2 in Appendix A.

The individual fuel control systems do not allow power to the pump if any of the high level switches are activated, or if the timer relay times out prior to the relay being reset by normal operation of the L3 high level switch.

Review of the As-Built drawings for the 2003 fuel control panels indicate that, if the MCC selector switch is placed in manual, the control circuit bypasses the L2 level switch (normal call for fuel). Pumping is started immediately, but stopped, as in normal operations, by L3 level switch. The pump then cycles around the L3 switch, starting and stopping with the opening and closing of L3. The timer is activated, but does not reset until the MCC selector switch is reset to either Off or Auto. This means that, during a manual fill operation, the pump will be controlled by L3 switch. L4 and L5 are still in the circuit providing overfill protection. Eventually the pump timer will expire, causing a "Time-out" pump failure and alarm, regardless of the level in the day tank.

Day Tank Vents – General Description

Each day tank is fitted with a ¾" NPS vent stack, which extends upwards from the tank, then horizontally through the plant wall, and vertically into the bottom of a 3" NPS common vent manifold. The vent manifold has an elbow at the end, with a vertical section draining into a lined 45 gallon drum.

In the event of an overfill resulting in fuel in the vent manifold, fuel will spill into the 45 gallon drum as well as spill into the other day tanks.

Sequence of Events Leading Up to September 21/22 Overfill

The following sequence of events prior to the spill, and immediately after its discovery, was pieced together over a period of several days through discussions with several people who were working on or around the EMD Plant fuel system, on or near the day of the overfill. Information was provided to the Engineering Department mainly by Dennis Glenn, Generation Manager, North Slave; Tom Deleff, Telecontrol Technician, North Slave; and Doug Mortimer, Orbis Engineering.

In December 2003 the EMD Plant Day Tank Level Control System underwent modifications related to the removal of a 90,000 litre auxiliary supply tank outside the plant. The EMD Plant Day Tank overflow/vent piping was connected to this tank, so removal of the tank required an alternative to the overfill protection provided by the overflow pipe.

The control system was modified to provide the level of overfill protection normally installed in plants where the vent line cannot be connected to the supply tank. This protection strategy was reviewed in early 1993 by the GNWT Safety and Public Services Division in consultation with other jurisdictions and the Canadian Standards Association. The review resulted in approval of the control strategy for use in systems where it was not practical to run auxiliary tank vent lines back to the main supply tank.

In September 2004, Orbis Engineering was contracted to add PLC's to the Local Engine Control Panels (LECP) for the EMD units. Orbis completed work on Unit G5 and left site September 18. Orbis also did some work on Unit G8. Status of the work on Unit G8 is not clear. Orbis reports that when they left site on Saturday, Sept 18, Unit G8 fuel pump and LECP DC power were locked out, Unit G5 LECP DC power was on, and Unit G5 fuel pump Motor Control Centre (MCC) selector was in Auto. Units G2 and G3 were operating on the original 2003 control system during the period in question.

The Orbis work on G5 included transferring the level control system from the fuel control panel to the PLC. Orbis maintains that the control system was accurately duplicated in the PLC. Review of documentation supplied by Orbis to date appears to confirm this.

Unit G5 was operated briefly several times during the period September 17 – 21, presumably for testing and adjustment. On September 20, the fuse in the MCC control circuit for G5 fuel pump blew. The open circuit caused by the blown fuse rendered the fuel pump inoperable. This resulted in the engine being taken off line and shut down. The fuse was replaced, and pump MCC main switch reclosed, leaving the pump control circuit energized and in the Auto position. At this time the electrician spoke with the operator to see if they could determine visually what the level switch positions were. The operator advised the electrician that the fuel tank was now full.

On September 21, G5 was run twice in the morning for short periods, presumably to carry out more trouble shooting on the system. Total run time was 14 minutes, with no fuse problem. The event log from the SCADA system indicates that the unit was started again at 16:16, and breaker closed at 16:22. At 16:38, the fuse in the pump control circuit blew again, giving an alarm with indication of fuel pump failure. G5 was subsequently unloaded, and the breaker was opened at 16:44. At 17:12, G5 was shut down. Apparently during this period maintenance personnel were trying to determine the cause of the blown fuse. At some point during the time 16:44 to 17:12, a decision was reached to leave G5 off for the night. The blown fuse was re-inserted, and the fuel pump MCC was switched to the Off position. In this condition, there is no power available to the pump or its control circuit.

At 17:21, the local screen on G5 control panel recorded a High Fuel Level Alarm. This would be fuel level in G5 activating the second high level switch, L4. The L4 switch position on G5 is about ¼" above the top of the tank, meaning that fuel was at a level just entering the vent stack (3/4" pipe). 21 seconds later, the control panel screen recorded a High-High Fuel Alarm, indicating that the fuel level in G5 had now activated the third high level switch, or L5. This switch is positioned 6½" above L4. The fuel was now filling the vent stack.

At the present time, the EMD Plant fuel systems alarms are all sent to the Control Centre SCADA System as a single common alarm signal. There is no allowance for stacking of different alarms in this system. Once a fuel system alarm is annunciated in the Control Centre SCADA, no other EMD Plant fuel system alarm can be received until the original alarm is acknowledged and reset at the source. The original alarm for the pump failure at 16:38 on September 21 would have shown up in the Yellowknife Systems Control Centre as an EMD Plant High Fuel Level Alarm. When the maintenance personnel discovered the problem, they would normally reset the alarm and the annunciation would clear from the System Control panel. In the case of the blown fuse on September 21, it is likely that the maintenance personnel advised the Systems Operator of the problem with the pump on G5. When they left for the night with the pump in the off position, the alarm would have remained latched on the System Control screen, blocking annunciation of the later high level alarms. The System Operator would have no way of knowing that the L4 and L5 alarms had also been triggered.

September 22, about 08:00, personnel arrive in the EMD Plant to continue testing on G5. At this time they noticed fuel on the floor around G5 and G8, and fuel dripping from the vent stack outside the plant. All fuel valves and controls were immediately shut off, and procedures for handling a spill were begun. Day tanks on units G5 and G8 were completely full. Units G2 an G3 were operating, with day tanks at normal levels.

A short time after discovery of the spill, Unit G2 had a Pump Time-out alarm, meaning the pump timer relay had run out, shutting off power to G2 fuel pump. Notes from Dennis Glenn indicate that the alarm was reset and the pump started refilling the day tank. The notes also indicate G2 day tank was about ½ full at the time.

Approximately 10 minutes later, Unit G3 suffered the same alarm, with the same action taken. The day tank for G3 was reported to be slightly less than ½ full at the time.

Level switches and alarms were tested and found to be in working order.

Discussion

A brief summary of the time prior to the discovery of the spill (September 17 to September 21) is shown below.

- Unit G8 was out of service – all power and control systems locked out.
- Unit G5 was operated sporadically between September 17 and September 21. The unit experienced a blown fuse on September 20, and was operated again on September 21, running for at least 36 minutes before the fuse blew for the second time, giving an alarm for pump failure.
- Time of the alarm was recorded at the G5 LECP screen as 16:38.
- Unit G5 was shut down at 17:12, September 21. The blown fuse in the control circuit was re-inserted and the MCC was shut off. No power was available to the pump.
- Alarms on G5 Control Panel indicate fuel in G5 day tank reached the level of the vent stack at 17:21, 9 minutes after G5 had been shut down and 43 minutes after the blown fuse indicated a call for fuel.
- All level switches and alarms were checked by maintenance personnel on September 21, and reported to be operating properly. The proper operation of the level switches on G5 is evidenced by the recording of both high level alarms at 17:21 on September 21.

Units G2 and G3 had been running without incident for several hours or days prior to the spill discovery. These engines were reportedly loaded to around 2200 kW, which corresponds with consumption of a little over 600 litres per hour. This means that the day tank fill systems of these engines would be cycling in under 1 hour. The engines are presently operating without incident, suggesting that they were not involved in the spill. The time-out alarm experienced by both these units, shortly after discovery of the spill, was a one-time occurrence. Review of the circuit diagrams indicates that this time-out would occur if the MCC selector switches were in the Manual or "Hand" position. Given the urgency of the moment at the time of the spill discovery, it is quite possible that these switches were shut off in reaction to the spill, then put in Manual either by mistake, or in an effort to maintain fuel flow to the loaded engines.

Unit G8 was out of service during the entire period, with all power disconnected or locked out. Therefore, the fuel transfer system for Unit G8 is not considered to have contributed to the overfill incident. Unit G8 is directly beside Unit G5. The vent connection from G8 to the common horizontal vent manifold is also beside the connection from G5. It is thought at this time that the day tank on G8 filled through the vent line from the overfill of G5.

Unit G5 was undergoing periodic testing from September 17 to September 21. On September 20, and again on September 21, a fault in the control system wiring caused the control circuit fuse to blow. Orbis discovered a wiring error in the control system on the morning of September 22. A sketch of the wiring error, provided by Orbis after its discovery, indicates that the fault causing the blown fuse would occur at activation of L2 level switch, which completes the pump control circuit, allowing power to the pump, solenoid valve, and timer. This suggests that, in order for G5 to have been able to run for a period of time between faults, some fuel must have been added to the tank, or the pump control was left in the Off position at the MCC. If the L2 level switch remained in the call-for-fuel position, the fault should have resulted in another blown fuse immediately on resetting the MCC selector to auto or manual. The fact that the fuel tank was reported to be full after the electrician had completed his investigation into the pump failure on September 20 indicates that the day tank was manually filled using the gravity bypass during the time between the pump failure alarm and the re-energizing of the pump circuit after replacement of the blown fuse.

All fuel system alarms are individually annunciated on the local fuel pump control panels. On the new G5 PLC installation, all alarms are individually presented on the Local Engine Control Panel screen. At the present time, all fuel system alarms from the EMD Plant are annunciated as a single common alarm at the K-Plant and in the Systems Control SCADA. The original alarm for the pump failure at 16:38 on September 21 would have shown up in the Yellowknife Systems Control Centre as an EMD Plant High Fuel Level Alarm. When the maintenance personnel discovered the problem, they would normally reset the alarm and the annunciation would clear from the System Control panel. In the case of the blown fuse on September 21, it is likely that the maintenance personnel advised the Systems Operator of the problem with the pump on G5. When they left for the night with the pump in the off position, the alarm would have remained latched on the System Control screen, blocking annunciation of the later high level alarms.

The pumping rates for the fuel transfer pumps of G2, G3 and G5 are given by the manufacturer as 26 litres/minute. Calculation for full flow gravity feed from the main supply tank through an open bypass valve indicates a maximum flow of 77 litres/minute with the main supply tank at ½ full. Calculation for the amount of fuel missing over the time between the G5 High-High Level Alarm and discovery of the spill at 08:30 the next morning indicates an average flow rate of 12.6

to 15.6 litres/minute. This is also consistent with the pumping rate required to take the G5 day tank from a call-for-fuel level at 14:38 to an L4 alarm level at 17:21.

Possible Causes of Day Tank Overfill

Fuel pump for Unit G8 was locked out for the period in question. Power for Unit G5 pump was shut off at the MCC after the 16:38 pump failure, and was left in the Off position for the night of September 21/22. In addition, the overfill protection provided by the level switches L4 and L5 on G5 was operating properly. This is evidenced by the record of alarms on the G5 LECP panel, and confirmed by testing on the morning of September 22. The possibility of either of these two pumps or their control circuits contributing to the overfill is thereby ruled out.

If the system was filled by the pumps of the running engines, a failure of the G2 or G3 Level Control System would be indicated. This would require simultaneous failure of 3 level switches on each engine, or possibly a pre-existing failed condition of the high level alarm (L4) and high level lockout (L5) switches, followed by a normal failure of the high level fill (L3) switch. The pump timers should prevent this occurrence, unless the time-out interval is long enough to allow one pump to fill all tanks. The information available indicates that the pumps on the running engines operated normally overnight, providing fuel as required. This plus the fact that the day tank levels were found to be at, or less than, half full at the time of discovery, and the normal result of the level switch test, all indicate that these units did not contribute to the overfill.

Gravity feed of the day tank could occur as a result of a problem with the solenoid valve. A wiring error involving the solenoid valve was discovered along with the other wiring problem on the morning of September 22. The solenoid valve wiring error resulted in a very small amount of current being delivered to the solenoid valve through the PLC at any time the MCC selector switch was not in the Off position. An assessment at the time was that this small amount of current was not sufficient to cause the solenoid valve to move away from its seat. The MCC was on, with the switch in Auto, overnight on September 20 after the blown fuse was replaced. The engine did not run overnight, so there was no call for fuel, leaving the circuit energized throughout the night. If the solenoid wiring error were at fault, an overfill of G5 tank would have occurred overnight on September 20. That was not the case, therefore the indication is that the solenoid valve did not contribute to the overfill.

Overfill by gravity feed may also result from leakage at one of the manual bypass valves, or failure of a manual bypass valve to be fully closed after a manual fill operation. There is evidence of a manual gravity feed operation being carried out shortly after the pump failure alarm on September 20. Had the valve been improperly closed at that time, a spill would have occurred overnight September 20/21. There is no evidence at this time of a manual fill being carried out after the September 21 pump fail alarm. However, with a substantial amount of activity in the area of the bypass valves on the evening of September 21, during the time personnel were investigating the second pump failure alarm, it is possible that one of the valves for G5 or G8 was accidentally cracked open by a passing body, tool box, or something similar. It appears by the estimated flow rates that this would have occurred shortly after September 21 pump failure alarm.

Fuel Systems Upgrade Recommendations

As a result of the overfill incident, the following upgrades have been recommended for the EMD Plant Fuel system. The upgrades address four areas – overfill protection, operation of the manual gravity-feed bypass valves, alarm annunciation, and finally anti-siphon protection for pumping system in the event of solenoid fail-to-close. The recommendations for upgrade to the overfill protection system are not intended to suggest that this system is deficient in any way. Rather, the upgrades simply take advantage of the interconnecting vent manifold to provide an extra level of protection in this unique fuel system.

Overfill Protection

The overfill protection upgrade consists of three parts – modification to the common vent manifold, addition of a 4th high level detection switch, and modification to the pump lockout operation at high level.

First, on activation of L5 (High-High Level Switch), pump lockout will be extended to lock out ALL fuel transfer pumps, not just the engine with the activated L5.

Second, a vertical section will be added at the end of the existing 3" vent manifold to force any overflow to spill into the other units' day tanks. In the event of a pump control failure, the overflow from one day tank will spill into the other day tanks before spilling on the ground. If the pump timer allows an extended pumping time, one or more all of the other day tank L5 switches will activate on L5, shutting off power to ALL of the day tank transfer pumps. This scheme provides quadruple redundancy to the pump lockout at the L5 level.

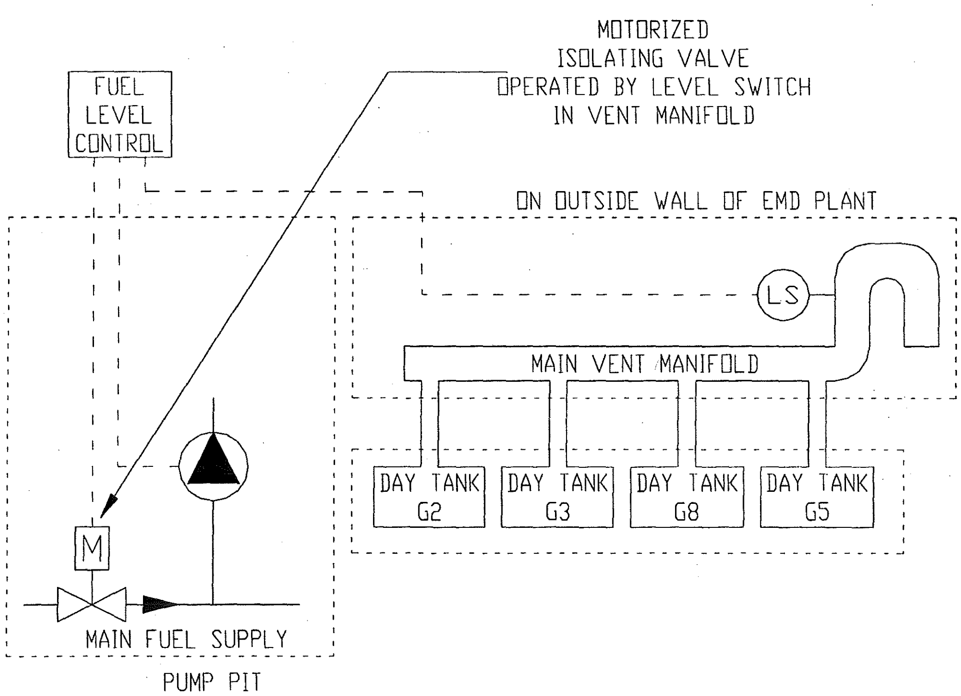

Figure 2 - Proposed Day Tank Venting/Overfill Protection

In addition, a single level switch will be added to the vertical section of the main vent manifold. In the event of overfill of all day tanks and subsequent filling of the vent manifold, the vent level switch will lock out ALL fuel transfer pumps, and activate a motorized valve on the fuel supply line. This will stop all flow of fuel into the EMD Plant, preventing further overfill including that caused by failure of a bypass valve allowing gravity feed of the EMD Plant fuel system. See sketch in figure 2 above. The physical modification to the vent manifold was completed September 22.

Gravity Feed Bypass Protection

The present piping set-up allowing for manual bypass of the transfer pumps and gravity fill of individual tanks will be reinforced by the addition of a second bypass shut-off valve, in series with the original single valve. Recommendation is for a lockable ball valve, locked in the closed position. Proper fuel transfer procedures will be put in place for the operation of this valve, providing control over the use of the manual fill system, and instituting a system of checks for insuring the system is properly locked out after use. As an interim measure, lockable valve guards have been placed on all manual bypass valves.

Alarm Annunciation

The present alarm annunciation between the EMD Plant and the System Control Centre is set to be upgraded with the installation of the new Local Engine Control Panels in the EMD Plant.

All alarms generated by the fuel systems in the EMD Plant will be individually annunciated, so that Plant Operators and System Operators will know exactly what alarm is active on what engine.

Anti-Siphon Protection

Anti siphon protection between the EMD Plant and the main supply tank is already provided by the solenoid valve in the individual engine pump-to-daytank line. This valve also provides further prevention of overfilling if the pump starter malfunctions causing the motor to keep running after a control signal to shut off. In addition to the solenoid valve, a back pressure regulator will be added at the outlet of each pump, requiring the pump to overcome a specified pressure prior to fuel flow. The back pressure regulator is a self contained mechanical valve which prevents flow unless opening pressure is supplied by the transfer pump. The back pressure regulator is set to open at a pressure unattainable by the static head in the system with the main supply tank 100% full. This type of anti-siphon protection is now standard on NWTPC fuel transfer systems. See Figure 3 below for schematic representation of the modified pump piping.

A simple check can be performed to test for proper seating of the back pressure regulator. Installation of a pressure gauge on either side of the back pressure regulator will allow monitoring of the main supply head and the plant distribution system head. To test the valve, the pump inlet valve can be closed, locking in the supply head between the inlet valve and the back pressure valve. Pressures are then monitored for a short period of time to insure that the different

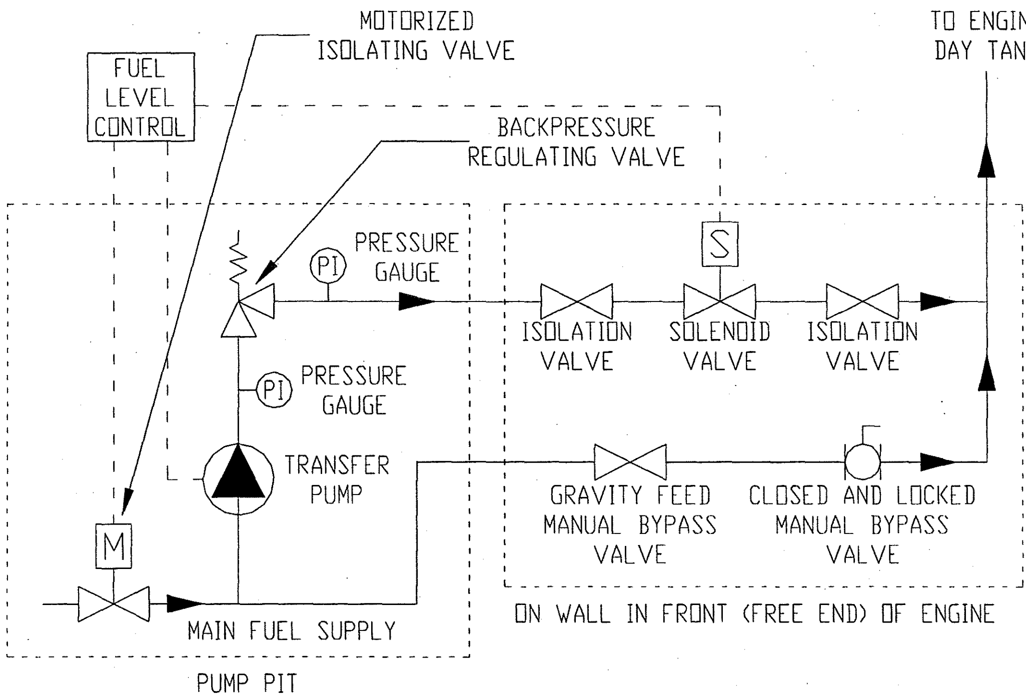

Figure 3 - Recommended Fuel System Modifications

pressures on each side of the valve are not tending to equalize. Equalization of the two pressures indicates a leaking back pressure valve. The individual pump may then be taken out of service until the back pressure valve is replaced.

It is estimated that the above recommendations can be completed within the next 90 days. In the interim, a security firm has been contracted to carry out a visual inspection of the property every 2 hours during unattended periods, looking for any signs of fuel leakage or spillage.

Removal of Fuel Control from PLC

In addition to the above, it is also recommended that the fuel level control systems for G8 and G5 be removed from the engine PLC's and restored to the hard-wired Fuel Control Panels. G2 and G3 fuel control systems should be upgraded as outlined above, but not transferred into the PLC's. This addresses concerns over the single-point-of-failure present with a single pump run output from the PLC. In the PLC set-up, all protection is generated in the programming of the PLC, and the single output is for the pump to run or stop. If this single set of contacts ever fails to open for some unforeseen reason, all other protection is eliminated.

All fuel level alarms should be sent as discrete signals from the Fuel Level Control Panels into the PLC's for communications with the SCADA system.

APPENDIX A - Existing System Photographs

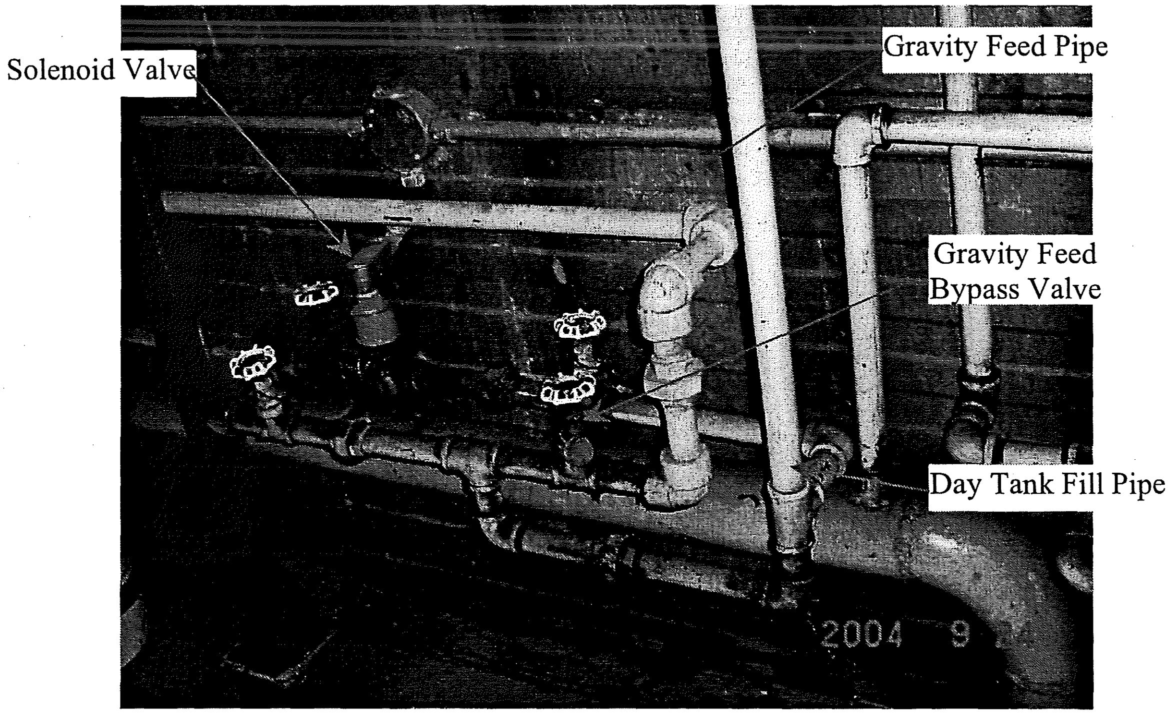

Figure 1 - Unit G8 Fill System Solenoid and Bypass Group

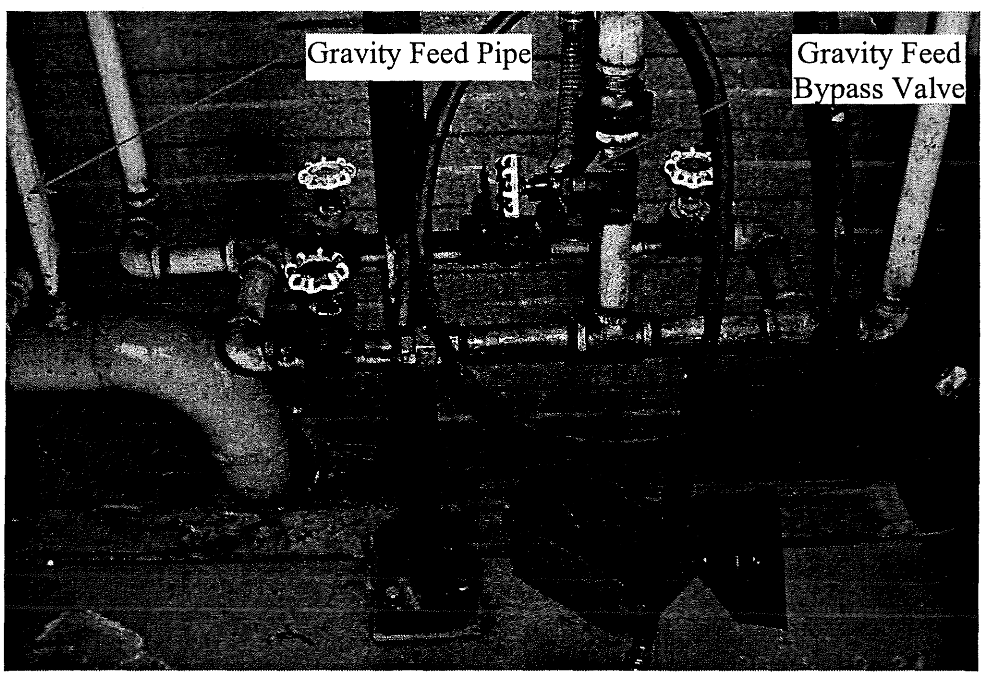

Figure 2 - Unit G5 Fill System Solenoind and Bypass Valve Group

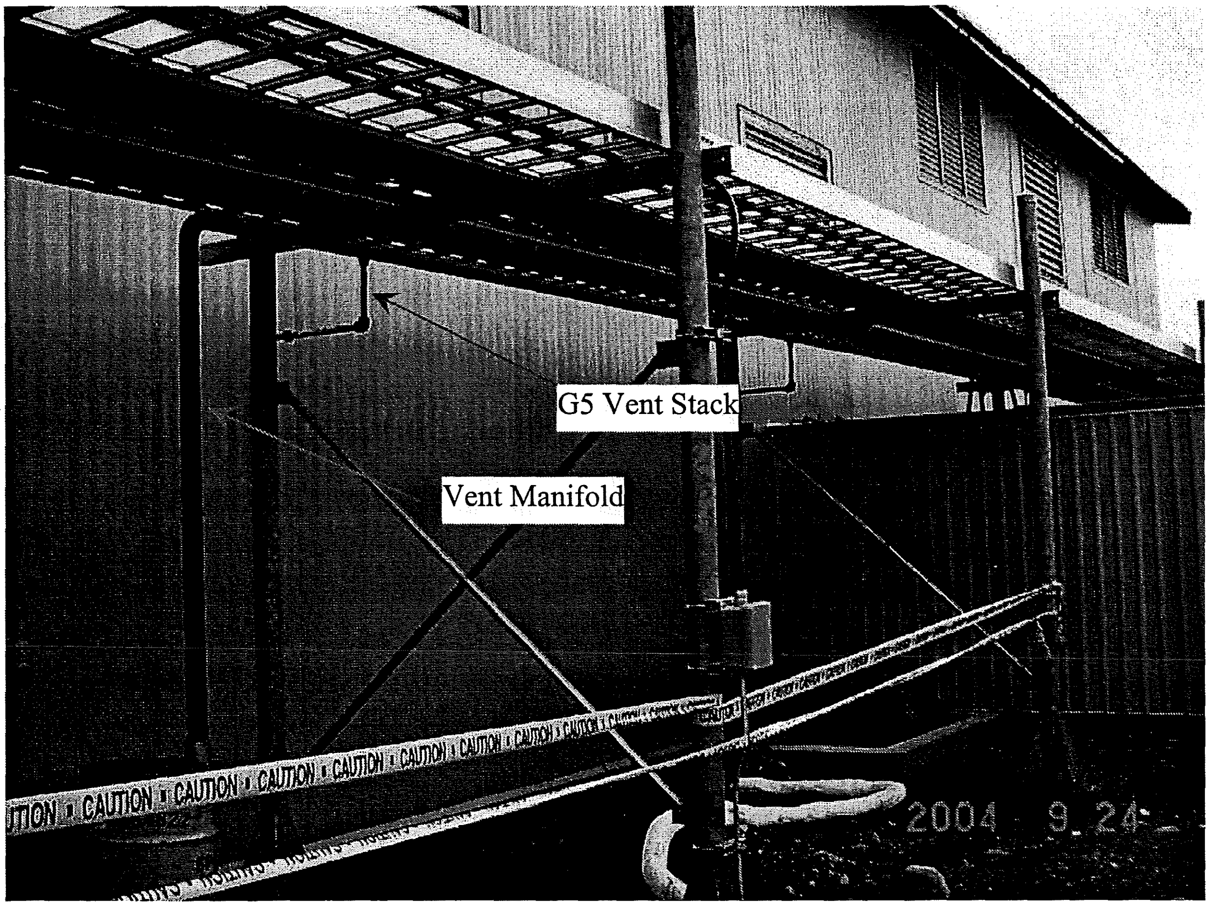

Figure 3 - EMD Plant Vent Manifold

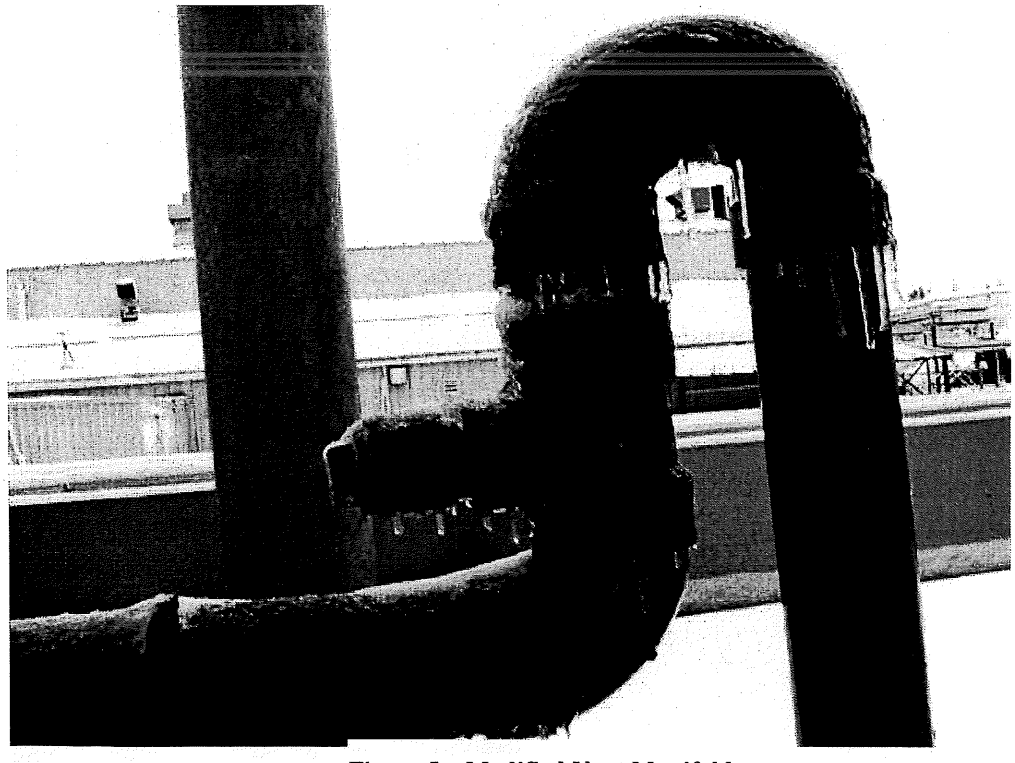

Figure 5 – Modified Vent Manifold

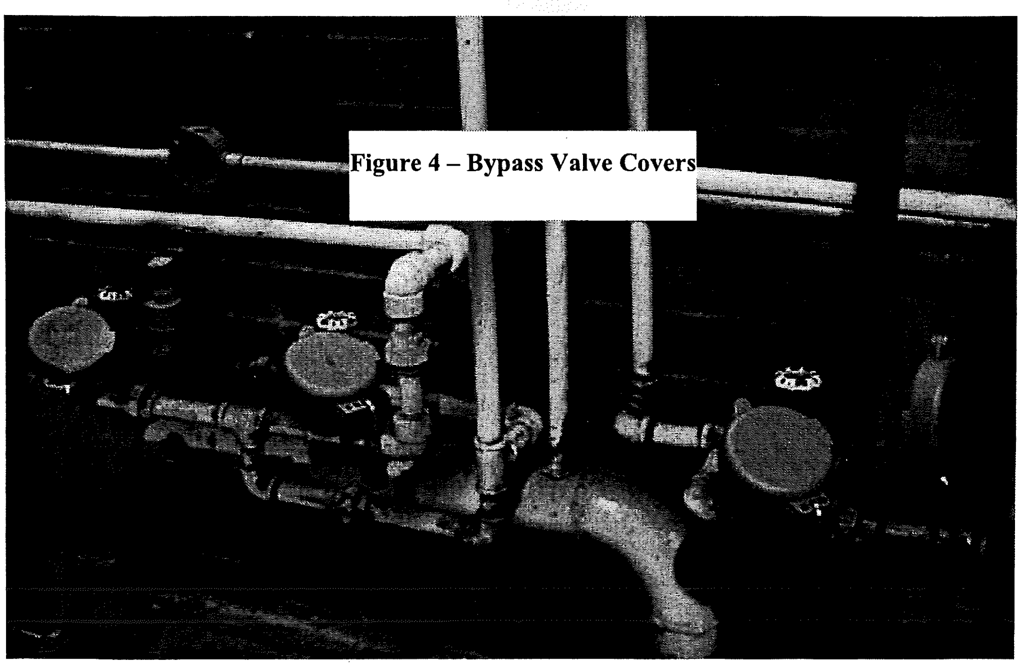

Figure 4 – Bypass Valve Covers