<table>
<thead>
<tr>
<th>Rev</th>
<th>DESCRIPTION</th>
<th>DATE</th>
<th>CREATED</th>
<th>REVISED</th>
<th>APPROVED</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.3</td>
<td>After review with Alan</td>
<td>9/1/2008</td>
<td>MU</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0.2</td>
<td>Draft sent out for review</td>
<td>22-aug-08</td>
<td>MU</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0.1</td>
<td>Initial Draft</td>
<td>07-Aug-2008</td>
<td>MU</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Rev**

**DESCRIPTION**

**DATE**

**CREATED**

**REVISED**

**APPROVED**

---

**TITLE:** SCADA Functional Design Document

**PLACE:** Perth, Australia

**PROJECT:** DBNGP SCADA Upgrade

**Telvent Document Number:** 4JD465-11-0001FDS-S

**Client #:**

**Revision**

0.3

**SHEET N°**

1 of 130
## REFERENCE DOCUMENTS

<table>
<thead>
<tr>
<th>DOCUMENT NUMBER</th>
<th>DOCUMENT TITLE</th>
</tr>
</thead>
<tbody>
<tr>
<td>XXX</td>
<td>Requirements workshop results v11.xls</td>
</tr>
<tr>
<td>XXX</td>
<td>DBNGP SCADA Upgrade Technical Spec v1-6.doc</td>
</tr>
<tr>
<td>4JD465-11-0002DSG</td>
<td>Display Style Guide</td>
</tr>
<tr>
<td>4JD465-11-0003DM</td>
<td>Data Migration Document</td>
</tr>
</tbody>
</table>
PROPRIETARY NOTICE

This document submitted in confidence, contains proprietary information and shall not be transferred to other documents or disclosed to others or used for manufacturing or any other purpose without the prior written permission of Telvent.
### Telvent Revision History

<table>
<thead>
<tr>
<th>Revision</th>
<th>Author</th>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
<td>M. Ulrich</td>
<td>07-Aug-2008</td>
<td>Initial Creation</td>
</tr>
<tr>
<td>0.2</td>
<td>M. Ulrich</td>
<td>22-Aug-2008</td>
<td>Draft sent out for review</td>
</tr>
<tr>
<td>0.3</td>
<td>M. Ulrich</td>
<td>01-Sep-2008</td>
<td>After review with Alan</td>
</tr>
<tr>
<td>CATEGORY</td>
<td>ITEM</td>
<td>BY</td>
<td>COMMENT</td>
</tr>
<tr>
<td>----------</td>
<td>------</td>
<td>----</td>
<td>---------</td>
</tr>
<tr>
<td>Alarms</td>
<td>19</td>
<td>ED</td>
<td>Alarms strategy is developed to suit all the business requirements (incl. operators, maintenance, technical system etc)</td>
</tr>
<tr>
<td>Alarms</td>
<td>33</td>
<td>AB</td>
<td>Must have visual indication of comms failure</td>
</tr>
<tr>
<td>Alarms</td>
<td>47</td>
<td>ML</td>
<td>Comms urgent alarms are displayed in SCADA system</td>
</tr>
<tr>
<td>Alarms</td>
<td>83</td>
<td>RL</td>
<td>Magic delete button. Filter alarms that have been acknowledged and acted upon but are still in alarm state</td>
</tr>
<tr>
<td>Alarms</td>
<td>83.1</td>
<td>AP</td>
<td>Sort acknowledged alarms into field equipment groupings. GTL - Easy for tabular report but do we want to customize the Contractors proprietary dynamic alarm display?</td>
</tr>
<tr>
<td>Alarms</td>
<td>83.2</td>
<td>AP</td>
<td>An alarm shift page capturing outstanding alarms, (i.e. still in alarm state, possible already acknowledged) for the previous shift.</td>
</tr>
<tr>
<td>Alarms</td>
<td>85</td>
<td>RL</td>
<td>Grouping of alarms (parent and child alarms) to manage alarm flooding</td>
</tr>
<tr>
<td>Alarms</td>
<td>87</td>
<td>RL</td>
<td>Alarm escalation to loudspeaker after a configurable time period. Not necessary to escalate to mobile phone SMS after a configurable time period. GTL - Alarm escalation packages are designed to escalate to mobile phone, not to loudspeakers</td>
</tr>
<tr>
<td>Alarms</td>
<td>89</td>
<td>RL</td>
<td>Must support change of state alarms. i.e. alarm on SET and alarm again on CLEAR</td>
</tr>
<tr>
<td>Alarms</td>
<td>90</td>
<td>RL</td>
<td>Controller requires ability to change alarm limits e.g. HH alarm limit. Note must have audit trail and an audit trail report. Must be able to see and report alarm limits as a popup and a tabular report. E.g. Report of alarm name, description LL L H HH; is this a setpoint high limit or a shutdown alarm high limit???</td>
</tr>
<tr>
<td>Alarms</td>
<td>93</td>
<td>RL</td>
<td>Must have ability to apply an out-of-service tag. (A text message attached to a point that always displays on a schematic as a &quot;Tag&quot; symbol and can be listed in a report) Must have Area of Responsibility protection. I.e. can only be applied by control room. Text to be displayed on mouse-over or similar.</td>
</tr>
<tr>
<td>Alarms</td>
<td>98</td>
<td>BB</td>
<td>Correlation of events with process parameters</td>
</tr>
<tr>
<td>Alarms</td>
<td>132</td>
<td>AB</td>
<td>Ability to have the system SMS the call out engineer in case of system critical alarms</td>
</tr>
<tr>
<td>Alarms</td>
<td>135</td>
<td>AB</td>
<td>Alarm escalation SMS or email for system critical alarms</td>
</tr>
<tr>
<td>Alarms</td>
<td>155</td>
<td>AP</td>
<td>Ability to search for tags by field types, like “all pressure tags”, or by description</td>
</tr>
<tr>
<td>API</td>
<td>56</td>
<td>JH</td>
<td>Ability for performance counter to be accessible from third party performance monitoring tools</td>
</tr>
<tr>
<td>API</td>
<td>58</td>
<td>SN</td>
<td>Must have ability to access data via standard interface (e.g. ODBC)</td>
</tr>
<tr>
<td>API</td>
<td>59</td>
<td>SN</td>
<td>Must have data query tool</td>
</tr>
<tr>
<td>API</td>
<td>60.1</td>
<td>SN</td>
<td>Published schema for all historical databases</td>
</tr>
</tbody>
</table>

This table may be removed in the final document.
<table>
<thead>
<tr>
<th>CATEGORY</th>
<th>ITEM</th>
<th>BY</th>
<th>COMMENT</th>
<th>SPEC</th>
<th>FDS</th>
</tr>
</thead>
<tbody>
<tr>
<td>API</td>
<td>173</td>
<td>BB</td>
<td>Bentley Nevada vibration protection package (1701, 2201, 3300). Currently reactive protection system. Hope to move to proactive detection system (System 1) or similar. Raw time waveform, FFT, orbits, rolling buffer of data for start, stop, trip and continuous. Would be nice to be able to fully integrate with this new system, and retrieve and present all this data to end users.</td>
<td>10.4</td>
<td>Dupl. of 105</td>
</tr>
<tr>
<td>API</td>
<td>175</td>
<td>BB</td>
<td>Better integration between SCADA and MAXIMO for things like scheduling maintenance tasks. Run-times are especially important.</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Auditing</td>
<td>75</td>
<td>JH</td>
<td>Must ensure database configuration changes and control commands are tracked and logged.</td>
<td>15.16</td>
<td>3.5.1.4</td>
</tr>
<tr>
<td>Auditing</td>
<td>114</td>
<td>SJ</td>
<td>Audit trail or event log of who acknowledged an alarm and timestamp of when.</td>
<td>21.6</td>
<td>3.5.1.4</td>
</tr>
<tr>
<td>Auditing</td>
<td>134</td>
<td>AB</td>
<td>Audit tracking on configuration items within the system Screens and Database</td>
<td>15.7</td>
<td>3.5.1.4</td>
</tr>
<tr>
<td>Calculations</td>
<td>26</td>
<td>ED</td>
<td>Must retain ability to use FLOW COMPUTER snapshot accumulator functionality using MSW and LSW for hourly accumulator read. SCADA must perform the following calculation to establish total for hour just passed: Add current MSW and LSW with 1000 offset and then subtract previous hour MSW and LSW addition value. Note must for MSW rollover at 999,999</td>
<td>18.1</td>
<td>3.4.1.1 10.3.3</td>
</tr>
<tr>
<td>Calculations</td>
<td>118</td>
<td>SJ</td>
<td>Ability to perform simple calculations in tags e.g. Volumetric flow conversion to standard flow or to Mass flow</td>
<td>12.4 20.10.5</td>
<td>3.4.1.1 2.7.1.10 10.3.3</td>
</tr>
<tr>
<td>Cleanup</td>
<td>20</td>
<td>EDJ H</td>
<td>Undertake audit to eliminate unused data points before transfer</td>
<td>6.1</td>
<td>16.3.1.1.b</td>
</tr>
<tr>
<td>Cleanup</td>
<td>104</td>
<td>BB</td>
<td>Need to determine what points are required. How do we do this? Also need to purge unused points</td>
<td>6.1</td>
<td>16.3.1.1.a</td>
</tr>
<tr>
<td>Cleanup</td>
<td>124</td>
<td>GM</td>
<td>There may be errors in the data were we have interchanged MODBUS-Daniels and MODBUS-enron during the installation of the Telvent system. Values are “close” but not correct</td>
<td>14.7.7</td>
<td>16.3.1.1.b</td>
</tr>
<tr>
<td>Cleanup</td>
<td>125</td>
<td>GM</td>
<td>Some important points are not trended</td>
<td>23.2</td>
<td>16.3.1.1.b</td>
</tr>
<tr>
<td>Cleanup</td>
<td>151</td>
<td>AP</td>
<td>Need to finish this pre-work before tender</td>
<td>6.4</td>
<td>16.3.1.1.b</td>
</tr>
<tr>
<td>Cleanup</td>
<td>159</td>
<td>SN</td>
<td>Develop an internal formalized point configuration notification process</td>
<td>36</td>
<td>16.3.1.1.a</td>
</tr>
<tr>
<td>Cleanup</td>
<td>171</td>
<td>BB</td>
<td>All known and unknown faults need to be fixed before upgrade to ease the cutover</td>
<td>6</td>
<td>Dupl. of 20</td>
</tr>
<tr>
<td>Cutover</td>
<td>69</td>
<td>JH</td>
<td>Must be seamless and transparent for operations</td>
<td>35.1</td>
<td>13.2.9.3</td>
</tr>
<tr>
<td>Data Output</td>
<td>62</td>
<td>GD</td>
<td>Must prepare hourly and daily billing and field data</td>
<td>25</td>
<td></td>
</tr>
<tr>
<td>Data Output</td>
<td>64</td>
<td>GD</td>
<td>Must have ability to extract data on scheduled basis (e.g Worsley/Alcoa data) to file and then FTP to other locations</td>
<td>17.8</td>
<td>3.4.3.1 5.7.3.2</td>
</tr>
<tr>
<td>Data Output</td>
<td>165</td>
<td>RB</td>
<td>Ability to retrieve instantaneous and historical data for modeling purposes</td>
<td>15.13 16.11</td>
<td>Dupl. of 58</td>
</tr>
<tr>
<td>Data Output</td>
<td>177</td>
<td>SJ</td>
<td>Must have a report customization facility</td>
<td>24.11</td>
<td>5.7.3</td>
</tr>
<tr>
<td>Documentation</td>
<td>60</td>
<td>SN</td>
<td>Must have system documentation from vendor and relevant training</td>
<td>33 34</td>
<td>13. 14.</td>
</tr>
<tr>
<td>Documentation</td>
<td>92</td>
<td>RL</td>
<td>Must provide sys admin training documentation</td>
<td>34.2</td>
<td>14.</td>
</tr>
<tr>
<td>Documentation</td>
<td>154</td>
<td>AP</td>
<td>Online help linked and driven by alarm conditions</td>
<td>21.14</td>
<td>10.3.4.2</td>
</tr>
<tr>
<td>CATEGORY</td>
<td>ITEM</td>
<td>BY</td>
<td>COMMENT</td>
<td>SPEC</td>
<td>FDS</td>
</tr>
<tr>
<td>----------</td>
<td>------</td>
<td>-----</td>
<td>---------</td>
<td>------</td>
<td>-----</td>
</tr>
<tr>
<td>Field data</td>
<td>1</td>
<td>ED</td>
<td>All data from field devices should be returned to SCADA historian</td>
<td>10.4</td>
<td>3.3</td>
</tr>
<tr>
<td>Field data</td>
<td>2</td>
<td>MD</td>
<td>Must support sequence of events (SOE) for all new sites which have a transport layer such as DNP3</td>
<td>12.1</td>
<td>3.3.2.2</td>
</tr>
<tr>
<td>Field data</td>
<td>3</td>
<td>JH</td>
<td>Replicate current sequence of events (SOE) capability on CONITEL sites</td>
<td>12.7</td>
<td>3.3.2.2</td>
</tr>
<tr>
<td>Field data</td>
<td>4</td>
<td>ED</td>
<td>Current subset of data from all sites must be present in the new system (including historical data)</td>
<td>10.4</td>
<td>16.3.3</td>
</tr>
<tr>
<td>Field data</td>
<td>5</td>
<td>ED</td>
<td>Must be able to talk CONITEL</td>
<td>9.15</td>
<td>14.7.4</td>
</tr>
<tr>
<td>Field data</td>
<td>6</td>
<td>ED</td>
<td>Must be able to talk MODBUS - RTU, DANIEL/ENRON, IEEE floating point and &quot;MODICON&quot; floating point</td>
<td>14.7</td>
<td>3.3.2.2</td>
</tr>
<tr>
<td>Field data</td>
<td>7</td>
<td>MD</td>
<td>CONITEL will be phased out in an estimated next 3 years due to non-standard comms infrastructure and RTU are obsolete</td>
<td>10.6</td>
<td>noted</td>
</tr>
<tr>
<td>Field data</td>
<td>12</td>
<td>ED</td>
<td>Capture all data via MODBUS</td>
<td>14.7</td>
<td>Dupl of 5</td>
</tr>
<tr>
<td>Field data</td>
<td>13</td>
<td>ED</td>
<td>Capture all data via MODBUS. Note: We currently use MODBUS RTU and do not use MODBUS ASCII. We should support MODBUS IP</td>
<td>14.7</td>
<td>Dupl of 6</td>
</tr>
<tr>
<td>Field data</td>
<td>27</td>
<td>MD</td>
<td>Do not continue practice of RTU performing a snapshot of RTU accumulators for flow total data for new RTUs. Must support it for now</td>
<td>18.1</td>
<td>4.2.1.2</td>
</tr>
<tr>
<td>Field data</td>
<td>29</td>
<td>MD</td>
<td>SCADA system able to control and download RTU configuration</td>
<td>Protocol dependent</td>
<td></td>
</tr>
<tr>
<td>Field data</td>
<td>32</td>
<td>AB</td>
<td>Do not want protocol converter as an interface (FEP). It is important to note that a passive interface device may be acceptable however an interface which needs to be programmatically configured will not be acceptable</td>
<td>15.12</td>
<td>None provided</td>
</tr>
<tr>
<td>Field data</td>
<td>105</td>
<td>BB</td>
<td>Moving towards on-line monitoring of vibration using a proprietary local system. Can identify root cause of a problem very early. How will this hook into the new SCADA? i.e. only alarms? Probably connect via MODBUS</td>
<td>10.4</td>
<td>9.2.1</td>
</tr>
<tr>
<td>Field data</td>
<td>122</td>
<td>GM</td>
<td>Should have front end communication device to perform communication with remote devices</td>
<td>10.2</td>
<td>3.3.5.8</td>
</tr>
<tr>
<td>Field data</td>
<td>127</td>
<td>DS</td>
<td>Need to integrate and drill down. Don’t know what you need until it occurs</td>
<td>20.6.4</td>
<td>5.2.3.3</td>
</tr>
<tr>
<td>Field data</td>
<td>147</td>
<td>AB</td>
<td>Physical termination to the system will be via RS232</td>
<td>12.5</td>
<td>2.9.1.5</td>
</tr>
<tr>
<td>Field data</td>
<td>170</td>
<td>BB</td>
<td>all digitals from all units at all sites should be brought in</td>
<td>10.4</td>
<td>16.3.1.1.e</td>
</tr>
<tr>
<td>Field data</td>
<td>174</td>
<td>BB</td>
<td>would be nice to bring in vibration data from site, and store it in a centralized location</td>
<td>10.4</td>
<td>Dupl. of 105</td>
</tr>
<tr>
<td>General</td>
<td>48</td>
<td>GD</td>
<td>Ensure no shortfall between comms and SCADA upgrade scopes for remote operator stations</td>
<td>8</td>
<td>5.</td>
</tr>
<tr>
<td>General</td>
<td>49</td>
<td>ML</td>
<td>Must ensure suitable review and supervision of commissioning and installation and handover plans and drawings</td>
<td>32.7</td>
<td>13.2.9</td>
</tr>
<tr>
<td>General</td>
<td>50</td>
<td>JH</td>
<td>1. Must be able to run old and new systems in parallel 2. Cutover strategy requires further development</td>
<td>32.2</td>
<td>13.2.9.3</td>
</tr>
<tr>
<td>General</td>
<td>55</td>
<td>JH</td>
<td>Must have timely notification of bugs and patches</td>
<td>38</td>
<td>13.2.2.1.c</td>
</tr>
<tr>
<td>General</td>
<td>65</td>
<td>JH</td>
<td>Must replicate existing functionality</td>
<td>12.1</td>
<td>Noted</td>
</tr>
<tr>
<td>General</td>
<td>67</td>
<td>GD</td>
<td>Must ensure existing screens, data points and functionality are transferred to the new system accurately</td>
<td>31.5</td>
<td>16.3.1.1.c</td>
</tr>
<tr>
<td>CATEGORY</td>
<td>ITEM</td>
<td>BY</td>
<td>COMMENT</td>
<td>SPEC</td>
<td>FDS</td>
</tr>
<tr>
<td>----------</td>
<td>------</td>
<td>-----</td>
<td>---------</td>
<td>-------</td>
<td>------</td>
</tr>
<tr>
<td>General</td>
<td>166</td>
<td>BB</td>
<td>ability to associate data into logical groups</td>
<td>15.9</td>
<td>5.5.1.5</td>
</tr>
<tr>
<td>General</td>
<td>169</td>
<td>BB</td>
<td>be able to assign custom meta-data tags to all points, i.e. compressor units, compressor site, unit type, data type (pressure, temp, flow etc)</td>
<td>15.9</td>
<td>3.6.1.4</td>
</tr>
<tr>
<td>GMAS</td>
<td>63</td>
<td>GD</td>
<td>Must understand the benefits of Epic Energy’s GMAS and the effect it could have on our billing process</td>
<td>GMAS</td>
<td></td>
</tr>
<tr>
<td>Hardware</td>
<td>41</td>
<td>JH</td>
<td>Must be fully redundant in a hot standby arrangement</td>
<td>27.3</td>
<td>12.2.3.2</td>
</tr>
<tr>
<td>Hardware</td>
<td>57</td>
<td>JH</td>
<td>Client must be deliverable to a Microsoft Windows platform</td>
<td>3.2</td>
<td>5.1.1.3</td>
</tr>
<tr>
<td>Hardware</td>
<td>77</td>
<td>JH</td>
<td>System must be able to handle existing and future point count and follow on effect with regards to software, hardware and data requirements</td>
<td>14.2</td>
<td>11.2.1.1</td>
</tr>
<tr>
<td>Hardware</td>
<td>78</td>
<td>ED</td>
<td>Must ensure printing capabilities suit stakeholder requirements</td>
<td>13.13</td>
<td>12.4</td>
</tr>
<tr>
<td>Hardware</td>
<td>80</td>
<td>GD</td>
<td>Must ensure new system is suitable for existing utilities (power, HVAC)</td>
<td>1.2.3.1.b</td>
<td></td>
</tr>
<tr>
<td>Hardware</td>
<td>82</td>
<td>JH</td>
<td>Must ensure new hardware fits into 19” racks</td>
<td>13.15</td>
<td>12.5.1.1</td>
</tr>
<tr>
<td>Hardware</td>
<td>130</td>
<td>AB</td>
<td>Need to introduce a test system which is a direct imitation of the production system</td>
<td>9.14</td>
<td>2.3.2.8</td>
</tr>
<tr>
<td>Hardware</td>
<td>133</td>
<td>AB</td>
<td>Remote XOS stations need to be placed at all of the compressor stations which will only have the ability to view not operate the asset. The terminals need to be locked down so that interference to the system is kept to a minimum</td>
<td>10.8</td>
<td>2.7.2</td>
</tr>
<tr>
<td>Hardware</td>
<td>140</td>
<td>AB</td>
<td>It is the intention that the successful supplier will purchase the hardware from Perth Australia, unless agreed, and then FAT at their location</td>
<td>13.7.2</td>
<td>12.1.1.8</td>
</tr>
<tr>
<td>Hardware</td>
<td>141</td>
<td>AB</td>
<td>The successful tender will supply all of the necessary hardware for the system including the EBS and Test</td>
<td>9.14</td>
<td>1.2.2.1.d</td>
</tr>
<tr>
<td>Hardware</td>
<td>142</td>
<td>AB</td>
<td>Must have dual LAN capability for all servers as well as the operator consoles. Not required on compressor station ROS</td>
<td>8.4</td>
<td>2.7.1.18</td>
</tr>
<tr>
<td>Hardware</td>
<td>143</td>
<td>AB</td>
<td>Hardware should be HP machines</td>
<td>13.7.2</td>
<td>12.1.1.4</td>
</tr>
<tr>
<td>Hardware</td>
<td>144</td>
<td>AB</td>
<td>Requirement to have separate real-time and historical server</td>
<td>13.7.3</td>
<td>2.7.2</td>
</tr>
<tr>
<td>Hardware</td>
<td>146</td>
<td>AB</td>
<td>Dual power supplies should be included in all servers</td>
<td>13.7.10</td>
<td>12.3.1.3</td>
</tr>
<tr>
<td>Historical</td>
<td>Dupli cate</td>
<td>GM</td>
<td>Currently compressor historical data is deleted after 14 days. It would be good if this was stored for years in a corporate historian</td>
<td>10.4</td>
<td>11.3.1.1</td>
</tr>
<tr>
<td>Historical</td>
<td>18</td>
<td>JH</td>
<td>All data is captured in historian and retained online indefinitely (7 years)</td>
<td>16.5</td>
<td>11.3.1.1</td>
</tr>
<tr>
<td>Historical</td>
<td>21</td>
<td>JH</td>
<td>Seamless transition of historical data within SCADA system</td>
<td>16.5.2</td>
<td>16.3.3.2</td>
</tr>
<tr>
<td>Historical</td>
<td>22</td>
<td>JH</td>
<td>More minutely data available online to operators and trending (i.e. 2 years as per business requirement)</td>
<td>16.5.2</td>
<td>11.3.1.1</td>
</tr>
<tr>
<td>Historical</td>
<td>23</td>
<td>JH</td>
<td>Adequate performance of historical subsystem to ensure operator screens perform at acceptable levels</td>
<td>13.7.4</td>
<td>11.1</td>
</tr>
<tr>
<td>Historical</td>
<td>61</td>
<td>SN</td>
<td>Historical subsystem and historian are transparent to user regarding data retrieval</td>
<td>16.5.2</td>
<td>4.2</td>
</tr>
<tr>
<td>Historical</td>
<td>96</td>
<td>BB</td>
<td>Several years of data retention (possibly 12 months to 2 years)</td>
<td>16.5.2</td>
<td>11.3.1.1</td>
</tr>
<tr>
<td>Historical</td>
<td>157</td>
<td>SN</td>
<td>be able to access the data quality of historical data</td>
<td>23.8</td>
<td>4.2.3.8</td>
</tr>
<tr>
<td>CATEGORY</td>
<td>ITEM</td>
<td>BY</td>
<td>COMMENT</td>
<td>SPEC</td>
<td>FDS</td>
</tr>
<tr>
<td>----------------</td>
<td>------</td>
<td>-----</td>
<td>-------------------------------------------------------------------------</td>
<td>------------</td>
<td>-----------</td>
</tr>
<tr>
<td>Historical</td>
<td>162</td>
<td>RB</td>
<td>Marking bad telemetry data, i.e. instrument fail, frozen value, creep detection, rate of change. Store this data quality in the historical system</td>
<td>12.13</td>
<td>4.2.3.8</td>
</tr>
<tr>
<td>HMI</td>
<td>25</td>
<td>JH</td>
<td>User friendly screen navigation</td>
<td>19.6</td>
<td>5.2.3</td>
</tr>
<tr>
<td>HMI</td>
<td>72</td>
<td>ED</td>
<td>Must have ability to have custom built in help for operator screens to enable ease of operation</td>
<td>19.5, 20.10.9</td>
<td>5.1.1, 5.1.1.7</td>
</tr>
<tr>
<td>HMI</td>
<td>88</td>
<td>RL</td>
<td>Screen building must be straightforward. DBNGP to be able to perform simple changes in house</td>
<td>20.3, 14.3.1.2, 10.3.1.4</td>
<td></td>
</tr>
<tr>
<td>HMI</td>
<td>91</td>
<td>RL</td>
<td>Process to convert existing screens must be well defined</td>
<td>31.5, 16.3.4</td>
<td></td>
</tr>
<tr>
<td>HMI</td>
<td>106</td>
<td>BB</td>
<td>Only one person at a time can login to the HMI. But may need equipment supplier to also dial in at the same time</td>
<td>10.4, 2.1.1.16, 6.3.9</td>
<td></td>
</tr>
<tr>
<td>HMI</td>
<td>108</td>
<td>BB</td>
<td>Colors and symbols must be standard. E.g. red active or inactive? E.g. normally open valve, normally closed valve</td>
<td>19, 5.2.2</td>
<td></td>
</tr>
<tr>
<td>HMI</td>
<td>116</td>
<td>SJ</td>
<td>Capability of minor changes to a graphic on-line without shutting down the SCADA system</td>
<td>15.8, 20.3</td>
<td>10.3.1.x</td>
</tr>
<tr>
<td>HMI</td>
<td>119</td>
<td>SJ</td>
<td>Symbols should comply with IEEE or ISA engineering standards</td>
<td>19</td>
<td>10.3.2.11</td>
</tr>
<tr>
<td>HMI</td>
<td>149</td>
<td>AP</td>
<td>User friendly database configuration tool, with varying access controls, to allow certain users certain configuration rights</td>
<td>15.7, 3.1.1.7</td>
<td></td>
</tr>
<tr>
<td>HMI</td>
<td>150</td>
<td>AP</td>
<td>Screen building package to have all the bells and whistles. Want ability to display animations etc.</td>
<td>20.3, 10.3</td>
<td></td>
</tr>
<tr>
<td>HMI</td>
<td>160</td>
<td>SN</td>
<td>a .NET compliant web service (e.g. XML)</td>
<td>17.13</td>
<td>10.3.1.1, 2.2.1.7</td>
</tr>
<tr>
<td>Installation</td>
<td>81</td>
<td>GD</td>
<td>Must label all interconnecting cables at both ends, hardware components etc.</td>
<td>13.2, 12.7.1.9</td>
<td></td>
</tr>
<tr>
<td>Installation</td>
<td>102</td>
<td>BB</td>
<td>Events and alarms are unreliable. PLC is sending events to SCADA but ?? We need to verify that events are correctly represented in SCADA. Must do end to end testing of say 10% of points</td>
<td>32</td>
<td>16.3.7.1</td>
</tr>
<tr>
<td>Network</td>
<td>51</td>
<td>JH</td>
<td>Integrated remote management system incorporated. (From SCADA Support)</td>
<td>17.12</td>
<td>6.3.9.1</td>
</tr>
<tr>
<td>Network</td>
<td>52</td>
<td>JH</td>
<td>Remote web based operator client. Thin Client?? Is this about deployment of software onto client PCs??</td>
<td>11, 10.8</td>
<td>6.3.9</td>
</tr>
<tr>
<td>Network</td>
<td>53</td>
<td>JH</td>
<td>Web based data access. Read-only. Export to MS Excel</td>
<td>11, 16.1</td>
<td>6.3.9, 2.7.1.3</td>
</tr>
<tr>
<td>Network</td>
<td>100</td>
<td>BB</td>
<td>BB requires remote access to the data that is currently in Cimplicity/ControlView</td>
<td>10.4</td>
<td>6.3.9</td>
</tr>
<tr>
<td>Network</td>
<td>101</td>
<td>BB</td>
<td>Must have good remote access e.g. Bogs down when more than 5 users</td>
<td>13.7.4</td>
<td>6.3.9.2</td>
</tr>
<tr>
<td>Network</td>
<td>129</td>
<td>AB</td>
<td>Need to have the ability to configure the SCADA system remotely. This can be done either by direct access via a VPN or using Citrix interface</td>
<td>17.11</td>
<td>6.3.9.4</td>
</tr>
<tr>
<td>Network</td>
<td>158</td>
<td>SN</td>
<td>Access via something like a web page to configuration information regarding the sources to calculated points.</td>
<td>15.1</td>
<td>6.3.9.4</td>
</tr>
<tr>
<td>Network</td>
<td>176</td>
<td>BB</td>
<td>Insufficient access licenses for remote and/or web clients</td>
<td>14.8, 2.7.3.1</td>
<td></td>
</tr>
<tr>
<td>Noted</td>
<td>97</td>
<td>BB</td>
<td>Cimplicity in use in 2 out of 18 compressor stations. Plan is to roll out to all. Previously had ControlView. Approx 10 screens per compressor</td>
<td>10.4, Noted</td>
<td></td>
</tr>
<tr>
<td>Omnicom</td>
<td>35</td>
<td>AB</td>
<td>Retain fast scan capability. This is know as interleave scanning where the poll process is diverted from being one slave after the other to the selected slave being polled every second time</td>
<td>12.8.3, 3.3.10.3</td>
<td></td>
</tr>
</tbody>
</table>

Version: 0.3  Proprietary and Confidential to Telvent  Page 9 of 130
<table>
<thead>
<tr>
<th>CATEGORY</th>
<th>ITEM</th>
<th>BY</th>
<th>COMMENT</th>
<th>SPEC</th>
<th>FDS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Omnicom</td>
<td>36</td>
<td>JH</td>
<td>Able to put remote into fast scan while executing a command (e.g. Moving a valve) so as not to wait for a long duration reply (due to scan rate limitations).</td>
<td>12.8.3</td>
<td>3.3.10.3</td>
</tr>
<tr>
<td>Omnicom</td>
<td>37</td>
<td>JH</td>
<td>Must send control command immediately</td>
<td>12.8.7</td>
<td>3.3.10.7</td>
</tr>
<tr>
<td>Omnicom</td>
<td>37.1</td>
<td>MD</td>
<td>Critical Control Valves must have select then execute</td>
<td>20.12</td>
<td>3.3.7.3 3.3.7.4</td>
</tr>
<tr>
<td>Omnicom</td>
<td>38</td>
<td>AB</td>
<td>Must need software protocol analyzer preferably integrated into SCADA package. Must get contractor to select the package</td>
<td>27.8</td>
<td>9.2.1.11</td>
</tr>
<tr>
<td>Omnicom</td>
<td>39</td>
<td>AB</td>
<td>Must be able to define and select a minimum of two data paths to the RTU/PLC. Currently done by routing through Xyplex B instead of Xyplex A by selecting a comm's channel failover on a XOS workstation</td>
<td>8.6</td>
<td>3.3.1.8</td>
</tr>
<tr>
<td>Omnicom</td>
<td>40</td>
<td>AB</td>
<td>System could automatically fail over between alternate data paths</td>
<td>3.3.1.11 3.3.1.12</td>
<td></td>
</tr>
<tr>
<td>Omnicom</td>
<td>43</td>
<td>JH</td>
<td>Must retain dialup capability to remote RTUs. Current have approximately 3 sites</td>
<td>12.5 12.7</td>
<td>3.3.1.3 3.3.6.1.d</td>
</tr>
<tr>
<td>Omnicom</td>
<td>44</td>
<td>GTL</td>
<td>Should include support for Telstra IP-WAN</td>
<td></td>
<td>3.3.1.14</td>
</tr>
<tr>
<td>Omnicom</td>
<td>45</td>
<td>AB</td>
<td>Must retain pulse and latch commands</td>
<td>12.2.4 3.3.2.1</td>
<td></td>
</tr>
<tr>
<td>Omnicom</td>
<td>95</td>
<td>MD</td>
<td>Continue with the planned rollout of SCADApack RTUs</td>
<td></td>
<td>3.3.2.1 11.2.1.1</td>
</tr>
<tr>
<td>Omnicom</td>
<td>117</td>
<td>SJ</td>
<td>Different scan rate for different importance points i.e. do not want to scan all points at the same rate</td>
<td>12.8.1</td>
<td>3.3.10.6</td>
</tr>
<tr>
<td>Omnicom</td>
<td>120</td>
<td>GM</td>
<td>Would be good if we can communicate with Allen Bradley Ethernet/OPC as well as serial OR additionally MODBUS/IP</td>
<td>10.2</td>
<td>3.3.10.5 2.7.3.1 3.3.3</td>
</tr>
<tr>
<td>Omnicom</td>
<td>121</td>
<td>GM</td>
<td>Should be able to automatically switch COMMS CHANNEL to alternate route without human intervention</td>
<td></td>
<td>Dupl. of 40</td>
</tr>
<tr>
<td>Omnicom</td>
<td>123</td>
<td>GM</td>
<td>Evaluate OPC and DNP3</td>
<td>10.2</td>
<td>2.7.3.1</td>
</tr>
<tr>
<td>Omnicom</td>
<td>128</td>
<td></td>
<td>Need to have a central point of configuration. This means that we do not want to have to configure several interface devices for one single point</td>
<td>15.12</td>
<td>3.1.1.7</td>
</tr>
<tr>
<td>Omnicom</td>
<td>148</td>
<td>AB</td>
<td>System should be able to host at least 20 separate communication channels. The communication channels may have up to 40 different multi dropped slaves attached to the system</td>
<td></td>
<td>3.3.1.5</td>
</tr>
<tr>
<td>Omnicom</td>
<td>163</td>
<td>RB</td>
<td>Straight forward way to get all the temperature and pressure values from all key points on the pipeline</td>
<td>11</td>
<td>3.3</td>
</tr>
<tr>
<td>Performance</td>
<td>24</td>
<td>JH</td>
<td>Screen response time less than 0.5 seconds. We need to give some thought to how we specify this</td>
<td>13.7.4</td>
<td>11.1.4</td>
</tr>
<tr>
<td>Performance</td>
<td>70</td>
<td>JH</td>
<td>CPU utilization at top hour must not exceed a defined percentage</td>
<td>13.7.5</td>
<td>11.1.3</td>
</tr>
<tr>
<td>Performance</td>
<td>164</td>
<td>RB</td>
<td>It would be nice for all the data to come in under 1 minute, but 5 minutes is good enough</td>
<td>16.5.2</td>
<td>11.1.5 1.1.1.7</td>
</tr>
<tr>
<td>Protocol</td>
<td>8</td>
<td>ED</td>
<td>ASCII protocols be retained</td>
<td>14.7</td>
<td>2.7.3.1</td>
</tr>
<tr>
<td>Protocol</td>
<td>9</td>
<td>MD</td>
<td>1. MODBUS IP to be provided. 2. MODBUS high speed serial to be provided (at least 9600 baud)</td>
<td>14.7</td>
<td>9.2.1 3.3.2.1 2.7.3.1</td>
</tr>
<tr>
<td>Protocol</td>
<td>10</td>
<td>ED</td>
<td>Daniel / Enron support not required</td>
<td>14.7.7</td>
<td>Noted</td>
</tr>
<tr>
<td>Protocol</td>
<td>11</td>
<td>JH</td>
<td>Must be able to time-sync MODBUS (No need to time-sync CONITEL) Current implementation is to transfer 6 integers with YY MM DD HH MM SS and a seventh</td>
<td>13.18</td>
<td>9.2.1.13</td>
</tr>
<tr>
<td>CATEGORY</td>
<td>ITEM</td>
<td>BY</td>
<td>COMMENT</td>
<td>SPEC</td>
<td>FDS</td>
</tr>
<tr>
<td>----------</td>
<td>------</td>
<td>----</td>
<td>---------</td>
<td>------</td>
<td>-----</td>
</tr>
<tr>
<td>Protocol</td>
<td>14</td>
<td>MD</td>
<td>Ability for modular Protocols upgrades in new system</td>
<td>10.2</td>
<td>3.3.2.2</td>
</tr>
<tr>
<td>Protocol</td>
<td>15</td>
<td>MD</td>
<td>Must include DNP3 protocol in SCADA system. Note: DBNGP is currently developing a set of DNP3 implementation standards</td>
<td>14.7</td>
<td>2.7.3.1 3.3.2.2</td>
</tr>
<tr>
<td>Protocol</td>
<td>30</td>
<td>AB</td>
<td>Must have extended slave addressing (multiple 247 lines)</td>
<td>9.2.1.2</td>
<td></td>
</tr>
<tr>
<td>Protocol</td>
<td>31</td>
<td>AB</td>
<td>Ability for modular Protocols upgrades in new system Ability for modular Protocols upgrades in new system</td>
<td>12.6</td>
<td>3.3.1.16</td>
</tr>
<tr>
<td>Protocol</td>
<td>31.1</td>
<td>AB</td>
<td>Must be able to configure baud rate on interface for MODBUS to 1200bps and greater (8n1) and hardware handshake (RTS/CTS)</td>
<td>12.6</td>
<td>3.3.1.16</td>
</tr>
<tr>
<td>Protocol</td>
<td>46</td>
<td>AB</td>
<td>Must be able to download timely gas quality data to RTUs. 1. Read in gas quality data from RTUs, then perform error check and average, then download to nominated RTUs. Require ability to maintain list of nominated RTUs. Require ability to delay the download to nominated sites. 2. Do we want to do this in SCADA or should the RTUs collect data from other RTUs without involvement of SCADA? Note: The GQDD data stored in a database has to have the ability to be downloaded in either Daniel/Enron format or IEEE depending on the field device protocol.</td>
<td>17.5</td>
<td>GMAS</td>
</tr>
<tr>
<td>Redundancy</td>
<td>42</td>
<td>JH</td>
<td>1. Must be able to have functionality of master station in backup system 2. Do we want primary and standby SCADA servers at backup site? 3. Must be more automated than current</td>
<td>9.13 13.2</td>
<td>2.7.3.1</td>
</tr>
<tr>
<td>Redundancy</td>
<td>74</td>
<td>JH</td>
<td>Must provide seamless transfer to standby site</td>
<td>9.13</td>
<td>2.3.1</td>
</tr>
<tr>
<td>Regulations</td>
<td>68</td>
<td>MD</td>
<td>Must understand Department of Industry and resources/Department of Consumer and Employment Protection requirements</td>
<td>Noted</td>
<td></td>
</tr>
<tr>
<td>Security</td>
<td>78.4</td>
<td>AP</td>
<td>Operator workstations must be separate from any corporate workstations. Must not use existing corporate workstations to run the operator console</td>
<td>13.8</td>
<td>2.3.2.4 2.5.1.5</td>
</tr>
<tr>
<td>Security</td>
<td>84</td>
<td>RL</td>
<td>Don't have generic logons</td>
<td>26.1</td>
<td>6.3.4.1</td>
</tr>
<tr>
<td>Security</td>
<td>109</td>
<td>BB</td>
<td>Vibration data may need its own security. Must be read only. Cannot accidentally delete data</td>
<td>26.4</td>
<td>3.3.7.3</td>
</tr>
<tr>
<td>Security</td>
<td>112</td>
<td>SJ</td>
<td>Need permission checking before a command is sent</td>
<td>26.3</td>
<td>6.3.4</td>
</tr>
<tr>
<td>Security</td>
<td>145</td>
<td>AB</td>
<td>Virus checking needs to be installed prior to commissioning. However it must be noted that the intention is to not have the system connected to the internet. This may have implication to updating the virus patches.</td>
<td>13.11 1.2.3.1.p</td>
<td></td>
</tr>
<tr>
<td>Sizing</td>
<td>103</td>
<td>BB</td>
<td>Probably need less than double the number of points currently collected from a compressor station</td>
<td>10.4</td>
<td>11.2.1.1</td>
</tr>
<tr>
<td>Specials</td>
<td>94</td>
<td>RL</td>
<td>Pipeline profile display is customized so that each section is color coded with the pressure status. E.g. low pressure in a segment will be red</td>
<td>11.7</td>
<td>16.3.4 Jake has details.</td>
</tr>
<tr>
<td>Specials</td>
<td>115.1</td>
<td>AP</td>
<td>Be nice for the simulator to be able to simulate real world conditions from a known start. i.e. a leak which brings down the pressure and reduces linepack etc.</td>
<td>GMAS</td>
<td></td>
</tr>
<tr>
<td>CATEGORY</td>
<td>ITEM</td>
<td>BY</td>
<td>COMMENT</td>
<td>SPEC</td>
<td>FDS</td>
</tr>
<tr>
<td>-------------</td>
<td>------</td>
<td>------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------------</td>
<td>-----------</td>
</tr>
<tr>
<td>Specials</td>
<td>161</td>
<td>SN</td>
<td>ability to kick off a simulation by provided a set of parameters (e.g. simulation time, compressor start/stop, consumer start/stop) and overlay the simulated pressure profile on the main display</td>
<td>GMAS</td>
<td></td>
</tr>
<tr>
<td>Specials</td>
<td>167</td>
<td>BB</td>
<td>unified data interfaces. Data coming in directly into PI and data coming into SCADA Master station should be accessible from the same user interface, and contain similar meta-data capabilities</td>
<td>23.1</td>
<td>PI</td>
</tr>
<tr>
<td>Support</td>
<td>17</td>
<td>ED</td>
<td>Seek clarification on ownership, strategy, procurement and maintenance of RTUs.</td>
<td></td>
<td>Noted</td>
</tr>
<tr>
<td>Support</td>
<td>71</td>
<td>JH</td>
<td>Must ensure availability of vendor support for a certain period of time</td>
<td>38</td>
<td>1.2.2.r</td>
</tr>
<tr>
<td>Support</td>
<td>73</td>
<td>JH</td>
<td>Must have ability to do first in fault diagnostics and provide verbose debugging information</td>
<td>27.6</td>
<td>1.2.2.r</td>
</tr>
<tr>
<td>Support</td>
<td>178</td>
<td>SJ</td>
<td>Must have a version control repository e.g., SourceSafe or CVS etc.</td>
<td>36</td>
<td>15.1.1.3</td>
</tr>
<tr>
<td>System</td>
<td>131</td>
<td>AB</td>
<td>The test system needs to have the ability to transfer FAT data direct to the production system for release control of database configurations.</td>
<td>13.5</td>
<td>2.3.2.8</td>
</tr>
<tr>
<td>Functions</td>
<td>16</td>
<td>JH</td>
<td>SCADA system daylight saving capability. RTUs must use UTC and be time synced in UTC. User displays must display in local time.</td>
<td>13.18</td>
<td>9.2.1.13</td>
</tr>
<tr>
<td>System</td>
<td>34</td>
<td>JH</td>
<td>Define SCADA boundary with regards to comm infrastructure</td>
<td>8</td>
<td>2.5.2</td>
</tr>
<tr>
<td>Functions</td>
<td>78.1</td>
<td>AP</td>
<td>Must be able to print in color to existing corporate printers.</td>
<td>13.13</td>
<td>5.7.1.3.a</td>
</tr>
<tr>
<td>System</td>
<td>78.2</td>
<td>AP</td>
<td>When printing anything from the operator console, be able to chose to send it via email instead of to a printer, Also be able to add subject and brief description in body of email.</td>
<td>9.4</td>
<td>5.7.2.4</td>
</tr>
<tr>
<td>Functions</td>
<td>79</td>
<td>JH</td>
<td>Must have nightly database dumps to a portable media</td>
<td>13.1</td>
<td>3.4.3.1.g</td>
</tr>
<tr>
<td>System</td>
<td>83.3</td>
<td>AP</td>
<td>must be able to understand the concept of shift changes</td>
<td>26.1</td>
<td>6.3.4.6</td>
</tr>
<tr>
<td>Functions</td>
<td>113</td>
<td>SJ</td>
<td>Time Sync must be done at all levels, including servers, PLCs, RTUs and historian servers</td>
<td>13.18</td>
<td>9.2.1.13</td>
</tr>
<tr>
<td>System</td>
<td>136</td>
<td>AB</td>
<td>Auto Recovery of system failure. In the event of a system failure like loss of power the system has to be able to boot up into the system without human interference.</td>
<td>9.11</td>
<td>11.5.1.4</td>
</tr>
<tr>
<td>Functions</td>
<td>137</td>
<td>AB</td>
<td>Auto Archiving. The system should be able to archive / Back up the system automatically to an offsite repository.</td>
<td>9.13</td>
<td>3.4.3.1.g</td>
</tr>
<tr>
<td>System</td>
<td>138</td>
<td>AB</td>
<td>Auto Imaging / Ghost. Server and Client to be able to be imaged seamlessly with out loss of operation.</td>
<td></td>
<td>3.4.3.1.g</td>
</tr>
<tr>
<td>Functions</td>
<td>139</td>
<td>AB</td>
<td>Schedule system back up to offsite disk. This should be done with a 7 day rotation.</td>
<td></td>
<td>1.2.3.1.q</td>
</tr>
<tr>
<td>CATEGORY</td>
<td>ITEM</td>
<td>BY</td>
<td>COMMENT</td>
<td>SPEC</td>
<td>FDS</td>
</tr>
<tr>
<td>--------------------</td>
<td>------</td>
<td>----</td>
<td>-----------------------------------------------------------------------------------------------</td>
<td>--------</td>
<td>--------</td>
</tr>
<tr>
<td>System Functions</td>
<td>152</td>
<td>AP</td>
<td>Create an outage scheduling window, that reflects the maintenance outage plan. Tie a sequence of commands to these events. Automatically execute the sequence upon acceptance from the controller.</td>
<td>35.1</td>
<td>3.3.8.17</td>
</tr>
<tr>
<td>System Functions</td>
<td>153</td>
<td>AP</td>
<td>Be able to program a sequence of events that the system will perform autonomously. E.g. Stopping a Unit when running in series operation. Step1: Reduce station Disc. Pressure setpoint, to reduce station DP. Step2: Monitor station DP until at acceptable level. Step3: Issue unit stop. Step4: Wait until unit stopped. Step5: Increase station Disc. Pressure setpoint back to MAOP.</td>
<td>25</td>
<td>3.3.8.17</td>
</tr>
<tr>
<td>System Functions</td>
<td>156</td>
<td>AP</td>
<td>Ability to perform bulk point editing.</td>
<td>15.7</td>
<td>10.2.1.8</td>
</tr>
<tr>
<td>Tools</td>
<td>28</td>
<td>ED</td>
<td>Provide field maintenance tools to allow diagnostics of RTUs and comms.</td>
<td>15.1</td>
<td>9.2.1.11</td>
</tr>
<tr>
<td>Tools</td>
<td>54</td>
<td>JH</td>
<td>Programming tools and SDK exists and are ergonomic / user friendly. Must be based on standards</td>
<td>12.4</td>
<td>1.5</td>
</tr>
<tr>
<td>Tools</td>
<td>66</td>
<td>JH</td>
<td>Must have ability to replicate existing dataBASIC functionality.</td>
<td>18.11</td>
<td>16.3.3</td>
</tr>
<tr>
<td>Training</td>
<td>111</td>
<td>BB</td>
<td>Training is important. Previous training was weak. Require &quot;how do I do this&quot; help.</td>
<td>33</td>
<td>14</td>
</tr>
<tr>
<td>Training</td>
<td>115</td>
<td>SJ</td>
<td>Training simulator with copy of &quot;live&quot; data</td>
<td>9.14</td>
<td>2.3.2.8</td>
</tr>
<tr>
<td>Training</td>
<td>126</td>
<td>DS</td>
<td>Require quick overview of the whole system</td>
<td>11</td>
<td>14</td>
</tr>
<tr>
<td>Trending</td>
<td>76</td>
<td>ED</td>
<td>Must have single point trend for every analogue. Ensure at least 3 default duration selections prev 30min, prev 24 hrs, prev 5 days. Require one button export of displayed data to CSV / Excel format.</td>
<td>23.5</td>
<td>4.2.3.7.a.5.4</td>
</tr>
<tr>
<td>Trending</td>
<td>76</td>
<td>AP</td>
<td>Trending must display multiple trends on the one trend chart. Must have user friendly method of selecting points.</td>
<td>23.5</td>
<td>5.4</td>
</tr>
<tr>
<td>Trending</td>
<td>76.1</td>
<td>AP</td>
<td>Single point trend for minutely analog, to be previous 30 minutes, 6hr, 12hr, 1d, 2d, 1w, 2w,1mon on a drop down list from the trend window popped up</td>
<td>23.5</td>
<td>5.4</td>
</tr>
<tr>
<td>Trending</td>
<td>76.2</td>
<td>AP</td>
<td>Trending must display multiple trends on the one trend chart. Must have user friendly method of selecting points.</td>
<td>16.5.2</td>
<td>Dupl. of 86</td>
</tr>
<tr>
<td>Trending</td>
<td>78.3</td>
<td>AP</td>
<td>When field techs have a trend up, click an &quot;email&quot; button, and the trend is sent as an image and the raw CSV data to the specified address</td>
<td>9.4</td>
<td>5.7.2.4</td>
</tr>
<tr>
<td>Trending</td>
<td>86</td>
<td>RL</td>
<td>Must have at least 2 years of time series trend data online. Must be viewable from SCADA system. Must be quick. Must be single click. Must be multiple trends.</td>
<td>16.5.2</td>
<td>5.4.1.1</td>
</tr>
<tr>
<td>Trending</td>
<td>99</td>
<td>BB</td>
<td>Trending is currently very poor in Cimplicity - must manually select every point.</td>
<td>23</td>
<td>Noted</td>
</tr>
<tr>
<td>Trending</td>
<td>107</td>
<td>BB</td>
<td>Screen Navigation and trend building is cumbersome. E.g. Need to see point names and point descriptions for building trends.</td>
<td>23.9</td>
<td>5.2.3</td>
</tr>
<tr>
<td>Trending</td>
<td>110</td>
<td>BB</td>
<td>Require pre-defined trend definitions that can be saved and reused</td>
<td>23.15</td>
<td>5.4.5.4</td>
</tr>
<tr>
<td>Trending</td>
<td>168</td>
<td>BB</td>
<td>be able to predefine trends, and make them available to all users, including those outside the control room</td>
<td>23.15</td>
<td>5.4.5.4</td>
</tr>
<tr>
<td>CATEGORY</td>
<td>ITEM</td>
<td>BY</td>
<td>COMMENT</td>
<td>SPEC</td>
<td>FDS</td>
</tr>
<tr>
<td>----------</td>
<td>------</td>
<td>----</td>
<td>---------</td>
<td>-------</td>
<td>-----</td>
</tr>
<tr>
<td>Trending</td>
<td>172</td>
<td>BB</td>
<td>drag and drop ability to add and remove tags to trends, and have trend auto-scale etc.</td>
<td>23.9</td>
<td>5.4</td>
</tr>
</tbody>
</table>
# Table Of Contents

1. **Introduction** .................................................................................................................. 21
   1.1 General ......................................................................................................................... 21
   1.2 Responsibilities of Involved Parties ........................................................................... 22
      1.2.1 General .................................................................................................................. 22
      1.2.2 Telvent’s Responsibilities .................................................................................... 22
      1.2.3 DBNGP Responsibilities ..................................................................................... 23
   1.3 Organization of The FUNCTIONAL DESIGN SPECIFICATIONS ......................... 24
      1.3.1 General .................................................................................................................. 24
   1.4 Terms .......................................................................................................................... 24
      1.4.1 General .................................................................................................................. 24
   1.5 Standards .................................................................................................................... 29
      1.5.1 General .................................................................................................................. 29

2. **System Architecture** ..................................................................................................... 30
   2.1 Introduction .................................................................................................................. 30
      2.1.1 General .................................................................................................................. 30
   2.2 General System Requirements .................................................................................... 32
      2.2.1 General .................................................................................................................. 32
   2.3 Distributed System Architecture ................................................................................. 33
      2.3.1 General .................................................................................................................. 33
      2.3.2 Supported Architectures ....................................................................................... 34
   2.4 Distributed Middleware Architecture ........................................................................... 35
      2.4.1 General .................................................................................................................. 35
   2.5 System Redundancy through a Distributed Architecture ........................................... 36
      2.5.1 General .................................................................................................................. 36
      2.5.2 Network Model ...................................................................................................... 37
   2.6 System Expansion and Life Cycle ................................................................................. 37
      2.6.1 General .................................................................................................................. 37
   2.7 System Overview and Design ....................................................................................... 38
      2.7.1 General .................................................................................................................. 38
      2.7.2 System Diagram .................................................................................................... 41
      2.7.3 System Sizing ........................................................................................................ 42
   2.8 SCADA System Configuration, Monitoring and Control Management Environment .... 43
      2.8.1 General .................................................................................................................. 43
   2.9 Communications ........................................................................................................... 43
      2.9.1 General .................................................................................................................. 43
      2.9.2 Routers ................................................................................................................... 44
      2.9.3 Bridges ................................................................................................................... 45
      2.9.4 Concentrators ...................................................................................................... 45
      2.9.5 Network Interface Cards ...................................................................................... 45
      2.9.6 Data Acquisition Equipment ............................................................................... 46

3. **Real-Time Subsystem** ..................................................................................................... 47
   3.1 Introduction ................................................................................................................... 47
      3.1.1 General .................................................................................................................. 47
   3.2 Real-time Database ....................................................................................................... 48
      3.2.1 General .................................................................................................................. 48
   3.3 Data Acquisition .......................................................................................................... 49
      3.3.1 General .................................................................................................................. 49
      3.3.2 Protocols ............................................................................................................... 51
3.3.3 OPC Client Protocol ................................................................. 51
3.3.4 Physical Termination / Connection ........................................ 51
3.3.5 Managing Connections .......................................................... 52
3.3.6 Modes of Communication ..................................................... 53
3.3.7 Supervisory Control ................................................................. 53
3.3.8 Control functions ................................................................. 54
3.3.9 Control Point Tagging ............................................................. 55
3.3.10 Communication Scheduling ................................................ 56
3.3.11 Data Processing ................................................................. 57
3.3.12 Analog Data Processing ....................................................... 57
3.3.13 Digital Status Input Processing .......................................... 58
3.3.14 Accumulator (or Rate) Point Processing ......................... 58
3.3.15 Data Quality ................................................................. 59
3.4 Data Manipulation and Calculated Values ........................................ 60
3.4.1 General ................................................................. 60
3.4.2 Procedure Properties ......................................................... 60
3.4.3 Procedure Execution Triggers ............................................. 61
3.5 Event Logging / History ............................................................ 61
4. Historical Data Archiving Subsystem ............................................. 64
4.1 Introduction ............................................................................. 64
4.1.1 General ............................................................................. 64
4.2 Database Format ....................................................................... 64
4.2.1 General ............................................................................. 64
4.2.2 Historical Data Replication ................................................ 65
4.2.3 On-line Historical Data ...................................................... 65
4.2.4 Archiving/De-archiving Historical Data .............................. 67
4.2.5 Editing Historical Data ....................................................... 69
4.3 Failure Protection ................................................................. 69
4.3.1 General ............................................................................. 69
5. Human Machine Interface Subsystem .......................................... 71
5.1 Introduction ............................................................................. 71
5.1.1 General ............................................................................. 71
5.2 Windowing System ................................................................. 74
5.2.1 General ............................................................................. 74
5.2.2 General Presentation and Layout ...................................... 74
5.2.3 Navigation ........................................................................... 75
5.2.4 Data Presentation ............................................................... 76
5.2.5 Dynamic Data Presentation .............................................. 76
5.2.6 Data Quality Flags ............................................................. 77
5.2.7 Tag Indicators ................................................................. 77
5.3 Controller Input Functions ...................................................... 77
5.3.1 General ......................................................................... 77
5.3.2 Data Entry ..................................................................... 78
5.3.3 Setpoint Control ................................................................. 78
5.3.4 Commands ..................................................................... 78
5.4 Trending ........................................................................... 79
5.4.1 Trend Manipulation ............................................................ 79
5.4.2 Trend Configuration ........................................................... 80
5.4.3 Trend Traces ................................................................... 80
5.4.4 Individual pen parameters .................................................. 80
5.4.5 Other trending functions ................................................... 81
5.5 Area(s) of Responsibility .................................................... 81
5.5.1 General ......................................................................... 81
5.6 Alarming ........................................................................... 82
5.6.1 General ......................................................................... 82
5.6.2 Alarm Severity ................................................................. 83
5.6.3 Alarm Annunciation ........................................................... 83
5.6.4 Alarm States ................................................................... 83
5.6.5 Alarm Message ................................................................. 84
5.6.6 Alarm Logging ................................................................. 84
5.6.7 Alarm Acknowledging ......................................................... 84
5.6.8 Alarm Interaction ............................................................... 85
5.6.9 Alarm Inhibiting ................................................................. 85
5.6.10 Silencing of Audible Alarms ............................................... 85
5.6.11 Alarm Limits ................................................................. 85
5.6.12 Standard Displays ............................................................ 85
5.7 Printing ........................................................................... 86
5.7.1 General ......................................................................... 86
5.7.2 Displays and Screens ........................................................ 86
5.7.3 Reports ......................................................................... 87
5.8 Security ........................................................................... 88
6. Security ........................................................................... 88
6.1 Introduction ....................................................................... 88
6.1.1 General ......................................................................... 88
6.2 Security Management Practices ............................................... 88
6.2.1 AIC - The Three Pillars of Information Security .................. 88
6.2.2 General Standards .......................................................... 88
6.3 Access Control .................................................................. 88
6.3.1 General ......................................................................... 88
6.3.2 Password Management .................................................... 88
6.3.3 Access to the Operating System ........................................... 89
6.3.4 Access to the SCADA system ............................................... 89
6.3.5 Access to High Responsibility Controls .............................. 90
6.3.6 Automatic Logout ........................................................... 90
6.3.7 Single-Sign-On (SSO) ......................................................... 90
6.3.8 Two-Factor (or Three-Factor) “Strong” Authentication .......... 90
6.3.9 Remote Access .............................................................. 91
6.4 Physical Security .............................................................. 91
6.4.1 General ......................................................................... 91
6.5 Networking Security .......................................................... 91
7. **System Software** .................................................................................. 92
   7.1 Introduction ......................................................................................... 92
   7.1.1 General ....................................................................................... 92
   7.2 Computer Systems Software ......................................................... 92
   7.2.1 General ....................................................................................... 92
8. **Enterprise Information Technology Integration** ..................................... 94
   8.1 Directory Services ........................................................................... 94
   8.1.1 Domain Name Services (DNS) ..................................................... 94
   8.1.2 Dynamic Host Configuration Protocol (DHCP) ......................... 94
   8.1.3 Lightweight Directory Access Protocol (LDAP) ......................... 94
   8.1.4 DBNGP Corporate Security Policies & Procedures ................. 94
9. **System Applications** ........................................................................... 95
   9.1 Introduction ....................................................................................... 95
   9.1.1 General ....................................................................................... 95
   9.2 Applications .................................................................................... 95
   9.2.1 MODBUS TCP/IP Protocol ......................................................... 95
10. **System Management Tools** ............................................................... 97
    10.1 Introduction .................................................................................... 97
    10.1.1 General ..................................................................................... 97
    10.2 Database Editor ............................................................................. 97
    10.2.1 General ..................................................................................... 97
    10.3 Display Editor ................................................................................ 98
    10.3.1 General ..................................................................................... 98
    10.3.2 Dynamic Data ........................................................................... 99
    10.3.3 Calculated Points ...................................................................... 99
    10.3.4 Soft Push Buttons .................................................................... 100
    10.4 Network Management, Diagnostic and Monitoring Utilities ........ 100
    10.4.1 General ..................................................................................... 100
    10.4.2 DIAGNOSTICS ....................................................................... 100
11. **System Requirements** ....................................................................... 103
    11.1 Performance Requirements ........................................................... 103
    11.1.1 General ..................................................................................... 103
    11.1.2 System Loading ................................................................. 103
    11.1.3 Heavy Loading Scenario ...................................................... 103
    11.1.4 Screen Response Times .......................................................... 104
    11.1.5 Data Acquisition Times ......................................................... 104
    11.1.6 Control Output Times ............................................................. 105
    11.1.7 Database Update Times ......................................................... 105
    11.1.8 Failover Times ................................................................. 105
    11.1.9 System Start-up Times ............................................................ 106
    11.1.10 Controller Workstation Performance .................................. 106
    11.2 Database Sizing ............................................................................ 107
    11.2.1 General ..................................................................................... 107
    11.3 Historical Database Sizing ............................................................ 108
    11.3.1 General ..................................................................................... 108
    11.4 Equipment Requirements ............................................................ 108
    11.4.1 General ..................................................................................... 108
    11.5 System Failure and Restart ......................................................... 108
### 11. System Hardware

11.6 System Availability

11.6.1 General

11.7 System Expansion

11.7.1 General

12. System Hardware

12.1 Introduction

12.1.1 General

12.2 Controller Workstations

12.2.1 General

12.2.2 Main Memory

12.2.3 Keyboard

12.2.4 Cursor Control Device

12.2.5 Workstation Graphics Devices

12.3 Servers

12.3.1 General

12.3.2 Main Memory

12.3.3 Mass Storage Devices

12.3.4 Removable Storage Device

12.3.5 Magnetic Tape Drives

12.3.6 Keyboard

12.3.7 Cursor Control Device

12.4 System Printers

12.4.1 General

12.4.2 Report Printers

12.4.3 Screen Hardcopy Printers

12.5 Equipment Cabinets

12.6 Communication Peripherals

12.6.1 General

12.7 Network Connections

12.7.1 General

12.7.2 Local Area Network (LAN)

12.7.3 Wide Area Network (WAN)

### 13. Documentation Requirements

13.1 Introduction

13.1.1 General

13.2 Project Documentation

13.2.1 General

13.2.2 Project Quality Plan (PQP)

13.2.3 System Configuration Plan (SCP)

13.2.4 Application Definition Documents (ADDs)

13.2.5 Test Plan

13.2.6 FAT Test Procedures

13.2.7 SAT Test Procedures

13.2.8 Test Reporting

13.2.9 Commissioning Plan

13.2.10 Project Status Reports

### 14. Training Requirements
14.1 Introduction ........................................................................................................... 123
14.1.1 General ............................................................................................................. 123
14.2 General Requirements .......................................................................................... 123
14.2.1 General ............................................................................................................. 123
14.3 Training Course Contents ..................................................................................... 123
14.3.1 General ............................................................................................................. 123
14.4 Extended Training Options .................................................................................. 124
14.4.1 Onsite, Just-in-Time Training ........................................................................... 124
14.4.2 Coaching ........................................................................................................... 124
15. Project Implementation ............................................................................................ 125
15.1 Introduction ........................................................................................................... 125
15.2 Project Management ............................................................................................... 125
15.2.1 General ............................................................................................................. 125
15.3 Correspondence ..................................................................................................... 125
15.3.1 General ............................................................................................................. 125
15.4 Equipment Shipment ............................................................................................. 126
15.4.1 General ............................................................................................................. 126
16. Additional services ................................................................................................... 127
16.1 Introduction ........................................................................................................... 127
16.1.1 General ............................................................................................................. 127
16.2 Project Management ............................................................................................... 127
16.2.1 General ............................................................................................................. 127
16.3 Technical Expertise ............................................................................................... 127
16.3.1 General ............................................................................................................. 127
16.3.2 Requirements Analysis ..................................................................................... 128
16.3.3 Database Development and Conversion .......................................................... 128
16.3.4 Graphical Display Development and Conversion ............................................. 128
16.3.5 Application Development and Testing ............................................................. 128
16.3.6 Communications Infrastructure Development .................................................. 129
16.3.7 Site Commissioning .......................................................................................... 129
Appendix 1 – Training Course Descriptions ............................................................... 130

Table of Figures
Figure 2-1- Typical System Overview Diagram ............................................................. 42
Figure 5-1- Baseline Desktop Layout ......................................................................... 72

Table of Tables
Table 1- Table of Acronyms ......................................................................................... 28
Table 2- System Component Quantities ...................................................................... 43
Table 3- Navigation Menu ............................................................................................. 73
Table 4- Device and Environment Control Commands List ......................................... 79
Table 5- Realtime Database Sizing ............................................................................. 107
Table 6- Historical database sizing ............................................................................. 108
Table 7- Training Courses ............................................................................................ 124
1. INTRODUCTION

1.1 GENERAL

1.1.1.1 The Dampier to Bunbury Natural Gas Pipeline (DBNGP) is supervised by a Telvent OASyS 5.2.2UX SCADA system. This system was commissioned in 1999, with the application remaining largely unchanged since that time. A Telvent historian is used for data archiving however the capacity of the historian is limited. The Telvent platform is presently supported by TUSC, however the hardware platform is at the end of life and support is dependent on continuing arrangements with a third party supplier.

1.1.1.2 In 2006 a SCADA strategy was prepared by WestNet as part of the overall review of SCADA systems utilized for the operation of assets within Australia. Although the SCADA system was still performing, the core functions well and without significant failure, this strategy highlighted the requirement for DBNGP to upgrade its SCADA system. The reasons for this recommendation were:

- Age of system (software and hardware) is increasing the risk of failure of the asset
- Limited vendor support of system (software and hardware) is increasing the risk of failure of the asset
- Limited ability to expand the system
- Any benefits from changes in communication technology not able to be accessed
- Changes in security requirements within industry not able to be reflected in the system
- Business requirements for access to data not being met
- Lack of available training on the system
- Data accessibility from the historian is limited
- Resources to support system not readily available
- Technology limits ability to improve service to asset owner through inability to consider additional applications for core functions
- Growth of the DBNGP is crystallizing the current limitations of the SCADA system.
1.2 RESPONSIBILITIES OF INVOLVED PARTIES

1.2.1 General

1.2.1.1 This section outlines the expectations incumbent upon both Telvent and DBNGP during the requirements, design, implementation, testing, and commissioning phases of the project. The intent is to provide a high-level picture of the general expectations of both parties. The technical requirements shall appear in later sections of this specification.

1.2.2 Telvent’s Responsibilities

1.2.2.1 Telvent shall be responsible for the design, procurement, implementation and construction, factory testing, delivery, installation, site testing, initial start-up and documentation of the SCADA system. The specific obligations shall appear throughout this document. For reference, here is a brief outline of Telvent’s major obligations:

a) Co-design of the complete SCADA system in conjunction with DBNGP;

b) Design of all software connectors necessary to interface with DBNGP corporate infrastructure;

c) Compliance with DBNGP existing policies and procedures regarding information processing & information security;

d) Supply of all computer hardware, workstations, memory, peripherals, printers, communications interface equipment, cables and other equipment necessary to provide a complete and functioning SCADA system;

e) Configuration and assembly of all software including licenses necessary to meet the requirements of this specification;

f) Supply of management and administration tools required to properly support the SCADA system in the field;

g) Design and supply of interfaces to the RTUs, and PLCs

h) Integration of all hardware and software into a complete and operational SCADA system;

i) Preparing test procedures and conducting tests under DBNGP supervision;

j) Testing of the system in accordance with the requirements of this specification at factory and on site after initial installation and startup;

k) Connection of all power, data, and telecommunications wiring for all SCADA system elements to DBNGP provided connection points;

l) Start-up, and site testing of the SCADA system, which shall include testing of all hardware, software and SCADA communications;
m) Preparation of complete hardware and software documentation as specified elsewhere in this document;

n) Training of DBNGP system controllers, programmers, and system administration personnel;

o) Project Management services during all phases of the project, including preparation of monthly progress reports and organizing scheduled meetings to identify action items, review issues and resolve problems;

p) Develop and install the new SCADA database, graphical displays and reports based on the requirements of the specification;

q) Unpack, setup and connect all equipment on site;

r) Provide first-line support for all aspects of delivered system during warranty phase.

s) Offer standard VIP Customer Support packages to support system after warranty expires including optional 24 x 7.

1.2.3 DBNGP Responsibilities

1.2.3.1 During the implementation of the SCADA system, DBNGP shall endeavor to provide Telvent with all required information on a timely basis. Following is a list of information and services that DBNGP shall contribute to the SCADA project:

a) Co-design of the complete SCADA system in conjunction with Telvent

b) Provide a primary and back-up source of electrical power to all equipment

c) Provide a suitable environment for housing all computer and communications equipment

d) Provide Telvent with facility drawings showing the layout of the site, location of power and communications connections, and access routes if requested

e) Ensure the availability of all communications facilities with local and/or regional telecommunications companies

f) Provide Telvent with an IT Security liaison to ensure security configuration requirements are properly addressed on both Telvent and DBNGP responsibilities for this project

g) Supply Telvent with an electronic copy of the SCADA database points

h) Provide copies of screen layouts and report forms for Telvent’s reference during DBNGP development of the graphical displays and reports

i) Take training from Telvent during the project implementation

j) Review Telvent’s proposed designs, equipment layouts, test plans and procedures, and provide timely feedback about these documents

k) Participate in scheduled project meetings

l) Participate in Factory and Site Acceptance Testing
m) Provide approvals as and when required for elements of the project which meet DBNGP requirements as defined in this specification

n) Provide access to all locations where Telvent is required to install or test equipment

o) Shipment of all equipment and software from FOB Calgary to its final destination including unloading

p) Install any corporate anti-virus software and maintain it.

q) Do daily system maintenance like backups, printer maintenance and other system monitoring once system is operational.

1.3 ORGANIZATION OF THE FUNCTIONAL DESIGN SPECIFICATIONS

1.3.1 General

This document shall contain the technical specifications for DBNGP's new SCADA system.

The Functional Design Specifications (FDS) consists of major categories as follows:

- Introduction, Overview, Terms and Standards (Section 1)
- System Architecture (Section 2)
- Real-Time Subsystem (Section 3)
- Historical Data Archiving Subsystem (Section 4)
- Human Machine Interface Subsystem (Section 5)
- Security (Section 6)
- System Software (Section 7)
- Enterprise Information Technology Integration (Section 8)
- System Applications (Section 9)
- System Management Tools (Section 10)
- System Requirements (Section 11)
- System Hardware (Section 12)
- Documentation Requirements (Section 13)
- Training Requirements (Section 14)
- Project Implementation (Section 15)
- Additional services (Section 16)

1.4 TERMS

1.4.1 General
<table>
<thead>
<tr>
<th>Acronym</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACE</td>
<td>Automatic Calculation Engine</td>
</tr>
<tr>
<td>ACL</td>
<td>Access Control List</td>
</tr>
<tr>
<td>ADAM</td>
<td>Active Directory Application Mode</td>
</tr>
<tr>
<td>ADD</td>
<td>Application Definition Document</td>
</tr>
<tr>
<td>ADE</td>
<td>Advanced Database Editor - a DNA 7.5 feature that largely replaces the DMT, though both may be used. In this document, references to the DMT and the ADE may be considered as functionally synonymous. See DMT in this list.</td>
</tr>
<tr>
<td>ADS</td>
<td>Active Directory Service</td>
</tr>
<tr>
<td>AES</td>
<td>Advanced Encryption Standard</td>
</tr>
<tr>
<td>ANSI</td>
<td>American National Standards Institute</td>
</tr>
<tr>
<td>AOR</td>
<td>Area of Responsibility</td>
</tr>
<tr>
<td>ATM</td>
<td>Asynchronous Transfer Mode</td>
</tr>
<tr>
<td>BCP</td>
<td>Business Continuity Plan</td>
</tr>
<tr>
<td>BSAP</td>
<td>Bristol Standard Asynchronous Protocol</td>
</tr>
<tr>
<td>CC</td>
<td>Common Criteria</td>
</tr>
<tr>
<td>CISSP</td>
<td>Certified Information Security Professional</td>
</tr>
<tr>
<td>COM</td>
<td>Component Object Model</td>
</tr>
<tr>
<td>CPU</td>
<td>Central Processing Unit</td>
</tr>
<tr>
<td>DAC</td>
<td>Discretionary Access Control</td>
</tr>
<tr>
<td>dbll</td>
<td>Database Lister/Loader. A tool for dumping and loading the contents of the DNA realtime database.</td>
</tr>
<tr>
<td>DBNGP</td>
<td>Dampier to Bunbury Natural Gas Pipeline</td>
</tr>
<tr>
<td>DC</td>
<td>Domain Controller</td>
</tr>
<tr>
<td>DCOM</td>
<td>Distributed Component Object Model</td>
</tr>
<tr>
<td>DES</td>
<td>Data Encryption Standard</td>
</tr>
<tr>
<td>DHCP</td>
<td>Dynamic Host Configuration Protocol</td>
</tr>
<tr>
<td>DMT</td>
<td>Database Management Tool - a set of dialogs that permit configuration and editing of the realtime database contents (and, occasionally, configuration of parts of the historical database). Under DNA 7.5, an alternate window display mechanism known as ADE is being introduced and is expected to replace all or parts of the DMT. In this document, references to the DMT and the ADE may be considered as functionally synonymous. See ADE in this list.</td>
</tr>
<tr>
<td>Acronym</td>
<td>Definition</td>
</tr>
<tr>
<td>---------</td>
<td>------------</td>
</tr>
<tr>
<td>DNA</td>
<td>Dynamic Network of Application, OASys DNA – Telvent’s flagship window based distributed SCADA product</td>
</tr>
<tr>
<td>DNS</td>
<td>Domain Naming System</td>
</tr>
<tr>
<td>DRP</td>
<td>Disaster Recovery Plan</td>
</tr>
<tr>
<td>DSS</td>
<td>Decision Support Server which provides SCADA access to non-critical users</td>
</tr>
<tr>
<td>DSS</td>
<td>Digital Signature Standard</td>
</tr>
<tr>
<td>ECC</td>
<td>Elliptic Curve Cryptosystem</td>
</tr>
<tr>
<td>ECDSA</td>
<td>Elliptic Curve Digital Signature Algorithm</td>
</tr>
<tr>
<td>ENG</td>
<td>Engineering</td>
</tr>
<tr>
<td>EPL</td>
<td>Evaluated Products List sequence</td>
</tr>
<tr>
<td>FAT</td>
<td>Factory Acceptance Testing</td>
</tr>
<tr>
<td>FDS</td>
<td>Functional Design Specifications</td>
</tr>
<tr>
<td>FTP</td>
<td>File Transfer Protocol</td>
</tr>
<tr>
<td>GIAC</td>
<td>Global Information Assurance Certification</td>
</tr>
<tr>
<td>GMAS</td>
<td>Gas Measurement Accounting System</td>
</tr>
<tr>
<td>GUI</td>
<td>Graphical User Interface</td>
</tr>
<tr>
<td>HIS</td>
<td>Historical Information Service</td>
</tr>
<tr>
<td>HMI</td>
<td>Human Machine Interface</td>
</tr>
<tr>
<td>HSRP</td>
<td>Hot Standby Routing Protocol</td>
</tr>
<tr>
<td>HVAC</td>
<td>Heating, Ventilation, and Air Conditioning</td>
</tr>
<tr>
<td>HW</td>
<td>Hardware</td>
</tr>
<tr>
<td>ICMP</td>
<td>Internet Control Messaging Protocol</td>
</tr>
<tr>
<td>IDEA</td>
<td>International Data Encryption Algorithm</td>
</tr>
<tr>
<td>IDS</td>
<td>Intrusion Detection System</td>
</tr>
<tr>
<td>IPSec</td>
<td>Internet Protocol Security</td>
</tr>
<tr>
<td>IED</td>
<td>Intelligent Electronic Device</td>
</tr>
<tr>
<td>ISQL</td>
<td>Interactive Structured Query Language</td>
</tr>
<tr>
<td>IS-IS</td>
<td>Intermediate System to Intermediate System routing protocol</td>
</tr>
<tr>
<td>ISSO</td>
<td>Information System Security Officer</td>
</tr>
<tr>
<td>L2TP</td>
<td>Layer 2 tunneling protocol</td>
</tr>
<tr>
<td>LAN</td>
<td>Local Area Network</td>
</tr>
<tr>
<td>Acronym</td>
<td>Definition</td>
</tr>
<tr>
<td>---------</td>
<td>------------</td>
</tr>
<tr>
<td>LDAP</td>
<td>Lightweight Directory Access Protocol</td>
</tr>
<tr>
<td>LMS</td>
<td>Liquid Management System</td>
</tr>
<tr>
<td>MCS</td>
<td>Main Control Station</td>
</tr>
<tr>
<td>MD5</td>
<td>Message Digest version 5</td>
</tr>
<tr>
<td>MS</td>
<td>Microsoft Corporation</td>
</tr>
<tr>
<td>NIC</td>
<td>Network Interface Card</td>
</tr>
<tr>
<td>NMC</td>
<td>Network Management Console</td>
</tr>
<tr>
<td>OASyS</td>
<td>Open Architecture System</td>
</tr>
<tr>
<td>ODBC</td>
<td>Open Database Connectivity</td>
</tr>
<tr>
<td>OLE</td>
<td>Object Linking and Embedding</td>
</tr>
<tr>
<td>OPC</td>
<td>OLE for Process Control</td>
</tr>
<tr>
<td>OSPF</td>
<td>Open Shortest Path First protocol</td>
</tr>
<tr>
<td>PKI</td>
<td>Public Key Infrastructure</td>
</tr>
<tr>
<td>PLC</td>
<td>Programmable Logic Controller</td>
</tr>
<tr>
<td>PLDS</td>
<td>Pipeline Leak Detection system</td>
</tr>
<tr>
<td>PQP</td>
<td>Project Quality Plan</td>
</tr>
<tr>
<td>PubSub</td>
<td>Publish Subscribe OASyS messaging subsystem</td>
</tr>
<tr>
<td>RADIUS</td>
<td>Remote Authentication Dial-in User Service</td>
</tr>
<tr>
<td>RAID</td>
<td>Redundant Array of Independent Disks</td>
</tr>
<tr>
<td>RBAC</td>
<td>Role Based Access Control</td>
</tr>
<tr>
<td>RDBMS</td>
<td>Relational Database Management System</td>
</tr>
<tr>
<td>RISC</td>
<td>Reduced Instruction Set Computing</td>
</tr>
<tr>
<td>RSA</td>
<td>The Rivest, Shamir, Adleman asymmetric encryption algorithm</td>
</tr>
<tr>
<td>RTS</td>
<td>RealTime Service</td>
</tr>
<tr>
<td>RTU</td>
<td>Remote Terminal Unit</td>
</tr>
<tr>
<td>SAT</td>
<td>Site Acceptance Test</td>
</tr>
<tr>
<td>SCADA</td>
<td>Supervisory Control and Data Acquisition</td>
</tr>
<tr>
<td>SCNA</td>
<td>Security Certified Network Architect</td>
</tr>
<tr>
<td>SCNP</td>
<td>Security Certified Network Professional</td>
</tr>
<tr>
<td>SCP</td>
<td>System Configuration Plan</td>
</tr>
<tr>
<td>SCS</td>
<td>Standby Control Station</td>
</tr>
<tr>
<td>SEAM</td>
<td>Serial Encryption and Authentication Module</td>
</tr>
<tr>
<td>Acronym</td>
<td>Definition</td>
</tr>
<tr>
<td>---------</td>
<td>------------------------------------------------</td>
</tr>
<tr>
<td>SHS</td>
<td>Secure Hash Standard</td>
</tr>
<tr>
<td>SOAP</td>
<td>Simple Object Access Protocol</td>
</tr>
<tr>
<td>SOE</td>
<td>Sequence Of Events</td>
</tr>
<tr>
<td>SQL</td>
<td>Structured Query Language</td>
</tr>
<tr>
<td>SRM</td>
<td>Security Reference Monitor</td>
</tr>
<tr>
<td>SRM</td>
<td>Security Reference Monitor</td>
</tr>
<tr>
<td>SSCP</td>
<td>Systems Security Certified Practitioner</td>
</tr>
<tr>
<td>SSCR</td>
<td>System Setup and Configuration Reference</td>
</tr>
<tr>
<td>SSO</td>
<td>Single Sign-On</td>
</tr>
<tr>
<td>SW</td>
<td>Software</td>
</tr>
<tr>
<td>SWANA</td>
<td>Software Analyzer, a Telvent tool</td>
</tr>
<tr>
<td>TCB</td>
<td>Trusted Computing Base</td>
</tr>
<tr>
<td>TCP/IP</td>
<td>Transmission Control Protocol / Internet Protocol</td>
</tr>
<tr>
<td>TTA</td>
<td>Two-Token Authentication</td>
</tr>
<tr>
<td>UDP</td>
<td>User Datagram Protocol</td>
</tr>
<tr>
<td>UHF</td>
<td>Ultra High Frequency</td>
</tr>
<tr>
<td>UTP</td>
<td>Unshielded Twisted Pair</td>
</tr>
<tr>
<td>UPS</td>
<td>Uninterruptible Power Supply</td>
</tr>
<tr>
<td>VDU</td>
<td>Visual Display Unit</td>
</tr>
<tr>
<td>VSAT</td>
<td>Very Small Aperture Transmission (satellite)</td>
</tr>
<tr>
<td>WAN</td>
<td>Wide Area Network</td>
</tr>
<tr>
<td>WMI</td>
<td>Windows Management Instrumentation</td>
</tr>
<tr>
<td>WORM</td>
<td>Write Once, Read Many</td>
</tr>
<tr>
<td>XML</td>
<td>Extensible Markup Language</td>
</tr>
</tbody>
</table>

*Table 1 - Table of Acronyms*
1.5 STANDARDS

1.5.1 General

1.5.1.1 The design, construction and performance of the SCADA system shall conform to the requirements of the latest published edition of the following standards and standards organizations unless otherwise stated in this specification:

- American Gas Association (AGA)
- American National Standards Institute (ANSI)
- American Petroleum Institute (API)
- American Society of Mechanical Engineers (ASME)
- Electrical Industry Association (EIA)
- Federal Information Processing Standards (FIPS)
- International Electro-technical Commission (IEC)
- Institute of Electrical and Electronics Engineers (IEEE)
- International Information System Security Certification Consortium (ISC)²
- Instrument Society of America (ISA)
- International Standards Organization (ISO)
- National Electrical Codes (NEC)
- National Electrical Manufacturers Association (NEMA)
- National Institute of Standards and Technology (NIST)
- National Security Agency (NSA)
- Occupational Safety & Health Administration (OSHA)
2. SYSTEM ARCHITECTURE

2.1 INTRODUCTION

2.1.1 General

2.1.1.1 The SCADA system shall provide a strategy for Real-Time solutions that shall go beyond SCADA, offering the end user access to an open and enterprise-friendly data management system.

2.1.1.2 Included in the SCADA system's family of products shall be a Graphical User Interface (GUI), a fully integrated Real-Time sub-system, and a fully integrated Relational Database Management System (RDBMS).

2.1.1.3 The SCADA system shall also provide for easy and open integration with third party application software via non-proprietary industry standards.

2.1.1.4 The SCADA system shall allow the user of the system the flexibility to accommodate diverse business applications.

2.1.1.5 The SCADA system shall provide capability to extend Real-Time data from the field to the enterprise by providing access to operational and historical data anytime, and anywhere.

2.1.1.6 The SCADA system shall allow corporate information systems and specialized applications packages access to the SCADA data through a Decision Support Server (DSS).

2.1.1.7 The SCADA system architecture shall utilize non-proprietary industry standards all to enable transparent connectivity to other hardware, software, and networks.

2.1.1.8 Telvent shall adhere to DBNGP security policies and procedures in order to ensure the overall security of the new SCADA system, corporate information systems, and associated specialized applications.

2.1.1.9 Where such policies and procedures require further clarification because of this SCADA project, Telvent shall provide security specialists for consultation with DBNGP IT and security staff.

2.1.1.10 This collaboration shall ensure a tight mapping between the SCADA system’s security capabilities and the requirements implied by DBNGP corporate security policies and procedures.

2.1.1.11 Telvent shall select materials and components that best fit Telvent's SCADA system and meet the requirements outlined in this document.

2.1.1.12 The SCADA system shall provide for single sign-on that shall reduce redundancy and shall simplify user security management by administrating all network security from the common Active Directory service (ADS).
2.1.1.13 The system shall use the Active Directory Services to manage all users, security and resources.

2.1.1.14 The system shall provide replication and local caching of Domain Name System (DNS) and Dynamic Host Configuration Protocol (DHCP) information, keeping the SCADA system robust and responsive.

2.1.1.15 The use of Active Directory Services shall reduce directory management to a single user definition, offering the opportunity to integrate the SCADA system into the DBNGP enterprise directory.

2.1.1.16 Single logon access shall centralize user tasks and definitions and shall free the SCADA system from proprietary control of user name and password.

2.1.1.17 The end user shall be able to comply with DBNGP enterprise standards.

2.1.1.18 A Network Management Console (NMC) shall be available for configuration, administration, and monitoring of the SCADA system. This console shall leverage existing technology such as Windows Management Instrumentation (WMI) and ADS for information.

2.1.1.19 The NMC shall present a visual interface into the systems and services on the network, including current configuration and status.

2.1.1.20 The NMC shall offer access familiarity, plus the ability to see the status of sub-components on each system.

2.1.1.21 Administrators shall be able to quickly assess, diagnose and respond to the health of systems on the network.

2.1.1.22 It shall be possible to use the NMC to configure and administrate:
   a) Systems
   b) Services
   c) Computer SCADA properties
   d) Device SCADA properties
   e) Users, authorities and permissions

2.1.1.23 It shall be possible to use the NMC to monitor:
   a) Service states
   b) Processes
   c) Machine health
   d) Error logs
2.2 GENERAL SYSTEM REQUIREMENTS

2.2.1 General

2.2.1.1 The objectives of performance, flexibility, expandability and open access are fundamental in determining the utility and longevity of any SCADA system. The SCADA system shall utilize a software architecture that allows functions to be mobile, flexible and robust. It shall also permit distribution of processing among different SCADA system components to optimize overall system performance.

2.2.1.2 N-tier architecture shall be used to facilitate the realization of the above objectives. N-tier architecture shall allow both centralized and distributed accommodation of business rules, operational considerations, and information security requirements in this landscape of changing business requirements for SCADA data.

2.2.1.3 The enabling N-tier architecture shall glue applications together. This shall offer the flexibility to address the variety of issues facing inter-process communications, and shall improve the resulting functionality overall.

2.2.1.4 In this N-tier model, there shall be a discrete separation between the user interface, the logic used to present data to the user and the data itself. The most common form of n-tier is considered to be the 3-tier application, where user interface programming is in the user’s computer, business logic is in a more centralized computer, and needed data is in a computer that manages a database. When there are more than three distribution levels or tiers involved, the additional tiers in the application shall usually be associated with the business logic tier.

2.2.1.5 Functionality and the application of business and security rules shall be consistent remotely, or in a control room. Further, the distributed N-tier architecture used shall allow for optimization of overall system performance.

2.2.1.6 The N-tier model used shall provide for:
   a) the possibility for any one tier to run on an appropriate processor or operating system platform
   b) the possibility for any one tier to be updated independently of the other tiers
   c) scalability from small to large systems

2.2.1.7 The SCADA system architecture shall utilize non-proprietary industry standards such as TCP/IP, ANSI SQL, ODBC and Component Object Model (COM) interfaces, and Extensible Markup Language (XML) encoding.

2.2.1.8 The system shall provide support for the use of industry recognized
embedded RDBMS database technology.

2.2.1.9 Customization of "off the shelf" hardware or software shall not take place. Configuration of this software is acceptable.

### 2.3 DISTRIBUTED SYSTEM ARCHITECTURE

#### 2.3.1 General

2.3.1.1 The SCADA system shall conform to the concepts of a distributed information system.

2.3.1.2 Components provided as part of Telvent’s system must have the ability to share historical and real-time data between independent systems and geographical locations. This shall enhance the overall system reliability and functionality by providing shared access to components and applications.

2.3.1.3 Telvent’s distributed system shall provide configuration options that allow multiple systems to share telemetry data, alarming, eventing, telecommunication, and control functionality.

2.3.1.4 User permissions and security restrictions regarding all aspects of the system shall propagate seamlessly across the SCADA system’s distributed architecture.

2.3.1.5 All computers in the SCADA system shall connect with each other using the latest industry standard Local-Area Network (LAN) and Wide-Area Network (WAN) technology. Multiple LANs, WANs, bridges, servers and routers shall complement each other to meet the requirements of system performance, reliability, security and expandability.

2.3.1.6 System peripherals shall connect either directly to the system's LAN, through servers connected directly to the system's LAN, or attached to workstation parallel or serial ports. This shall allow access to any device from any computer in the system with the appropriate access authority.

2.3.1.7 The system shall provide support for distributed network equipment such as networked printers, networked PC's, and mass storage/backup devices.

2.3.1.8 The SCADA system shall be configured using industry standard, unmodified, hardware and software. The hardware and software supplier's standard products shall constitute the primary components for the system.

2.3.1.9 The system shall not be dependent upon specialized, unique, or proprietary equipment or software available from only a single supplier to the greatest extent possible (besides Windows).

2.3.1.10 The system shall provide bi-directional item by item replication of data between systems. To handle the large amounts of data being exchanged between systems without requiring excessive WAN bandwidth usage, Real-Time data shall only be shared between those systems with defined
It shall be possible to define these system relationships to share all records or only specified fields within records. To further reduce the network load between locations, it shall be possible to store historical data locally by each system.

The system shall support a controller friendly method (such as a single push button or dialog box) to change the operational state of the system.

Under normal operating condition, in no case shall it be necessary to shutdown and/or restart any systems in order to activate or deactivate the processing of data at a system.

**Supported Architectures**

Due to changing regulatory and business requirements, DBNGP desires a solution that provides flexibility and expandability of the initial system to accommodate changes with a minimum of cost and effort.

Telvent's base product shall also support PRIMARY/BACKUP, PEER-TO-PEER, MASTER/SUB-MASTER, and TEST/DEVELOPMENT architectures. (Telvent's “base product” means that the requested configuration can be accommodated without customization, recompilation or regeneration of the entire system. It is understood that some changes may require licensing additional Telvent products or modules.)

Each system, consisting of real-time and historical servers, shall be capable of single or redundant real-time and historical servers.

Each system shall be capable of supporting a DSS or Decision Support Server to supply data to corporate and other non-SCADA users. This system shall operate in a view only mode (no control or configuration capability).

PRIMARY/BACKUP - It shall be possible to configure Telvent's base product such that one system operates as the primary control and operation system, and the second system operates as the backup system.

PEER TO PEER – It shall be possible to configure Telvent's base product such that each system nominally monitors and controls a subset of the overall data, and each system also functions as the backup for the other.

MASTER/SUB-MASTER(S) – It shall be possible to configure Telvent's base product such that one system monitors and controls all field data, with many sub-master systems responsible for field communications.

OFFLINE TEST/DEVELOPMENT – It shall be possible to configure Telvent’s base product such that one of the systems may operate as an offline test and development system used to implement and verify changes to the SCADA system before deploying them to the production environment. This server shall be called the Engineering Server.
2.3.2.9 Depending on the configuration and the relationships defined between systems:

a) Field devices owned by one system shall be controllable by another system

b) Systems can act as backups, or load-balancing partners, for other systems

c) All or part of the historical and real-time data belonging to a given system shall also be sharable with other systems

In this way, real-time functional elements of the SCADA system shall inter-operate regardless of their physical location, allowing elements in separate locations to “know” what the other systems are doing.

2.4 DISTRIBUTED MIDDLEWARE ARCHITECTURE

2.4.1 General

2.4.1.1 The distributed components of Telvent’s system shall be modular in design and open in architecture to allow connectivity by way of a middleware data bus.

2.4.1.2 This middleware data bus shall be open in architecture and generic in implementation, sufficient to allow communication between individual components and applications, some of which may be “third-party”, to Telvent’s software components.

2.4.1.3 Each of these modules shall be independently upgradeable, without requiring an upgrade to the middleware architecture.

2.4.1.4 The middleware data bus shall allow distributed “event-driven” applications.

2.4.1.5 The middleware data bus shall allow one application to transmit or publish information to other applications without waiting for the other applications to receive the information.

2.4.1.6 Multiple subscribers to the data on the middleware data bus shall each receive a broadcast message from the network to minimize network traffic in highly integrated distributed system environments.

2.4.1.7 Additional subscribers shall have no impact on the performance of the other publishers connected to the middleware data bus.

2.4.1.8 Real-Time Middleware shall provide the communication protocols to glue together the n-tier architecture and render seamless integration between the presentation, logic, and data tier. Real-Time Middleware shall comprise of three key components:

a) Business Object Engine
b) SQL Engine  
c) Real-Time Pub/Sub

2.4.1.9 The Business Object Engine shall process raw SCADA data for access throughout the DBNGP enterprise. Using Microsoft COM+ with support for Simple Object Access Protocol (SOAP), any application, including web-enabled, shall have access to the Business Object Engine.

2.4.1.10 The Business Object Engine shall provide functionality that can be updated with a much shorter risk of down time because of componentization, n-tier modeling, thin client architecture (business logic moves out of the client), pure data-store scalability and performance.

2.4.1.11 Telvent shall ensure that the publisher/subscriber middleware provided consists of the following attributes:

a) Distributed  
b) Bi-directional  
c) Guaranteed message delivery during normal operations  
d) Integrity updates after network connectivity restoration  
e) High performance (up to 20,000 messages/second)  
f) Multithreaded  
g) Able to deliver messages across multiple routed network segments  
h) Able to integrate with non-real-time publisher/subscriber systems

2.5 SYSTEM REDUNDANCY THROUGH A DISTRIBUTED ARCHITECTURE

2.5.1 General

2.5.1.1 Due to the critical nature of SCADA system functions, there shall be no single point of failure on any critical system component. A critical component is any component whose failure directly and adversely affects the system's overall performance or its ability to continue performing the critical SCADA functions of monitoring and control.

2.5.1.2 The system shall make use of modular components such that the failure of a single component does not render inoperative other components.

2.5.1.3 The system shall provide redundancy for all critical SCADA functions.

2.5.1.4 The components comprising the standby system shall receive continually updated data, as appropriate, to provide a “hot-standby” capability in case of a hardware or software initiated failover.

2.5.1.5 The SCADA system shall make connection to any corporate or other networks in such a way that a failure of any of these networks shall not affect the SCADA system's ability to perform its critical functions.
2.5.1.6 The redundancy model shall be self-healing with critical functions and devices being monitored by health monitoring software provided by Telvent. This shall be considered a key component of system robustness and for ease of support and administration.

2.5.1.7 System Monitors shall check critical components for failures, and take the least intrusive course of action to recover from any failure. The system integrity shall not be impacted.

2.5.2 Network Model

2.5.2.1 The network configuration shall provide a simplified network model that shall allow dual redundancy, yet it shall look like a single virtual LAN to the user. The redundancy model shall be both robust and self-healing. When a single component fails, that component’s partner shall take over without impacting the rest of the system.

2.5.2.2 Single virtual LAN robustness shall be achieved through the provision of:

2.5.2.3 Dual intelligent redundant switches - Each switch shall be interconnected, providing the advantage of network communication between cards and redundancy in case of the failure of one card.

2.5.2.4 Dual intelligent redundant network cards - The use of intelligent cards and drivers shall provide for the cards to sense when a network or the other card fails, resulting in the healthy card taking over.

2.5.2.5 Floating IP addresses - For a pair of redundant servers, a single address shall be assigned to the active server. This shall allow connectivity to active servers without having to know what physical machine is currently active.

2.5.2.6 The system shall provide a fail-over mechanism that shall be an inherent part of the SCADA system.

2.5.2.7 The system shall provide critical task monitoring by health monitoring software to ensure system robustness.

2.5.2.8 Monitor processes periodically shall ask critical software components to check in. If the critical component fails to check in, that one component and all its sub-components shall fail-over; all others shall stay live. (e.g. Historical or Realtime service)

2.6 SYSTEM EXPANSION AND LIFE CYCLE

2.6.1 General

2.6.1.1 The system shall have the capacity for 100% expansion initially with no hardware or software design limitations that would preclude upgrading the performance and capacity of the system.

2.6.1.2 The system shall have a useful operating life exceeding 5 years with routine...
and preventative maintenance.

2.6.1.3 There must be a viable progression path available for upgrading both the hardware and software to future versions.

2.7 SYSTEM OVERVIEW AND DESIGN

2.7.1 General

2.7.1.1 The SCADA system shall provide a distributed real-time platform incorporating interoperable applications linked by open connectivity standards such as ODBC, XML, ADO, JDBC, OLEDB, SQL, JAVA, and SOAP.

2.7.1.2 The SCADA system shall accommodate interconnectivity options and data store connectivity portals for legacy and future third-party enterprise IT systems.

2.7.1.3 The SCADA system shall allow the import and export of data to and from external sources, and allow data access using common desktop tools such as Microsoft Excel, Microsoft Access, Crystal Reports, and large enterprise applications.

2.7.1.4 The SCADA system shall include open connectivity standards that enable integration with applications such as:
   a) Microsoft Excel, Microsoft Access
   b) Crystal Reports
   c) Large enterprise applications such as SAP, PeopleSoft, Siebel, and ERP systems
   d) Internet or Intranet access
   e) Sybase, PI, AspenTech, Oracle, DB2, and MSSQL data stores

2.7.1.5 It shall be possible to add, remove, upgrade or replace Applications in a building block fashion. Duplication of data shall be eliminated, reducing database management and administration tasks.

2.7.1.6 The SCADA system shall functionally consist of three main components:
   a) Real-time and Time-Critical Applications (Realtime)
   b) Operator Interface Applications (XOS)
   c) Historical Data Storage (Historical)

2.7.1.7 The Real-Time and Time-Critical Applications, and Operator Applications, shall be considered critical and essential to the safe operation of the SCADA system.

2.7.1.8 The Historical Data Storage shall provide data capture for historical data analysis, enterprise application integration, and regulatory reporting needs.
2.7.1.9 These categories shall further be subdivided into the following types of functions in each category:

a) Real-Time SCADA and Time-Critical Applications
   • Real-Time SCADA and Time-Critical Applications
   • Application Specific Time-Critical Processes
   • Real-Time Database Applications/Support
   • Application Specific Non-Time-Critical Processes
   • System Security Applications and Processes

b) Operator Interface Applications
   • Interface Support
   • Applications
   • Controller Interface

c) Historical Data Storage
   • Historical Database
   • Historical Data Capture
   • Application Specific Historical Data Manipulation Processes

2.7.1.10 The Real-Time SCADA and Time-Critical Applications provided by Telvent shall be considered the most critical category of functionality as they provide the basic monitoring and control capabilities of the SCADA system. Typical functions in the Real-Time SCADA and Time-Critical Applications category include:

a) Data Acquisition
b) Engineering Units Conversions
c) Alarm Detection and Annunciation
d) Alarm/Event Logging
e) Interaction with the Operator Workstations
f) General Control Output and Status Change Validation
g) Maintenance of the System’s Real-Time Database
h) Monitoring of the System Performance
i) Capture of Instantaneous Data to Support Historical and Regulatory Data Requirements

2.7.1.11 Typical real-time database support functions provided by Telvent shall include applications such as:

a) On-line Calculations/Derived Values
b) Database Save/Transfer Utilities
c) Real-Time Data Sampling

2.7.1.12 Typical Operator Interface support functions provided by Telvent shall include applications such as:
   a) Output of Controller and Software Initiated Control Commands
   b) Alarm Annunciation/Alarm Logging
   c) Updating Alarm Displays
   d) Responding to Periodic Requests to Display Real-Time Data

2.7.1.13 Telvent shall provide Operator Applications comprising the next most critical area of functionality for the system, and shall include the following functions:
   a) Display Generation
   b) Data Presentation
   c) Display Navigation
   d) Data Manipulation
   e) Control Actions
   f) Alarm Presentation
   g) Controller Entry of Parameters or Data
   h) Report Generation
   i) Format Editing/SCADA System Maintenance

2.7.1.14 The Historical Data Storage module provided by Telvent is considered the least critical function. Although the functions of this module support the operation of the field system, none of the functions shall require data in real-time. The SCADA system shall provide the following typical functions in this category:
   a) Data Archival/Retrieval
   b) Historical Data Manipulations/Calculations
   c) Device Operating Times
   d) The interface to the corporate network

2.7.1.15 A high speed redundant LAN shall interconnect the computer systems, local real-time Human Machine Interfaces, and support equipment.

2.7.1.16 The Local Area Network shall consist of high-speed redundant interconnected switches. Support equipment not capable of direct connection to the Local Area shall connect through routers, or workstations, as appropriate. Where appropriate, Telvent shall duplicate support equipment for each portion of the redundant LAN in such a fashion as to provide redundant functions through each of the LANs.
2.7.1.17 The computer systems and local real-time Human Machine Interfaces shall independently connect to each portion of the redundant LAN and shall have access to all support equipment on that LAN.

2.7.1.18 The Local Area Network configuration shall offer near invisible dual LAN redundancy through the use of a single “virtual” LAN configuration concept. This model shall offer the high reliability of a dual LAN, while presenting the simplicity of a single LAN to the end user.

2.7.1.19 The entire SCADA system shall be synchronized to a single time source. This time source shall come from the GPS system. Redundant GPS servers shall be used. One as the primary and one as the secondary but both shall always be hot.

2.7.2 System Diagram

A typical diagram to highlight the important features of the system proposed for the main control center of the DBNGP pipeline is shown in Figure 2-1 below. It will consist of dual redundant Realtime Servers, dual redundant Historical Servers, an Engineering Server, several workstations, printers and network gear. The main control system will be located at the existing A2 location.

There will be an identical system at the backup (disaster) location. The servers will all be located at the Jandakot site while the operation stations will continue to be located at the GHD location. At some future time these operator stations may be relocated to the Jandakot site as well.

The dual LAN will be structured in such a way that to the SCADA machines it appears as a single virtual LAN. This offers redundancy on a hardware level while easing the implementation of software redundancy.

The SCADA LAN will be separate from the Corporate LAN except for one well known access points that can easily be controlled from a security and data “leaking” (having SCADA data choke the Corporate LAN or vice versa) standpoint.

It will also be possible to access the system from remote or offsite locations. The remote locations will be connected through the existing microwave network or the new faster microwave network. The access from home or for remote support by Telvent will be handled through a Cisco PIX device.

A DMZ (demilitarized zone) can be setup for serving out reports and offering access to SCADA data from the Corporate LAN to a server called the DSS. Another server, the Engineering server shall be used to allow database and display modifications and offline testing of new applications to happen before they are put onto the operational systems.

The entire system is time synchronized to a GPS timeserver that sits on the network and gathers its time from the Global Positioning System. Failing this it uses its internal Stratum–1 clock.
Printers are available to be used anywhere on the network by anyone. All the servers will be 19" rack mounted and all displays will be LCD panels. It will be possible to have a video switch to send SCADA displays to the existing large screen monitors at the A2 site or optionally even larger monitors could be installed.

![Diagram](image.png)

*Figure 2-1- Typical System Overview Diagram*

### 2.7.3 System Sizing

#### 2.7.3.1

This section details quantities of key components of the system. The SCADA system shall consist of the following:

<table>
<thead>
<tr>
<th>Component</th>
<th>#</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sites</td>
<td>2</td>
<td>Master Control Center (A2) and Backup Control Center (Jandakot)</td>
</tr>
<tr>
<td>Servers</td>
<td>8</td>
<td>2 Realtime, 2 Historical at MCC and BCC</td>
</tr>
<tr>
<td>XOS</td>
<td>17</td>
<td>3 at MCC, 2 at BCC and 10 at the CS, 2 at Jandakot</td>
</tr>
<tr>
<td>Printers</td>
<td>1</td>
<td>1 new color laser at MCC others reuse existing</td>
</tr>
<tr>
<td>Remote Users</td>
<td>15</td>
<td>Concurrent casual users</td>
</tr>
<tr>
<td>Protocols</td>
<td>4</td>
<td>MODBUS serial, Conitel serial, MODBUS/IP, DNP3</td>
</tr>
<tr>
<td>GPS</td>
<td>2</td>
<td>One at each site for time synchronization</td>
</tr>
</tbody>
</table>
2.8 SCADA SYSTEM CONFIGURATION, MONITORING AND CONTROL MANAGEMENT ENVIRONMENT

2.8.1 General

2.8.1.1 Telvent shall provide a single management environment for SCADA software configuration, monitoring and control.

2.8.1.2 This management environment shall include the following attributes:
   a) Accessibility from any machine in the SCADA installation
   b) Enable monitoring of SCADA software and machine states
   c) Enable viewing of machine log files
   d) Enable viewing/modification of all SCADA machine/database/application privileges and User Areas of Responsibility.
   e) Enable viewing/modification of SCADA system and machine properties.
   f) Enable addition/removal of SCADA software systems from the SCADA domain.
   g) Enable addition/removal of SCADA machines.
   h) Enable SCADA software and third-party integrated component control (i.e. startup/shutdown/failover)

2.9 COMMUNICATIONS

2.9.1 General

2.9.1.1 The communication subsystem provided shall contribute to the longevity, usability and ultimate performance of the SCADA system. The communication subsystem shall have adaptability inherent in its design, and shall readily allow for future expansion.

2.9.1.2 There shall be three primary forms of communication which shall be inherent in the SCADA system as follows:
   a) Synchronous/Asynchronous Communications (dedicated circuits and dial-up circuits)
   b) Local-Area Networks
   c) Wide-Area Networks

2.9.1.3 The SCADA system shall support varying types of physical networking media (e.g., fiber optics, shielded twisted pair, microwave, radio, satellite, etc.). The use of any particular type of networking media shall be transparent to the system.

2.9.1.4 The network interface hardware and software shall handle any inherent
differences between these various types of physical network media.

2.9.1.5 Serial communications device interfaces shall be compliant with the EIA-232D standard and can either be synchronous or asynchronous.

2.9.1.6 All serial interfaces selected for use with the SCADA system shall support full hardware modem control.

2.9.1.7 The redundant SCADA LAN shall use an industry standards compliant LAN technology operating at a minimum speed of 100 Mbps with support for 1Gbps.

2.9.1.8 The SCADA LAN shall be fault-tolerant and shall utilize a network configuration, which shall prevent any single point of failure disabling the system.

2.9.1.9 The LAN shall be redundant and shall support shared data paths or 100 percent operation on either LAN.

2.9.1.10 All Wide Area Networks (WAN) shall be logical extensions of the Local Area Networks (LAN). Any interfaces between LANs and WANs shall be through routers, bridges and/or concentrators and data control units.

2.9.1.11 All LAN/WAN communication equipment shall support the following common features, as applicable to the type of equipment used:
   a) Network Management - SNMP (Simple Network Management Protocol), CMIP (Common Management Information Protocol), or both
   b) Multiple Protocols - TCP/IP, X.25, etc.,
   c) IP Routing
   d) Destination Address Filtering
   e) Protocol Filtering
   f) Source Address Filtering
   g) Spanning Tree Algorithm

2.9.1.12 The SCADA system shall include system management tools for monitoring/analyzing/troubleshooting of all system Local-Area Networks, Wide-Area Networks and connected equipment.

2.9.2 Routers

2.9.2.1 Routers shall provide a communication path between computers on an 802.3/Ethernet Local Area Network and other computers not physically connected to the SCADA LAN. Routers shall communicate via layer three (network layer) of the ISO Open Systems Interconnection (OSI) networking protocol model.

2.9.2.2 All SCADA system routers shall support full hardware modem control.
2.9.2.3 Connectivity between any two computers in the entire system shall be transparent as a consequence of the flexibility inherent in the routing configurations used by Telvent in the SCADA system.

2.9.2.4 All routers shall perform automatic diagnostic checks on start-up and during operation and report their status to the controlling host computer.

2.9.2.5 Telvent shall keep all out-of-band router communications to a minimum.

2.9.2.6 All routers shall be capable of high filtering and forwarding rates.

2.9.2.7 All routers shall be capable of network nodal addressing analysis.

2.9.3 Bridges

2.9.3.1 Bridges, if used, shall function similarly to routers except, unlike routers, bridges shall be transparent to the sending entity. Bridges shall communicate via layer 2 (data link layer) of the ISO Open Systems Interconnection (OSI) networking protocol model.

2.9.3.2 Bridges shall connect two segments of a Local Area Network. On the SCADA system, bridges shall provide the following functionality:

   a) Isolate the redundant SCADA LAN segments so that a single LAN failure shall not cause a general network failure.

   b) Form Wide Area Networks from geographically separated Local Area Networks.

2.9.3.3 Bridges shall intercept transmissions at the Local Area network connection point and determine the validity of the destination node (including loop avoidance) before allowing a message to proceed across the bridge.

2.9.3.4 The bridge shall be capable of high filtering and forwarding rates.

2.9.4 Concentrators

2.9.4.1 Concentrators are a special type of bridge, which shall allow multiple Local Area Networks to interconnect with each other.

2.9.4.2 All concentrators, if used, shall be capable of dual homing and shall support the use of an optional bypass mechanism to maintain LAN integrity in the event of a concentrator failure.

2.9.5 Network Interface Cards

2.9.5.1 Each SCADA server shall have two network interfaces, implemented as two separate Network Interface Cards (NICs), or as dual ported NICs. Each port shall plug into a separate switch with the exception of the Decision Support Server because it is deemed as non-critical.
2.9.5.2 Failure of a single NIC shall not affect any of the SCADA server processes.

2.9.5.3 Each NIC shall support IPSec to encrypt all data traffic on the LAN if desired.

2.9.6 Data Acquisition Equipment

2.9.6.1 The SCADA system shall be capable of gathering data from various RTU/PLC and IED units in the field. The communication media may be leased lines, dial-up telephone circuits, fiber optic cables, radios, and microwave or satellite channels.

2.9.6.2 The system shall be capable of supporting more than one additional, alternative, dial back-up communication path.

2.9.6.3 At the host SCADA, this dial-up channel shall connect through a different communication server/modem combination than the primary dedicated channel.

2.9.6.4 It shall be possible to manually initiate the dial-up path after the loss of a critical, primary path. However, once a dial-up path has been selected for a particular remote terminal unit, or programmable logic controller, the system shall perform the necessary tasks to establish and maintain the link.

2.9.6.5 The system shall also provide for automatic fail-over to the alternate path. If the Automatic Fail-over to Alternate Path is set, the system shall monitor the alternate path on a regular basis, and fail over to the alternate path when the primary path is declared failed.

2.9.6.6 The SCADA system shall allow for easy expansion for additional dial-up paths in the future.

2.9.6.7 The system shall be capable of supporting any protocol over any communications path, provided the appropriate ancillary communication hardware, such as modems, is available.

2.9.6.8 The system shall be capable of supporting any number of communication link paths (connections) from the SCADA host to any single RTU/PLC or IED.

2.9.6.9 All serial communication interfaces shall support full hardware modem control and full duplex operation. RTU/PLC response time-out values shall be user definable on an individual RTU/PLC basis. Separate time out values shall be available for dedicated and for dial-up lines.

2.9.6.10 The system communications shall be field upgradeable to 100% of the original installed capacity with the simple addition of communication servers, cabling and modems, etc. The SCADA Servers must support this within the framework of the initially supplied hardware.
3. REAL-TIME SUBSYSTEM

3.1 INTRODUCTION

3.1.1 General

3.1.1.1 The Real-Time Service shall provide the basic monitoring and control function for the SCADA system.

3.1.1.2 The Real-Time Service shall incorporate the database model of the physical system and the mechanisms to acquire and process the data from the field. This subsystem shall be considered critical to the process operation; therefore, it shall be highly reliable.

3.1.1.3 The Real-Time Service shall be a memory-resident SCADA kernel that shall perform all of the Real-Time functions, including RTU polling, supervisory control, alarm detection, alarm processing, and user-defined calculations.

3.1.1.4 For performance and reliability, the Real-Time Service shall utilize shared memory or similar mechanism to exchange data between applications and processes.

3.1.1.5 Polling and data acquisition shall be functional components of this subsystem utilizing a field polling engine.

3.1.1.6 The system shall provide the following within the Real-Time Services:
   a) Real-Time Services shall support SQL access to both data through an SQL Engine component
   b) Replication Services shall support the replication of all or parts of the Real-Time services to other Real-Time servers on the network
   c) The system shall provide intelligent alarming capabilities including alarm disturbance and alarm suppression modes
   d) The system shall have a Real-time Database

3.1.1.7 To accommodate system changes, an interactive editor shall be provided to add, delete, or modify system parameters. This editor is called ADE (Advanced Database Editor). It offers a single point of database modifications.

3.1.1.8 Modified portions of the database shall be in effect when they are loaded into system memory. In no case shall existing database content modifications require a system shutdown, or failover, or recompilation of the SCADA system.
3.2 REAL-TIME DATABASE

3.2.1 General

3.2.1.1 The system shall supply a centralized data store for all real-time data. The real-time database shall contain in a common accessible format:

a) All Telemetered Data
b) All Manually Entered Data
c) All System Configuration Data
d) All Run-Time Calculated Values

3.2.1.2 The real-time database(s) shall have the following features:

a) On-line database value modification capability (e.g., conversion coefficients, factors, limits, etc.) via an editor
b) On-line database record modification capability (e.g., modifies, adds, replaces or deletes RTUs, points, units, lines, etc.) via an editor
c) A single “logical” SCADA applications database, (i.e., data common to all functional areas should only need to be changed by one function and, preferably, exist in only one place)
d) Physical reconfiguration of the data acquisition subsystem shall be transparent to interactive and programmatic database access (e.g., changing the position of a scanned quantity on a RTU or moving it to another RTU shall not affect retrieval of that quantity)
e) Shall support definable data types including nested data types
f) Shall be compatible with ODBC-2 accessible databases such as Microsoft Excel, Microsoft Access and SQL servers

3.2.1.3 Replication Services support the replication of all or parts of the real-time Services to other real-time servers on the network.

3.2.1.4 The database(s) shall persist in main memory (RAM) for maximum access speeds. It shall be mapped to disk and periodically flushed there.

3.2.1.5 Telvent shall minimize data redundancy through proper database structure normalization, such as “Domain-Key” normalization. Such database normalization shall require that records in any table be accessible by a key name. The system shall provide for database records to be keyed for indexed database access. The database shall support multiple key fields in a table.

3.2.1.6 The design of the real-time database(s) provided by Telvent shall accommodate industry standard interfaces using ODBC, and SQL.

3.2.1.7 The real-time database(s) shall be accessible via ANSI SQL-compliant calls. It shall be possible for SQL compliant commands to define tables, index fields,
3.3 DATA ACQUISITION

3.3.1 General

3.3.1.1 The system shall provide for data acquisition to take place through a variety of physical connections using many different protocols and modes of communication.

3.3.1.2 The polling engine shall poll the attached RTUs for data according to the user-programmed scan frequency and scan profiles.

3.3.1.3 This engine shall provide enhanced dialup support and connection control.

3.3.1.4 The polling engine shall handle basic polling and control of field devices by using a layered, object oriented design for efficient integration of new protocols.

3.3.1.5 The polling engine shall be capable of handling a virtually unlimited number of communication lines. (Limited by RAM.)

3.3.1.6 System load shall be mostly independent of the number of communication lines; it shall be dependent only on the number of telemetry points and alarms generated per second.

3.3.1.7 The polling engine shall use a generic approach to communicate with physical media.

3.3.1.8 It shall be possible to configure multiple communication paths for a remote from the primary site and any alternate site (e.g. the primary may be a dial-up line [single or multi-drop] and the alternate may be a UHF connection.)

3.3.1.9 It shall be possible to associate a cost factor with each communication path.

3.3.1.10 The cost factor shall be used to locate the least expensive available connection to a remote.

3.3.1.11 It shall be possible for communications to fail-over to an alternate path based on user command or system detected path failure.

3.3.1.12 It shall be possible to enable and disable the automatic fail-over of communication paths on a per remote basis.

3.3.1.13 A failed communication path shall be periodically tested and be restored when tests return a successful communication to a field device.

3.3.1.14 The polling engine shall handle these connection types:
   a) Network I/O (leased lines or hard wired through a terminal server, VSAT, radio, Ethernet)
b) Handles population/configuration of cross-reference tables (i.e. TCP/IP to X.25)

3.3.1.15 The polling engine shall allow for the dynamic configuration of terminal server ports and modems.

3.3.1.16 The polling engine shall allow multiple modems to be used for the dial-out lines and RTUs to communicate at various baud rates (like 300, 600, 1200, 2400, 4800, 9600, 19200, 38400).

3.3.1.17 The system shall allow for the following modem handling capabilities:
   a) Configurable modem strings;
   b) Configurable modem response delay times;
   c) Configurable modem expected response;
   d) Multi-drop dial capabilities;
   e) A modem bank database which shall allow the user to control the modem used by a certain connection, and to allow the reservation of modems for specific uses.

3.3.1.18 A modem testing process shall be provided which shall test unused modems in the background (individually or by modem pool).

3.3.1.19 The polling engine shall handle multiple communication ports with one or more RTUs per port. Each physical connection shall accommodate numerous multi-dropped RTUs via radio or telecommunications bridging equipment using leased line, fiber optic, radio, satellite or Cellular Digital Packet Data (CDPD).

3.3.1.20 The polling engine shall provide support for many communication lines and RTUs as necessary, with no artificial maximum number of lines that would limit the capacity or performance of the system. The system shall be capable of acquiring data sequentially from each RTU on a communication channel and in parallel from all communication channels.

3.3.1.21 The polling engine shall support multiple line rates. Communication rates shall be user configurable anywhere from 300 to 115,200 bits per second serially, synchronous or asynchronous, clocked or non-clocked, bit-oriented or byte-oriented operation, with the ability to change the parity of the serial communication link on the fly, as needed. Any limitations on the speed of data acquisition shall be solely contingent upon the bandwidth of the communication channel and the communication equipment. TCP/IP rates shall be supported up to the maximum rate available on the LAN.

3.3.1.22 The communication system shall support multiple protocols during a single connection.

3.3.1.23 The communications facility shall provide the capability to move remotes from one circuit and communication platform to another on-line without
requiring a SCADA software recompilation.

3.3.1.24 The system shall be capable of acquiring data sequentially from each RTU on a communication channel and in parallel from all communication channels.

3.3.1.25 The SCADA system shall support the capability to add additional communication facilities as part of normal system growth.

3.3.2 Protocols

3.3.2.1 The SCADA system shall have the capability to communicate using the MODBUS-TCP/IP protocol. The protocol shall account for analog, digital status, and accumulator points, and shall support control of remote devices.

3.3.2.2 The SCADA system can optionally support other protocols for field device communications the details of which are described in their respective ADDs.

3.3.3 OPC Client Protocol

3.3.3.1 The polling engine shall be capable of communicating with an OPC server to receive telemetry information. The OPC client protocol shall fully support the Data Access 2.0 OPC Interface.

3.3.4 Physical Termination / Connection

3.3.4.1 The SCADA system shall have the capability to accept telemetry data over the following types of terminations / connections:
   a) RS-232
   b) RS-423
   c) Leased Line
   d) Dial-up
   e) VSAT
   f) Microwave
   g) TCP/IP – LAN, MAN, & WAN technologies, including:
      • ATM
      • Frame Relay
      • X.25
      • Fractional T1 & T3 Circuits
      • SONET
      • FDDI
   h) Radio Communications - 1/2 and full duplex using:
      • 802.11 wireless LAN (for Station SCADA telecommunications)
• GPRS Cellular Data communication
• 2-meter & 70-cm FM-radio telemetry for collection fields and storage facilities
• Microwave Spread-Spectrum

3.3.5 Managing Connections

3.3.5.1 The distributed SCADA system shall allow for the following configuration for any connection:
   a) It shall be possible to restrict connection for particular remote devices to one system exclusively in the entire SCADA installation.
   b) Alternatively, it shall be possible to transfer control of a particular remote device between systems in the entire SCADA installation.
   c) It shall also be possible to configure connections to belong to multiple systems.

3.3.5.2 There shall not be a limit on the number of connections configurable for, or assignable to, any single remote device.

3.3.5.3 A “circuit” shall be defined as a configurable grouping of connections. The polling engine within the SCADA system shall not execute more than a single command at any time over any single circuit. This shall allow for reliable testing of alternate connections to a given remote, even if that remote contains a single port.

3.3.5.4 Each connection definition shall accommodate, where needed, or optionally, an associated cost factor. Upon a connection failure, the polling engine shall switch over to the connection with the highest-speed-lowest cost rating. This cost factor shall be configurable without a recompilation of the SCADA system software.

3.3.5.5 In order to ensure maximum performance of the polling engine during peak loads, communications lines’ testing routines shall not be part of the polling engine. Rather, Telvent shall provide external utilities to control the timing and logic of communications lines’ testing.

3.3.5.6 In order to ensure maximum performance of the polling engine during peak loads, fail-over, and fail-back logic shall not be part of the polling engine. Rather, Telvent shall provide utilities to accommodate fail-over and fail-back logic.

3.3.5.7 Additionally, it shall be possible for DBNGP to modify these utilities, or to write external utilities to determine the logic of how and when to perform fail-over or fail-back operations.

3.3.5.8 The polling engine shall be configurable to access a remote device through redundant terminal servers, and in the event of a failure of the hot terminal server, the polling engine shall start using a designated
connection on the alternate terminal server.

### 3.3.6 Modes of Communication

**3.3.6.1** The SCADA system shall have the ability to communicate using any of the following modes of communication:

- **a)** Polled Circuit – solicited data acquisition with command issuing capabilities.
- **b)** Listen only – data acquisition only, acquired information is by remote device end initiation only.
- **c)** Listen with commands – listen only plus the capability to issue commands and/or acknowledgments.
- **d)** Dial-out – SCADA system initiated dialing out on the first available modem to an RTU modem.
- **e)** Dial-in – RTU initiated (also known as Cry-out) an RTU modem dials into the SCADA system unsolicited.

### 3.3.7 Supervisory Control

**3.3.7.1** The system shall provide a consistent mechanism to schedule communications on all circuits.

**3.3.7.2** It shall be possible for the supervisory control commands to be issued automatically by a system application, or manually by the user.

**3.3.7.3** Real-Time Services shall require controller-initiated or user-initiated supervisory control to follow a two-step sequence:

- **a)** The controller shall select the point to be controlled, and then
- **b)** Shall complete the sequence within a user adjustable time-out period with the desired control action.

**3.3.7.4** If the controller does not complete the select-check-operate control sequence within the time-out period, the selection shall automatically be canceled. This approach shall minimize the chances of controllers inadvertently issuing incorrect commands.

**3.3.7.5** Control commands issued to a remote shall take priority over all other communication.

**3.3.7.6** The control output shall be issued at the earliest opportunity. The maximum delay before issuing a command shall be no longer than the time for the longest message returned from a remote on the line.

**3.3.7.7** The system shall support the capability for application programs to issue control outputs.

### 3.3.8 Control functions
3.3.8.1 It shall be possible to configure a minimum scan cycle for a remote device.

3.3.8.2 A "discrete" control represents a given point's current state, (i.e. open or closed, on or off, etc.). Discrete controls shall include on/off, or start/stop commands. The SCADA system shall check all discrete controls for conditions requisite with successful control of the device.

3.3.8.3 Following the execution of the control command, the system shall expect a change in the status of the device to an appropriate state.

3.3.8.4 If the system does not detect a change within a time-out period, an alarm shall be annunciated and an event shall be logged in the historical database.

3.3.8.5 The time-out period shall be user configurable on a point-by-point basis. Status change alarming shall be inhibited for points to which controls are being issued for a user-defined duration.

3.3.8.6 The SCADA system shall support three separate types of control operations:
   a) blind control
   b) two-state control, and
   c) three & four-state control

3.3.8.7 In blind control operation, there is no telemetry based discrete point in the field associated with the point receiving the blind control. Blind control operation shall be complete with the sending of the control. Blind control shall not require a corresponding discrete point change-of-state message in reply.

3.3.8.8 In a two-state control operation, successful execution of the issued command shall require confirmation through monitoring the change of the device through a separate telemetry point. A successful two-state control operation shall require the discrete point to change to the commanded state.

3.3.8.9 The SCADA system shall support individual timeout values for each state change for each control point.

3.3.8.10 The SCADA system shall support different control point addresses for “trip” or “open” and for “close” operations.

3.3.8.11 The SCADA system shall interpret events that occur because of control operations and shall correctly report all changes of state.

3.3.8.12 Three- and four-state control operation shall be similar to the two-state control, except that the associated status point shall change state from one stable state (open or closed) to the transit or traveling state, and finally to the opposite stable state (closed or open, respectively).
3.3.8.13 Setpoint controls shall issue analog setpoint values to the RTU/PLCs. The controller shall select a point for setpoint control, and then be prompted for the control value.

3.3.8.14 Entry of the control value shall be in engineering units. The Real-Time Service shall provide the appropriate conversions for the RTU/PLC selected.

3.3.8.15 Prior to issuing the setpoint control, the SCADA system shall check the value entered against the acceptable limits for the device. If the value is outside acceptable limits, the SCADA system shall alert the controller.

3.3.8.16 Subsequent to the issuance of the control request, the system shall expect positive feedback that the setpoint has changed at the field device. If the SCADA system does not detect this change within a time-out period, an alarm shall be annunciated to indicate a failed control. The time-out period shall be user configurable on a point-by-point basis.

3.3.8.17 It shall be possible for control sequences to be triggered off:
   a) user commands
   b) particular time of day
   c) change of state of any status point
   d) change of value of any analog point
   e) “external” application software
   f) specified calculations
   g) specified time intervals

3.3.9 Control Point Tagging

3.3.9.1 Tagging shall inhibit supervisory control, or automatic control of remote field devices.

3.3.9.2 This tagging functionality shall accommodate up to eight tags per control database point.

3.3.9.3 The system shall record the author of the tag and shall allow the inclusion of comments with each tag.

3.3.9.4 Tagged points shall not accept control commands from any controller station, or control algorithm.

3.3.9.5 Any attempt to issue a control to a tagged point shall result in the generation of an alarm message, alerting the controller to the attempted issuance of a prohibited control.

3.3.9.6 Each tag shall support at least six types of tag indicators:
a) Warning Tag – the controller cannot issue any commands directly, but can optionally override the warning. Application programs shall not be able to issue tags.

b) No Program Commands Tag – the controller can issue commands, but an application program cannot.

c) No Controller Commands Tag – An application program can issue commands, but the controller cannot.

d) No Open Commands Tag – Neither the controller nor an application program can issue “open” commands, but both can issue “close” commands.

e) No Close Commands Tag – Neither the controller nor an application program can issue “close” commands, but both can issue “open” commands.

f) No Commands Tag – Neither the controller nor an application program can issue commands.

3.3.10 Communication Scheduling

3.3.10.1 Scheduling (Round Robin) – The system shall provide polling with the round robin scheduling format. This means that the scanning of remote units shall take place in a previously defined order returning to the first device upon completion of a full cycle.

3.3.10.2 Upon not receiving a reply from a remote device, the system shall attempt a user configurable number of poll retries before declaring a time-out and continuing with the next device.

3.3.10.3 It shall be possible to fast scan, meaning scan a particular RTU at a faster rate than under normal conditions, using two methods:

a) Manual - User initiated fast scan (or interrogation) of an RTU.

b) Command (automated) - Software initiated fast scan (or interrogation) of an RTU.

3.3.10.4 Fast scanning shall cause the particular RTU to receive a scan every other poll cycle for a given polling process.

3.3.10.5 The system shall support multiple protocols in the following two ways:

a) On circuits - It shall be possible to have two circuits each using a different protocol.

b) Shared circuits - It shall be possible to have one circuit using more than one protocol (polling RTUs with different protocols).

3.3.10.6 It shall be possible to configure a minimum scan cycle for any remote device.

3.3.10.7 Commands shall take priority over normal polling functions and shall
interrupt a given poll cycle to ensure immediate processing of the command to the target device in the field.

3.3.11 Data Processing

3.3.11.1 The SCADA system shall be able to acquire and process three types of numeric data from the RTUs:
   a) analog points
   b) digital status points
   c) accumulator points.

3.3.11.2 The SCADA system shall provide flexible raw data to engineering unit conversion. Conversion to engineering units shall be carried out in such a manner that errors of conversion are no more than +/- one least significant bit weight of the data field.

3.3.11.3 The system shall provide for manipulation of non-telemetered database points to allow for the manual entry of data not directly accessible from the field by the user. There shall be no differentiation between telemetered and non-telemetered points for purposes of logging, calculations, and reporting.

3.3.11.4 It shall be possible for the historical system, trending, applications, and data manipulation procedures to access the data stored in non-telemetered database points.

3.3.12 Analog Data Processing

3.3.12.1 The system shall provide for processing of field analog points and shall update the analog quantities displayed at all controller interfaces.

3.3.12.2 Engineering units conversion - All analog point raw values shall be converted into an engineering units format via a linear transformation of the form $EU = A \times (\text{raw data}) + B$, where the scale “$A$” and the offset “$B$” are applied as soon as the data is received by the system. The scale “$A$” and offset “$B$” shall be configurable for each analog point.

3.3.12.3 Alarm checking - The system shall support the processing of each analog point against four types of configurable limits as follows. Alarm limits shall incorporate a configurable dead-band for each point. The deadband prevents repeated alarm-normal cycles when the value is close to the alarm limit.
   a) high-high – extreme high value usually of high importance
   b) high – high value usually of medium importance
   c) low – low value usually of medium importance
   d) low-low – extreme low value usually of high importance
3.3.12.4 Alarm severity - Each analog point shall be associated with one of three alarm severity levels (Low, Medium and High). These severity levels shall indicate to the user the importance of any alarms generated by the corresponding point.

3.3.12.5 Rate-of-change alarming - The system shall support rate-of-change alarming where the limits shall be configurable in engineering units per time unit change for each point.

3.3.12.6 Instrument Fail alarming - The system shall support instrument fail alarming where the RTU/PLC and the associated protocol support the same.

3.3.12.7 Creep Detection alarming - The system shall support creep detection alarming where an analog device deviates by a specified amount from a given value over any duration.

3.3.12.8 Averaging - It shall be possible to retrieve current and previous averages for hour, day, and month by accessing the appropriate fields in the real-time databases.

3.3.13 Digital Status Input Processing

3.3.13.1 The system shall provide processing for digital status points and shall update the digital status quantities displayed at all controller interfaces.

3.3.13.2 States - The system shall allow digital status inputs to be single bit (two states) or two bit (four states) status points.

3.3.13.3 Alarm severity - Each digital status point shall be associated with one of three alarm severity levels (Low, Medium and High). These severity levels shall indicate to the user the importance of any alarms generated by the corresponding point.

3.3.13.4 Messaging – The text corresponding to each state shall be configurable by the user on a point-by-point basis.

3.3.14 Accumulator (or Rate) Point Processing

3.3.14.1 The system shall provide for processing of accumulator points and shall update the accumulator point quantities displayed at all controller interfaces.

3.3.14.2 Engineering unit conversion - The system shall provide for the conversion of all accumulator point raw values into an engineering unit format by subtracting the previous value from the new value and multiplying the result by a unit of measure. If the result is negative, a meter rollover calculation shall take place.

3.3.14.3 Alarm checking - The system shall support the processing of each rate (present accumulator value minus previous accumulator value divided by
time change) against four types of configurable limits being high-high, high, low and low-low. Alarm limits shall incorporate a configurable dead-band on a point-by-point basis in the same way as for analog points.

3.3.14.4 Alarm severity - Each accumulator point shall be associated with one of three alarm severity levels (Low, Medium and High). These severity levels shall indicate to the user the importance of any alarms generated by the corresponding point.

3.3.14.5 Rate-of-change alarming - The system shall support rate-of-change alarming where the limits shall be configurable in engineering units per time unit change on a point-by-point basis. An alarm is generated if the rate exceeds the set limit.

3.3.14.6 Averaging - It shall be possible to retrieve current and previous averages for hour, day and, month by accessing appropriate fields in the real-time database.

3.3.14.7 Accumulator resets - The system shall be able to accommodate accumulator resets at any time.

3.3.15 Data Quality

3.3.15.1 Anywhere a telemetered or derived value is maintained in the realtime or historical databases, the point’s data quality shall be stored with the stored value. Indicators shall be stored to represent at a minimum:

a) Normal  
b) Off line - stale data  
c) Manual override  
d) Off scan - removed from polling sequence  
e) Alarm condition - point is in alarm state  
f) Point is inhibited from alarm

3.3.15.2 Data acquisition processing shall provide for data quality flags associated with each numeric and discrete point, both telemetered and calculated. These data quality flags include:

a) Stale - If a database point does not receive an update from the field within the defined scan or calculation period, or if a point fails an exception or integrity scan, the current value in the database for the point shall be marked as stale. When a valid data value is again available, the stale indication shall disappear.

b) Alarm Inhibited - If a point is marked as alarm inhibited, any change in state or value shall not result in the generation of an alarm.

c) Deactivated - Deactivation of a point shall ensure that the system blocks supervisory control, ceases scanning for telemetry updates, and marks as suspect any calculations using values from the deactivated point.
d) Manual Override – If a point is in manual override, the system shall indicate this regardless of alarm level

3.4 DATA MANIPULATION AND CALCULATED VALUES

3.4.1 General

3.4.1.1 The SCADA system shall provide a utility, called Automatic Calculation Engine (ACE), which allows for the creation of procedures, which can access and manipulate the real-time database(s) without the further intervention of the user.

3.4.1.2 This utility shall use a high level computer language for the calculations.

3.4.2 Procedure Properties

3.4.2.1 The procedures provided shall be versatile, meaning that it shall be possible to pass arguments to them. This shall allow procedures to be reusable in more than one place.

3.4.2.2 All procedures shall be able to access any value in the real-time database(s).

3.4.2.3 All procedures shall have the ability to write to any available field in the real-time database(s).

3.4.2.4 The following data processing constructs shall be supported:
   a) Basic mathematical operators (+, -, *, /, ^, and integer modulus).
   b) Logical operators (AND, NOT, OR, and XOR).
   c) Comparison operators (=, <, <=, >=, <>).
   d) Mathematical functions (abs, atn, cos, exp, log, sin, sqr, tan, rnod)
   e) Conversion functions:
      • between DECIMAL, BINARY, OCTAL, and HEX
      • any number to integer, double precision or string
      • floating point number to integer (truncated at the decimal point)
      • string to single precision
   f) File handling statements (open-for-as, read, write, close).
   g) Miscellaneous statements:
      • if-then-else-endif, for-to-next, while, wend
      • goto, gosub
      • sleep
      • print
      • let, declare, clear
3.4.3 Procedure Execution Triggers

3.4.3.1 The provided utility shall trigger a data manipulation procedure on any of the following criteria:
   a) Trigger point changes value or digital state
   b) Trigger point changes alarm state
   c) Controller Request
   d) System startup or failover
   e) Calculated database point is accessed for read
   f) Continuous execution
   g) Time scheduled (absolute or interval)

3.5 EVENT LOGGING / HISTORY

General

3.5.1.1 The SCADA system shall log all events.

3.5.1.2 This shall include, but not be limited to, all alarms, controls, manual changes and acknowledgments.

3.5.1.3 No events shall be lost due to internal buffer overflow, equipment failure, device failure or failover to redundant equipment.

3.5.1.4 Each event shall identify when and where (what subsystem, operator or workstation) the event took place on.

3.5.1.5 Control actions shall indicate the name of the controller who issued them.

3.5.1.6 It shall be possible to inhibit event logging for particular events.

3.5.1.7 The system shall have the ability to store event logs in a database (allowing for SQL access), spool to an event printer, as well as export to a file format.

3.6 ALARM DETECTION / RECORDING

General

3.6.1.1 The system shall provide alarm detection. This shall be contingent upon a constant monitoring of real-time database values.

3.6.1.2 In particular, the SCADA system shall monitor limit breaches, return-to-normals, loss of communications (to system devices as well as field equipment) and equipment failures.
3.6.1.3 Only active alarms shall appear in an alarm summary. The non-active alarms shall be stored in the historical database.

3.6.1.4 Alarms shall be recorded as events that include date and time, description, comment, database point id, remote device id, alarm category and field value.

3.6.1.5 Alarm acknowledgments shall be recorded as events that include the original alarm information as well as the Controller’s name and the name of the workstation where the acknowledgement took place.

3.7 FAILURE PROTECTION

3.7.1 General

3.7.1.1 In the event that a critical device fails or is not reachable, the data acquisition processes shall transfer to the standby as seamlessly as possible.

3.7.1.2 If the other system is in a failed state, a failover shall not take place.

3.7.1.3 Every system shall always know the state of the other systems.

3.7.1.4 A system in a standby state shall always be ready to go to a hot state.

3.7.1.5 The failure protection mechanism shall account for:
   a) No single point of failure shall cause a general system failure
   b) Self monitoring for all equipment
   c) Critical task monitoring
   d) Declaration of failure by standby
   e) Minimal failover time
   f) Seamless transfer for Controllers (i.e. no requirement to log off and log back on after a server failover)
   g) No latching T-switch gear
   h) Alarm and event logs for failures
   i) System manager failover demand switch.

3.7.2 Communication between hosts

3.7.2.1 The hot/standby configuration for the Real-Time Services shall facilitate host failure protection through constant communication.

3.7.2.2 When the state of a Real-Time host changes, the “hot” system shall log the change in the tabular Events Summary and generate an alarm message.

3.7.2.3 The Real-Time hosts in the SCADA system shall exchange the following information:
a) Pulse Broadcast - All Real-Time hosts in the SCADA system shall broadcast their state on the SCADA LAN

b) Automatic real-time database updates - Automatic updates shall take place for data that are relatively static such as the name of a record

c) Demand real-time database updates - Demand updates (immediate) shall take place for significant non-repeatable events (such as an alarm summary record)

d) Periodic real-time database updates - Periodic updates shall take place for data that will change often (such as an analog value).

3.8 TOOLS REAL-TIME ACCESS

3.8.1 General

3.8.1.1 The system shall provide Real-time access tools as follows:

3.8.2 Software Protocol Analyzer

3.8.2.1 The system shall provide a utility to monitor communications on each communication line including outgoing queries and incoming responses.

3.8.2.2 The utility shall be flexible enough that filter search criteria can selectively display messages.

3.8.2.3 There shall be an option to send gathered data to a file for future analysis.

3.8.2.4 Database Lister / Loader – a utility to dump and load database contents from file format

3.8.2.5 The system shall provide a utility to list the real-time database(s) properly in formatted ASCII files.

3.8.2.6 The system shall provide a utility to load the database points in ASCII file format into the real-time database(s).

3.8.3 Database Field Lister

3.8.3.1 The system shall provide a utility to list database-record field-names corresponding to the real-time database(s). This shall be considered a data-dictionary class of utility.
4. **HISTORICAL DATA ARCHIVING SUBSYSTEM**

4.1 **INTRODUCTION**

4.1.1 **General**

4.1.1.1 Historical data plays an important part in analyzing and optimizing the use of plant/system resources, and also an increasing role as a corporate decision support tool, and in dealings with regulatory agencies. To support this, the SCADA system shall provide extensive historical data storage and retrieval capabilities.

4.1.1.2 History shall derive from real-time, calculated, controller-entered, and RTU files.

4.1.1.3 History shall be readily accessible to SCADA controllers connected to the SCADA LAN. It shall also be possible for selected historical data to propagate to a wide range of casual users from an information server using ANSI SQL compliant query and reporting packages.

4.1.1.4 The SCADA information server shall connect to the SCADA LAN but shall isolate the casual users from the SCADA system.

4.1.1.5 The Historical Services shall provide for the long-term storage of Real-Time measurement, event, alarming and other pertinent data monitored or generated by the SCADA system.

4.2 **DATABASE FORMAT**

4.2.1 **General**

4.2.1.1 Instantaneous data shall be available to be transferred and saved from the real-time database to the Historical Data Subsystem.

4.2.1.2 It shall be possible to summarize instantaneous data to generate hourly, daily, monthly and yearly values.

4.2.1.3 The summarized values shall reside in the Historical Data Subsystem.

4.2.1.4 The historical database shall be based on a mature, commercially available, off the shelf (unmodified) relational database management system (RDBMS).

4.2.1.5 The historical RDBMS shall provide facilities for importing data from, and exporting data to, other RDBMS systems.

4.2.1.6 The historical RDBMS shall support the following minimum features:

a) Report editing/generation capabilities

b) Forms editing/generation capabilities
c) Data integrity checking, transaction recovery capabilities

d) The historical RDBMS shall support a complete implementation of the SQL Interface language. The historical RDBMS shall use an ANSI compliant implementation of SQL.

e) The historical RDBMS shall support network access to the database from other clients on the network.

f) The historical RDBMS depends on client/server architecture and supports multiple servers, which each operate independently from one another leveraging clustering technologies.

g) The historical RDBMS shall support mirroring/shadowing of the on-line database to a backup storage device.

h) The historical RDBMS shall be ODBC compliant.

4.2.1.7 The SCADA system shall have live access to the historical data for use in reports and on displays.

4.2.1.8 The historical database size shall only be limited by the physical capacity of the storage media available.

4.2.1.9 There shall be no license limitations impeding future expansion of the system. DBNGP shall be able to purchase additional licenses when required to expand the system.

4.2.1.10 The RDBMS shall support the storage of data in more than one physical device partition. This shall allow the possibility of distributing data across more than one partition/device to reduce the likelihood of data loss caused by device failures.

4.2.2 Historical Data Replication

4.2.2.1 Distributed sites shall receive historical data via replication between sites.

4.2.2.2 The system shall also allow for export of data from Historical Services using OLEDB and ODBC into the enterprise.

4.2.3 On-line Historical Data

4.2.3.1 On-line historical data shall be accessible to controllers for reports, queries, analysis, display, and trending.

4.2.3.2 It shall be possible to save the following data types as on-line historical data:
   a) status point values
   b) analog point values
   c) rate point accumulator values or rate point flow-rate values
   d) hourly and daily volumes
e) alarms
f) events
g) messages
h) communication statistics for host to field devices

4.2.3.3 Historical data shall be collectable on a periodic basis with a minimum resolution of one minute.

4.2.3.4 It shall be possible to configure historical data collection to occur by exception when a value changes by more than a user-defined dead-band amount.

4.2.3.5 Data stored by exception shall be recorded at least once per hour whether it has changed or not.

4.2.3.6 All data, whether acquired or calculated by the system, shall be eligible for historical data storage.

4.2.3.7 The following attributes shall be configurable on a point-by-point basis:
   a) Enable collection for trending
   b) Trending collection interval (configurable between 1 minute to 1 hour or on an exception basis)
   c) Enable trend averaging (for smooth transitions between points on the trend)
   d) Type of collection for long term storage (sample period or by exception)
   e) Long term storage collection interval (configurable between 1 minute and 1 hour)
   f) Exception dead-band (if collection by exception is chosen)
   g) Enable summary processing (summarizing data into hourly, daily, monthly and yearly averages, with minima and maxima)

4.2.3.8 Sufficient information shall be stored in the historical database to enable the retrieval of the data value with its associated point ID, the time tag, and any data quality attributes attached to the value.

4.2.3.9 Telemetered data which is missing for some reason (such as telemetry failure) then subsequently available shall be stored with the correct time-tag (for field devices, which support time tagging). Any summary calculations which have run shall update with this new information.

4.2.3.10 Historical data storage shall be provided for the following intervals:
   a) instantaneous
   b) top of hour and hourly minimums, maximums, averages
   c) top of day and daily minimums, maximums, averages
d) top of month and monthly minimums, maximums, averages  
e) top of year and yearly minimums, maximums, averages

4.2.3.11 Historical data storage shall be according to the following capacity schedule:
   a) 180 Days of Instantaneous Collect Data  
   b) 180 Days of Hourly Data  
   c) 180 Days of Daily Data  
   d) 120 Months of Monthly Data  
   e) 10 Years of Yearly Data

4.2.4 Archiving/De-archiving Historical Data

4.2.4.1 The SCADA system shall have a mechanism for automatically archiving historical data, onto offline storage media, that has aged beyond a user-configurable period. This data is no longer required to be kept on-line in the historical database.

4.2.4.2 The data shall archive to a Write Once, Read Many (WORM), or similar optical storage device, after which the system administrator shall easily purge (or automate the purging) of all archived on-line historical data to make room for new data.

4.2.4.3 The Historical Data Subsystem shall allow for different on-line and off-line archiving of data. For example, the system shall allow for events to be kept on-line for a different period than the communications statistics.

4.2.4.4 The archiving function shall ensure that the correct media is loaded in the archive WORM drive prior to transferring any data.

4.2.4.5 If the correct media is not present, an alarm shall be generated requesting controller intervention.

4.2.4.6 No data shall transfer until the correct media is available.

4.2.4.7 All archive media shall have a software label that the system shall validate before data archiving can begin.

4.2.4.8 When insufficient space remains on the archive media for further data storage, an alarm shall annunciate prompting the controller to insert new media.

4.2.4.9 No data shall be lost in case there is a problem with the archiving function.

4.2.4.10 Deletion of on-line historical data shall not occur until the data has been successfully stored on the archive media.

4.2.4.11 A utility shall exist to initialize a new archive media for writing.
4.2.4.12 The initialization process shall perform any media formatting required and write a unique label on the media.

4.2.4.13 The label shall be used by the archive and de-archive systems to determine if the correct volume is present.

4.2.4.14 The historical archiving system shall keep a catalog of the data that has been archived in conjunction to the media that the data is stored in. This catalog shall be used by the system to locate the appropriate archive media when de-archiving into the system.

4.2.4.15 The SCADA system shall generate an alarm when historical RBDMS tables are nearing capacity. The alarm shall serve to indicate a requirement for additional fine-tuning of the frequency of data archiving and purging or addition of historical disks.

4.2.4.16 The Historical system shall support selectable archived data output formats.

4.2.4.17 The SCADA system shall generate an alarm when the long-term archive storage device is nearing capacity, and continue to generate the alarm, until additional storage becomes available.

4.2.4.18 The SCADA system shall support the on-line access to historical/archived historical data.

4.2.4.19 It shall be possible to recover off-line archived data.

4.2.4.20 The system shall provide an interactive utility to access archived information.

4.2.4.21 The user shall specify a database name, table name, and start and end times for the recovery process.

4.2.4.22 Once the data has been de-archived, all of the report and query facilities available for the on-line historical data shall be available for the de-archived data.

4.2.4.23 An on-line catalog shall maintain a listing of the archives that exist.

4.2.4.24 When de-archiving, the system shall prompt for the correct archive media based on the media label.

4.2.4.25 Multiple media de-archiving shall take place by prompting for each archive medium, as it is required.

4.2.4.26 A “clean-up” utility shall be available to remove de-archived data from the system.

4.2.4.27 The “clean-up” utility shall be executed manually after the user completes any queries or reports that make use of the de-archived data.
4.2.5 Editing Historical Data

4.2.5.1 Occasionally, it may be necessary to edit certain historical data in order to correct errors or omissions caused by upset conditions. The system shall provide a facility to edit this data.

4.2.5.2 It shall be possible for appropriately authorized personnel to edit the on-line historical database and manually overwrite questionable or missing data.

4.2.5.3 The system shall provide a means of adding or changing the following historical information:
   a) Field communication statistics,
   b) Real-time values, and
   c) Accumulator values.

4.2.5.4 If a record is edited, the system shall automatically ensure that the changed data is archived, even if the original data was already archived.

4.2.5.5 De-archiving shall always restore the most recently changed data.

4.3 FAILURE PROTECTION

4.3.1 General

4.3.1.1 A hardware mirroring option shall be utilized to mirror all historical databases onto on-line disks available to the SCADA system.

4.3.1.2 All historical databases on disks shall be mirrored, so that a failure of a disk shall not cause a failure of a particular historical database.

4.3.1.3 When a disk fails, the mirrored disk shall have the same copy of data as the master disk. This disk shall make available to the system the historical data for the failed disk.

4.3.1.4 Once the failed disk is replaced, the system shall automatically copy the information from the mirror disk back onto the new disk.

4.3.1.5 In the event that a critical device fails or is not reachable, the historical processes shall transfer to the standby as seamlessly as possible.

4.3.1.6 If the other historical system is in a failed state, a failover shall not take place.

4.3.1.7 The primary historical system shall always know the state of the other system.

4.3.1.8 A historical system in a standby state shall always be ready to go to a hot state.
4.3.1.9 The failure protection mechanism shall account for:

a) No single point of failure shall cause a general system failure
b) Self monitoring for all equipment
c) Critical task monitoring
d) Declaration of failure by standby
e) Minimal failover time
f) Seamless transfer for controllers (i.e. no requirement to log off and log back on after a server failover)
g) Alarm and event logs for failures
h) System manager failover demand switch
5. HUMAN MACHINE INTERFACE SUBSYSTEM

5.1 INTRODUCTION

5.1.1 General

5.1.1.1 Controller interaction with the SCADA system shall be through the Human Machine Interface (HMI) Subsystem.

5.1.1.2 The HMI shall be a full graphics windowing system capable of supporting the diverse requirements of the system.

5.1.1.3 The HMI shall present users with an intuitive, consistent and flexible Microsoft® Windows operating system based interface for all SCADA and applications information.

5.1.1.4 User interaction shall be icon and menu driven using a point and select device such as a mouse, or trackball.

5.1.1.5 Telvent shall provide a mechanism allowing controllers to select often-used functions without needing to go through a hierarchy of menus and screens.

5.1.1.6 Each application shall provide the same “look and feel” across all controller stations.

5.1.1.7 The Operator interface shall include the following:
   a) On line documentation
   b) Some context sensitive help
   c) Quick Trending capability to allow users to trend a non-historical point
   d) Support for running SCADA Controller Station under multiple Windows user accounts
   e) Meter dial and horizontal bar objects
   f) Table Summaries with query filters
   g) Alarm Summaries
   h) Column control for flashing color
   i) Event summary color by event type and alarm severity
   j) Custom sound-files for alarms
   k) Password expiry and complex password support
   l) Multiple views of the same display at the same time
   m) Standard Windows® functionality including customization of displayed time zone based on user logon.

5.1.1.8 Baseline Graphic Screen Layout
The HMI system for this project will be reusing existing custom displays that have been converted to run under OASyS DNA 7.5 for most of the station graphics. This section only describes the system displays that are “global” in nature and critical to the operation of the SCADA system.

The HMI allows the operator to navigate through each Compressor Station, issue commands and set parameters. By selecting the preferred area of operation in the system, the operator is able to view station and system communications, current condition of the station, real time & historical trends.

The operator’s desktop is a direct link into the system. From the desktop the operator will be able to control, monitor, and acquire information to do the job quickly and effectively. The default desktop layout for this project is as shown in the figure below.

A separate document details the display building convention and styles to use for the custom displays.

![Baseline Desktop Layout](image)

Figure 5-1- Baseline Desktop Layout

The Desktop is divided into the main viewing area, the Navigation Menu on the left, and at the bottom of the screen the Newest Priority Alarms window.
The Navigation Menu which helps the operator to navigate between windows is divided into 3 sections as follows:

- Tools
- System Displays
- Summaries

The various tools/displays available in the Navigation Menu are listed in the table below.

*Table 3- Navigation Menu*

<table>
<thead>
<tr>
<th>Tools</th>
<th>System Displays</th>
<th>Summaries</th>
</tr>
</thead>
<tbody>
<tr>
<td>AOR View</td>
<td>Alarms</td>
<td>Analog</td>
</tr>
<tr>
<td>AOR Control</td>
<td>Events</td>
<td>Status</td>
</tr>
<tr>
<td>Model Select</td>
<td>Tags</td>
<td>Remote</td>
</tr>
<tr>
<td>Documentation</td>
<td>Mode</td>
<td>Connection</td>
</tr>
<tr>
<td>XE</td>
<td>DistribuSYS</td>
<td></td>
</tr>
<tr>
<td>ADE</td>
<td>Global Trendset</td>
<td></td>
</tr>
<tr>
<td>Historical Edit</td>
<td>ACE</td>
<td></td>
</tr>
<tr>
<td>Archive</td>
<td>Datapump</td>
<td></td>
</tr>
<tr>
<td>Shift Change</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Print</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reporting Services</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Zoom</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ezXOS Shutdown</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Main Viewing Area**

The main viewing area occupies the larger portion of the screen. Normally this area is used in its entirety for the display of graphical and tabular overviews, however smaller windows and popups will also overlay this main window area. The popups and some other windows activated from the main window are movable, but will not initially overlay the tool bar or the status bar.

**Newest Priority Alarms Area**
The Newest Priority Alarms window located at the bottom of the desktop, lists only the unacknowledged alarms or events generated on the system, with the latest alarm shown at the top of page one. If there are multiple alarms listed, the most severe are listed first. If there are multiple alarms of the same severity level, those alarms are listed in the order received.

5.2 WINDOWING SYSTEM

5.2.1 General

5.2.1.1 A Graphical User Interface (GUI) shall exist for the SCADA system.

5.2.1.2 The GUI shall allow data presentation in a graphical environment, which shall be controllable with a pointing device like a mouse or trackball.

5.2.1.3 The GUI shall comply with Win32 standards.

5.2.1.4 The windowing system shall provide the user with the capability of viewing multiple windows on one console screen.

5.2.1.5 There shall be no configurable limit for the number of simultaneously visible windows.

5.2.1.6 The windowing system shall not hinder the use of the SCADA system in any way.

5.2.1.7 The dimensions and position of each window on a console screen shall be independently adjustable by the controller.

5.2.1.8 Support shall include provisions for managing overlapping windows.

5.2.1.9 These provisions shall also allow for static or immovable windows.

5.2.2 General Presentation and Layout

5.2.2.1 The presentation and layout of the displays of the SCADA system shall be consistent and logical.

5.2.2.2 It shall be flexible enough, however, to allow the user to modify the presentation and layout into a completely different standard.

5.2.2.3 New windows shall appear in positions where they are visible in their entirety.

5.2.2.4 Multi-Headed HMI stations shall be supported. On multi-headed stations, new windows shall appear on a specified console display.

5.2.2.5 There shall be no configurable limit for the number of simultaneously open
and visible windows.

5.2.2.6 All windows on a console display shall refresh with real-time data appropriate to the particular window on which it appears, with a configurable refresh rate no faster than once per second.

5.2.2.7 Displays are windows, which cumulatively make up the Graphical User Interface (GUI) to the SCADA system. A display shall appear in an appropriate consistent location and size when first displayed, so as not to be obstructed by any other display.

5.2.2.8 All information required for daily operation of the SCADA system shall be contained in the displays. All baseline displays shall share a generic color scheme and layout. (Customer generated displays can use this scheme or a customer specific one.)

5.2.2.9 Pop-ups are displays that shall be configurable to disappear from a console display after a period of inactivity or via an operator click on an “Ok” or “Dismiss” button for example. A pop-up shall appear in an appropriate location and size when first displayed so as not to be obstructed by any other display.

5.2.2.10 Pop-ups shall appear in intuitive locations. In general, pop-ups shall facilitate controller entry to the system. Following are examples of the functions that shall be available through pop-ups:
   a) Discrete controls
   b) Setpoint controls
   c) Communications control
   d) Setting Area of Responsibility

5.2.3 Navigation

5.2.3.1 DBNGP anticipates creating custom displays for their system. The style and design of these displays shall be described in a separate document.

5.2.3.2 A logical and practical methodology shall be required to provide rapid access to any particular display.

5.2.3.3 A hierarchical structure shall link and organize the various system displays. Screen control within the SCADA system shall allow for movement within the Human Machine Interface being as intuitive as possible. This not only shall include movement between displays, but also within displays.

5.2.3.4 Access to displays shall be through “soft” pushbuttons, or active areas on displays. The style, color and shape of an active area shall be configurable by the user.

5.2.3.5 The user shall have the capability to move and resize windows at any time. If a user calls or moves a window such that it overlaps another window, the
5.2.3.6 “Close” buttons shall be on all displays not requiring visibility greater than 90% of the time. Related displays shall have buttons allowing for toggling between the displays.

5.2.3.7 On displays configured for zooming, it shall be possible to initiate a continuous zoom into any area of the display that the user chooses.

5.2.3.8 If zooming has resulted in the removing of some of the display's graphical information from view, panning to off screen areas shall be possible.

5.2.3.9 Text information shall be “greeked” (replaced with lines) at specific zoom levels, or de-cluttered (removed entirely) at other zoom levels, to reduce overall clutter on the user interface screen.

5.2.3.10 Simple mouse clicks and movements shall control panning and zooming.

5.2.3.11 The system shall support fully functional display layers, whose visibility is under controller control.

5.2.3.12 Pop-ups spawned by other displays shall automatically dismiss upon the dismissal of the parent display.

5.2.4 Data Presentation

5.2.4.1 All displays shall be completely configurable by a manager or supervisor using a Display Editor. Configurable items include the following items:

   a) Static background information;
   b) Dynamic data (real-time or calculated); and
   c) Active areas

5.2.4.2 Static background information represents system components (such as highways, property lines, and geographical features), which are necessary for context in operations, but are not attached to database points. Additional static background information may include station names, building outlines, mileposts, pipe segments, etc. Static backgrounds shall be in browser compatible format or bitmap pictures, such as the photograph of a power station, or DXF (Drawing Exchange Format) vector files to allow the user to import standard AutoCAD® drawings.

5.2.4.3 Telvent shall provide drawing tools that allow the user to create background images in a variety of colors and shapes.

5.2.5 Dynamic Data Presentation

5.2.5.1 Presentation of dynamic data is the essential element of the SCADA system from an operational perspective. The system shall provide several methods
of displaying dynamic data as follows:

a) Numerical - Numerical data shall be viewable using integer fields, real fields, slider bars, meters, gauges and graphs. Colors of numerical data shall correspond to the Alarm State of the point to which the number corresponds.

b) Graphic Object - Graphic objects corresponding to real-time database points shall appear in the color of the Alarm State of that point. The shape and/or color of a graphic object corresponding to a real-time database point shall also correspond to the value of that point.

c) Text - Dynamic text data shall appear in fields or browser type (scrollable) text areas for larger blocks of text. Foreground and Background colors shall indicate the integrity of the value displayed.

5.2.6 Data Quality Flags

5.2.6.1 Data quality flags for any particular point shall be capable of appearing anywhere that the point’s value/status appears including tabular summary displays and schematic displays (where applicable).

5.2.6.2 If more than one data quality flag is set for any point, the data quality flag with the highest severity shall take precedence and appear. Following is a list of the applicable data quality flags:

a) Normal

b) Off line - stale data: If data does not update for a configurable duration, the abnormality shall have a visible indication to the user (e.g., stale data is in reverse video, and fresh data appears in normal video). Foreground and Background colors can interpret the integrity of the value displayed.

c) Manual override

d) Off scan - removed from scan

e) Alarm condition - point is in alarm state

f) Inhibit alarms for the given point

5.2.7 Tag Indicators

5.2.7.1 Current tag indicators for any control point assigned by the controller shall appear anywhere that the point’s control symbol or tabular information appears.

5.2.7.2 The tag shall indicate to the controller that the point is not controllable or is marked in a warning state (that still allows control) from any controller station or control algorithm.

5.3 CONTROLLER INPUT FUNCTIONS

5.3.1 General
5.3.1.1 Primary user input to the SCADA system shall be via a cursor control device (such as a mouse, keypad, or trackball). The secondary input device shall be the keyboard.

5.3.2 Data Entry

5.3.2.1 Altering data or adding new data into the SCADA system shall require a minimum of two user actions in all instances.

5.3.2.2 If the user attempts to enter data into fields not set to accept data, the system shall deny entry to the field(s) and shall warn the user.

5.3.2.3 Similarly, any attempts to enter text into numeric fields shall generate a similar denial and warning to the user.

5.3.2.4 Data input shall be via text fields, integer fields, real fields, slider bars, soft push buttons and similar GUI objects.

5.3.3 Setpoint Control

5.3.3.1 Setpoint control shall be available only to users with the appropriate Area of Responsibility (AOR) permissions to view and/or control the setpoint value for a given point.

5.3.3.2 It shall be possible to initiate this type of control from either a tabular or a schematic display.

5.3.3.3 The procedure required for setpoint control shall be as follows:
   a) On the appropriate tabular or schematic display, the user shall select the desired device to control. This shall bring up a control window displaying, on button objects, the types of controls available for that particular device, one of them being a setpoint control.
   b) The user shall be able to enter the desired setpoint value using the keyboard or the cursor control device via a slider bar followed by the SUBMIT function.
   c) The action shall be refused with an appropriate message if:
      d) The device has view authorization but not control
      e) The device is off scan
      f) Communication to the RTU has failed
      g) The device’s tagging precludes the setting of a setpoint.

5.3.3.4 The system shall allow the setpoint control action to be canceled at anytime before submitting the request by selecting the DISMISS button on the device control windows.

5.3.4 Commands

5.3.4.1 Commands shall be provided for the functionality described in Table 4.
Selection and execution of control commands shall require the controller to have the appropriate AOR and control authorization.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Put Data</td>
<td>This command inserts a specified piece of data into a specified point in the real-time database.</td>
</tr>
<tr>
<td>Control On</td>
<td>This command sends an “on” command to a device via a corresponding point in a real-time database.</td>
</tr>
<tr>
<td>Control Off</td>
<td>This command sends an “off” command to a device via a corresponding point in a real-time database.</td>
</tr>
<tr>
<td>Acknowledge</td>
<td>This command sends an alarm acknowledgment to a specified point in a real-time database.</td>
</tr>
<tr>
<td>Alarm</td>
<td>This command silences alarms for the issuing console. It does not however acknowledge alarms.</td>
</tr>
<tr>
<td>Silence</td>
<td>This command disables sound for the issuing console.</td>
</tr>
<tr>
<td>Sound Disable</td>
<td>This command disables sound for the issuing console.</td>
</tr>
<tr>
<td>Sound Enable</td>
<td>This command enables sound for the issuing console.</td>
</tr>
</tbody>
</table>

Table 4- Device and Environment Control Commands List

5.4 TRENDING

5.4.1 Trend Manipulation

5.4.1.1 It shall be possible to view up to twelve (12) different trend lines on one graph.

5.4.1.2 It shall be possible to scroll back and forth in time on the trend window using mouse drag.

5.4.1.3 It shall be possible to have the trend display dynamically update with the latest data or be frozen at a certain time. Freezing the display shall have no effect on the collection process but displays an on-screen indicator. Freezing occurs automatically when scrolling or zooming the trend.

5.4.1.4 There shall be a data cursor that indicates the exact value at the intersection of the cursor and the pen traces. The cursor shall be movable using the mouse.

5.4.1.5 It shall be possible to nudge the cursor by a single pixel using the left and right arrow keys.

5.4.1.6 It shall be possible to snap the cursor to the nearest data sample value in the pen trace.

5.4.1.7 It shall be possible to highlight a single pen trace. Doing this shall hide all other pen traces and turn on snap mode.
5.4.1.8 It shall be possible to zoom in, zoom out, and restore the display to its initial view.

   a) The mouse wheel zooms the time axis
   b) The mouse zoom box zooms the time and y axes

5.4.1.9 It shall be possible to create a new trend from an existing trend.

5.4.1.10 It shall be possible to display up to 1500 data values per trend.

5.4.2 Trend Configuration

5.4.2.1 It shall be possible to configure a trend title.

5.4.2.2 It shall be possible to define primary and secondary timescales (x-axis).

5.4.2.3 The title color, trend background color, axis color and grid color shall be user configurable and selectable from a palette of at least 256 colors.

5.4.2.4 Trend start and end times shall be enterable as absolute time (dd/mm/yyyy h:mm:ss) or relative time (+/-YY:MM:DD:hh:mm:ss)

5.4.3 Trend Traces

5.4.3.1 It shall be possible for a pen trace to use any Y and either X axis.

5.4.3.2 A pen trace shall be able to use auto scaled, user defined, or values from the database as it's Y axis limits

5.4.3.3 The pen trace shall be connected to a database point and field.

5.4.3.4 It shall be possible to modify, edit and delete X and Y axes.

5.4.3.5 It shall be possible to move a pen trace between respective X or Y axes.

5.4.4 Individual pen parameters

5.4.4.1 It shall be possible to define the following attributes of a pen trace:
    a) label
    b) data marker size (possibly none)
    c) trace style (interpolated, staircase)
    d) line color
    e) line style
    f) line thickness

5.4.4.2 Pen trace line color shall correspond to the state at the time of collection, user assigned color or system selected color.
5.4.4.3 It shall be possible to interpolate in a linear fashion, one or more values on the pen trace if data is missing.

5.4.4.4 It shall be possible to trend hourly averages, daily averages, hourly maximums, daily maximums, hourly minimums and daily minimums.

5.4.4.5 It shall be possible to add, modify and delete pen traces.

5.4.4.6 It shall be possible to define a “threshold” as a type of pen trace. A threshold is a value of interest from a static value. This value can be customized through Visual Basic scripting to become “dynamic”.

5.4.4.7 The line style and color of a threshold shall be user definable.

5.4.4.8 It shall be possible to add, modify and delete thresholds.

5.4.5 Other trending functions

5.4.5.1 It shall be possible to obtain quick trends of a point without having to define a complete trend configuration.

5.4.5.2 It shall be possible to scroll back and forth in time on a quick trend window (assuming the point is collecting history).

5.4.5.3 For points that are not collecting history, the quick trend window shall update with a new value at least every 15 seconds.

5.4.5.4 It shall be possible to store personal trends on a per user basis and global trends that are accessible to everyone.

5.5 AREA(S) OF RESPONSIBILITY

5.5.1 General

5.5.1.1 The system shall have the ability to logically group points into Areas of Responsibility (AORs), based on geographical, operational, and security requirements.

5.5.1.2 The two general categories for all AORs shall be:
   a) Viewable (no alarm acknowledgement, no control)
   b) Controllable

5.5.1.3 AORs shall be definable / configurable by the manager, or some other person with an appropriate level of responsibility as defined by role-based security considerations defined by DBNGP

5.5.1.4 A user assigned to a particular AOR shall have the ability to display system screens and data, and as an option, control devices and acknowledge alarms within that AOR.
5.5.1.5 Each point in the real-time database(s) shall belong to one group and each group belongs to one or more areas of responsibility. Which AOR(s) belong to a particular user shall be configurable.

5.5.1.6 Upon system startup, a user shall already be assigned to an AOR. This means that only that particular AOR can be monitored and controlled by that user.

5.5.1.7 Data displayed shall be controlled by the current AOR selection(s), and the console being worked at shall only receive those alarms that occur in the selected AOR(s).

5.5.1.8 At no time shall a user be able to view or control points, objects, database entries, receive or acknowledge alarms for points corresponding to AORs outside of the user’s AOR permissions.

5.6 ALARMING

5.6.1 General

5.6.1.1 Alarms shall appear and log according to the selected AOR, however acknowledging alarms shall be possible only by users with control permissions for those AORs.

5.6.1.2 Unacknowledged alarm messages shall appear in a high priority window designed to appear at each active console at all times.

5.6.1.3 All active alarms shall also appear in a tabular alarm summary.

5.6.1.4 Alarms shall also appear on appropriate schematics and tabular point summaries.

5.6.1.5 Providing access to an intelligent alarming subsystem is critical to responsive SCADA operations. The SCADA system shall offer the advanced capabilities of both Alarm Disturbance Mode and Alarm Suppression.

5.6.1.6 With Alarm Disturbance mode, it shall be possible to configure alarms so that low priority alarms are not processed. With this feature, lower priority alarms shall be suspended during peak periods of volume alarms.

5.6.1.7 To reduce nuisance alarms, the system shall support a configurable Alarm Suppression function. Hierarchical alarm suppression shall prevent large numbers of alarms from cluttering a controller’s display when they are triggered as the result of a single device going into alarm. Control Initiated suppression shall prevent controller-initiated commands from having the same outcome.

5.6.1.8 The concept of a group or station alarm shall be supported by the system. It shall be possible for each station to have devices contained within it, and when these devices are in alarm, the station to which it belongs shall be notified. A controller shall be able to access these alarms by clicking the
station on the geographic or schematic display, causing a station alarm summary to appear.

5.6.1.9 Station alarm summaries shall behave in the same manner as the system alarm summary, and shall contain a severity and time-ordered list of all the alarm messages for all the devices within that station.

5.6.1.10 Real-Time Services shall generate alarms and events from telemetered and calculated point data, as well as from application programs within the alarming subsystem. These alarm records shall be maintained online for a user-specified period of time, then archived offline.

5.6.1.11 It shall be possible to configure systems so that specific alarms or events automatically trigger or activate programmed actions in response.

5.6.2 Alarm Severity

5.6.2.1 The severity of generated alarms shall be configurable for all alarm generating points or devices.

5.6.2.2 Severity of an alarm message shall be configurable to be one of three levels of severity (high, medium or low).

5.6.2.3 Alarm severity shall be distinguishable by a configurable color scheme, audible signal and relative placement in the tabular alarms displays.

5.6.3 Alarm Annunciation

5.6.3.1 Audible Alarms shall be configurable to issue a beep pattern or play a "wav" file.

5.6.3.2 Inhibiting alarm annunciation shall be possible for each operational console.

5.6.3.3 Inhibiting alarming shall inhibit only the currently annunciating alarms.

5.6.3.4 Any alarms arriving at the console subsequent to inhibiting annunciation shall not be subject to the prior action, but shall announce to indicate the arrival of a new alarm.

5.6.4 Alarm States

5.6.4.1 The number of alarm states for a particular point or device shall vary depending on the nature of the data processing. If the data is numerical (e.g. a value or a rate), the point or device shall appear in one of eight alarm states:

a) High-high
b) High
c) Normal
d) Low

e) Low-low

f) Rate-of-change

g) Creep detection

h) Instrument fail.

5.6.5 Alarm Message

5.6.5.1 The alarm message shall appear in the alarm window and in the tabular summary of alarms.

5.6.5.2 The alarm message shall include the time and date of the alarm, the point that caused the alarm, the severity of the alarm (via color and audible signal) and the state of the point.

5.6.6 Alarm Logging

5.6.6.1 Alarms shall appear in a detailed log of events.

5.6.6.2 The alarm message shall include where, when and who acknowledged the alarm.

5.6.6.3 The system shall provide separate log entries for the alarm and its acknowledgement.

5.6.7 Alarm Acknowledging

5.6.7.1 Alarms shall be acknowledgeable by use of the cursor control device via the appropriate selection of an active area in the Alarms window, the tabular alarm summary or the control window for the appropriate point.

5.6.7.2 Alarms shall also be acknowledgeable via a PAGE ACKNOWLEDGE button on the tabular alarm summary.

5.6.7.3 Only alarms in view on the displayed page shall be acknowledgeable.

5.6.7.4 Acknowledging an alarm shall also silence the audible alarm if any.

5.6.7.5 Alarm acknowledgment shall be limited to users with appropriate AOR logged onto consoles also with appropriate AOR.

5.6.7.6 It shall not be possible for the system to automatically acknowledge alarms.

5.6.7.7 Alarm Acknowledgement shall be done in two ways:

   a) The row head button of an alarm summary shall be pressed by a controller with sufficient authority.
b) All alarms listed on the system alarm summary, or any of the station
alarm summaries, can be acknowledged one page at a time (authority
level permitting).

5.6.8 Alarm Interaction

5.6.8.1 If more than one alarm is unacknowledged at any one time, the cancelled
audible signal shall be the one associated with the most severe of the
alarms.

5.6.8.2 The alarms shall appear in the alarm list chronologically by default, from
the newest to the oldest, sorted by their severity.

5.6.9 Alarm Inhibiting

5.6.9.1 It shall be possible to inhibit alarms for any point configured to generate
alarms.

5.6.9.2 In the case of points with the high-high, high, normal, low and low-low
alarm states, it shall be possible to inhibit any of the high-high, high, low,
low-low alarms or all alarms.

5.6.9.3 The user shall also be able to inhibit rate of change and creep alarms.

5.6.10 Silencing of Audible Alarms

5.6.10.1 Selecting a Silence Alarms button in the Alarms window shall perform
silencing the audible alarm.

5.6.10.2 Newly arriving alarms shall override any silencing in effect at the time.

5.6.11 Alarm Limits

5.6.11.1 Alarm limits shall be configurable for all alarms generated from checking
numeric fields.

5.6.12 Standard Displays

5.6.12.1 The SCADA system shall have all of the following baseline displays:
   a) Primary display - A display always present on the controller interface
      screen(s)
   b) Summary tables for all telemetered tables (filterable by data quality
      flag). These shall convey data, data quality and alarm status. Control
      popups for the database points shall be accessible from these tabular
      summaries. Only database points contained in selected view authorized
      AORs shall appear and be accessible.
   c) Tabular summaries of communication lines, modems, tags, and events
d) Tabular filterable alarm summary - This display shall list alarms filtered by acknowledgment. The list of alarms shall be in order of severity and occurrence time (newest alarm first within groupings by severity).

e) An alarms window - A primary display listing unacknowledged alarms

f) A status window - A schematic display accessible from one of the primary displays showing all major system components and communication links.

g) Trend control and trend graph displays - Windows from which trend parameters such as trending point names can be selected from a list of available points.

h) A systems key toolbar - A primary display, from which navigation is possible within the SCADA system including accessing the various summaries, trends and notes displays

i) A notes display - This shall be a display where any user can enter free form text. The user shall be able to configure access to any notes records based on whatever logical associations are desired (i.e. station name, user, console, etc). Any addition or change to any area in the notes display shall be accessible from any console on which the controller interface of the SCADA system is running.

5.7 PRINTING

5.7.1 General

5.7.1.1 Printing of reports, screens, summaries, and displays shall be on printing equipment defined under this heading.

5.7.1.2 The controller shall be able to choose which printer on which to execute a print job.

5.7.1.3 The printers included as part of this SCADA system include:

   a) One (1) new color laser printer in the operations center
   b) No dot matrix printer in the operations center.
   c) Reuse existing laser printer in the backup center
   d) No dot matrix printer in the backup center.

5.7.2 Displays and Screens

5.7.2.1 The system shall provide an easy method of printing the SCADA system displays and screens.

5.7.2.2 This shall include displays or entire screens visible on any operator’s console.

5.7.2.3 It shall be possible to print in either black and white or color.
5.7.2.4 It shall be possible to capture anything visible on the screen and paste it into an email or document using standard Windows shortcut keys.

5.7.3 Reports

5.7.3.1 A report shall be selectable from a predefined report selection list.

5.7.3.2 Scheduling and periodic automatic generation of reports shall also be available.

5.7.3.3 The user shall be able to select a report printer from a list presented in a popup window.
6. SECURITY

6.1 INTRODUCTION

6.1.1 General

6.1.1.1 Information security is about mitigating risk. DBNGP has in place a comprehensive set of security policies and procedures to mitigate the risks we face in our industry to levels acceptable to DBNGP senior management.

6.2 SECURITY MANAGEMENT PRACTICES

6.2.1 AIC - The Three Pillars of Information Security

6.2.1.1 All security risk mitigation activities and technologies provided shall address the three pillars of information security:

a) Availability
b) Integrity
c) Confidentiality

6.2.2 General Standards

6.2.2.1 The Common Criteria for Information Technology Security Evaluation (CCITSE), known internationally as the Common Criteria (CC) as well as ISO 15408, is an internationally endorsed, independently tested, and stringent set of standards that evaluate the security of information technology products.

6.2.2.2 Telvent shall provide a system capable of passing the CC to the level of at least EAL3 (Evaluation Assurance Level 3 methodically tested and checked) or EAL4 (methodically designed, tested, and reviewed) preferred out of the spectrum of assurance levels defined under the Common Criteria from EAL1 (functionally tested security) to EAL7 (formally verified design and tested).

6.3 ACCESS CONTROL

6.3.1 General

6.3.1.1 Access control mechanisms shall consist of a combination of discretionary access control (DAC) and role based access control (RBAC).

6.3.2 Password Management

6.3.2.1 The systems on which the SCADA system operates shall be capable of supporting password management procedures, including:

a) Minimum Length
b) Complexity Requirements
c) Password Expiration  
d) Variable Clipping Levels  
e) Password usage tracking  
f) Password Auditing

6.3.3 Access to the Operating System

6.3.3.1 Access control at the operating system level shall be discretionary (DAC).

6.3.3.2 Access to all operating system components shall be determined on an individual user basis in accordance with permissions assigned to the user.

6.3.3.3 For operating system components, only users belonging to the group “security manager” shall have the ability to modify operating system level parameters, add or remove devices, add or remove user logins, or view files and/or directories in their native state.

6.3.3.4 Where the Common Criteria (CC) is concerned, and at DBNGP option, the Operating System shall be capable of enforcing Mandatory Access Control (MAC) features such as those required for (CC) Controlled Access Protection (CAP). This shall bring the Evaluation Assurance Level for the Operating System to EAL4.

6.3.4 Access to the SCADA system

6.3.4.1 Access to the SCADA system shall be non-discretionary and role based (RBAC).

6.3.4.2 Areas of Responsibility (AOR) shall map against User Accounts which have permissions associated with each Group to which the user belongs.

6.3.4.3 These groups shall correspond to the roles in place for DBNGP user base of enterprise and SCADA information.

6.3.4.4 Key hosts in the SCADA network shall be classifiable as “Sensitive Data Protection Devices” or “Software Signature Creation Devices” should such measures ever be required.

6.3.4.5 Access to SCADA data shall be granular enough to support row-level access control measures based on the RBAC mechanisms in the operating system. This means that only those rows of data defined as matching the access control matrix for a given user shall ever return in a query given to the historical databases.

6.3.4.6 There shall be the concept of a shift change for logoff and logon during shift changes. This allows you, at the start of your shift, to log on to the system without having the previous operator log off first by using the Shift Change function.

The log off of the current user and the log on of the new user are performed at
the same time. If the user logging on has a different authorization level than that of the user being logged off, the old display set will be closed and a new set opened. When this occurs, there will be a delay of about 15 seconds during which the console will be inactive. No commands can be issued from the console during this period. When the user logging on has the same authorization level as that of the user being logged off, the displays do not change.

6.3.5 Access to High Responsibility Controls

6.3.5.1 Within the SCADA software proper privilege levels shall dictate what objects a user can view or control.

6.3.5.2 The manager shall specify the privilege level of a particular user.

6.3.5.3 Each privilege level shall be configurable (by the manager). At least four privilege levels shall accompany the SCADA system upon delivery including:
   a) Viewer - Can only view
   b) Controller - Can view and control assigned areas
   c) Supervisor - Can view and control any area. Can initiate manual system failover
   d) Manager - Can view and control any area, initiate manual system failover, access database and display editors, and assign/change privileges

6.3.6 Automatic Logout

6.3.6.1 Inactivity at the user's HMI Workstation shall cause the Operating System to log-off the current user.

6.3.6.2 The time-out period shall be configurable by the system manager/administrator.

6.3.7 Single-Sign-On (SSO)

6.3.7.1 Telvent shall provide a system capable of supporting SSO using Kerberos Authentication to access all applications relevant to the services and applications (third-party, or Telvent produced) supported by the middleware data bus. User Areas of Responsibility and privileges shall only require configuration once.

6.3.7.2 Users shall not have to type in a username and password for each application running as part of the system.

6.3.8 Two-Factor (or Three-Factor) “Strong” Authentication

6.3.8.1 Telvent shall supply “out of the box” strong authentication at the user level.

6.3.8.2 Given the three authentication mechanisms available (something you know, something you have, and something you are), the SSO solution shall
also be able to support two-factor or three-factor authentication.

### 6.3.9 Remote Access

6.3.9.1 Telvent shall provide a VPN solution that complies with the RADIUS (IEEE 802.1x) standard for remote access while requiring an IPSec tunneling solution coupled with strong authentication mechanisms.

6.3.9.2 The remote access hardware security solution shall not degrade performance of the SCADA network.

6.3.9.3 Alternatively, Telvent shall ensure that all remote access terminals to DBNGP corporate network(s) comply with DBNGP VPN solution for access to the SCADA network.

6.3.9.4 It shall be possible to accomplish all functions remotely exactly as if local access was used. Access restriction shall be through user logon privilege.

### 6.4 PHYSICAL SECURITY

6.4.1 General

6.4.1.1 DBNGP shall ensure that all monitors, keyboards, hosts, networking cabinets, telecommunication racks, and server racks are physically secure, using appropriate locks and cables.

### 6.5 NETWORKING SECURITY

6.5.1 General

6.5.1.1 Telvent shall work with DBNGP to ensure that a proper Firewall infrastructure is in place to ensure the Trusted SCADA computing base remains secure using throttling capable routers with remotely managed access control lists (ACLs) and routing tables using standard routing protocols such as OSPF and HSRP. Firewalls shall be provided by DBNGP.

6.5.1.2 A Demilitarized Zone (DMZ) shall be a required component of this firewall infrastructure.
7. SYSTEM SOFTWARE

7.1 INTRODUCTION

7.1.1 General

7.1.1.1 Telvent shall provide a proven multi-tasking, multi-user operating system with a large installed base. For this project we are providing Microsoft® Windows operating system on all SCADA computers.

7.1.1.2 Telvent shall provide pass-through hardware support from the original equipment manufacturers for all SCADA system components that fall under the scope of this specification.

7.1.1.3 The operating system shall additionally be Common Criteria (CC) certified at Evaluation Assurance Level EAL4 without any modifications to the operating system.

7.2 COMPUTER SYSTEMS SOFTWARE

7.2.1 General

7.2.1.1 All computers shall utilize the same basic system software.

7.2.1.2 In addition, the system software shall not preclude the addition of other computers to the SCADA systems, which use different but compatible software packages.

7.2.1.3 The operating system software used shall have the following features:
   a) Multi-user and multi-tasking
   b) Support process scheduling
   c) Support process prioritizing
   d) Support batch processing
   e) Support inter-processor communications
   f) Support shared/virtual memory management
   g) Support device mirroring
   h) Provide performance/trouble-shooting/analysis tools
   i) Provide code management facilities
   j) Support standards compliant compilers and debugger for software development and maintenance
   k) Provide access control mechanisms to prevent unauthorized users from accessing system/SCADA functions through use of a Security Reference Monitor through which all system resource requests shall be arbitrated
and evaluated based on non-discretionary Access Control rules applied to the operating system

l) Support multi-headed workstations

m) Support for message routing to network devices of all types.

7.2.1.4 The operating system shall provide access to all the various types of network devices used in the system. Access to network resources shall likewise require arbitration by the Security Reference Monitor (SRM) in the operating system.
8. ENTERPRISE INFORMATION TECHNOLOGY INTEGRATION

8.1 DIRECTORY SERVICES

8.1.1 Domain Name Services (DNS)

8.1.1.1 The SCADA installation shall be capable of plugging seamlessly into the existing enterprise DNS server(s).

8.1.2 Dynamic Host Configuration Protocol (DHCP)

8.1.2.1 The SCADA installation shall consist of (an) independent virtual LAN(s). Network IP address assignments shall be through DHCP.

8.1.3 Lightweight Directory Access Protocol (LDAP)

8.1.3.1 The SCADA installation shall have the ability to authenticate users, as well as the ability to administer user and object permission structures from a single location using LDAP. LDAP shall provide the mechanisms necessary for central definition, deletion, and modification of user accounts.

8.1.3.2 This centrality of administration shall include the possibility, at DBNGP option, of central administration using DBNGP corporate IT infrastructure using LDAP, and this central administration shall allow DBNGP system administrators to assign SCADA permissions to corporate domain users as necessary.

8.1.4 DBNGP Corporate Security Policies & Procedures

8.1.4.1 The SCADA installation shall comply with all DBNGP corporate security policies and procedures.

8.1.4.2 This compliance shall include attention to DBNGP models for data Integrity, Confidentiality, and Availability, including provisions for continued operation during crisis scenarios defined under DBNGP Business Continuity and Disaster Recovery Plans (BCP & DRP).
9. SYSTEM APPLICATIONS

9.1 INTRODUCTION

9.1.1 General

9.1.1.1 In addition to basic monitoring and control functions, the system shall provide specialized applications, offering additional operations support capability.

9.1.1.2 These applications shall provide controllers tools and means of rapid analysis of the data collected by the SCADA system to aid in decision-making.

9.1.1.3 The following section outlines the applications that are deliverable by Telvent as an integral part of the SCADA system:

9.2 APPLICATIONS

9.2.1 MODBUS TCP/IP Protocol

9.2.1.1 The protocol shall be based on master-slave relationship with OASyS DNA acting as the master.

9.2.1.2 The protocol shall support up to 247 slaves on a single communication line using address 1 to 247.

9.2.1.3 The protocol shall allow multiple blocks of contiguous RTU register ranges to be configured for polling from each RTU.

9.2.1.4 The protocol shall allow the frequency with which each block of contiguous RTU registers is polled to be specified.

9.2.1.5 The protocols shall support the following data types: short word (16 bits), long word (32 bits), or float (IEEE).

9.2.1.6 The protocol shall support the polling of data from the RTU / PLC.

9.2.1.7 The protocol shall support digital commands.

9.2.1.8 The protocol shall support setpoint commands.

9.2.1.9 The protocol shall filter noise between query and response.

9.2.1.10 The protocol shall send multiple messages whenever the host must poll more registers than the maximum holding register size allows.

9.2.1.11 The supplied software protocol analyzer (SWANA) can be used to verify the data packet sent to the remote.
9.2.1.12 The protocol shall provide an interface for the configuration of the parameters.

9.2.1.13 The protocol shall allow for sending time synch commands to the RTU to enable time synchronization. This time shall be UTC based.
10. SYSTEM MANAGEMENT TOOLS

10.1 INTRODUCTION

10.1.1 General

10.1.1.1 DBNGP shall have the ability to modify the SCADA system to reflect technical and operational changes in the SCADA system.

10.1.1.2 System management tools shall allow the user to effectively maintain and manage the SCADA system and applications.

10.1.1.3 Utilities for on-line interactive, off-line interactive and off-line batch modifications shall be integrated components of the system.

10.1.1.4 These utilities shall allow the user to add, modify or delete:
   a) Database points
   b) Communication parameters
   c) Displays
   d) Reports
   e) Equipment

10.1.1.5 Altering these elements shall not require either a shutdown of the system, or editing of source code.

10.1.1.6 The following sections shall define the functionality of the management tools that shall be included with the SCADA system:

10.2 DATABASE EDITOR

10.2.1 General

10.2.1.1 Telvent shall provide a Database Editor utility capable of easily configuring and editing the SCADA system’s real-time database(s).

10.2.1.2 The Database Editor utility’s accessibility from a machine in the system shall be configurable.

10.2.1.3 The Database Editor shall have the capability to add, remove or edit all real-time database points. This shall include inputs, outputs and points that act as RTUs, communication channels and other industry specific telemetry, manual entry, or calculated database points.

10.2.1.4 Any telemetry point shall be configurable to run small programs that are also programmable within the Database Editor.

10.2.1.5 The system shall allow assignment of points to the historical trending component(s) of the system through this Database Editor.
10.2.1.6 The Database Editor shall be considered the central administration tool for all SCADA database configurations.

10.2.1.7 The system through this Database Editor shall support on-line additions, deletions and modifications of database information.

10.2.1.8 The database editor shall allow bulk editing of points.

10.2.1.9 The database editor shall allow search and replace functionality.

10.2.1.10 The database editor shall be able to run standalone as a Windows® application.

10.2.1.11 The database editor shall allow exporting and importing data values from Excel™.

10.3 DISPLAY EDITOR

10.3.1 General

10.3.1.1 The SCADA system Display Editor shall use a sophisticated Graphical User Interface, using industry standard VB.NET scripting, with industry standard CAD software drawing and editing capabilities.

10.3.1.2 The Display Editor shall support both vector and bit-mapped display development.

10.3.1.3 The Display Editor shall be installed only on select machines. The Display Editor shall not be accessible from the controller workstations even by an administrator.

10.3.1.4 The Display Editor shall have access to all display files and shall provide the capability to edit any display in the SCADA system.

10.3.1.5 Changing a display or adding a new format shall not affect the current displays in use by the SCADA system.

10.3.1.6 Modifications to displays shall become active only after distribution to the workstations by the system manager or system administrator.

10.3.1.7 Individual display modifications shall not require the shutdown, or reboot of the controller consoles, and shall not interfere with the live operations of the SCADA system.

10.3.1.8 The system shall allow import of existing facility drawings and GIS maps and diagrams, in DXF format, as the basis for HMI drawings.

10.3.1.9 It shall be possible to make a display larger than what can be displayed on one physical monitor. In a multi-monitor environment this will cause the display to be visible across several monitors.
10.3.2 Dynamic Data

10.3.2.1 The Display Editor shall have the capability to include any real-time database point or historical database point for display.

10.3.2.2 The real-time and historical (relational) database(s)’ querying languages shall possess the capability to filter query results for display.

10.3.2.3 For data values extracted from the real-time or historical database(s), data quality indicator characters shall (optionally) be available to appear.

10.3.2.4 Data points from the real-time database(s) shall include annotations corresponding to that point’s current alarm status.

10.3.2.5 It shall be possible to display any numerical data as an integer, real, slider bar, meter, gauge, or graph on any HMI display.

10.3.2.6 This data representation shall be movable and transferable between any HMI displays.

10.3.2.7 It shall be possible to place multiple data representations on any display (e.g., two trend graphs and four meters). This shall only be limited by the HMI format size.

10.3.2.8 It shall be possible to annotate graphic objects. For example, it shall be possible to cause a graphic of a valve to change color dynamically to reflect the corresponding point’s current alarm level.

10.3.2.9 It shall be possible to increase the size of a graphic to correspond dynamically with a value in the real-time database.

10.3.2.10 It shall be possible to rotate a graphic dynamically to correspond with a value in the real-time database.

10.3.2.11 The Display Editor shall consist of a comprehensive Symbol Library of graphics symbols for OIL and GAS pipeline operational needs. They shall be IEEE or ISA standard when possible.

10.3.2.12 The Symbol Library shall define representations of real world objects such as pumps, valves, etc.

10.3.2.13 Placement of the graphic symbol on a display shall automatically invoke a pop-up menu prompting the user for the linkage of the dynamic display to a real-time or historical database field.

10.3.3 Calculated Points

10.3.3.1 It shall be possible to configure a dynamic field capable of displaying the result of a mathematical equation, with inputs taken from the real-time database(s).
10.3.3.2 This field shall appear to be an “integer” or “real/float” field from the user’s perspective.

10.3.4 Soft Push Buttons

10.3.4.1 It shall be possible to place any number of soft push buttons on any HMI display, limited only by format size of the display, and ergonomic considerations for the controllers.

10.3.4.2 These buttons shall be able to be configured to call up other displays, dismiss the current display, call up a URL, and call up online help.

10.4 NETWORK MANAGEMENT, DIAGNOSTIC AND MONITORING UTILITIES

10.4.1 General

10.4.1.1 The system shall provide a monitoring utility which dynamically shows the raw CPU usage percentages used by the processes that take up the largest portion of the CPU power on each of the workstations.

10.4.1.2 The monitoring utility shall also provide dynamic information regarding memory load, page file swaps and disk spindle accesses.

10.4.1.3 The monitoring utility shall monitor disk space utilization on all critical hosts in the system, and generate alarms based on user-defined thresholds for disk space utilization.

10.4.2 DIAGNOSTICS

The SCADA system shall provide the following diagnostic tools to monitor the healthiness of various components.

10.4.2.1 The Network Management Console (NMC)

The NMC is a member of the OASyS DNA suite of products. The NMC is a monitoring tool that allows users to view their system’s configuration properties and monitor the state of their SCADA system. OASyS DNA provides multiple continuously updating logs, which provides valuable system information. The Log Viewer utility is an effective tool for monitoring and reviewing OASyS DNA log files.

10.4.2.2 NMC Log Viewer

The OASyS DNA NMC log viewer continuously provides valuable system information. For instance, information related to the failure of a system component.

The NMC provides the interface, which allows the administrator to monitor machine, service, and process states by drilling down and observing icons. It also displays the results reported by automated monitors such as process monitors and Windows Management Instrumentation (WMI) monitors such
as the disk and virtual memory monitors.

Monitoring is divided as follows:

- System, service, machine, and process states
- Process monitoring (i.e. the process monitor service)
- WMI monitors under Common: Disk, Virtual Memory, NIC

Each monitor is a component or snap-in with the NMC. Monitors primarily use PubSub(Publish & Subscribe) to communicate the state of individual OASyS DNA components. Most monitors are event driven and will update as a service changes. PubSub refers to a centralized information-processing system in which material fed into the system from a variety of sources (that's the "publish" part) is sorted, matched, reformatted, and sent along to "subscribers" according to their particular interests.

10.4.2.3 Process Monitoring

For each service on a given machine within OASyS, the process monitor monitors process health. Within each service, a single instance of the process monitor, monitors processes associated with that service.

Using the NMC, the SCADA administrator will be able to view the status of each process.

The process monitor is composed of two major elements:

- The actual process monitor process that runs on the server and performs the actual monitoring of the processes.
- The NMC snap-in that supplies the user interface for the process monitor.

The communication between the NMC snap-in and the process monitor is facilitated through a PubSub process.

When the process monitor publishes a failure status for a given process (or alternatively an OK status), it publishes messages to the NMC process monitor snap-in and the arbitration health server. The arbitration health server is then expected to take any arbitration actions required.

10.4.2.4 WMI Monitoring

Windows Management Instrumentation (WMI) is a new management technology allowing scripts to monitor and control managed resources throughout the network. Resources include hard drives, file systems, operating system settings, processes, services, shares, registry settings, networking components, event logs, users, and groups. Virtual memory and Network Adaptors are specific cases of WMI monitors in this case. ConfigWMIIMonitor tool is provided to create additional monitors, by the system administrator.
When the disk monitor publishes a failure status for a given disk (or alternatively an OK status), it publishes a message to both the NMC disk monitor snap-in and the arbitration health server.

10.4.2.5 Virtual Memory Monitor

The NMC uses the virtual memory monitor on each machine to monitor virtual memory space. Each machine will be configured for:

- a warning condition and
- a failure condition

To ensure that its configuration is consistent, the virtual memory monitor stores process properties within the local machine registry. When virtual memory monitor service starts, it reads this configuration from the registry and publishes this information via PubSub.

When the virtual memory monitor publishes a failure status (or alternatively an OK status), it publishes a message to both the NMC virtual memory monitor snap-in and the arbitration health server. The arbitration health server takes any arbitration actions required.

10.4.2.6 Health State

Health state is a high-level indicator that monitors several key components of a given service. Each service has a Health State indicator icon - if not in a good state, further investigation can be done using the error logs.
11. SYSTEM REQUIREMENTS

11.1 PERFORMANCE REQUIREMENTS

11.1.1 General

System performance is critical to the overall usefulness of the system. Poor performance diminishes overall user confidence in the system and the data it provides. System performance shall weigh heavily in the design of the system. This section shall define specific performance requirements for the SCADA system.

11.1.2 System Loading

11.1.2.1 System loading is defined as the activity levels on the SCADA servers, and the local and wide area networks as measured by the system and network performance monitoring tools.

11.1.2.2 Performance levels shall be measured under a heavy loading condition. Heavy loading is the loading level expected during serious pipeline upset conditions. This scenario is viewed as a transient condition simulating an upset condition under which a large amount of activity occurs for a period of time before pipeline operations stabilize.

11.1.2.3 Under this condition, scanning shall proceed while many change-of-states and alarm conditions are returned from a large number of remote terminal units. A high level of Pipeline System Controller activity at the HMI shall be assumed.

11.1.2.4 The Heavy loading test shall be conducted over any ten (10) minute period.

11.1.2.5 The field data shall be simulated for the maximum expanded initial system.

11.1.2.6 The simulated data shall be evenly distributed over the system’s communication lines.

11.1.2.7 Simulators may be used to artificially simulate the required loading scenarios.

11.1.3 Heavy Loading Scenario

11.1.3.1 Using a continuous polling technique, the system shall poll all data on all communication lines while experiencing the following number of changes for the duration of the test:

a) Five (5) discrete input point changes per second

b) One hundred (100) analog input, tank level input, accumulator input point changes per second

c) Three (3) alarm conditions detected per second (rotating among the above data types).
d) Fifteen (15) discrete control outputs and fifteen (15) analog control outputs issued from the HMI every five (5) minutes.

e) All Workstations on-line with ten (10) new graphics and two (2) new trends requested by each controller console every minute.

f) All printers on-line and two (2) new reports and two (2) CRT hardcopies requested every five (5) minutes.

g) All other system functions (i.e., computer links, historical data processing, applications, etc.) on-line and functioning properly.

11.1.3.2 The average Real-Time server CPU utilization (averaged over a five minute period) shall not exceed sixty percent (60%).

11.1.3.3 Under the Heavy loading conditions, the Historical Database server throughput shall be as follows:

a) 100 real time data point values being collected to the historical database per hour with each data point being collected an average of 60 times per hour.

b) 1000 event messages recorded in the database per hour. This includes 800 alarms and 200 miscellaneous messages associated with controller control actions and alarm acknowledgments.

c) 20 queries for 100 historical data points from the Historical database during the course of an hour. These queries shall return data in under 40 seconds, excluding any delay introduced by the casual user LAN.

11.1.4 Screen Response Times

11.1.4.1 The Pipeline System controllers shall be able to display real-time SCADA Displays (150 dynamic data fields or less with no historical data) in ten (10) seconds or less.

11.1.4.2 SCADA formats with 300 dynamic data fields and no historical data shall display in less than ten (10) seconds.

11.1.4.3 Standard four pen trends (50 data points per pen), using data from the real-time table, shall display in fifteen (15) seconds or less.

11.1.4.4 Standard four pen trends (50 data points per pen), using data from the summary tables, shall display in thirty (30) seconds or less.

11.1.4.5 Once a format is displayed, the refresh rate of real time data shall be configurable on a per console basis.

11.1.4.6 Historical data shall be updated at configurable intervals, in one-minute increments.

11.1.5 Data Acquisition Times

11.1.5.1 Under heavy loading conditions, field changes shall appear on the CRT
displays within five (5) seconds of changing at the remote terminal. Note: this assumes that a three (3) second single-circuit physical communication time is achieved and the display is on continuous refresh.

11.1.5.2 Telvent shall be responsible for ensuring that field data changes are reflected at the controller consoles no more than five (5) seconds after the field data has been received at the communication line terminal server. This shall be measured by comparing the data point’s timestamp (which indicates when the data was received by the host) with the time that the data is displayed on the controller console if possible.

11.1.6 Control Output Times

11.1.6.1 Under normal loading conditions, the maximum time to begin to transmit a control (discrete or analog) after completion of the initiation sequence shall be one-half (1/2) second (assuming no wait for a current scan to complete). This requirement shall apply to both Pipeline System controller initiated commands and Automatic Control Sequence initiated commands.

11.1.6.2 If a scan is in progress when a control is initiated, the control shall be sent immediately after completion of the in-progress scan.

11.1.7 Database Update Times

11.1.7.1 Updates of critical values, such as points in alarm or user changes to the database, shall propagate to the standby server within five (5) seconds of changing on the hot server.

11.1.7.2 Integrity updates of non-critical values, such as analog points that are not in alarm and are being scanned during the regular polling process shall propagate to the standby server within two (2) minutes of changing on the hot server.

11.1.7.3 Historical data shall be maintained on a set of mirrored disks that are shared by the redundant historical servers. Thus there shall be no explicit data updates between the historical servers.

11.1.7.4 The real time data replicated from the real time servers to a decision support server shall be updated within two (2) minutes of changing on the real time server.

11.1.8 Failover Times

11.1.8.1 The real-time and historical servers have an associated warm standby computer available. This configuration shall allow for a minimum of time between detection of a server failure and the ability to be operational on the standby computer. Real time and historical servers shall be discussed separately below.

11.1.8.2 Under heavy loading conditions, failures on the real time server, other than an actual network "break" (which requires the TCP/IP network time-out of
11.1.8.3 Under heavy loading conditions, the time for the HMI consoles to connect to the newly established "hot" computer is 30 seconds or less.

11.1.8.4 The time for historical server failure detection shall be less than 300 seconds.

11.1.9 System Start-up Times

11.1.9.1 A cold start occurs when the SCADA system computers are started from the powered off state. The start up time for the various components of the SCADA system is as follows:
   a) Operating System startup time (including self diagnostics) shall be less than 10 minutes
   b) Real time startup time shall be less than 5 minutes after the Operating System is up.
   c) Historical startup time shall be less than 2 minutes after real time has started.
   d) HMI startup time shall be less than 2 minutes after the Operating System has started.

11.1.9.2 A “warm start“ shall be starting the SCADA servers when the operating system is operational. The times for warm starts shall be the same as the times to start individual components as described in the previous sections.

11.1.9.3 Whenever the real time servers are in the process of starting up and no real time server is available, any HMI station that is running shall display dynamic field data in a grayed out format to indicate that actual real time data is not yet available.

11.1.10 Controller Workstation Performance

11.1.10.1 The system shall respond to controller-entered commands within 500 milliseconds. In the event the time required to process the controller-entered command exceeds 500 milliseconds, a visual indication shall appear to the controller to indicate that the command has arrived at the system and is processing.

11.1.10.2 For dynamic displays, new values shall appear on the screen within 2 seconds of arrival from the field device. A screen refresh shall take place once a minute in any event, whether or not new field data has arrived.

11.1.10.3 The date and time shall appear on all controller screens and shall update once a second.

11.1.10.4 Displays requested by the controller for the first time shall appear complete with static and dynamic data within an average of 2 seconds after
the request. In general, displays shall appear in under 5 seconds.

11.1.10.5 All alarms shall annunciate to the controller within 1 second after the raw data has arrived from the remote telemetry equipment. The alarm message shall be spooled to the event/alarm printer within 5 seconds of the raw data arrival from the remote telemetry equipment.

11.2 DATABASE SIZING

11.2.1 General

11.2.1.1 The SCADA system shall support the following initial number of points plus 50% expansion without requiring any additional hardware or software:

<table>
<thead>
<tr>
<th>Description</th>
<th>Initial Number</th>
<th>Ultimate Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>almsum</td>
<td>59</td>
<td>100</td>
</tr>
<tr>
<td>analog</td>
<td>9169</td>
<td>15000</td>
</tr>
<tr>
<td>collect</td>
<td>9038</td>
<td>15000</td>
</tr>
<tr>
<td>commline</td>
<td>65</td>
<td>100</td>
</tr>
<tr>
<td>conitel</td>
<td>127</td>
<td>200</td>
</tr>
<tr>
<td>device</td>
<td>80</td>
<td>150</td>
</tr>
<tr>
<td>flow_total</td>
<td>15</td>
<td>50</td>
</tr>
<tr>
<td>gasquality</td>
<td>23</td>
<td>50</td>
</tr>
<tr>
<td>group</td>
<td>17</td>
<td>50</td>
</tr>
<tr>
<td>jsh</td>
<td>228</td>
<td>500</td>
</tr>
<tr>
<td>modbus</td>
<td>146</td>
<td>250</td>
</tr>
<tr>
<td>process</td>
<td>85</td>
<td>250</td>
</tr>
<tr>
<td>rate</td>
<td>1396</td>
<td>2000</td>
</tr>
<tr>
<td>remote</td>
<td>273</td>
<td>500</td>
</tr>
<tr>
<td>spooler</td>
<td>5</td>
<td>50</td>
</tr>
<tr>
<td>status</td>
<td>11776</td>
<td>20000</td>
</tr>
<tr>
<td>syslogins</td>
<td>34</td>
<td>100</td>
</tr>
<tr>
<td>sysusers</td>
<td>79</td>
<td>200</td>
</tr>
<tr>
<td>tag</td>
<td>33</td>
<td>500</td>
</tr>
<tr>
<td>terminal_server</td>
<td>4</td>
<td>50</td>
</tr>
<tr>
<td>trend</td>
<td>9030</td>
<td>15000</td>
</tr>
<tr>
<td>xistrendset</td>
<td>55</td>
<td>200</td>
</tr>
<tr>
<td>xoscontrol</td>
<td>98</td>
<td>200</td>
</tr>
<tr>
<td>xosdisplay</td>
<td>37</td>
<td>500</td>
</tr>
<tr>
<td>xoslogins</td>
<td>56</td>
<td>100</td>
</tr>
</tbody>
</table>

Table 5- Realtime Database Sizing

11.2.1.2 The SCADA system shall be able to accommodate the Ultimate Number without degradation of performance through the addition of memory, disk and additional processor. No recompilation of the software shall be required.
11.3 HISTORICAL DATABASE SIZING

11.3.1 General

11.3.1.1 The historical database shall have adequate on-line storage (disk) capacity to store all of the initial inputs plus 50% expansion for the following periods:

<table>
<thead>
<tr>
<th>Sample Frequency</th>
<th>On Line Storage Period</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minutely Scanned Data</td>
<td>365 days</td>
</tr>
<tr>
<td>Event Log</td>
<td>365 days</td>
</tr>
<tr>
<td>Communications Statistics</td>
<td>365 days</td>
</tr>
<tr>
<td>Hourly Data</td>
<td>365 days</td>
</tr>
<tr>
<td>Daily Data</td>
<td>365 days</td>
</tr>
<tr>
<td>Monthly Data</td>
<td>10 years</td>
</tr>
<tr>
<td>Yearly Data</td>
<td>10 years</td>
</tr>
</tbody>
</table>

Table 6- Historical database sizing

11.3.1.2 The system shall be capable of supporting the above storage periods for the Ultimate Number count with the simple addition of disk and memory without any recompilation of software.

11.4 EQUIPMENT REQUIREMENTS

11.4.1 General

11.4.1.1 An equipment delivery list is provided separated from this Functional Design Specification document.

11.5 SYSTEM FAILURE AND RESTART

11.5.1 General

11.5.1.1 The startup of the system from a failed state shall be as per Section 11.1.9. The system shall be considered started when it responds to controller requests (i.e., displays may be requested and are output to the controller's workstation at the required response time and scanning of field data has started.

11.5.1.2 On a restart, the system shall synchronize its operation with the “hot” computer system. Data on “standby” system(s) shall automatically synchronize with that on the “hot” system. The completion of the data synchronization and the “standby” status of the backup system shall be alarmed to the controller. There shall be a visual indication to the
controller of which processor is “hot” and which processor is in “standby” mode. Synchronization of data between the “hot” system and the “standby” system shall not require more than 10 minutes to complete regardless of system loading.

11.5.1.3 The SCADA system shall have a mechanism for detecting if two master computers have both initialized in a “hot” mode. The SCADA system shall then arbitrate which master computer shall remain as “hot”, and which shall stand down to a “standby” mode.

11.5.1.4 The main servers shall be configured to automatically restart on a power or system failure without human intervention.

11.6 SYSTEM AVAILABILITY

11.6.1 General

11.6.1.1 The SCADA redundancy model shall be self-monitoring with critical functions and devices under constant evaluation as to their availability. This is a key requirement for system robustness and for ease of support and administration. Automated monitors shall check all critical components for failures, and take the least disruptive course of action to recover from any disruption or failure. In all cases, component failure and recovery shall not compromise system integrity.

11.6.1.2 The SCADA system software, hardware, and associated equipment shall meet design specifications capable of providing 99.99% system availability. Telvent shall implement equipment and software service redundancy capable of providing automatic failover to redundant equipment. Software services ensuring protection from any single point of failure, which would cause a general system failure, shall also be implemented. System availability shall be defined as the ratio of system ‘mean time between failures’ to ‘mean time between failures’ plus the ‘mean time to repair’.

\[
\text{Availability} = \frac{\text{MTBF}}{\text{MTBF} + \text{MTTR}}
\]

11.6.1.3 Verification of system availability shall be during a stable benchmark period of system use.

11.7 SYSTEM EXPANSION

11.7.1 General

11.7.1.1 The SCADA system shall be sized for present and future projected requirements. The system shall be scalable beyond the projections made at the time of the award of this contract, without major structural modifications to the core SCADA system.

11.7.1.2 The system shall provide a logical growth path to allow for future
expansion of the area controlled/monitored by the SCADA system.

11.7.1.3 Under no circumstances shall the future expansion of the field area controlled by the SCADA system require the complete replacement of the SCADA system software in order to satisfy the future growth requirements.

11.7.1.4 The computer system chassis and power supplies shall provide for future additions/capacity expansion. The system initial sizing shall take into account future projected growth.
12. SYSTEM HARDWARE

12.1 INTRODUCTION

12.1.1 General

12.1.1.1 The system hardware in large measure shall define the functionality and usefulness of the software. Current technology allows for increased fault tolerance by isolating functions to self-sustaining devices. Distributed Systems shall be defined as those types of SCADA systems consisting of numerous separate devices performing specific functions, which collectively form a fully functional system. Failures of devices within a distributed system shall not cause the entire system to fail. Distributed systems shall allow more flexibility in the choice of devices.

12.1.1.2 It shall be possible to integrate new devices seamlessly into a functioning system, to add new functionality, or to increase capacity. In general, distributed systems shall provide greater reliability, increased functionality, and greater flexibility than has previously been possible with centralized, proprietary SCADA solutions. Therefore, the new SCADA system shall conform to this concept and philosophy of a distributed system.

12.1.1.3 The hardware requirements specified in this section represent the minimum set of requirements for the SCADA system hardware. Telvent shall supply whatever additional items it deems necessary to satisfy the functional requirements of this document and to provide a fully functional system.

12.1.1.4 All workstations and computers ordered for the SCADA system shall preferably be from HP when possible, and are of new manufacture.

12.1.1.5 It is preferred that all workstations and computers shall be of the same generation/product line.

12.1.1.6 Equipment and firmware shall be of the manufacturer's latest revision levels.

12.1.1.7 Computer systems supplied shall all be identical in configuration and be capable of providing backup to the functions of any other similarly functioning computer in the SCADA system.

12.1.1.8 All hardware, when practical shall be purchased in Canada and later shipped to Australia, transferring the warranty at that time to DBNGP.

12.2 CONTROLLER WORKSTATIONS

12.2.1 General

12.2.1.1 The requirements of this subsection shall apply equally to all the controller workstations used in the SCADA system.
12.2.1.2 The system processors shall have the following minimum features:
   a) Intel Core 2 Duo processor architecture
   b) Running at a minimum 2.4GHz clock rate
   c) Internal word length of a minimum of 32 bits
   d) An internal bus throughput of at least 150 MB per second
   e) Equipped with an internal IDE-connected hard drive with minimum 73GB capacity
   f) Able to support NT file system (NTFS)

12.2.2 Main Memory

12.2.2.1 The requirements of this subsection shall apply equally to all the controller workstations used in the SCADA system.

12.2.2.2 The system memory shall have the following minimum features:
   a) Standard memory technology consisting of semi-conductor memory which must be directly accessible by the CPU
   b) Have a minimum word length of 32 bits
   c) Equipped with a minimum of 2GB Random Access Memory
   d) Support multi-bit error detection and single bit error correction
   e) Expandable with simple plug compatible memory modules
   f) Minimum memory requirements shall be contained on the processor motherboard without the requirement for an expansion box.

12.2.3 Keyboard

12.2.3.1 The controller workstation keyboards shall have the following minimum features:
   a) A 94 key low profile ergonomically designed unit
   b) Four button cursor controls (left, right, up, down)
   c) Country/language specific or QWERTY type keyboard
   d) 10 key numeric keypad
   e) USB or Smart-Card-like strong authentication device Port

12.2.4 Cursor Control Device

12.2.4.1 All controller workstations shall have a typical cursor control device such as a mouse, trackball, touchpad or stylus.

12.2.4.2 The cursor control device shall have a conveniently located select push-button to initiate appropriate actions based upon the cursor location at the time of the button press.
12.2.5 Workstation Graphics Devices

12.2.5.1 All controller workstations shall have one, two, three, or more color monitors with the following minimum features:
   a) 22 or 24-inch Flat Panel LCD Monitor
   b) Active Matrix TFT technology
   c) 1280 x 1024 pixels native resolution
   d) 0.30mm Dot Pitch
   e) Anti Glare Hard Coating
   f) Wide viewing angle, which shall allow users to view the screen from various positions without compromising image quality
   g) Analog/Digital DVI capability for crisp images shall be supported
   h) A high contrast ratio that will generate sharp, crisp lines and images
   i) Fast response times that will provide superior clarity for moving images with "no ghosting"
   j) Premium brightness that allows for brilliant images with good blacks and richer colors

12.3 SERVERS

12.3.1 General

12.3.1.1 The requirements of this subsection shall apply equally to all the server-class hosts used in the SCADA system.

12.3.1.2 The system processors shall have the following minimum features:
   a) Intel Xeon Processor architecture
   b) Internal word length of a minimum of 32 bits

12.3.1.3 All server class machines shall have dual power supplies. These shall be hot swappable if possible.

12.3.2 Main Memory

12.3.2.1 The requirements of this subsection shall apply equally to all the server-class hosts used in the SCADA system.

12.3.2.2 The system memory shall have the following minimum features:
   a) Equipped with 4GB of internal Random Access Memory
   b) Standard memory technology consisting of semi-conductor memory which must be directly accessible by the CPU
   c) Have a minimum word length of 32 bits
   d) Expandable with simple plug compatible memory modules
e) Support multi-bit error detection and single bit error correction

12.3.3 Mass Storage Devices

12.3.3.1 The requirements of this subsection shall apply equally to all the servers used in the SCADA system.

12.3.3.2 The mass storage devices shall have the following minimum features:

a) All servers and workstations shall be equipped with an internal IDE-connected hard drive for the operating system, program files and virtual memory.

b) In general, disk redundancy shall be required for operating systems, program files, and virtual memory on servers but not workstations running in a RAID 1 configuration.

c) Historical servers shall have additional needs for historical databases. In addition to the operating system disk above, Historical servers shall also be equipped with SCSI-connected (or equivalent) RAID controllers and disks. The RAID model used shall be simple disk "mirroring" (RAID 1) to maximize performance. The RAID functionality and the disks may exist within the server chassis or be externally supplied if only a single Historical server is used.

d) Dual Historical servers shall share an external RAID enclosure through redundant SCSI connectors.

e) Hot-swap capability for the RAID disks shall be required.

f) Data access times of 15 milliseconds or less and peak transfer rates of 2MB/sec.

12.3.4 Removable Storage Device

12.3.4.1 Removable storage devices, used for data archive on Historical servers only, shall have unique requirements. In this case, specification of the devices shall be in a manner that will minimize the likelihood of failure to retrieve data over a 10-year span:

a) Tape drive technology will be supplied

b) Media capacity greater than 400GB/tape compressed

c) Removable cartridges shall encapsulate all backup media. The media shall not be removable from the cartridges in order to minimize the potential for mishandling.

d) Utilize media that remains readable for at least 10 years.

12.3.5 Magnetic Tape Drives

12.3.5.1 The magnetic tape drives shall be individually accessible by any of the computer systems at the local site.

12.3.5.2 The magnetic tape drives shall have the following minimum features:
a) Magnetic tape drives shall be an integrated system consisting of the tape transport and tape controller hardware.

b) The tape systems shall be compatible with performing disk backups, installing new/upgraded software, and miscellaneous other functions such as the archiving/de-archiving of historical data.

c) Support Small Computer System Interface (SCSI) interface

d) Support a minimum of 200GB native capacity

e) Support a minimum of 150GB/hr sustained native data transfer rate

f) Make use of streaming technology

g) Support data compression to increase storage capacity

h) Provide error correction code and error recovery procedures.

12.3.6 Keyboard

12.3.6.1 The computer keyboards shall have the following minimum features:

a) A 94 key low profile ergonomically designed unit

b) Four button cursor controls (left, right, up, down)

c) Country/language specific or QWERTY type keyboard

d) 10 key numeric keypad

e) USB or Smart-Card-like strong authentication device port

12.3.7 Cursor Control Device

12.3.7.1 All server computers shall have a typical cursor control device such as a mouse, touchpad, trackball, or pointing stylus.

12.3.7.2 The cursor control device shall have a conveniently located select push-button to initiate appropriate actions based upon the cursor location at the time of the button press.

12.4 SYSTEM PRINTERS

12.4.1 General

12.4.1.1 The SCADA system shall provide printers for the following functions:

a) Report Printer

b) Screen Hardcopy Printer

12.4.2 Report Printers

12.4.2.1 The report printers shall have the following minimum features:

a) Can be either serial or network printers, and support for both types of printers must be provided.
b) Use standard fan-fold, sprocket-feed paper or white bond paper

c) Low noise output (<60 dB at 3 feet from the printer)

12.4.3 Screen Hardcopy Printers

12.4.3.1 The screen hardcopy printer shall provide the primary function of producing hard copies of the various CRT displays on controller demand.

12.4.3.2 The screen hardcopy printer shall accurately reproduce the screen image and colors.

12.4.3.3 The screen hardcopy printer shall have a minimum resolution equal to that of the CRT screen and support the same range of colors.

12.4.3.4 The screen hardcopy printer shall have the following minimum features:

   a) Use state-of-the-art color laser printing technology requiring no routine maintenance

   b) Use standard Xerographic bond paper

   c) Shall be network accessible

   d) Shall print in color

12.5 EQUIPMENT CABINETS

12.5.1 General

12.5.1.1 Telvent shall supply all necessary standard 19" cabinets for adequate housing of the SCADA system and all rack and shelf mount peripheral equipment associated with it.

12.5.1.2 All equipment enclosures shall be of finished metal construction.

12.5.1.3 The design of the cabinets shall support twice the expected maximum weight of all the equipment installed within the cabinet.

12.5.1.4 All enclosures and other ancillary structures shall be primed and painted in a non-offensive/aesthetically pleasing color and texture.

12.5.1.5 All enclosures shall be free standing and have an industry standard design and dimension.

12.5.1.6 All cabinets shall be accessible from the front and rear and shall consist of front and rear access doors, and removable side panels.

12.5.1.7 The cabinet shall provide for bottom entry of cabling.

12.5.1.8 Where adequate housing of the SCADA system requires more than one cabinet, the cabinets shall be capable of simple conjoining.

12.5.1.9 Each cabinet shall have a grounding terminal that can accept a grounding
cable of 2 to 12 gauge.

12.5.1.10 Equipment arrangement and mounting within the cabinet(s) shall provide adequate ventilation for heat dissipation.

12.5.1.11 DBNGP shall supply forced air cooling, if required, to maintain the cabinet temperature within the range of operating temperatures specified by the equipment manufacturers.

12.5.1.12 The sizing of all equipment enclosures shall accommodate fitting through a 36 inch-by 72-inch opening.

12.6 COMMUNICATION PERIPHERALS

12.6.1 General

12.6.1.1 The communications methods may consist of radio, microwave, dedicated leased circuits, dial-up telephone lines, and satellite or network connections.

12.6.1.2 The system shall be capable of communicating through direct serial devices as well as multi-dropped serial and network devices.

12.6.1.3 The system shall be capable of performing asynchronous and synchronous communication.

12.6.1.4 All communication peripherals shall conform to industry standards and shall be off the shelf standard products.

12.7 NETWORK CONNECTIONS

12.7.1 General

12.7.1.1 Telvent shall provide the following minimum requirements for the SCADA system Local-Area (LAN) and Wide-Area (WAN) networks.

12.7.1.2 Telvent shall supply all network cables, transceivers, bridges, routers, concentrators required for the SCADA system up to, and including, any modems or data control units.

12.7.1.3 Telvent shall use network equipment that can support Thin-wire, Twisted pair or Fiber-Optic network connections.

12.7.1.4 The network cabling shall provide the highest quality, most reliable communications possible. It shall support data rates up to 1Gbps.

12.7.1.5 All network cable connections shall be plug ended and properly terminated with appropriate termination hardware if necessary.

12.7.1.6 Cable lengths shall be only as long as is necessary to complete the connections between equipment in their anticipated final arrangement.
12.7.1.7 All cabling and wiring necessary to provide a functional SCADA system shall be Telvent’s responsibility.

12.7.1.8 All cables shall be continuous and without intervening splices or connection between equipment cabinets. Terminations outside the equipment cabinets shall not be acceptable.

12.7.1.9 All cabling shall include clear labeling with descriptive permanent labels at both ends.

12.7.1.10 All LAN/WAN communication equipment shall support the following common features, as applicable to the equipment type:

   a) Network Management - SNMP (Simple Network Management Protocol), CMIP (Common Management Information Protocol), or both
   b) Multiple Protocols - TCP/IP, UDP, FTP, ICMP, SOAP, XML, etc.
   c) Integrated IS-to-IS Routing
   d) Destination Address Filtering
   e) Protocol Filtering
   f) IPSec and L2TP (Layer 2 Tunneling Protocol)
   g) Source Address Filtering
   h) Spanning Tree Algorithm

12.7.2 Local Area Network (LAN)

12.7.2.1 All servers/computers/workstations/ peripherals shall be interconnected and exchange data through a redundant LAN capable of operating at a data transfer rate of 100 Mbps minimum.

12.7.2.2 In all cases, the LAN shall have sufficient bandwidth such that throughput under heavy loading will not affect system performance/operation.

12.7.2.3 The LAN shall consist of at least two separate independent LANs with each server computer and workstation/console having access to both LANs simultaneously.

12.7.2.4 Each server computer shall have a separate independent interface to each LAN and shall automatically switch between LANs if the system detects a critical hardware or software failure.

12.7.2.5 Any failure in a server LAN card shall be transparent to the software running on that or any other server.

12.7.2.6 The LAN shall be fault-tolerant utilizing a network configuration that will prevent any single point of failure from causing a general system failure or loss of critical SCADA functions.

12.7.2.7 The following minimum requirements are mandatory for the Local Area
Networks:

a) Compliant with Ethernet/IEEE 802.3 network standards
b) Support TCP/IP protocols, including IPSec provisions within the TCP/IP protocol stack
c) Operate at a minimum data rate of 100Mbps
d) Operate over unshielded twisted pair (UTP) cat 5 cabling
e) Provide redundancy

12.7.3 Wide Area Network (WAN)

12.7.3.1 The Wide Area Networks shall be logical extensions of the Local Area Networks.

12.7.3.2 Telvent shall select equipment capable of supporting routers, bridges, concentrators and data control units for connections to a corporate Wide Area Network.

12.7.3.3 The operating system software shall provide facilities for network routing, and serving as a gateway to other networks using WAN protocols such as Frame Relay and Asynchronous Transfer Mode (ATM).

12.7.3.4 The operating system shall support address resolution protocols and shall support the use of routing tables, etc.
13. DOCUMENTATION REQUIREMENTS

13.1 INTRODUCTION

13.1.1 General

13.1.1.1 Documentation for the system shall consist of a principal category:
   a) Standard documentation

13.1.1.2 Standard documentation shall describe the design, operation and maintenance of Telvent’s baseline system.

13.2 PROJECT DOCUMENTATION

13.2.1 General

13.2.1.1 This documentation shall detail how the system shall meet this Functional Design Specifications and how Telvent shall meet the contract requirements.

13.2.1.2 Telvent shall present the documentation listed below to DBNGP for approval in the first third of the project implementation cycle.

13.2.2 Project Quality Plan (PQP)

13.2.2.1 The PQP shall detail project execution by Telvent to meet contractual requirements for both Telvent and DBNGP. This document shall include:
   a) A list of personnel and subcontractors assigned to the project, the responsibilities of each and their status reporting procedures
   b) A list of submittals that shall be provided to DBNGP
   c) A list of services and support that shall be provided and their associated procedures
   d) Project milestone definitions
   e) The Project Schedule as an attachment

13.2.3 System Configuration Plan (SCP)

13.2.3.1 The SCP document shall describe system configuration, and will require DBNGP approval. The SCP document shall include:
   a) An overview of the system configuration
   b) Development system requirements
   c) Cabling and installation issues
   d) A list of hardware and software deliverables
   e) A system block diagram, elevation drawings and RTU cabinet layouts (if applicable)
13.2.4 Application Definition Documents (ADDs)

13.2.4.1 An ADD shall be an application software functional description. An ADD document shall be built for each customized application to meet this Functional Design Specification beyond Telvent’s baseline system. Each ADD shall include:

a) Description of the functions that the software will perform in addition to Telvent's baseline system

b) Operational/management user interface description

c) Constraints, of any reasonable type, which may exist

d) Verification and validation criteria used to evaluate the software for functional compliance

13.2.5 Test Plan

13.2.5.1 The Test Plan document shall include a detailed compliance description with direct reference to this specification.

13.2.5.2 The Test Plan document shall also specify verification of technical compliance (by demonstration or test).

13.2.5.3 DBNGP shall provide input for this document.

13.2.6 FAT Test Procedures


13.2.6.2 This document shall contain all tests that Telvent proposes to be conducted at FAT time to show that the product adheres to the baseline functionality and additional ADD functionality as per the Test Plan.

13.2.6.3 Telvent shall provide this document to DBNGP at least four weeks before FAT.

13.2.6.4 DBNGP shall review the document and respond with comments and requests for change.

13.2.6.5 Telvent shall modify the document accordingly and submit it to DBNGP for final approval one week prior to FAT.

13.2.7 SAT Test Procedures

13.2.7.1 The Site Acceptance Test (SAT) Procedures shall also be the primary guide for all activities during SAT and shall comply with Telvent’s proposal and this Functional Design Specifications, and the Factory Acceptance Test Procedures document.

13.2.7.2 SAT procedures shall include all tests that Telvent determines are necessary
after system installation to show that the product adheres to this Functional Design Specifications document.

13.2.7.3 The Site Acceptance Test Procedures document shall be similar to the Factory Acceptance Test Procedures document, with additional steps for testing interaction with RTUs and connected field devices.

13.2.8 Test Reporting

13.2.8.1 Test Report documentation shall include the signed off FAT document and a summary of FAT discrepancies (to be included with the FAT acceptance certificates as approved by DBNGP and Telvent).

13.2.9 Commissioning Plan

13.2.9.1 The Commissioning Plan shall detail the procedures to commission the new system.

13.2.9.2 Telvent shall develop the Commissioning Plan, after which DBNGP shall evaluate the plan and grant ultimate approval.

13.2.9.3 The cutover shall be done without (or with minimal) downtime.

13.2.9.4 Any downtime shall be limited to individual parts (such as one or two consoles or polling channels) at any one time.

13.2.10 Project Status Reports

13.2.10.1 The contractor shall issue project Status Reports to DBNGP on a monthly basis.

13.2.10.2 These reports shall include the following as a minimum:
   a) Current outstanding problems and issues
   b) Items accomplished since last report
   c) Items to take place by the next report
   d) An updated schedule
   e) Current status of each milestone
   f) Current status of deliverables
   g) A contract and invoicing summary
14. TRAINING REQUIREMENTS

14.1 INTRODUCTION

14.1.1 General

14.1.1.1 Effective operation of the SCADA system shall require the availability of both on-site and Telvent facility training.

14.1.1.2 Telvent shall provide a comprehensive list of all courses offered by Telvent’s Educational Services Department.

14.2 GENERAL REQUIREMENTS

14.2.1 General

14.2.1.1 Telvent shall have a professional training or educational services department dedicated to providing state-of-the-art and Telvent specific SCADA industry training.

14.2.1.2 Experienced instructors that are qualified in the subject matter of the respective courses they teach shall conduct all training courses.

14.2.1.3 Telvent training staff resumes shall accompany Telvent’s proposal for each Training session.

14.2.1.4 All course material shall be an accurate reflection of the system delivered to DBNGP.

14.2.1.5 Courses shall consist of both theory and hands-on components, but in all cases shall consist of not less than 50% hands-on.

14.2.1.6 Each student or group of students shall have their own workstation on which to practice and perform the hands-on components of their training.

14.2.1.7 Telvent shall offer a certification track for SCADA personnel and managers that shall lead DBNGP staff through a graduated path of qualification and competency for Telvent’s software and system offerings.

14.2.1.8 Telvent shall provide Educational Services consultation to maximize DBNGP investment in their staff’s skill and knowledge base. Depending upon consultation outcomes, appropriate courses shall take place at Telvent’s facilities, or at DBNGP site.

14.3 TRAINING COURSE CONTENTS

14.3.1 General

14.3.1.1 Courses shall focus on the different building blocks that make up the SCADA system. The descriptions of available training courses are found in
Appendix 1.

14.3.1.2 The list of required topics and number of students for courses is as follows:

<table>
<thead>
<tr>
<th>Topic</th>
<th>Duration</th>
<th>No. of Students</th>
</tr>
</thead>
<tbody>
<tr>
<td>Component Administration</td>
<td>5 days</td>
<td>4</td>
</tr>
<tr>
<td>Display Building</td>
<td>5 days</td>
<td>4</td>
</tr>
<tr>
<td>Component Integration</td>
<td>4 days</td>
<td>4</td>
</tr>
<tr>
<td>Reporting Services</td>
<td>2 days</td>
<td>4</td>
</tr>
<tr>
<td>Operation &amp; Control</td>
<td>1-2 days</td>
<td>8</td>
</tr>
</tbody>
</table>

*Table 7- Training Courses*

14.4 EXTENDED TRAINING OPTIONS

14.4.1 Onsite, Just-in-Time Training

14.4.1.1 Telvent shall be competent in their ability and experience in providing on site, just-in-time training. It is expected that this shall be used during commissioning and startup of the new system. DBNGP shall approach Telvent when these additional courses will be required.

14.4.2 Coaching

14.4.2.1 Telvent shall be capable of providing subject area experts for any component of the system in order to assist DBNGP with technical issues. DBNGP shall approach Telvent when these additional courses will be required.

14.4.2.2 Subject area experts shall be available for on-site visits or via web, telephone or email. DBNGP shall approach Telvent when these additional courses will be required.
15. PROJECT IMPLEMENTATION

15.1 INTRODUCTION

15.1.1 General

15.1.1.1 In order to ensure the timely and successful integration, testing, delivery, installation, start-up, commissioning, acceptance and support of the SCADA system, Telvent shall have in place, a formal quality assurance program for the design, manufacture, installation and servicing of SCADA Systems.

15.1.1.2 This quality program shall receive certification from an appropriate third party agency.

15.1.1.3 The preferred quality assurance certification is ISO 9001.

15.1.1.4 Telvent shall provide documentary evidence of this certification as part of the proposal submittal.

15.1.1.5 Telvent shall make use of standard software-based project management tools to allow effective tracking of the progress of system development and integration.

15.2 PROJECT MANAGEMENT

15.2.1 General

15.2.1.1 Telvent shall designate one person as the Project Manager.

15.2.1.2 DBNGP shall also designate one person as a Project Manager. It shall be the collective responsibility of these Project Managers to ensure the requirements of this Functional Design Specifications document are clear enough to meet each requirement through tracking project schedules and costs.

15.2.1.3 The Project Managers shall be responsible for coordinating resources to ensure on time delivery of the system within budget. The Project Managers shall be the primary contacts between Telvent and DBNGP, unless otherwise specified in the Contract.

15.2.1.4 Telvent’s Project Manager shall be responsible for providing monthly progress reports, which shall arrive no later than 10 working days after the last day of the month.

15.3 CORRESPONDENCE

15.3.1 General

15.3.1.1 All contractual correspondence shall be between the two project managers.
15.3.1.2 Unless otherwise agreed upon, all correspondence shall be typewritten and dated with an indication of the document’s contents.

15.3.1.3 All correspondence relevant to system specifications shall indicate the relevant section from this specification as a reference.

15.3.1.4 Email shall be considered an official correspondence medium.

15.4 EQUIPMENT SHIPMENT

15.4.1 General

15.4.1.1 Telvent shall notify DBNGP 14 days prior to the shipment of the computer system to DBNGP site.

15.4.1.2 The equipment setup shall correspond to the “like new” condition of the equipment prior to shipment, and shall be insured by Telvent for damage during shipment unless otherwise agreed upon.
16. ADDITIONAL SERVICES

16.1 INTRODUCTION

16.1.1 General

16.1.1.1 It is expected that the implementation of this project may consume significant DBNGP resources. During the lifetime of the project DBNGP may want to use Telvent subject experts to assist in their responsibilities. These services are considered out of scope of this project but are offered at the regular published daily rates.

16.1.1.2 Telvent shall be capable of providing experts in Full Scope Engineering, SCADA, Gas Applications and Communications.

16.1.1.3 Telvent shall be able to provide the resources required, as mentioned above, on site at DBNGP locations, on short to long term assignments.

16.2 PROJECT MANAGEMENT

16.2.1 General

16.2.1.1 Telvent shall be capable of providing Project Management services in establishing and meeting DBNGP project schedules, cash flow results, project progress reports, scope control, understanding and meeting end-user requirements, conformance to DBNGP processes, planning, communicating with other DBNGP departments, managing the end-user relationship, documenting all project activities, and end-user satisfaction.

16.2.1.2 Additionally, Telvent shall be capable of providing Project Management services in monitoring performance, coordinating resources across DBNGP projects, managing risks, negotiating changes to scope, schedule or commercial terms, and ensuring proper project communication.

16.2.1.3 Management and negotiation of commercial terms is critical to the success of any project. Telvent shall be competent in the area of managing sub-contracts and subcontractors.

16.2.1.4 Telvent shall be capable of providing consulting services for building requirements specification, and performing co-Engineering to design a solution for petroleum and gas pipeline applications, pipeline modeling, and adherence to regulatory requirements.

16.3 TECHNICAL EXPERTISE

16.3.1 General

16.3.1.1 At certain phases of this project or future projects, DBNGP may find it useful to employ experts to help determine the best solution in any number of problem areas. Telvent shall be able to provide experience in:
16.3.2 Requirements Analysis

16.3.2.1 Telvent shall have competent experts in helping DBNGP to do Requirements Analysis for any SCADA or IT type projects that DBNGP may endure.

16.3.2.2 Telvent experts shall have experience in doing similar work on other projects and for other customers.

16.3.3 Database Development and Conversion

16.3.3.1 Telvent shall be capable of providing experts to add new stations, compressors, pumps or any other database inputs to a new or existing SCADA system and databases(s).

16.3.3.2 Telvent shall be able to provide guidance if a database conversion may be more efficient. If such cases, Telvent's experts shall be able to write and built any utilities that may be required for the conversion.

16.3.4 Graphical Display Development and Conversion

16.3.4.1 As new stations, compressors, valves or other devices are added to DBNGP's system, Telvent shall be able to provide experts to create and/or modify displays to accommodate those changes.

16.3.4.2 Telvent experts shall be able to offer advice in navigation and layout.

16.3.4.3 Telvent shall be able to provide guidance if a display conversion may be more efficient. In such cases, Telvent experts shall be able to write and built any utilities that may be required for the conversion.

16.3.5 Application Development and Testing

16.3.5.1 Telvent shall be capable of providing experts to add new DBNGP applications to the system. In such cases, the experts shall access the appropriate libraries in the system to interact with the Real-Time and or Historical databases.

16.3.5.2 Telvent experts shall also be able to fully test and commission these new applications.
16.3.6 Communications Infrastructure Development

16.3.6.1 The communication infrastructure is critical for a SCADA system and typically has unique requirements. Telvent experts shall have specialized SCADA knowledge in the areas of designing and implementing telecommunication systems such as VSAT, fiber, terrestrial, leased lines, WAN and other communication mediums, to ensure that the SCADA system is as reliable as current technology allows.

16.3.7 Site Commissioning

16.3.7.1 Telvent shall be capable of providing experts in the field of commissioning.

16.3.7.2 These experts shall be able to show similar experience on other projects.

16.3.7.3 Site commissioning may involve commissioning of applications, communications infrastructure, point-to-point testing of all PLC/RTU points including commands and setpoints, and commissioning of new processes and procedures.

16.3.7.4 Telvent experts shall be able to drive all site commissioning activities.

[End of main document]
APPENDIX 1 – TRAINING COURSE DESCRIPTIONS
Each of the following cutsheets describe one of the available courses applicable to this system