## ENGINEERING STANDARD PROCEDURE

### North Atlantic

<table>
<thead>
<tr>
<th>VALE #</th>
<th>PAGE</th>
<th>REV.</th>
</tr>
</thead>
<tbody>
<tr>
<td>PROC-84007</td>
<td>1/6</td>
<td></td>
</tr>
</tbody>
</table>

### TITLE

**SPECIALTY ENGINEERING**
**PROCESS AUTOMATION**
**SECURITY – ANTI-VIRUS MANAGEMENT**
**ANTI-VIRUS UPDATE PROCEDURE**

### REVISIONS

<table>
<thead>
<tr>
<th>Rev</th>
<th>Description</th>
<th>Rev’n by</th>
<th>App Sud</th>
<th>App PC</th>
<th>App Thom</th>
<th>App VB</th>
<th>App LH</th>
<th>App Clyd</th>
<th>App Act</th>
<th>Issue Date YYYY/MM/DD</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1st Issue</td>
<td>KM</td>
<td>PC</td>
<td>Pending</td>
<td>Pending</td>
<td>Pending</td>
<td>Pending</td>
<td>Pending</td>
<td>Pending</td>
<td>2013/06/21</td>
</tr>
</tbody>
</table>

Sud = Sudbury, Ontario, PC = Port Colborne, Thom = Thompson, Manitoba, VB = Voisey’s Bay, LH = Long Harbour, Act = Acton, England, Clyd = Clydach, Wales, N/A = Not Applicable
1.0 PURPOSE

This procedure describes the methodology for deploying signature updates to anti-virus software.

2.0 APPLICATION

This procedure applies at any Vale locations indicated with approval on the cover page, with the following exceptions:

2.1 EXCEPTIONS

None

3.0 REFERENCE DOCUMENTATION

The following documents were used in the development of this document or are related to it. They shall be used in their most recent revision.

PROC-84007a Process Automation Anti-Virus Management Policy
PROC-84006 Process Automation Patch Management
PROC-84006a Process Automation Patch Management Policy

4.0 OVERVIEW

Swift deployment of anti-virus updates is important to ensure inoculation against new forms of malware, and is typically performed in an automated fashion. However, updating malware signatures and detection engines is not without potential pitfalls. Occasionally an anti-virus update can contain a new signature which causes a critical process to malfunction on the target system. Therefore it is important to test individual signatures prior to deployment.

5.0 PROCEDURE – DEPLOYING ANTI-VIRUS UPDATES

- Step 1 – restore a recent backup of a sample target system to the test equipment
- Step 2 – ensure proper operation of the target system in the test environment
- Step 3 – apply the anti-virus update to the test system
- Step 4 – ensure proper operation of the target system in the test environment, documenting any problems or discrepancies
• Step 4a – if problems or discrepancies are noted, take appropriate time to attempt to solve the problem or discrepancy and bring the target test system to nominal operation
• Step 4b – if problems or discrepancies persist, perform appropriate rollback function if available, and document the process
• Step 4c – if an appropriate rollback function is not available, restore the system from the latest valid backup
• Step 4d – document the failure to update the Anti-Virus on each target system
• Step 5 – place the target system back into production operation, and document patch application

Each plant or mine will require a procedure detailing that plant or mine’s specific requirements due to differences in control system suppliers and network architecture.

Appendix B below describes known issues with and procedures for that control system vendor’s systems.

**Appendix A: Revision and Transition Notes**

(Revisions are listed in reverse chronological order with most recent revision at the top. Revision notes describe: what was changed, why it was changed, and the plan to implement the change, including whether changes are retroactive)

**Revision 1**
Document Format Changed, added references, added Plant Specific requirements

**Revision A**
Draft Issue (from Lofty Perch)

**Appendix B: Keywords**

Update, Security, Testing, Malware, Virus, Antivirus

**Appendix C: Vendor Specific Information**

1.0 KEPUWARE
Kepware does not provide additional guidance for the configuration of anti-virus software on Kepware servers.

2.0 MICROSOFT MS-SQL SERVER

There is extensive guidance publicly available regarding the configuration of anti-virus software on MS-SQL servers.

Exclusions for MS-SQL Servers

Exclude the following files: Edb*.log, Res1.log, Res2.log, Edb.chk, Tmp.edb, pagefile.sys (Windows paging file)

- Exclude the spool directory (%systemroot%\System32\Spool) and subfolders, if they exist.
- Exclude folder related to Windows Update (%systemroot%\SoftwareDistribution\Datastore) and subfolders.
- Exclude database backup and transaction log backup files.

Additional exclusions for clustered servers

- Exclude the quorum drive
- Exclude the \MSDTC directory in the MSDTC share drive
- Exclude the %Systemroot%\Cluster directory
- The temp folder for the Cluster Service account

3.0 ROCKWELL

Rockwell does not have any guidance on the use or architecture or deployment of anti-malware products available to the general public. Knowledgebase entry #35330 is referenced on the Rockwell site and also on Internet search engines when queried about Rockwell Automation and Anti-Virus.

However, some sources on the Rockwell web site claim that Rockwell products are tested with leading anti-virus/anti-malware software, and there are no conflicts.

4.0 WONDERWARE
Invensys provides only a small amount of configuration information for Wonderware to better integrate with anti-virus software. Nonetheless, Wonderware does have some suggestions about how to protect from viruses:

- Isolate the plant control network (PCN) from the corporate network
- Virus scan your systems on a regular basis.
- Wonderware does not endorse any particular anti-virus package due to the large number of such products available on the market
- Stay current on information related to virus protection trends.
- If your Wonderware application’s performance is impacted by running the anti-virus software:
  - Disable the anti-virus software or configure it to exclude certain Wonderware software directories (for example the InTouch directory, InSQL Data directory or the ArchestrA\Framework directory). On a production system it is our recommendation to make all the resources available to the Wonderware software and production control needs.

If your Wonderware application conflicts with anti-virus software:

- Ensure you have the latest version of the anti-virus software
- Run the anti-virus utility to ensure a clean machine
- Disable the anti-virus software, then run your application
- If possible periodically re-run the anti-virus software during scheduled maintenance times (planned downtime).
- When the anti-virus software is disabled, do not run any applications that could transfer a virus (for example email or file sharing).
- Wonderware will post Tech Alerts on any significant anti-virus software conflicts with our software products. Please check our web site at www.wonderware.com\support\mmi for the most current information.

5.0 IFIX BY GE

GE Intelligent Platforms > Support > KB > KB8190 -- Can I run AntiVirus software on machines running the iFIX and iHistorian software?

There are no known issues with running Antivirus software on machines running the iFIX and iHistorian software.
While we certainly recommend that machines have the latest version of the Antivirus software installed on them to ensure the machine is protected against any new virus strains, we do not recommend one Antivirus software product over another.

Many of our customers are running either the Symantec [Norton] Antivirus or MacAfee’s Antivirus software on their systems without any reported issues. It is generally recommended for the antivirus software to be disabled and each machine removed from the network if/when installing the iFIX software or any iFIX software improvement modules (SIMs) and then for the machines to be added back to the network and for the antivirus software to be re-enabled (either by manually restarting the application, or via restart of the machine if the antivirus application is started automatically).

One potential issue that has been encountered when installing antivirus software on iFIX machines which are using the GE Fanuc ABR driver and have Rockwell RSLinx software installed is that the ABR driver has lost communication with RS Linx. This is due to the fact that the antivirus software has been known to corrupt the RSLinx activation token.

If you should encounter this issue, you need to contact Rockwell Support http://support.rockwellautomation.com to obtain a new token.