



Best Practices for your HMI/SCADA Systems

Simple steps for reducing downtime, increasing efficiency and improving security for monitoring & control applications

Industries and utilities are becoming increasingly accountable for the safety, efficiency, and reliability of their systems. It is therefore important to establish a set of best practices to govern the operation of mission critical HMI/SCADA software applications. Once established, these guidelines need to be periodically re-evaluated to account for new technologies, threats and demands. The steps below will allow you to quickly review your system and identify areas for improvement.

Note:

- Most of these principles are applicable to any HMI/SCADA monitoring & control software product
- **Items in green are specific to VTS/VTScada software from Trihedral Engineering Ltd.**

Index/Checklist

HMI/SCADA Software Maintenance.....	2
<input type="checkbox"/> Purchase application development capability for in-house use	2
<input type="checkbox"/> Maintain current software licenses	2
<input type="checkbox"/> Maintain current software support	2
<input type="checkbox"/> Maintain proper user documentation	2
<input type="checkbox"/> Monitor VTS computer resources.....	2
<input type="checkbox"/> Monitor IP connections between primary servers and clients.....	2
<input type="checkbox"/> Train users and administrators on VTS	3
<input type="checkbox"/> Set up AutoStart for your HMI/SCADA applications.....	3
Server Redundancy and Data Backup	3
<input type="checkbox"/> Add redundant servers.....	3
<input type="checkbox"/> Backup system and application data	4
VTS & VTScada Optimization and Security	4
<input type="checkbox"/> Optimize polling cycles	4
<input type="checkbox"/> Add a 'Deadband' value to Analog Status Tags.....	4
<input type="checkbox"/> Ensure all changes are networked to all clients & servers	4
<input type="checkbox"/> Use proper security protocols	5
<input type="checkbox"/> Internet Client protection.....	5
<input type="checkbox"/> Use consistent GUI colors and layout.....	5
<input type="checkbox"/> Use consistent names for tags and areas.....	5
PC Setup and Maintenance	5
<input type="checkbox"/> Configure Dr. Watson on all computers.....	5
<input type="checkbox"/> Install malware detection software	5
<input type="checkbox"/> Remove the HMI/Scada application folder from antivirus scans.....	6
<input type="checkbox"/> Turn off Microsoft Windows Auto Updates.....	6
<input type="checkbox"/> Turn on 'Automatic Logon' in Windows	6
<input type="checkbox"/> Properly power down servers & client computers	6
<input type="checkbox"/> Install Uninterruptible Power Supplies (UPS).....	6
<input type="checkbox"/> Install lightning protection	6
Network Setup and Maintenance.....	7
<input type="checkbox"/> Document networking & hardware assets	7
<input type="checkbox"/> Remote Access	7
Summary	7
More Information.....	7

HMI/SCADA Software Maintenance

Purchase application development capability for in-house use

A full development license for your HMI/SCADA software installed at your site means that both you and the integrator who installed the system are able to make application changes as required.

Maintain current software licenses

HMI software companies regularly add new features to each new release of their products. Upgrading to the latest compatible version of your software ensures that you have access to this expanded functionality.

To see the latest features of VTS visit:

www.trihedral.com/products/visual-tag-system

Maintain current software support

Keep your support service contract up-to-date to ensure that your staff has access to technical support when they need them. Support packages are often cheaper at the time of purchase.

For more information on Trihedral's SupportPlus package visit:

www.trihedral.com/customer-support/support-packages/supportplus

Maintain proper user documentation

As trained operators move on, it is important to provide new employees with the resources they need to use their HMI applications effectively and consistently. Also, some features are used less frequently than others so it is helpful for even experienced operators to have user documentation for reference.

This includes user guides that come with the software and documentation specific to your application provided by the system integrator. It is recommended that paper or electronic versions be available at each HMI workstation. Documentation should be updated each time you upgrade to a new version of the software.

For access to VTS/VTScada documentation visit:

www.trihedral.com/customer-support/user-guides

Monitor VTS computer resources

To ensure that the PC's running your HMI continue to provide reliable service, VTS allows you to monitor remaining hard drive capacity, memory utilization and CPU usage. Alarms can notify operators when these resources become limited. These features are easily configured in any application.

For more information on creating WorkStation Driver Tags in VTS visit:

www.trihedral.com/customer-support/howto/workstationdrivertag

Monitor IP connections between primary servers and clients

Networked applications are dependant upon the IP connections between their HMI servers and clients.

VTS allows you to easily monitor these connections by creating 'Network Status' tags that can be drawn on any application display. Alarms can be configured within the tags to notify operators when connections are broken.

For more information about creating a VTS network Status Tag visit:

www.trihedral.com/customer-support/howto/networkstatustags

Train users and administrators on VTS

Training courses for operators help to ensure that HMI/SCADA applications are being used effectively and consistently across your organization. Many software manufacturers can provide training courses on-site or at their training facility.

Note: Trihedral's SCADA Software Operation & Configuration Course has been approved for Continuing Ed Credit in North Carolina.

For information about booking VTS/VTScada training courses visit:
www.trihedral.com/customer-support/training

 Set up AutoStart for your HMI/SCADA applications

If an HMI computer restarts unexpectedly, it is vital that your application restarts automatically to ensure the safe monitoring of your system and to prevent the loss of historical data.

Note: In order for your application to Auto-Start, you must first set up your operating system to log in automatically. See 'Turn on Automatic Logon in Windows' in the 'PC Setup and Maintenance' section below.

To enable AutoStart VTS:

1. Select the application in the 'VTS Application Manager'
2. Click the 'properties' button
3. Select the 'Auto-start Application' check box

Server Redundancy and Data Backup

 Add redundant servers

Server redundancy is essential in mission critical applications. In the event that a primary server goes off-line, a back-up server should be set up to replace it automatically and without operator intervention.

This ensures that:

- The safe monitoring & control of your system continues uninterrupted
- Staff continue to be notified about alarms
- Historical data continues to be collected without interruption
- Historical data is backed up
- Application data is backed up

This may require the purchase of additional HMI/SCADA software licenses for your redundant servers.

Note: It is highly recommended that redundant servers be located at separate locations from the primary servers in case one location is destroyed or becomes inaccessible.

VTS automatically handles primary to backup server failover, ensuring both thick client and Internet client connection transfers are fast and seamless. Moreover, when servers are restored, data and I/O communications are resynchronized to eliminate data loss.

For more information about VTS server redundancy, visit:
www.trihedral.com/products/visual-tag-system/networking

Backup system and application data

If you have set up your server redundancy properly, you will already have at least one up-to-date backup copy of your application and all your historical data. However, in the unlikely event that both your primary and backup servers are destroyed (or their data corrupted) you may choose to incorporate some form of additional data backup. This can include an external tape drive (e.g. Dell PowerVault 100T backup tape drive), CD-RW, DVD-RW or external hard drive.

This backup can include the following:

- Daily backup of differential historical data (e.g. files that have changed in the last 24 hours)
- Weekly backup of the present monthly historical databases and the application directory
- Application directory backup anytime the application changes

All backups should be completed on the backup historical database server to reduce resource utilization on the primary server.

Restore as required.

VTS & VTScada Optimization and Security

Optimize polling cycles

For many utilities, radios and transmitters are responsible for communicating with numerous remote monitoring devices. In addition, telemetry methods such as cellular are expensive. If polling cycles are higher than necessary, your application can become slow and costly. Look closely at your system's requirements and decide on an appropriate polling frequency based on the cost of your telemetry. For example, when filling a reservoir, there is no need to poll for the water level every second.

Add a 'Deadband' value to Analog Status Tags

By default, many HMI/SCADA products log all changes in the value of Analog Status tags no matter how small. This can result in your application logging large amounts of meaningless data. By adding a deadband value to your Analog Status tags, only changes larger than the deadband value will be logged.

Note: Setting the deadband value too high can result in the loss of important data.

To set a deadband value in VTS:

1. Open the properties dialog for an Analog Status tag
2. Enter an appropriate deadband value on the I/O tab

Ensure all changes are networked to all clients & servers

Online configuration allows process monitoring to continue without interruption, while users make modifications to application displays and tag data. This is an essential feature of mission-critical applications.

In VTS, application changes are managed through the VTS edit-lockout manager. The locking mechanism allows multiple users to simultaneously lock and configure different application objects and ensures each object may only be locked by one workstation at a time.

Make sure that any changes that have been made are pushed out to all servers and internet clients by selecting "Update all" in the VTS edit-lockout manager. This also releases the lock on the edited screen or tag so that other can edit them.

Use proper security protocols

It is very easy for busy operators to sidestep security best practices in favor of convenience. Applications remain logged on indefinitely or use passwords like 1234. Often a single password is used for an entire application.

Make sure that your application:

- Provides each user their own password with privileges specific to their responsibilities
- Logs off when inactive for more than a few minutes
- Employs passwords that include numbers and both upper and lower case letters

Note: To remain effective, passwords should be changed periodically.

 Internet Client protection

Access to an application through the VTS Internet Client requires a standard VTS user account with an Internet Access privilege.

In addition, VTS supports encrypted access through the use of Secure Socket Layer (SSL) certificates. VTS can operate through the use of secure VPN tunnels. Such extended security is external to VTS and setup may require coordination with the customer's network administration group.

 Use consistent GUI colors and layout

HMI applications must be intuitive and easy for busy operators to read at a glance. For example, all pump stations screens should use one set of colors and feature consistent layout of data fields and navigation. These guidelines should be established during the design phase and then used for all new screens.

 Use consistent names for tags and areas

Proper naming conventions save time and reduce errors when adding new tags to your application. (For example, Analog Status tags for a pump station could be named PSInflow1, PSInflow2 etc). Creating consistent Area names allows operators to quickly sort Tags in the Tag Browser and simplifies the setup for auto dialers and Realm Area Filtering (if supported).

PC Setup and Maintenance

 Configure Dr. Watson on all computers

In the unlikely event that your application terminates unexpectedly, the Dr. Watson Utility generates a file called a 'Crash Dump' that can assist support staff in finding the reason.

Note: For Windows Vista computers, VTS 8.0 can generate crash Dump files without special configuration.

Detailed configuration information can be found on the Trihedral Support FAQ page:

www.trihedral.com/customer-support/supfaq

 Install malware detection software

All computers are vulnerable to malware, even those without permanent connections to the internet. Make sure that ALL computers (servers, internet clients and standalone workstations) are protected with anti-virus, anti-spy ware and anti-spam software. These programs will need to be updated regularly to ensure maximum protection.

Remove the HMI/Scada application folder from antivirus scans

Anti-virus software typically scans every file your computer opens. However, HMIs constantly open and close files during normal operation. To prevent your system from slowing down, make sure that your anti-virus software excludes the HMI/SCADA application folder from its scan list. Use the help tool of your anti-virus software to learn how to do this.

 Turn off Microsoft Windows Auto Updates

Updates to Windows Operating Systems need to be installed in a controlled manner. This prevents custom drivers for devices like Voice Modems from being overwritten by generic Windows drivers that often lack necessary functionality. This also prevents computers from rebooting in the middle of the night without supervision.

To disable this feature in Windows, open 'Automatic Updates' in the Control Panel and select 'Download updates but let me choose when to install them.'

 Turn on 'Automatic Logon' in Windows

If you have set up AutoStart for your HMI application, (See **HMI/SCADA Software Maintenance** above) you **MUST** first turn on 'Automatic Logon' in Windows. This change to the Windows registry allows the computer to fully restart without an operator needing to enter the Windows username and password. For more information on how to do this read this article from the Microsoft web site:

<http://support.microsoft.com/kb/315231>

Note: Before you make any changes to the registry, make sure to back it up and make sure that you know how to restore the registry if a problem occurs. Consult your IT department for more information.

 Properly power down servers & client computers

Application and system data can become corrupted if a computer is simply unplugged or switched off while an application is running. To power down a computer, it is important to first stop all HMI/SCADA applications and then to use the 'Shut Down' option on the 'Start' menu.

To stop an application in VTS:

- Go to the VTS Applications Manager (VAM) and select the running application
- Click the 'Stop' button

Note: There may be more than one application running in VTS at the same time. Be sure to select and stop each one.

- Click the 'Close' button to close VTS
- Power down the computer

 Install Uninterruptible Power Supplies (UPS)

To protect mission critical systems during inevitable power outages, each server and internet client computer should be plugged into a temporary backup power supply. Some devices (like the Tripp-Lite Power Protection UPS from Power Protection & Connectivity Products) can keep computers running for up to ten hours, others (like the APC Smart-UPS 1500) are designed to protect against short temporary lapses in power. Most can be configured to safely power down computers when their batteries are nearly depleted.

 Install lightning protection

Many kinds of remote equipment are vulnerable to lightning strikes, especially those that require some kind of antennae. Make sure your infrastructure is properly grounded and uses appropriate surge protectors and optic-isolators. Contact your system integrator for more information.

Network Setup and Maintenance

Document networking & hardware assets

Downtime and frustration can be significantly reduced by keeping a clear, up-to-date inventory of your hardware (e.g. PLCs, RTUs, radios, modems, PCs) and their related information (e.g. network addresses, phone numbers). Quick access to this information allows new assets to be added more quickly and consistently. It can also assist Technical Support in identifying the cause of issues that might occur.

Remote Access

In the event that one or more of your HMI installations becomes physically inaccessible (due to dangerous weather or blocked roads), it is vital to be able to access your HMI applications remotely. This can be achieved by setting up a VPN connection to your firewall and installing a software product such as Ultra VNC or PC Anywhere. This will allow you to log into your application through the Internet from any PC connected to the Internet. You will need to work with your IT department or system integrator to set this up securely.

Summary

It is impossible to completely prepare for every eventuality. However, following the steps above will help you avoid many of the common problems associated maintaining mission critical HMI/SCADA applications.

More Information

For more information about best practices, visit www.trihedral.com or contact one of our offices.

- **Trihedral Engineering Ltd. (Headquarters)**

1160 Bedford Hwy, Suite 400, Bedford, Nova Scotia, B4A 1C1, Canada

Tel: 902-835-1575

Contact: Patrick Cooke - pcooke@trihedral.com

- **Trihedral UK Ltd. (Scotland Office)**

Glover Pavilion, Campus 3, Aberdeen Science Park, Balgownie Drive, Aberdeen, AB22 8GW, UK

Tel: (011 44) 1224 258910

Contact: Keith Donaldson - keith.donaldson@trihedral.com

- **Trihedral. Inc. (Florida Office)**

Suite 243, 7200 Lake Ellenor Drive, Orlando, Florida, USA, 32809

Tel: 1.407.888.8203

Contact:

Bryan Sinkler - bryan.sinkler@trihedral.com

John Brosius - john.brosius@trihedral.com