Invensys offers advanced DCS system resources. RemoteWatch servers, located at customer sites, monitor Foxboro® I/A Series® Systems to ensure that critical resources are performing within proper bounds. If an unacceptable threshold is reached, then an alarm is sent and Invensys engineers are alerted to the changes before an issue develops. Remote connectivity is also designed to ensure that, if there is a problem, Invensys experts around the world can work with you to make appropriate adjustments to correct the issue and return your system to normal operation quickly and easily.

EMBEDDED COMPONENTS

Connecting a dedicated RemoteWatch server to your plant’s automation system network enables automated monitoring and analysis of configuration and resource utilization. RemoteWatch Services can greatly reduce the overall time involved in detecting performance abnormalities.

Daily updates from the I/A Series system are displayed in the LocalWatch user interface that shows a variety of details about the system, such as:

- Displays equipment listed by type, quantity, Lifecycle Phase
- Identifies installed software and compares to available Patches, QFs and Service Packs
- Data topology, sync/source for troubleshooting
- Identifies HW Levels & IDs out-of-rev/minimum useable Rev
- Identifies site specific Phase reports
- Presents physical topology diagrams

Hourly updates are also presented that include the number of:

- IPC Connections between stations
- Largest Available Memory Segment in CPs
- Percentage Used RAM
- Percentage Used Disk Space
- Times the 802.3 Ethernet Controller MAC Layer has been reset
- CRC Messages that have been dropped
- Checksum errors have been dropped
- Transmits have been deferred

The hourly updates are not only shown in the LocalView user interface, but are also automatically configured in the Wonderware Historian and presented as graphs and charts in the Wonderware Information Server, which is the basis for the on-demand reports.
Additionally, alerts are sent to Invensys technical support experts when alarm thresholds are exceeded, and these remote engineers analyze the data to determine the root cause and guide corrective activity. This capability facilitates proactive and reactive diagnostic analysis to help maximize the operational efficiency of the automation system and minimizes downtime.

RemoteWatch services capabilities include:

- Proactive Performance Monitoring
- On-demand status reports
- Resource trends and graphs
- Reactive Diagnostic Services

**BEST AVAILABLE PLATFORM FOR SECURE REMOTE CONNECTIONS**

These embedded features allow us to:

- Monitor critical resources to prevent process degradation
- Set up a platform for advanced diagnostic tools (i.e. Mesh or Nodebus analysis)
- Stage critical system patch
- Establish a Diagnostics ‘Tool Box’

**OPTIONAL ENHANCEMENTS**

In addition to the embedded RemoteWatch features, there are several optional capabilities that can be layered on top of the RemoteWatch services:

- Automated backup to the RemoteWatch Server’s RAID Drives
- NetSight Console Mesh Switch monitoring software which enables local and remote engineers to troubleshoot network issues
- Data Diode one-way outbound communication device located between the I/A Series system and the RemoteWatch Server providing a higher level of security from cyber attacks
- Invensys smoke-tested Microsoft OS Patch delivery to the RemoteWatch Server for local installation
- Delivery of Invensys Quick Fixes to the RemoteWatch Server

**PROACTIVE PERFORMANCE MONITORING**

The RemoteWatch server’s applications monitor system performance. Using scripts to collect and analyze system data, RemoteWatch looks for set points or anomalies that it will “tag” for further examination.

- Disk Partition Information
- 50 series, 70 series platform data
- Token ring counters
- Shared memory usage
- Control station resources and database linkages
- Object Manager (OM) resource usages
- Station performance counters

The RemoteWatch applications are configured to access system and network resource data, including:

On an automated schedule, the extracted dataset including the tagged data is transferred to the Invensys Remote Services Operations Center. Information received may be flagged as an issue, identified as non-critical or identified for further monitoring or may be deemed serious and immediate corrective action may be taken.

A copy of the extracted dataset is stored on the RemoteWatch Services server at the client site, and the transmitted data is held at Invensys for a period of time, dependant on size. If a developing issue is identified as needing action, an Invensys Remote Services engineer will contact client personnel who have Remote Services authority. Upon mutual agreement, corrective activity will ensue. Either an Invensys engineer will guide system personnel to make necessary changes or Invensys may remotely apply a correction to the client system, if permitted by the client.
ON-DEMAND REMOTEWATCH REPORTS

With the release of RemoteWatch V4.0, we have instituted local collection, historization and presentation of the resource data sent from the I/A Series system. A Wonderware Historian and Information Server acts as a unified web server that presents you with status information and historical data to allow you to make more informed decisions related to the maintenance and health of your system.

This is important because even if a trend has not developed to a point where it has reached a critical threshold, it may still be determined that action to return potential problem activity to a normal state is to the client’s benefit. This ability to review system health results in better management of system resources.

Analysis trending covers a defined timeframe that includes:
- Control Station processor memory usage
- Inter-Process Communication (IPC) connection availability
- Disk space availability

REACTIVE DIAGNOSTIC SERVICE

There may be an occasion when you wish to initiate a consultation with Invensys for technical assistance. If it is determined that remote connection is appropriate, Invensys will, with your permission, securely log on to the process control system. Authorization is requested prior to the log on session, and an Invensys engineer will be on the telephone with your designated staff as the connected session progresses. Once the root cause is identified, corrective action can be taken.

How the RemoteWatch server connects to the automation system and plant networks, and how it communicates with the Invensys Remote Services center.
A permanent connection to your system and having Invensys technical resources examining the issue, guiding your people and working towards a timely resolution, clearly benefits all parties involved.

Costly plant upsets may be averted and problems can be solved without sending an Invensys service engineer to site. If it is determined that a Field Service Representative is needed at site, then the individual will arrive with a clear set of actions to undertake upon arrival.

Additionally, replacement materials can be shipped in advance, ready for installation, when the service engineer arrives. These efficiencies result in faster resolution of system issues and sustained process performance.

SECURITY

Invensys employs the most secure technology available to protect against unauthorized access to the client’s system.

- HTTPS/SSL protocol provides end-to-end encryption and Key Exchange. This configuration, along with the client-server application software is used to implement a secure communication path connecting the RemoteWatch server at the client site and the Invensys Remote Services center server.
- All communication is initiated from the customer site and targeted to the Invensys Communication server.
- The data transfer mechanism between the client RemoteWatch server and the Invensys Remote Services center server uses IP connectionless data packets on the SSL port to transfer the data to the Invensys Communications server. The Communication server has two IP addresses, one for data transfer and another for remote access. The system architecture and the secure communication pathway prevent communication except between a single customer and the Remote Services Center.
- In addition to the security precautions described above, Invensys has physical infrastructure and staff security restrictions in place.
- All Invensys Remote Services infrastructure is physically secured, and only authorized staff is allowed access.
- All RemoteWatch (client site) and Remote Services center servers and workstations utilize McAfee security software that is kept up to date with the latest virus protection patches and malware security.
- Only trained and certified Invensys Remote Services personnel are able to log into a customer site. Every engineer that logs in is identified by name and all activity is recorded.

GETTING REMOTEWATCH

When Remote Services are selected as a deliverable of the Customer FIRST Support Agreement, Invensys will supply, install and support RemoteWatch components that include a server-class machine loaded with connectivity hardware, client-server application software, Invensys software applications that enable the monitoring, managing and servicing of intelligent system components.

For more information on RemoteWatch, please visit: http://iom.invensys.com/EN/Pages/Services_RemoteServices.aspx