

Condition Assessment Manual

Automation System Checklist and Inspection Form



Revision 1.0, 1/11/2012

HAP – Condition Assessment Manual – Appendix 1.12 - Automation System Inspection Form and Checklist

Prepared by
MESA ASSOCIATES, INC.
Chattanooga, TN 37402

and

OAK RIDGE NATIONAL LABORATORY
Oak Ridge, Tennessee 37831-6283
managed by
UT-BATTELLE, LLC
for the
U.S. DEPARTMENT OF ENERGY
under contract DE-AC05-00OR22725

Automation System - Inspection Form

General Information:

Date of Site Visit: _____ Units: _____

Plant name: _____

Source/s of data: _____

Control System Description: (Include any advanced controls such as supervisory and/or central control)

Maintenance History / Major Upgrades or Installation Description:

HAP – Condition Assessment Manual – Appendix 1.12 - Automation System Inspection Form and Checklist

PLC(s), RTU(s) and/or Controller(s): (The term “controller” to be used interchangeably for PLC, RTU or Controller)

Physical location: _____ Description: _____

Controller Model: _____ **FW Version:** _____

Memory & CPU and % used: _____

Qty of this model: _____ Approx. Age of this model: _____ Redundant: Y / N

Configuration Software: _____ **SW Version:** _____

Quantity of tags, I/O, communications or other hardware or license limitations (and % used if applicable)

Communication Interfaces on CPU (Include protocol such as Ethernet, serial, Profibus, Modbus+, DN3, proprietary etc. Note what devices are on the other end of the communications. Note the number of ports on the CPU and note if they are used. If the software driver(s) is known, note that too.)

Port: _____ Protocol: _____ Connected to: _____

Port: _____ Protocol: _____ Connected to: _____

Port: _____ Protocol: _____ Connected to: _____

Additional CPU Port info: _____

Communication Interfaces other than CPU (Include protocol and connected devices as above)

Interface model: _____ # of Ports: _____

Protocol(s): _____

Connected device(s) to communications port(s): _____

Interface model: _____ # of Ports: _____

Protocol(s): _____

Connected device(s) to communications port(s): _____

Interface model: _____ # of Ports: _____

HAP – Condition Assessment Manual – Appendix 1.12 - Automation System Inspection Form and Checklist

Protocol(s): _____

Connected device(s) to communications port(s): _____

(Controller continued)

I/O Modules: _____

CPU Power Supply(s): _____ Redundant: **Y / N** Redundant source: **Y / N**

I/O Racks Power Supply(s): _____ Redundant: **Y / N** Redundant source: **Y / N**

Brief description of controlled processes: _____

General physical condition of controller and its components. Capable of expanding control w/o upgrade?

Additional controller information such as current vendor release versions and vendor support:

HAP – Condition Assessment Manual – Appendix 1.12 - Automation System Inspection Form and Checklist

HMI (Human Machine Interface):

Physical location: _____ Description: _____

Computer Model: _____ Version: _____

Memory/CPU and other info: _____

Qty of this model: _____ Approx. Age of this model: _____ Redundant: **Y / N**

HMI Software: _____ SW Version: _____

HMI Software last update: _____

Operating System: _____ OS Version: _____

Anti-virus Version: _____ Last update: _____ Updated regularly: **Y / N**

OS patches last update: _____ Updated regularly: **Y / N**

Ports and Services evaluated: **Y / N** Last date ports and services were evaluated: _____

Default passwords for OS deleted: **Y / N** Default passwords for HMI software deleted: **Y / N**

Does the HMI run under an OS administrator account: **Y / N**

Ethernet Communications or Serial Communications

Interface model: _____

Protocol(s): _____

Connected device(s) to communications port(s): _____

Interface model: _____

Protocol(s): _____

Connected device(s) to communications port(s): _____

Compare to current version of the OS and to the currently available HMI software. Indicate any limitations in the HMI software such as obsolescence, points that can be accessed, ease of use etc.

HAP – Condition Assessment Manual – Appendix 1.12 - Automation System Inspection Form and Checklist

General physical condition of the HMI and its components:

Additional HMI information:

HAP – Condition Assessment Manual – Appendix 1.12 - Automation System Inspection Form and Checklist

Data Server or SCADA:(The term server will be used to represent either in this list)

Physical location: _____ Description: _____

Computer Model: _____ Version: _____

Memory/CPU and other info: _____

Qty of this model: _____ Approx. Age of this model: _____ Redundant: **Y / N**

Server Software: _____ SW Version: _____

Server Software last update: _____

Server points, tags or other license restrictions: _____

Operating System: _____ OS Version: _____

Anti-virus Version: _____ Last update: _____ Updated regularly: **Y / N**

OS patches last update: _____ Updated regularly: **Y / N**

Ports and Services evaluated: **Y / N** Last date ports and services were evaluated: _____

Default passwords for OS deleted: **Y / N** Default passwords for Server software deleted: **Y / N**

Does the Server run under an OS administrator account: **Y / N**

Ethernet Communications or Serial Communications to the Server

Interface model: _____

Protocol(s) and/or Driver(s): _____

Connected device(s) to communications port(s): _____

Interface model: _____

Protocol(s) and/or Driver(s): _____

Connected device(s) to communications port(s): _____

Interface model: _____

Protocol(s): _____

Connected device(s) to communications port(s): _____

HAP – Condition Assessment Manual – Appendix 1.12 - Automation System Inspection Form and Checklist

Compare to current version of the OS and to the currently available Server software. Indicate any limitations in the Server software such as obsolescence, points that can be accessed, ease of use etc.

General physical condition of the Server and its components:

Additional Server information:

Process Control Ethernet LANs:

Are there two or more separate Ethernet LANs? **Y / N** If yes, start with the primary control LAN.

If only one LAN, then fill in primary control LAN. Secondary LANs are assumed to be I/O LANs.

Primary Control LAN (controller to controller and/or controller to server/SCADA communications)

Redundant network: **Y / N** Ring network: **Y / N** Flat network (no ring, no redundancy): **Y / N**

Router: **Y / N** Model: _____ Connects to: _____

Does the primary control LAN connect to a business network: **Y / N** (firewall in separate section)

Network Switches: (include model, number of ports, managed or unmanaged and qty)

Additional Primary LAN data:

Secondary Control LAN(s) (I/O to controller and/or to 3rd party devices)

Redundant network: **Y / N** Ring network: **Y / N** Flat network (no ring, no redundancy): **Y / N**

Router: **Y / N** Model: _____ Connects to: _____

Does the secondary control LAN connect to a business network: **Y / N** (firewall in separate section)

Network Switches: (include model, number of ports and qty)

Additional Secondary LAN data:

Ethernet Firewall(s):

Primary Control LAN Firewall

Model Number: _____ Version/Firmware: _____

Age of Unit: _____ Configuration software available to be reviewed: **Y / N**

Is the unit frequently updated with current patches or revision levels: **Y / N**

Encryption used: **Y / N** If using encryption, what method is used: _____

Who maintains the firewall and configures it? Give a brief history of its configuration and maintenance:

Secondary LAN Firewall (if used)

Model Number: _____ Version/Firmware: _____

Age of Unit: _____ Configuration software available to be reviewed: **Y / N**

Is the unit frequently updated with current patches or revision levels: **Y / N**

Encryption used: **Y / N** If using encryption, what method is used: _____

Who maintains the firewall and configures it? Give a brief history of its configuration and maintenance:

Wireless LAN(if used – security is built into the unit)

Model Number: _____ Version/Firmware: _____

Age of Unit: _____ Configuration software available to be reviewed: **Y / N**

Is the unit frequently updated with current patches or revision levels: **Y / N**

What security is used with the wireless LAN: _____

Who maintains the wireless devices and configures them? Give a brief history of its configuration and maintenance and what is monitored or controlled via wireless:

HAP – Condition Assessment Manual – Appendix 1.12 - Automation System Inspection Form and Checklist

GPS Clock(time clock dedicated to the control system)

Model Number: _____ Age: _____

Describe the source of the clock and where it is used in the control system (PCs, controllers, SOE etc.)

Historical Archive(long term data storage)

Software used: _____ Version: _____

Computer hardware used: _____

Describe the hardware redundancy (if any, such as RAID) and backups to storage: _____

How does the operator use historical data: _____

Alarming(process alarms)

Software used: _____ Version: _____

Third party software alarm optimization: **Y / N**: _____

How many alarms per hour per operator (weekly or daily average): _____

What percentage of the alarms are actionable by the operator: _____

Do the alarms appear optimized in that there are minimal to no nuisance alarms: **Y / N**

Is there a sequence of events or first out indication for the operator on key items: **Y / N**

How are the first out or sequence events viewable by the operator: _____

Are alarms used for determining maintenance and if so, how: _____

Have all the alarms been verified and tested as accurate: _____

How does the operator use alarm data: _____

Machine Condition Monitoring

Turbine Probes

Guide Bearing 2-axis vibration: **Y / N** Mfg. _____ Connected to AS (Automation System): **Y / N**

Comments: _____

Guide Bearing temperature: **Y / N** Mfg. _____ Connected to AS: **Y / N**

Comments: _____

Draft Tube Vibration (or head cover): **Y / N** Mfg. _____ Connected to AS: **Y / N**

Comments: _____

Speed (Keyphasor): **Y / N** Mfg. _____ Connected to AS: **Y / N**

Comments: _____

List other Turbine probes

Type: _____ Mfg. _____ Connected to AS: **Y / N**

Comments: _____

Type: _____ Mfg. _____ Connected to AS: **Y / N**

Comments: _____

Type: _____ Mfg. _____ Connected to AS: **Y / N**

Comments: _____

Type: _____ Mfg. _____ Connected to AS: **Y / N**

Comments: _____

Machine Condition Monitoring

Generator Probes

Guide Bearing 2-axis vibration: **Y / N** Mfg. _____ Connected to AS : **Y / N**

Comments: _____

Guide Bearing temperatures: **Y / N** Mfg. _____ Connected to AS: **Y / N**

Comments: _____

Air Gap: **Y / N** Mfg. _____ Connected to AS: **Y / N**

Comments: _____

Thrust Bearing Oil Film Thickness: **Y / N** Mfg. _____ Connected to AS: **Y / N**

Comments: _____

End Winding Vibration: **Y / N** Mfg. _____ Connected to AS: **Y / N**

Comments: _____

Core Vibration: **Y / N** Mfg. _____ Connected to AS: **Y / N**

Comments: _____

Stator Frame Vibration: **Y / N** Mfg. _____ Connected to AS: **Y / N**

Comments: _____

Thrust Bearing Pad Vibration: **Y / N** Mfg. _____ Connected to AS: **Y / N**

Comments: _____

Thrust Bearing Temperature: **Y / N** Mfg. _____ Connected to AS: **Y / N**

Comments: _____

HAP – Condition Assessment Manual – Appendix 1.12 - Automation System Inspection Form and Checklist

Generator Winding Temperature: **Y / N** Mfg. _____ Connected to AS: **Y / N**

Comments: _____

Partial Discharge Probe: **Y / N** Mfg. _____ Connected to AS: **Y / N**

Comments: _____

Cooling Water Flow: **Y / N** Mfg. _____ Connected to AS: **Y / N**

Comments: _____

List other Generator probes

Type: _____ Mfg. _____ Connected to AS: **Y / N**

Comments: _____

Type: _____ Mfg. _____ Connected to AS: **Y / N**

Comments: _____

Type: _____ Mfg. _____ Connected to AS: **Y / N**

Comments: _____

Type: _____ Mfg. _____ Connected to AS: **Y / N**

Comments: _____

Automation Check List				
Topic	Yes	No	N/A	Comments/Details
PLC or RTU or Controller - Hardware, Software and Security - List 1/2				
Term controller used to represent any of the 3 items				
Controller – Hardware version documented				
Controller – Currently supported vendor hardware				
Controller – CPU and memory loading. Sufficient CPU and memory available for controls upgrade. Scan cycle < 100 ms.				
Controller – CPU has capability for expansion for more I/O for controls upgrade.				
Controller – CPU tags, I/O or other similar license limits investigated. Note limitations if any.				
Controller – Can be configured, without a major upgrade, to a supervisory control system with automatic remote efficiency set points.				
Controller redundant. Note which controllers are redundant.				
Redundant power to controllers.				
Redundant power supplies on CPU rack (if applicable).				
Controller(s) configured to fully operate plant in supervisory mode.				
Controller configuration software is latest release.				
If there is compiled code in the controller, all the source code is available.				
The plant can operate in local automatic mode and can be accessed remotely for some automatic control.				

Automation Check List				
Topic	Yes	No	N/A	Comments/Details
PLC or RTU or Controller (Hardware, Software and Security) List 2/2				
Term controller used to represent any of the 3 items				
Configuration backups are performed regularly, kept secure and additional backups are stored at a secure off-site repository.				
Controllers are protected by strong passwords or in a locked mode by a key or switch to keep someone from being able to download an unauthorized configuration.				
Controllers default passwords have been disabled or changed to strong passwords.				
Controllers are physically secure. Protected physical access.				
Controller Ethernet communications have been checked for ports and services. No unneeded services are running. The ability to browse the controller is disabled or at minimum requires a strong password.				
All wireless communications are secure if wireless I/O communications are installed.				

Automation Check List				
Topic	Yes	No	N/A	Comments/Details
HMI (Human Machine Interface) - Hardware, Software and Security				List 1/1
Easy to navigate the interface. Operator is comfortable using the HMI.				
Clear graphical diagnostic tools to scan system integrity for controllers, I/O and network LAN.				
The amount of tags and graphics the HMI can support has been verified for the current version. Indicate values or limitations.				
The support and current release version of the HMI has been investigated. Indicate any issues.				
The amount of tags and graphics the HMI can support will support a move to a fully automated system.				
Grayscale graphics are used as described in automation best practices. Not critical.				
All HMI computers run under user accounts with strong passwords. No administrator accounts are used for normal operations. There are no easy to guess passwords.				
All HMI computers are current with anti-virus and software patches.				
All HMI computers on the network have minimized the ports and services to only those that are required and these are kept to the minimum by a scheduled verification of at least once per year.				
Alarming has been optimized in that operator actions in response to alarms are clearly defined and actionable.				
All HMI computers are running a currently supported operating system.				

Automation Check List				
Topic	Yes	No	N/A	Comments/Details
Data Server or SCADA - Hardware, Software and Security				List 1/1
Software Drivers to controllers, I/O or other devices are responsive. HMI to device response < 1 sec.				
The amount of tags, graphics and communications to devices the Server can support, has been verified for the current version. Indicate any limitations.				
The support and current release version of the Server software has been investigated. Indicate any issues.				
The amount of tags and graphics the Server can support will support a move to a fully automated system.				
Servers are running a currently supported operating system.				
All Servers run under user accounts with strong passwords. No administrator accounts are used for normal operations. There are no easy to guess passwords.				
All Servers are current with anti-virus and software patches.				
All Servers on the network have minimized the ports and services to only those that are required and these are kept to the minimum by a scheduled verification of at least once per year.				

Automation Check List				
Topic	Yes	No	N/A	Comments/Details
LAN- Process Control Network - Hardware, Software and Security				List 1/1
Redundant LAN or network ring that minimizes a single point of failure.				
A firewall is installed if there is a connection to a business network or to the Internet. Firmware/software patches are current.				
All LAN device configurations (such as firewalls and managed switches) are protected by strong passwords.				
Switches and other devices on the network are current firmware and supported by the vendor.				
Syslogs are created and stored for all devices that support logging and are reviewed regularly.				
Bandwidth is optimized for high data volume systems through switch configuration or other network tools.				
Network diagnostics are readily available to the operator.				
There are no dual honed connections to the business network or to the Internet from a computer connected to the process control LAN. (i.e. a computer which has multiple LAN connections of which one is to the Process Control Network.)				

Automation Check List				
Topic	Yes	No	N/A	Comments/Details
Historical Archiving and Reporting - Hardware, Software and Security				List 1/1
Historical archiving software is a current version and vendor supported. Indicate limitations.				
Tags are archived for easy retrieval for the past several years.				
The number of tags that can be stored for long term (> 2years) is sufficient per the license. Indicate limitations.				
The operating system is current and all patches and anti-virus are installed. Indicate limitations.				
Alarming is optimized and recorded for long term analysis. Indicate limitations.				
Historical files are backed up and stored off-site on a regular basis.				
Historical data is available at central control, engineering and to the local operators.				
A GPS clock is used to synchronizes alarms and controllers.				

Automation Check List				
Topic	Yes	No	N/A	Comments/Details
Machine Condition Monitoring				
Verified all condition monitoring probes in the field as practical.				
Verified which probes are connected to the control system.				
Verified which probes (primarily vibration and temperature) are used to automatically trip the unit.				
Is there communications from the condition monitoring system to the control system. If so, comment on type of communications.				
Verified security method of condition monitoring system.				
Advanced control, such as partial discharge, used in the control system.				
Condition monitoring data is stored in long term historical archive for analysis.				

Automation Check List				
Topic	Yes	No	N/A	Comments/Details
Instruments for Unit Performance Measurement - Metering				
Verified calibration data and maintenance records on all meters where practical.				
Verified HMI data values match meter displayed values or checked with operators who are experienced with both.				
Verified communications protocols where applicable.				
Checked quality of wiring and mounting where practical and time allowed. (optional)				
Documented model numbers and age of the meters where practical.				

Additional help in evaluation of systems:

This is important for security patches and upgrades. Windows XP SP 3 is the oldest operating system that continues to be supported (as of Dec. 2011). Older XP service packs (service pack 1 or 2) are no longer supported. Windows 2000 is obsolete. The following tables are helpful in evaluation of operating systems:

Windows XP	Support end date	Comments
No service pack	Sep. 2004	Obsolete product
SP 1	Oct. 2006	Obsolete product
SP 2	Jul. 2010	Obsolete product
SP 3 & 4	Apr. 2014	Currently on extended support. All support ends in 2014. Recommended to move to Windows 7 or Windows 2008 Server or newer before 2014.

Windows Vista	Support end date	Comments
Versions < SP2	Apr. 2012	Obsolete product after Apr. 2012
SP 2	Apr. 2017	Will go to extended support after Apr. 2012. All support ends in 2017. There are few control systems that use Windows Vista.

The only reason, in many cases, to upgrade the operating system is for security to install the current anti-virus and operating system patches. Upgrading the operating system does not necessarily improve efficiency. Windows 7 is currently expected to be on extended support already in 2015. This is a serious challenge for automation systems. Every few years a major service pack must be installed and/or the operating system must be updated to the newest version. The computer hardware currently in service may not be able to support the operating system upgrade and/or the vendor software may

Windows 2003	Support end date	Comments
All versions < SP2 or does include R2	2009	Obsolete product
SP 2 and R2	Jul. 2015	Currently on extended support. All support ends in 2015. Recommended to move to Windows 7 or Windows 2008 Server or newer before 2015.

not work with the latest Windows version. The automation system assessment is complex and can be highly subjective when taking into account obsolescence. Vendors usually have support contracts with Microsoft and other suppliers for extended support as it is difficult for vendors to constantly change their software to keep up with the constant operating system changes. The automation vendor support and its supplier agreements are a significant factor in the assessment.

For overall questions
please contact:

Brennan T. Smith, Ph.D., P.E.
Water Power Program Manager
Oak Ridge National Laboratory
865-241-5160
smithbt@ornl.gov

or

Qin Fen (Katherine) Zhang, Ph. D., P.E.
Hydropower Engineer
Oak Ridge National Laboratory
865-576-2921
zhangq1@ornl.gov