

# **Best Practice Catalog**

*I&C for Automation*



Revision 1.0, 12/05/2011

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

## Contents

1.0	Scope and Purpose .....	4
1.1	Hydropower Taxonomy Position .....	4
1.1.1	Plant Automation Components .....	4
1.2	Summary of Best Practices .....	8
1.2.1	Performance / Efficiency & Capability - Oriented Best Practices.....	8
1.2.2	Reliability / Operations & Maintenance - Oriented Best Practices .....	9
1.3	Best Practice Cross-references .....	10
2.0	Technology Design Summary.....	11
2.1	Technological Evolution .....	11
2.2	Design Technology .....	11
2.3	State of the Art Technology .....	13
3.0	Operation & Maintenance Practices .....	15
3.1	Condition Assessment.....	15
3.2	Operations .....	21
3.3	Maintenance .....	24
4.0	Metrics, Monitoring and Analysis .....	25
5.0	Information Sources:.....	27

## 1.0 Scope and Purpose

The primary purpose of an automatic control system or automation system is to allow through computerized control the automatic starting, stopping, safe operation, and protection of any equipment being controlled. In the context of this document, that equipment is a hydro generating unit and its associated components and auxiliaries. An additional benefit to an automation system is the ability to operate the hydro generating unit in a more efficient manner. Hydro generating units have been monitored and controlled by human operators for many years, both locally and remotely.. Unfortunately, the generating efficiency is hard to be adequately optimized by human operators due to the vast number of variable parameters spanning multiple systems that can affect unit efficiency and also because the variables can change rapidly. However, a computer system has the capability to analyze numerous parameters to determine optimum performance settings for a generating unit many times per second, which brings such a system a distinct advantage when trying to squeeze every last megawatt out of a limited supply of water resources.

### 1.1 Hydropower Taxonomy Position

Hydropower Facility → Powerhouse → Instrument and Controls → I&C for Automation

#### 1.1.1 Plant Automation Components

Performance and reliability related components of a hydroelectric plant instrument and control system will vary based on the automation supplier's design. This component listing is based on a PLC (programmable logic controller) or RTU (remote terminal unit), PC based data server, PC based HMI (human machine interface), conventional panel boards for manual control and SCADA (Supervisory Control and Data Acquisition) software. The term 'controller' will be used to represent either a programmable logic controller or current technology RTU.

PLC (programmable logic controller): The function of a PLC is the heart of digital control system with programming capability that performs functions similar to a relay logic system. A PLC consists of a CPU (central processing unit), memory, power supply and a means of communications to I/O and other devices. The software includes ladder, block, sequential, structured text and other logic programming to control devices.

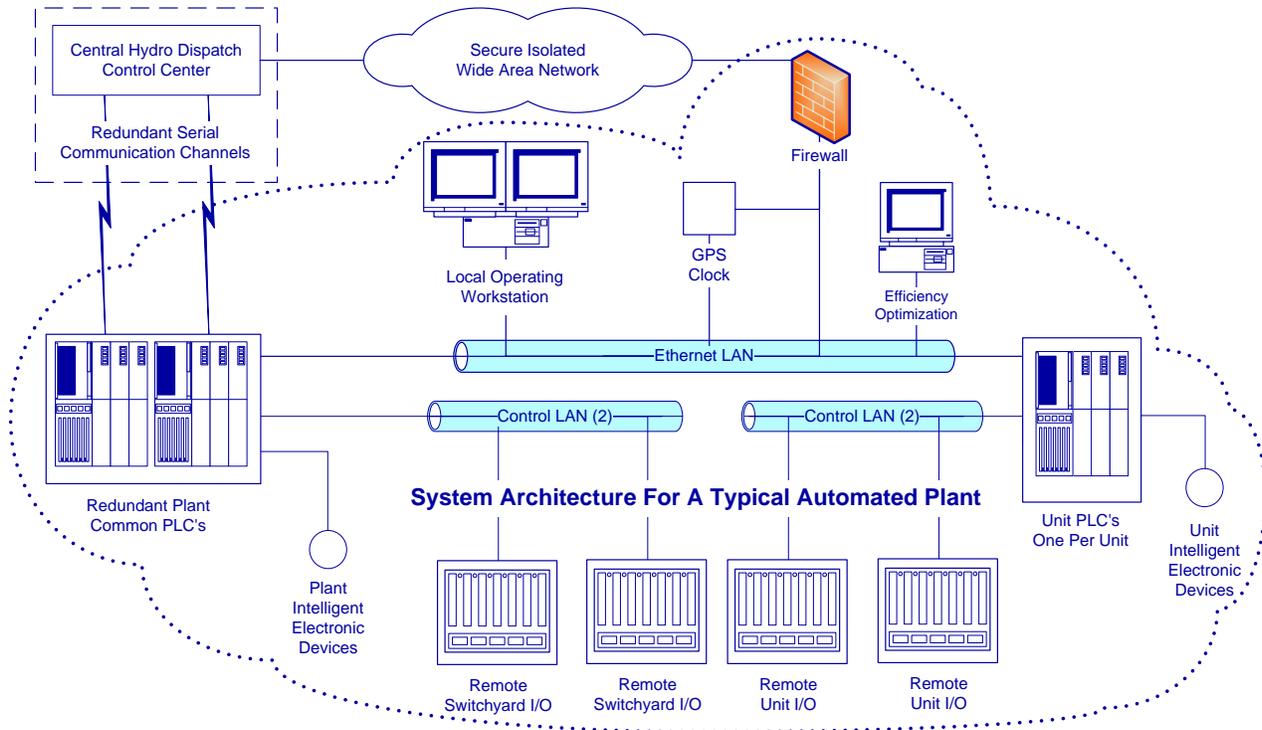
RTU (remote terminal unit): The function of an RTU is to collect data and is similar to a PLC. Sometimes, it may be termed as PLC depending on the vendor terminology. RTU is generally associated with older (prior to 1998) control systems with minimal control capabilities, though it may also be a perfectly acceptable term for a current vendor offering. Use caution when making a quick assessment of systems based on these acronyms of RTU and PLC. The RTU is not always a lesser controller.

Controller: This can refer to either a PLC controller or a current technology RTU.

HMI (human machine interface): The function of the HMI is to be the interface for the operator to the control system. The HMI is normally a PC as the client

portion of a client/server architecture. In some cases, the HMI and the server are the same PC.

**Data Server:** The function of a data server is to link to the controllers and the network to send data to the HMI and receive operator input from the HMI back to the controllers. The data server is normally a PC in a client/server application.



**Figure 1: Typical Control LAN**

**Network LAN (local area network):** There are normally two major networks in a hydroelectric control system.

- The TCP/IP network (Ethernet) links the server(s) to the HMIs, the controllers, data historians, firewall, and other Ethernet based devices. This is shown as the Ethernet LAN in Figure 1.
- The I/O network may also be Ethernet, though it is commonly a protocol used by the controls supplier such as Profibus™, Modbus™, DeviceNet™ etc. This is shown as the Control LAN in Figure 1.

- There are also secondary network connections to 3<sup>rd</sup> party devices tied directly to a controller through serial or Ethernet. This is shown as the links to the plant or unit electronic intelligent devices in Figure 1.

GPS Clock: This is for time synchronization in the control system.

SCADA (Supervisory Control and Data Acquisition): SCADA unfortunately tends to be an ambiguous acronym. Suppliers and end users have widely varying interpretations of what comprises a SCADA system. (See also RTU definition above.) As shown in Figure 2, an older SCADA system consists of RTUs (remote terminal units) that tie back to a central processor that primarily collects data and commonly uses proprietary communication protocols. Some controls suppliers refer to their current offerings (Dec. 2011) as a SCADA system, which has the same capabilities as a PLC based system or even is exactly a PLC based system. This can lead to some confusion. Generally, older SCADA/RTU systems (designed prior to 1998) have limitations in both logic handling and communications, which make them the candidates for upgrade. Over the decade, SCADA systems, PLC based systems and DCS (distributed control systems) have migrated towards being synonymous. These acronyms and their meanings are usually vary with the culture or industry in which they were initially installed.

I/O (wired input and output to field devices): The function of I/O is to send commands to devices or receive information from devices.

- Traditional Analog and Discrete I/O: These are wired inputs and outputs that use voltage or current representing the status of a device, values and/or set points.
- Hybrid I/O: Hybrid I/O varies from traditional I/O in that digital communications are carried on the same wires as the voltage or current. This digital information generally contains diagnostic information about the connected device. Devices that support HART™ on top of a voltage signal are an example of a hybrid.
- Smart I/O: This communication signal is entirely digitalized. The accuracy exceeds traditional analog and it contains diagnostic information about the connected device.
- Safety I/O: This varies from traditional I/O in that the controller periodically tests the I/O to verify that the controller hardware is functioning properly.

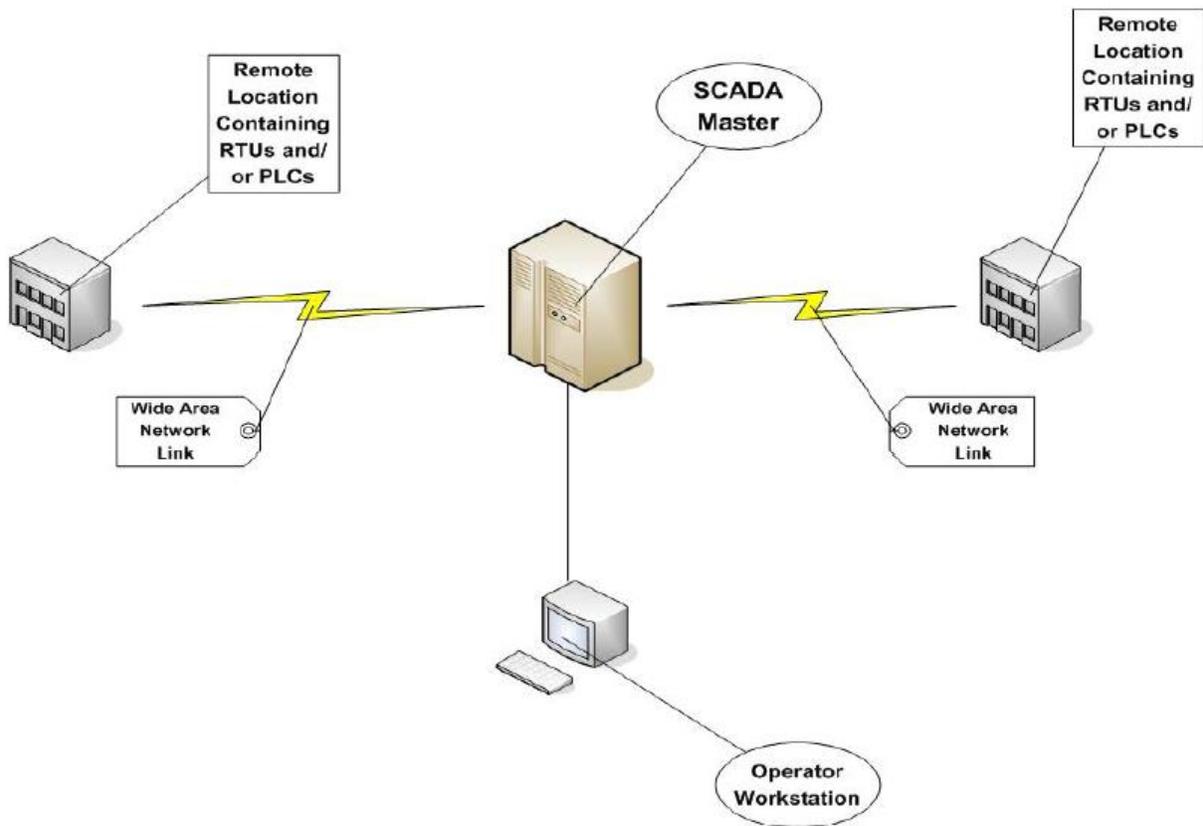


Figure 2: Common Older Style SCADA System [5]

Local Control (definition): Controls located at the equipment itself or within sight of the equipment. For a generating station, the controls are located on the unit switchboard-governor control station.

Automatic Control (definition): An arrangement of controls that provide for switching or controlling, or both, of equipment in a specific sequence and under predetermined conditions without operator intervention after initiation [1].

Non-performance but reliability related components of a control system.

Firewall: The function of a firewall is to restrict and protect the plant control network from outside unauthorized access. The firewall restricts communications in both directions protecting the process and data.

UPS (uninterruptible power supply): The function of the UPS is to provide temporary power to a system in case of main power failure. The UPS also acts as a power filter to protect control equipment. At hydro facilities, a large DC battery bank can also supply backup power through an inverter to the control system.

IDS (intrusion detection system): This device resides on the process control network to detect and log any intrusion attempts – failed or successful. Logs from firewalls can also be used as a limited form of intrusion detection.

Historical Archive: The function of the historical archive is to store historical information from the control system.

Reporting: The function of reporting is for GADS (Generating Availability Data System, as required by NERC - the North American Electric Reliability Corporation), production, scheduling etc.. This is often accomplished on the server or client.

Syslogs: This is an important function to meet NERC-CIP requirements as defined below. Syslogs record software events from the computers, firewalls and other network devices that support Syslogs.

Engineering Workstation: The function of the engineering workstation is to configure the software for the control system controllers, servers, HMIs and other controls equipment.

Efficiency Optimization: This is a program that runs on top of the control system to maximize efficiency of the plant.

## 1.2 Summary of Best Practices

### 1.2.1 Performance / Efficiency & Capability - Oriented Best Practices

- Use supervisory control that takes into account weather, demand, headwater and tailwater levels, fish habitat, outages, and other variables.
- Use advanced control algorithms, within the controller, to optimize generator efficiency.
- There should not be more than eight actionable alarms per hour per operator at any plant or for each operator at a central control facility.
- Test all software before downloading or installing.
- Design local control to be independent of the digital controller system in that the units can be operated from a bench board without the controllers and/or SCADA system in operation. Small generating units would be exempt from this practice.
- Compare long term trends, seasonal and annual, to measure performance. Figure 3 shows a complex control system LAN (local area network) with its own historian. This control system LAN ties back to a corporate LAN which has its own historian. This structure allows operators to create their own trends locally. The corporate historian allows technical personnel the ability to study long term data. Figure 4 shows a similar complex system in hierarchical form.

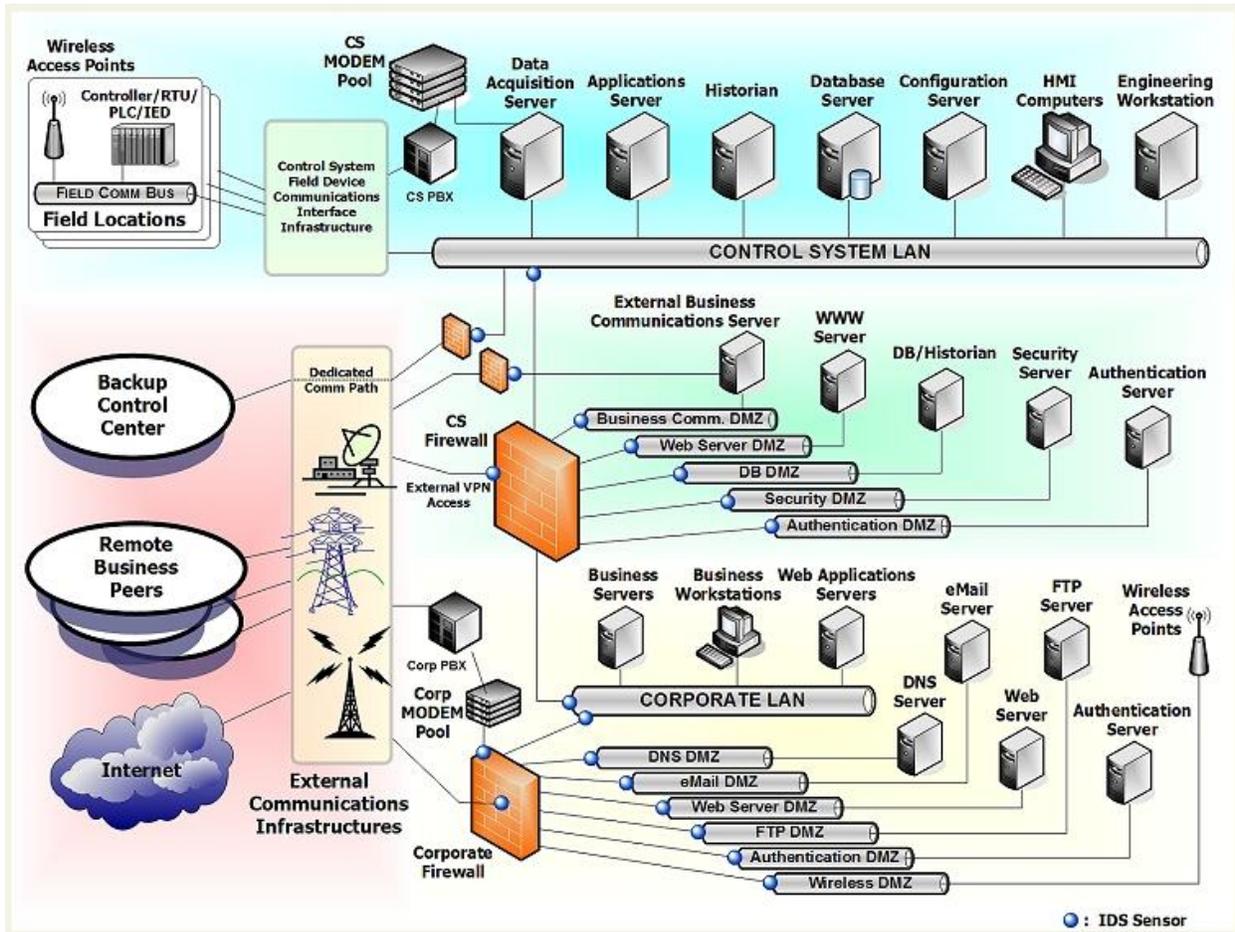


Figure 3: Control System at a Hydroelectric Plant, Showing Connections to a Central Location – Courtesy of CERT [4]

### 1.2.2 Reliability / Operations & Maintenance - Oriented Best Practices

- Use redundant power supplies and/or a UPS (uninterruptible power supply) or use the DC battery power, normally available at a hydroelectric facility, as an emergency backup.
- Use redundant controllers for critical control and communications
- Design the local control LAN to be redundant or in a ring.
- Design the I/O network (for remote I/O drops) to be redundant or in a ring.
- Units and all ancillary equipment should automatically go to a safe state on failure of a PLC or failure of critical instrumentation.
- Security is now part of reliability and is to be a part of the design, maintenance and upgrade of all parts of the control system.

- Use a firewall along with IPSEC (encryption) to protect the local control LAN.
- Periodically review the firewall Syslogs for intrusion attempts or unauthorized access. It is recommended to add an intrusion detection for large systems and at the central control.
- Analyze every port, service and application of all PCs on the control LAN. Remove or disable all unneeded ports, services and applications on those PCs. Review these PCs periodically.
- Train local maintenance to periodically monitor the health of the control system.
- Design the system so that online diagnostics are available and clear to operations.
- Monitor corrosion and temperature in cabinets.

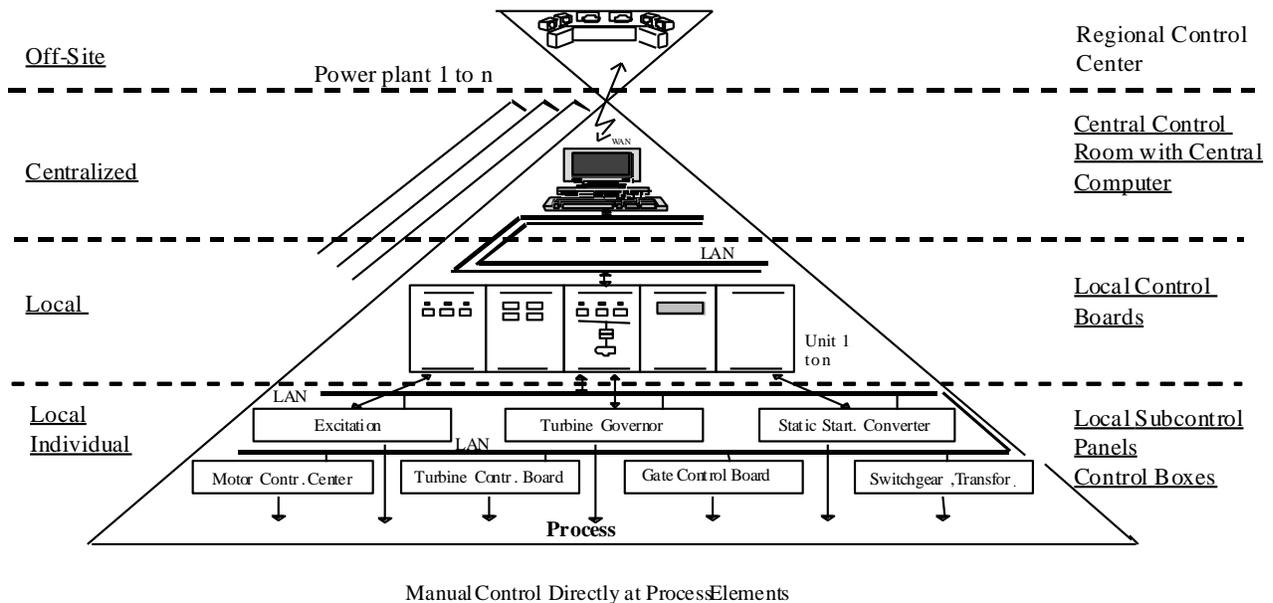


Figure 4: Central Control to Multiple Hydroelectric Plants [12]

### 1.3 Best Practice Cross-references

- I&C – Operator Base System
- I&C – Condition Monitoring
- Mechanical - Generator
- Mechanical – Governor

## 2.0 Technology Design Summary

### 2.1 Technological Evolution

Automatic control systems for hydroelectric units based on electromechanical relay logic have been in general use for many years and, in fact, were considered standard practice for the industry. Within the past few decades, microprocessor-based controllers have been developed that are suitable for operation in a power plant environment. These computer-based systems have been applied for data logging, alarm monitoring, and unit and plant control. Advantages of computer-based control include use of graphical user interfaces, the incorporation of sequence of events, trending, automatic archiving and reporting into the control system. The incorporation of artificial intelligence and expert system capabilities also enhance the system [2].

The initial upgrade for older hydroelectric plants has been from a system that relied primarily on electromechanical relay logic to a computer based Supervisory Control and Data Acquisition (SCADA) systems. In an era of deregulation and competition, management needs more information than ever before, and as quickly as possible, regarding its own costs, efficiency and the market price for energy. That need for information is leading to the upgrading and re-engineering of SCADA systems nationwide with new software and hardware that is more productive, reliable, and which utilizes open standards architecture [11]. The early SCADA systems used proprietary network communications and had rudimentary logic and information. Today's systems include more powerful controllers (PLCs or RTUs), open architecture (TCP/IP, DN3, Modbus™ etc.) and personal computers for HMIs (human machine interface).

### 2.2 Design Technology

Automation system design, operation, and maintenance have a major impact on unit efficiency, plant overall generation, and reliability. Best practice for the automation system begins with the ability to safely and securely control the entire facility both locally and remotely. The security of a control system supplants many previous design parameters, such as ease of remote network access, open wireless communications and easy physical access. Once a secure and fail-safe system is in place, the control system is then ready for optimization and high level control. Figure 5 shows a control system with firewalls and intrusion detection.

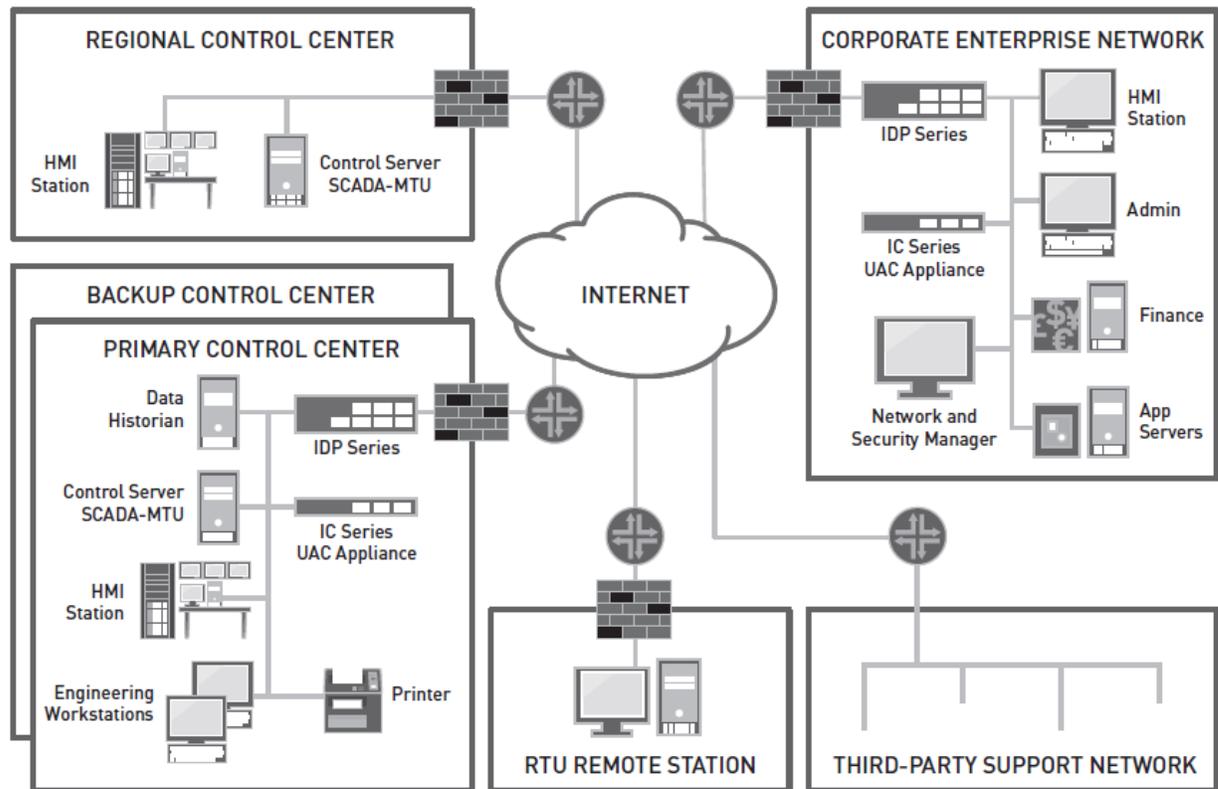


Figure 5: Securing a Typical Hydro Facility – Juniper Networks example [7]

### Cyber Security (some overlap with hardware and software design)

Government owned hydroelectric facilities cyber security policies will fall under federal compliance requirements with both NERC [13] (North American Electric Reliability Corporation) and FISMA [3] (Federal Information Security Management Act). The general rule is that larger government owned facilities and facilities considered ‘critical’ fall under the stricter NERC standards which include substantial penalties, if violations are egregious. The guidelines (NERC or FISMA) are determined by the management of each utility and their interpretation of the selection guidelines along with agreement from federal officials. Brief summaries of the two standards are listed in this document since they are crucial to the design or the upgrade of a government owned hydroelectric control system. NERC standards apply to private or public owned utilities that fall under the NERC domain. The standards are in the NERC-CIP 002-009 and in FISMA’s NIST 800-53 documentation. In particular, pay attention to appendix J of NIST 800-53 and NIST 800-82 [14].

At the 2011 “East Tennessee Cyber Security Summit”, several vendors remarked that 80% of security incidents are discovered by 3rd parties. These 3rd parties may be local law enforcement, FBI, banks or the media. The overwhelming number of corporate entities that were compromised did not have the ability to detect an intrusion nor a system in place to

track the intrusion. Intrusions may go on for weeks or months without being detected or reported. The importance of cyber security cannot be over stated.

### NERC Guidelines

NERC Critical Infrastructure Protection (CIP) standards relies heavily on documentation. Compliance with NERC-CIP should not be interpreted as being secure. [13]

## **2.3 State of the Art Technology**

A secure reliable automation system that supports high level supervisory optimization is no longer a difficult technical achievement. The proper design of the automation system will allow for fail-safe local control, redundancy, secure communications and automated scheduling with optimization. Optimization routines are readily available from 3<sup>rd</sup> party vendors or may be written in-house with software packages that are becoming easier to program and employ standard communication protocols.

As the state of the art technology, critical control systems that may cause physical harm, equipment damage or significant economic loss upon failure should have an appropriate level of redundancy. But, not all redundancy listed below is required or recommended for all systems due to the expense involved.

- **Redundant Power Source**

This is the most common form of redundancy and is recommended for all control systems. A redundant power source may be a UPS with the understanding that the UPS has a time limit in minutes based on the load and battery size. A UPS may also be used as a clean power source. Controllers commonly have the ability to be wired to dual power sources as a fundamental feature.

- **Redundant Controller**

If a redundant controller is not used, verify that a failure of the controller will not inflict equipment damage or harm personnel. The system must have a safe mode on a loss of the lone controller. The mean time between failures (MTBF) of a system with redundant controllers, redundant power supplies and redundant communications is nearly 10 times that of a standalone control system, see the result data in Table 1 from the study performed at the Large Hadron Collider Project in Europe using the Siemens 400 series PLCs [10].

**Table 1: Redundant Controller MTBF**

<b>Standard System</b>		<b>Redundant System</b>
1 CPU S7-414		2 CPU S7-414 4H (in separate racks)
1 Power Supply		2 Power Supplies (one in each rack)
1 Communications path to I/O		2 Communications paths to I/O
MTBF = 6.0 years		MTBF = 60.0 years

- **Redundant Servers and Clients**

In client/server architectures, it is critical to have redundant servers. A server can be removed from service for patches and security modifications without shutting down the system. Personal computers (servers) have a high failure rate compared to controllers and should always be redundant. HMIs (clients) should be redundant so that an operator will not be blind on the loss of a lone operator’s station. If the plant is normally operated remotely, a redundant operator station may not be required and its replacement may be made on the next business day without disrupting operations.

- **Redundant Networking**

The cost of networking equipment has dropped dramatically. It is recommended to have redundant networking on critical systems or use a network ring so that a single break in the network will not shut down communications. Dependency on a single network switch is problematic and should be avoided.

- **Redundant I/O**

This is rare for most hydro applications. It is more common to have critical data points, such as headwater level, to have dual sources. Vibration, temperature and other critical data also have multiple sources and are not dependent on a single input. Ideally these critical control inputs should be distributed among different I/O cards.

- **Safety I/O**

This I/O is continuously monitored by the controller through self-checks. The controller can detect a failed I/O point and respond appropriately to this failure. It is not a requirement to use safety I/O in the majority of hydro control systems. If it is available and the cost is not prohibitive, it is recommended.

- **Hot Swap**

An I/O or communications card should be replaceable without the need to power down the backplane (I/O rack) or without losing communications to the remainder of the cards mounted on the backplane.

- It is essential that the following functions can be carried out under backup conditions or failure of the main control system (PLC or RTU) [12]:

Emergency stop

Operation of spillways

Operation of high voltage circuit breakers and isolating switches

Starting and stopping of generator/turbine units

Operation of the intake gate/turbine isolation (shutoff) valve

Governor and excitation adjustments

### **3.0 Operation & Maintenance Practices**

#### **3.1 Condition Assessment**

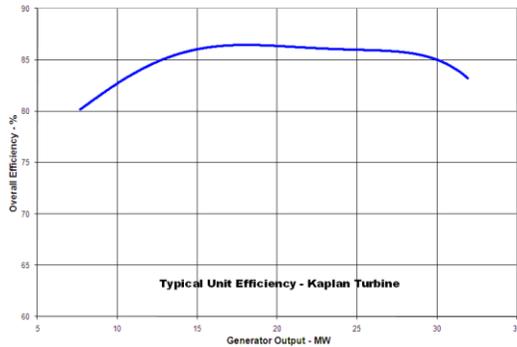
It is noticed that some key items are missing in control systems in even recent installations or upgrades of hydropower facilities in the United States (Dec. 2011). The items listed in this section will enhance IEEE Std 1249:1996 [1], which is now undergoing a revision. Engineering and operations should carefully consider all these items in the control system selection. The overall goal of automation system is dependability, as the majority of hydro facilities are not manned 24/7. This listing is to promote the best selection for a hydro control system based on the needs for maximum system availability, safety of equipment and personnel, system optimization, standardized communications protocols, ease of maintenance and security.

The first step in assessing an automation system would be the determination of the condition of existing equipment which must be controlled. A major portion of that assessment would be the condition and capabilities of any required sensors or feedbacks already present. The following information will be a guide through the various systems necessary and help determine any upgrades which might be required.

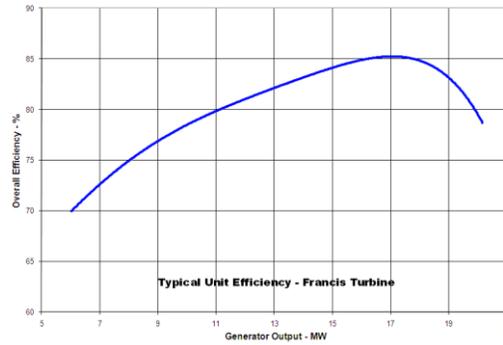
#### Turbines

While the actual best practices to be considered for hydro turbines is being covered in another guide, there is still important information which must be gathered in order to allow the automation system to operate a unit at optimum efficiency. Depending on the design of the turbine, different levels of testing will have to be performed to determine the overall operating characteristics of the turbine. For instance a set of efficiency curves will have to be developed for a Francis unit over a range of flow, headwater elevation, and tailwater elevation conditions. But for a Kaplan unit much more data must be collected to cover all the blade tilt positions as well as the range of water flow conditions. Each type of turbine will have its own specific variations but basically a complete set of turbine efficiencies must be available for input into the automation software. Additionally the flow instrumentation, headwater elevation instrumentation and tailwater elevation instrumentation must be accurate and must have data outputs which are compatible with the requirements for the automation

computer. Of course converters can be used if necessary. Typical efficiency curves for a Kaplan and a Francis turbine are shown below in Figures 6 and 7, respectively.



**Figure 6: Kaplan Turbine**



**Figure 7: Francis Turbine**

As can be seen from these curves the maximum efficiency point for a Francis turbine is extremely narrow while the Kaplan turbine has higher efficiencies over a much wider range. The Kaplan turbine achieves these wider ranges due to the added capability to alter the blade angle as operating parameters change. The control system needs to be assessed to verify that it can automatically control a unit in its highest efficiency range.

### Governor Systems

The condition of the governor system and its instrumentation is key to optimizing hydro unit efficiency. It really does not matter if the governor is digital, electronic, or mechanical as long as it is in good operating condition and has tight feedback loops. Obviously a digital governor has an advantage in the fact that it will be the easiest to interface with the automation system but as long as the governor has good tight response to control changes and accurate instrumentation to provide feedback to the automation system you can achieve optimal efficiency.

### Generator

While generator efficiency is mostly dictated by its initial design, the automation system must take into account the overall capabilities of the unit. Each generator has a specific capability curve which operating conditions must be monitored against to ensure no damage occurs to the unit. Of course these capabilities can be affected (lowered) by other components such as the excitation system, power cables, breakers capabilities, transformers, etc. The overall capability limits of the unit is vital information which must be considered by the automation software. In general the instrumentation required to monitor these limits will also be used by any efficiency calculations made by the system. A typical generator capability curve is shown below in Figure 8.

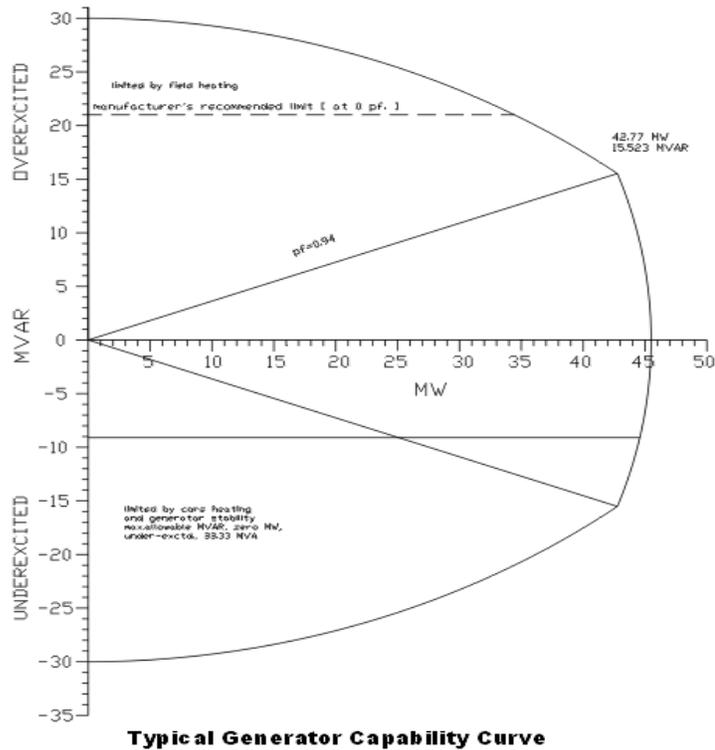


Figure 8: Typical Generator Capacity Curve

Excitation Systems

Again it really does not matter if the exciter is of digital or mechanical design as long as the equipment is in good working order and has adequate response times. However, a digital exciter again has an advantage in the fact that it will be much easier to interface with the automation system. Optimally the excitation system will have the capacity to operate the generator anywhere on the capability curve required. However, in some instances the existing exciter will not have the capacity required and those limits must also be considered in the automation system software.

Table 2 lists minimum instrumented inputs and outputs on an automated control system, such as a PLC, to control various devices or systems. The goal of having these levels of control is to allow fully automated control of a plant from a remote site with scheduling and minimize the need for operators at the plant full time. The existing system needs to be assessed to verify it can meet these minimal criteria.

**Table 2: Typical parameters necessary to implement automated control**

<b>Control Action</b>	<b>Inputs</b>	<b>Outputs</b>
Unit Start/Stop	Gate limit Gate position Breaker status Governor hydraulics Unit speed Unit protective relays Generator voltage	Brake release Gate operator Cooling water valve Exciter Start circuit Unit selection Breaker trip/close
Unit synchronizing	Unit speed Gate position Gate limit Breaker status Generator voltage Bus voltage	Breaker select Breaker closing Unit select Speed adjust Voltage adjust
AGC	Unit status MW MVar Unit protective relays Set point	Unit selection Power adjust
Synchronous condensing	Draft tube depression MW MVar	Power adjust Excitation Draft tube depression Unit selection
Turbine optimization	Head Blade angle Gate position MW	Gate operator Power adjust Unit selection
Trash rack control	Differential pressure	Trash raking system Power adjust Gate operator
Black start	Protective relays Bus voltages Generator status Breaker status Generator voltage Unit power	Generator start Unit synchronizing Breaker close (dead bus) Power adjust Voltage regulator Unit selection Breaker selection
Base load control	Unit status MW MVar Gate position Gate limit Set point	Power adjust Gate operator Unit selection

Control Action	Inputs	Outputs
Voltage control (AVC)	Unit status Breaker status MW MVar Bus voltage Set point Generator voltage	Voltage regulator Unit selection
Remedial action schemes	RAS initiation Generator selection Breaker status Unit status System frequency	Breaker trip Breaker selection
Forebay selective withdrawal	Water temperatures Gate position	Gate operator Unit select

Alarming

Audits, performed by the authors of this section, of hydroelectric control systems have found many installations with minimal alarming, or the alarming was initially configured but never optimized. Operators routinely ignored alarms and, as a result, missed critical information. Frequently, numerous alarms are presented to an operator when a single event occurs. Many of these alarms are excessive and may lead the operator to an incorrect action. These secondary alarms should be grouped into a single alarm, to a primary cause or inhibited based on the primary alarm. The existing alarming system needs to be assessed to see how it compares to the criteria in Table 3.

Controls studies have determined that the optimum number of actionable alarms that an operator can properly handle is 6-8 per hour [6 and 8]. Where alarms exceed this threshold, the alarming configuration or the operations of the system itself should be studied and corrected during engineering and operations. Alarms that require no action on the part of the operators should be investigated for removal from the system or placed automatically into a historical archive for reference only to free the operator. Table 3 lists reasonable goals for alarm systems.

Discrete devices, such as pressure switches, temperature switches, proximity switches, device statuses etc. should all be installed in a fail-safe manner. A failed device or an alarm state of the device will trigger an alarm. This is a fail-safe design. Where there are multiple discrete devices monitoring a single system, such as turbine vibration, the switches are recommended to be wired to different I/O cards. Just be mindful of not putting all critical measurements on one I/O card. If the I/O card fails, important information protecting the process can be compromised. Check the quality and type of discrete I/O of the existing

system. In some older facilities, the quality of the wiring may need to be assessed. Older wiring may have cracked or even missing insulation.

### Historical Data

Historical data is vital to troubleshooting and optimizing a control system. There are basically two types of historical trending. The first type is the near real-time trending, continuously displayed trend used by operators going back a few hours or minutes of a process and up to near real-time. The second type of trending is for long-term archiving. Audits of control systems have discovered the historical trending that was never archived or improperly configured, and/or the historical files were too short of duration to be of usefulness in troubleshooting or for optimizing. Assess the current ability to create long term trends and be able to export to a database for analysis.

All alarms should be trended and archived. Historical archiving of discrete points is recorded on an exception basis. Analog points should be archived based on common sense in terms of the deadband and frequency of data collecting. A slow-moving temperature measurement may only need to be collected every 5 seconds. A fast analog, such as flow or pressure, may be collected every second or even faster if the I/O is capable of scanning at high speeds (> 250 ms). The deadband of analog measurements to an archive is often set at 0.25% to 0.5%, which is the accuracy of most analog measurements. Audits of archives found analogs set at 2% or at even higher deadbands. This can lead to aliasing and mislead an investigator in analyzing events. Current historical archiving software is capable of data compression without significant loss of data. The cost of recording media has become minor.

Older analog inputs channels are frequently 12 bit. That is 0.25% accuracy for the full scale (1 bit out of 4095 total bits). The system may not be capable of obtaining a desired accuracy from the analog I/O.. The transmitter accuracy compounds the situation. Assess the analog input and output capability of the system. It should be at an absolute minimum of 13 bit accuracy with a preferred accuracy of 15 bits (or more). The accuracy of the measurement is an important factor in historical archiving, interpreting the data and controlling the process.

In modeling and optimizing generator performance, historical archiving for several years is required. Seasonal variations and overall control of the generator and dam performance can only be audited and improved using long term data.

**Table 3: ISA 18-2 Alarm Performance Metrics [6]**

Alarm Performance Metrics Based upon at least 30 days of data		
Metric	Target Value	
Annunciated Alarms per Time:	Target Value: Very Likely to be Acceptable	Target Value: Maximum Manageable
Annunciated Alarms Per Day per Operating Position	~150 alarms per day	~300 alarms per day
Annunciated Alarms Per Hour per Operating Position	~6 (average)	~12 (average)
Annunciated Alarms Per 10 Minutes per Operating Position	~1 (average)	~2 (average)
Metric	Target Value	
Percentage of hours containing more than 30 alarms	~<1%	
Percentage of 10-minute periods containing more than 10 alarms	~<1%	
Maximum number of alarms in a 10 minute period	≤10	
Percentage of time the alarm system is in a flood condition	~<1%	
Percentage contribution of the top 10 most frequent alarms to the overall alarm load	~<1% to 5% maximum, with action plans to address deficiencies.	
Quantity of chattering and fleeting alarms	Zero, action plans to correct any that occur.	
Stale Alarms	Less than 5 present on any day, with action plans to address	
Annunciated Priority Distribution	3 priorities: ~80% Low, ~15% Medium, ~5% High or 4 priorities: ~80% Low, ~15% Medium, ~5% High, ~<1% "highest" Other special-purpose priorities excluded from the calculation	
Unauthorized Alarm Suppression	Zero alarms suppressed outside of controlled or approved methodologies	
Unauthorized Alarm Attribute Changes	Zero alarm attribute changes outside of approved methodologies or MOC	

### 3.2 Operations

#### HMI - Human Machine Interface

The HMI is more than just a rehash of a P&ID (piping and instrumentation design drawing) with process descriptions. The software helps the operator in routine process management and optimization. The largest improvement in the HMI for operations has been in helping the operator respond to alarms. In the last few years emphasis has been placed in developing HMIs to assist the operator in abnormal situation management, which has been developed in a consortium with Honeywell [8]. The findings of this group have led to a radical graphical design change for operators. The normal color conditions for a process is gray and the

background is gray. Abnormal conditions change color based on the processes. Information such as efficiencies or key performance indicators often prompt the operator long before a serious alarm condition occurs. This group concludes that operators respond 40% faster to alarms than traditional displays with multiple colors and are less likely to make mistakes in responding to alarms.

### Optimization – Various Methods

Below are the minimum control capabilities in an operating system.

- Most Efficient Load (MEL)

This control mode will give the majority of efficiency benefits. The automation system will look at all the variables affecting unit efficiency, compare them to optimum, and automatically adjust the unit to achieve the highest possible efficiency for the operating conditions available. The system will continuously monitor all the parameters and, if any changes occur, it will automatically make necessary adjustments to again maintain maximum efficiency.

- Maximum Sustainable Load (MSL)

While this mode is not the most efficient, there are times, when the unit must be operated at maximum MW output due to other power system constraints.

- Fixed Turbine Flow

Occasionally there is a requirement to operate a plant at a fixed flow rate for periods of time. If there is only one unit at that plant, there is little opportunity during these periods to optimize efficiency. However, if there are multiple units at that plant, the automation system can match the individual unit efficiencies in such a way as to maximize the total flow requirement for the plant.

- Headwater / Tailwater Elevation Control

Occasionally there is a requirement to operate a plant such that a particular Headwater or Tailwater elevation is achieved. Just like the fixed turbine flow mode there is little opportunity to optimize efficiency if there is only one unit. But, as long as several units are available the automation system can match the individual unit efficiencies to maximize plant efficiency while maintaining the water elevations.

- Load Following / Automatic Generation Control

AGC is a topic which has caused much debate over the years among hydro utilities. The power system operators want to utilize hydro units for AGC due to the rapid response of the hydro units. Plant operation personnel tend to discourage that practice due to the belief that it causes increased maintenance requirements and reduced efficiency. Assuming that AGC is a requirement for the plant being automated, the automation system can take the load set point supplied by the power system and

calculate the most efficient loading of the individual units and still achieve the required AGC needs.

- **Condensing / Reactive Power Control**

Although there is no unit efficiency issue since no water is used in condensing mode, it is still an operating mode that must be considered in the software design as many units are operated this way for system voltage stability. In condensing mode, the turbine gates are closed and depending on the design of the unit, water is either naturally evacuated or a system of air compressors forces the water below the turbine blades. The unit is then operated as a synchronous condenser to supply reactive power to the power system for voltage control.

- **Automatic Load Reduction and Reinstatement for Temperature Considerations**

High temperature conditions for plant equipment is one of the fundamental issues that must be addressed. By supplying temperature sensors from plant equipment into the automation system, the system can monitor and trend those temperatures to ensure all components stay within their safe limits. One feature the automation system can accomplish is to allow the individual components to operate close to limits, but then if a temperature limit is reached, reduce loading to allow the temperature to stabilize at safe levels. Then as conditions change, which affect the cooling of that component, the automation system can automatically increase the load back to the desired level. Temperature sensors are almost always included in the generators, unit transformers, and critical bearings. Others critical to unit operation should be included as available.

### Sequence of Events and First Out

First out information should always be historically archived. This is critical information for operations and troubleshooting. The first out information for trending originates from the controller, not from comparing times of discrete alarms in the historical archive. Historical archiving software is usually not fast enough to analyze events that may take place for high-speed trips. First out alarming in high-speed applications, such as turbine control, is configured in the control system. These discrete inputs are most commonly scanned at 1 ms or faster. Standard discrete I/O is not normally scanned at this frequency.

The main controller should have a time sync program with a GPS clock. This accurate time should be shared in all the controllers and HMIs.

The control system software frequently has prebuilt SOE (sequence of events) blocks or first out blocks that capture the event that caused a system to trip or fail. This captured event is then historically trended and displayed to the operator for a quick analysis as to what just happened. A turbine can trip off line for many reasons. A high vibration trip will be programmed in a first out block along with temperatures, speeds, power, operator action etc. If a trip is caused by high vibration, it will be the trapped event in the first out block and displayed to the operator. The operator will be able to quickly comprehend the cause of the trip and take appropriate action. A restart of the tripped turbine will automatically reset the first out block and be ready to capture the next trip.

An alternate way of capturing first out events is to wire to an SOE device or high speed I/O card in parallel to the normal control I/O. The software in the controller (not the historical archiving software) will capture the individual times of each alarm. The actual time of the alarm will traditionally be in the message portion of the alarm and not the time the alarm appears in the archive. The operator will be required to look at all messages of the alarms in the alarm archive and search for the time of the first event that caused the trip. This is a common setup in systems that have evolved over the years and in older control systems that are still in service.

### **3.3 Maintenance**

#### Backing Up Systems – Disaster Recovery Plans

A disaster recovery plan is essential and must be part of a control system design. A disaster can occur from a fire, corrupt data, failed systems, poor configuration with a download or even sabotage. There should be a least two backup copies. On a scheduled basis (monthly or quarterly, depending on how frequently changes are made to the system) a backup copy should be made that is stored in a secure location offsite. There are companies that provide this as a commercial service to IT departments. Primary backups should be made after any change. Commercial software archiving programs are available to store backups. Images of PC based systems on a frequent scheduled basis is also recommended. Historical data should have a backup system as well. A plan for making backups should be made then adhered to.

It is critical to test a recovery system. There are numerous stories of backup systems that were found to be ineffective. In some cases the backup tapes or disks were found to be blank or the backup copies were corrupt.

Also, refer to NERC-CIP-009 “Recovery Plans for Critical Cyber Assets”

#### Patches and Software Updates or Changes

The NERC CIP-007-3 standard stresses the need to test modifications before installing the changes in the field. This is to minimize adverse effects on the production system or its operation. This includes verifying that no changes impact cyber security. Common practice to date has been to make changes in a control system without first testing on a bench or test system. The engineer or programmer has previously assumed no serious error or complications will occur with a change. This recommended practice of testing, even for a non-NERC site, will reduce errors in operations and create increased confidence from operators and management in the quality of process control software changes. In practice, the authors of this article have found the amount of time to test is quite minimal and has little impact on perceived productivity of the programmer when the time required to correct errors in the field with untested changes are taken into account.

Vendor patches, such as Microsoft, Siemens, Emerson, Honeywell etc, should be tested in a lab environment before field installation. Some vendors will test their software/hardware with recent patches and inform customers of the safe installation of the patches.

### Documentation

NERC CIP-003-3 standard outlines rigorous documentation requirements. All changes to a control system need to be documented in a systematic manner.

### Secure Passwords

All default passwords and/or administrative logins without passwords must be eliminated. All administrative passwords must be kept secure. The passwords should be ‘strong’. An ideal password is long (8 characters or more) and includes letters, punctuation, symbols, and numbers. It is permissible to write down passwords as it is difficult to memorize strong passwords. These written passwords should be stored in a secure place. These documents containing the passwords must be kept in a secure location. Refer also to NERC CIP-007-3 section 5.3.

### Predictive Maintenance Software – Condition Monitoring

Condition monitoring measures the health of an asset through monitoring and analysis of data. Common data monitoring points are vibration, temperature, wear, corrosion, pressure, proximity and flow. Newer instrumentation, such as a HART™ enabled digital control valve positioner, has digital feedback information to monitor hysteresis, valve stiction and instrument air pressure. Data is monitored in real time to alert operations to potential problems. Packages are available to predict required maintenance using these data points. Maintenance is performed only when required.

From Hydro World Vol. 19 Issue 3: “Most of the 1,560 MW of hydropower plants in Japan are unmanned. Operations and maintenance of these plants are handled using a wide-area maintenance system, in which one office manages multiple facilities. Unmanned plants are equipped with remote monitoring systems that continuously record data from various devices, such as tailrace level, turbine discharge, and generator vibration. Condition-based maintenance is used...

Extending the periodic inspection and overhaul cycles makes it possible to reduce the number of maintenance staff. Reducing the number of man-hours worked by engineers will enable their centralization to hydro plants and their allocation to maintenance with DEDE and other organizations. An estimated 2,025 man-hours can be saved by reducing the cycle of periodic inspections and overhauls. For example, before the demonstration, 2,130 man-hours were required for periodic inspection; this was reduced to 1,485 man-hours. For overhaul, 3,600 man-hours were required; this was reduced to 2,400 man-hours.”

## **4.0 Metrics, Monitoring and Analysis**

Various plant functions are required to be operated quickly and predictably in response to changes in process variables or operator commands. Failure of the control system to execute a programmed response within a specific time frame will result in operator frustration and dissatisfaction and may jeopardize the safety of personnel and equipment. To ensure that the control system responds in a manner commensurate with the expectations of plant operations,

the real-time ability of the control system should be defined in terms of the minimum time that it takes to process field events and operator-entered and program-generated commands.

Controls system response times are typically specified at the plant level. This excludes the interface with offsite control centers. The response times for offsite control will vary depending on the type and speed of the interconnecting communications link. In those situations, where the response time from offsite control centers is critical, it is necessary that the communications system be designed for secure, high-speed transmission with the plant control system.

The response time of the control system will depend on the system loading at the time of the event or control action as defined by its CPU and network load rate.

The CPU load rate is typically computed as a percentage of CPU capacity for "normal" and "worst case" system loading scenarios. A normal operating scenario is defined to be one where all field values are being updated at the required periodicity, a minimum number of active windows are open at the operator interface, communications are in normal configuration, application programs are in operation, and normal plant start/stop operations are being undertaken. A "worst case" scenario is typically a case where there are multiple unit trips in a short period of time. Such a condition has the effect of increasing the number of I/O (either field devices or operator-generated commands) that are simultaneously changing state.

Typical CPU load rates for normal operating scenarios are in the range of 40-60%. Some controllers set a percentage of CPU for logic and another percentage for communications. For worst-case loading scenarios, the CPU load rate will typically vary between 50-75% total. The network load (TCP/IP) should be less than 30% in the worst case scenario.

The time interval between the moments that a command is issued at the operator interface to the time the feedback (such as motor status) is displayed at the HMI should not exceed 1-2 seconds.

The time interval between the moments that a command has been issued at the operator interface to the time that the command is transmitted to the field device should be under 1 second. Ideally, discrete commands should be transmitted to the device in less than 200ms. The majority of I/O device drivers place a priority on write commands (write commands or operator inputs will normally execute before read commands) so that there is a quick response in the field to an operator screen input.

The time interval between the moments that a status change occurs at an input at the control system I/O to the time that the status change is displayed at one of the operator interfaces, should not exceed 1-2 seconds.

Update times to the system-wide database should be less than 1 second and typically range from 100 to 500 ms, depending on the type of I/O (digital input, analog input, or accumulator) and system loading.

Intrusion detection has historically been strictly an IT (information technology) function. This is falling upon process control engineers now. Intrusion detection logs should be automated and inspected by the process control engineer and IT. There should be no successful intrusion attempts.

Syslogs and firewall logs have also been an IT only function. Process control engineers should review these on a periodic basis.

Actionable alarms should not exceed 10 per hour. Ideally these alarms should not exceed 6 per hour per operator.

## 5.0 Information Sources:

Baseline Knowledge:

1. IEEE Std 1249:1996, *IEEE Guide for Computer Based Control for Hydroelectric Power Plant Automation*.
2. IEEE Std 1249:2010 working copy, *IEEE Guide for Computer Based Control for Hydroelectric Power Plant Automation*.
3. FISMA (NIST 800-53), *Recommended Security Controls for Federal Information Systems and Organizations*, NIST Special Publication 800-53.

The FISMA Implementation Project was established in January 2003 to produce several key security standards and guidelines required by the FISMA legislation. As a key element of the FISMA Implementation Project, NIST also developed additional guidance (in the form of Special Publications) and a Risk Management Framework which effectively integrates all of NIST's FISMA-related security standards and guidelines in order to promote the development of comprehensive, risk-based, and balanced information security programs by federal agencies. The Risk Management Framework and the associated publications are available at: <http://csrc.nist.gov/publications/PubsSPs.html>.

The National Institute of Standards and Technology (NIST) 800-53 provides recommended security controls of federal information systems and is used to determine the baseline security controls for the system. Federal IT systems must adhere to these security guidelines to comply with FISMA. The section that pertains to hydroelectric control systems is in appendix I of NIST 800-53.

4. United States Computer Emergency Readiness Team

The continuously updated site: [http://www.uscert.gov/control\\_systems/](http://www.uscert.gov/control_systems/)

The goal of the DHS National Cyber Security Division's CSSP is to reduce industrial control system risks within and across all critical infrastructure and key resource sectors by coordinating efforts among federal, state, local, and tribal governments, as well as industrial control systems owners, operators and vendors. The CSSP coordinates

activities to reduce the likelihood of success and severity of impact of a cyber attack against critical infrastructure control systems through risk-mitigation activities.

5. National Communications System, *Supervisory Control and Data Acquisition (SCADA) Systems*, NCS Technical Information Bulletin 04-1, Oct. 2004. [http://www.ncs.gov/library/tech\\_bulletins/2004/tib\\_04-1.pdf](http://www.ncs.gov/library/tech_bulletins/2004/tib_04-1.pdf)
6. *Hydro Life Extension Modernization Guide, Volume 7 – Protection and Control*, EPRI, Palo Alto, CA: 2000. TR-112350-V7.

*State of the Art:*

7. ANSI/ISA ISA 18.00.02-2009 “*Management of Alarm Systems for the Process Industries*”.
8. Juniper Networks, <http://www.juniper.net/us/en/local/pdf/whitepapers/2000276-en.pdf>, 2010
9. ASM Consortium, See <http://www.asmconsortium.net>. Refer also this white paper: [http://www.asmconsortium.net/Documents/OpInterfaceReqs\\_GoBeyond\\_Jan09.pdf](http://www.asmconsortium.net/Documents/OpInterfaceReqs_GoBeyond_Jan09.pdf) National Institute of Standards and Technology's (NIST) Advanced Technology Program assisted in funding this technology.
10. Hydro World Vol. 19 Issue 3
11. *CERN: Large Hadron Collider Project*, Power Point Presentation, [http://machine-interlocks.web.cern.ch/machine-interlocks/Presentations/PIC/Powering%20Interlocks%20Reliability\\_from\\_MZS.ppt](http://machine-interlocks.web.cern.ch/machine-interlocks/Presentations/PIC/Powering%20Interlocks%20Reliability_from_MZS.ppt)
12. Power Engineering, *Upgraded SCADA System Gives Hydro Plant Greater Reliability and Room to Grow*, <http://www.power-eng.com/articles/print/volume-103/issue-10/features/upgraded-scada-system-gives-hydro-plant-greater-reliability-and-room-to-grow.html>, 1999

*Standards:*

13. IEEE Std 1010:2006, IEEE Guide for Control of Hydroelectric Power Plants
14. National Electric Reliability Council NERC-CIP 002-009 Summary <http://www.nerc.com/>

CIP-002-3 “Critical Cyber Asset Identification”

Standard CIP-002 requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System. These Critical Assets are to be identified through the application of a risk-based assessment.

CIP-003-3 “Security Management Controls”

Standard CIP-003 requires that Responsible Entities have minimum security management controls in place to protect Critical Cyber Assets.

CIP-004-3 “Personnel and Training”

Standard CIP-004 requires that personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including contractors and service vendors, have an appropriate level of personnel risk assessment, training, and security awareness.

CIP-005-3 “Electronic Security Perimeters”

Standard CIP-005 requires the identification and protection of the Electronic Security Perimeter(s) inside which all Critical Cyber Assets reside, as well as all access points on the perimeter. All access points to the control system need to be documented. It is common for vendor or remote maintenance dial up access to be tied to a hydro control system. These should be eliminated whether a facility is under NERC or not. Access should be secured through firewalls and the use of VPNs. All access should be logged.

CIP-006-3 “Physical Security of Critical Cyber Assets”

Standard CIP-006 is intended to ensure the implementation of a physical security program for the protection of Critical Cyber Assets.

CIP-007-3 “Systems Security Management”

Standard CIP-007 requires Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as other other (non-critical) Cyber Assets within the Electronic Security Perimeter(s).

CIP-008-3 “Incident Reporting and Response Planning”

Standard CIP-008-3 ensures the identification, classification, response, and reporting of Cyber Security Incidents related to Critical Cyber Assets.

CIP-009-3 “Recovery Plans for Critical Cyber Assets”

Standard CIP-009 ensures that recovery plan(s) are put in place for Critical Cyber Assets and that these plans follow established business continuity and disaster recovery

15. FISMA (NIST 800-82), Industrial Control System Security, NIST Special Publication 800-82, [http://csrc.nist.gov/groups/SMA/fisma/ics/documents/oct23-2009-workshop/nist-ics3\\_10-23-2009.pdf](http://csrc.nist.gov/groups/SMA/fisma/ics/documents/oct23-2009-workshop/nist-ics3_10-23-2009.pdf)

*It should be noted by the user that this document is intended only as a guide. Statements are of a general nature and therefore do not take into account special situations that can differ significantly from those discussed in this document.*

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