

**SECTION 255500 - INSTRUMENTATION AND INTEGRATED CONTROL**

- 1.0 ASHRAE 90.1 Compliance: University of Pennsylvania buildings shall comply with the Commercial Energy Efficiency Requirements of ASHRAE Standard 90.1-2016. The ASHRAE 90.1-2016 compliance paths shall be followed instead of the International Energy Conservation Code (IECC) requirements as permitted by 2018 IECC Section 401.2 Application.
- 2.0 ASHRAE 90.1-2016 Compliance Requirements: Electrical Energy Monitoring. Measurement devices shall be installed in new buildings to monitor the electrical energy use for each of the following separately:
  - A. Total electrical energy
  - B. HVAC systems
  - C. Interior lighting
  - D. Exterior lighting
  - E. Receptacle circuits

For buildings with tenants, these systems shall be separately monitored for the total building and (excluding shared systems) for each individual tenant.

Up to 10% of the load for each of the categories shall be allowed from other electrical loads.

Recording and Reporting. The electrical energy use for all loads above shall be recorded a minimum of every 15 minutes and reported at least hourly, daily, monthly, and annually. The data for each tenant space shall be made available to that tenant. In buildings with a digital control system installed, the energy use shall be transmitted to the digital control system and graphically displayed. The data shall be displayed and stored locally in the building and shall not be put on the University SCADA system. The system shall be capable of maintaining all data for a minimum of 36 months. Exceptions include the following:

- A. Buildings less than 25,000 ft<sup>2</sup>.
  - B. Individual tenant spaces less than 10,000 ft<sup>2</sup>.
  - C. Dwelling units.
  - D. Residential buildings with less than 10,000 ft<sup>2</sup> of common area.
  - E. Critical and equipment branches of NEC Article 517.
- 3..0 All building mechanical systems shall be controlled via an electronic Building Automation System (BAS) interfacing with the existing University Supervisory Control and Data Acquisition (SCADA) system. The BAS shall be provided by one of the following automation equipment/system suppliers: Allen Bradley, American Automatrix, Automated Logic WebCTRL, Johnson Controls Inc. Metasys with NAE Architecture, Siemens Apogee Insight, and Smart Controls (LONworks). All commercial-grade electronic controllers shall be BACnet (Building Automation and Control Networks) Level 3 and OPC (Object Linking and Embedding for Process Control) compliant. All bidders shall be preapproved through the University of Pennsylvania prequalification process. All control companies shall follow Facilities & Real Estate Cyber Security guidelines which have been identified in Exhibit C: Cyber Security Policy (please see Appendix 1 at the end of this standard). All of the control companies identified below are to be contacted to bid on any control projects unless otherwise directed by the University of Pennsylvania Engineering Department:

- A. Automated Control Concepts Inc. (ACC)
  - B. Johnson Controls, Plymouth Meeting, PA Branch Office
  - C. Radius Systems, L.L.C.
  - D. Siemens Building Technologies, Blue Bell, PA Branch Office
  - E. Spry OSI, Inc.
  - F. Thermo Systems, L.L.C.
  - G. The Tustin Group
  - H. Proconex
- 4.0 Critical program spaces such as research laboratories, vivarium, or spaces with animal research shall be controlled by using Allen Bradley controls. Unless directed otherwise by the University of Pennsylvania Engineering Department, the following are approved Allen Bradley Controls Installers:
- A. Automated Control Concepts Inc. (ACC)
  - B. G7 Automation LLC
  - C. Proconex
  - D. Thermo Systems, L.L.C.
- 5.0 In general, for each project a BAS contractor shall furnish, install, wire, guarantee and service the entire BAS. The BAS contractor shall also be responsible for the selection, installation, and wiring of all components required for integration into the SCADA.
- 6.0 In general, the University prefers electric/electronic devices. If approved, pneumatic devices shall be limited to the following components:
- A. Electric-Pneumatic (EP) and Pneumatic-Electric (PE) switches
  - B. Control damper actuators and control valves actuators (control valves assemblies provided by control valve manufacturer)
  - C. Pilot positioning devices for control valve actuators and control damper actuators in modulating service
  - D. Current-to-Pneumatic (I/P) transducers
  - E. Pneumatic air supply and accessories such as air dryers and pressure reducing stations (where required)
- Electronic motors may be used as control valve actuators and control damper actuators provided they meet the torque requirements for closing/opening the device against the system pressure and the response of such actuators is adequate to maintain desired conditions of the process variable.
- 7.0 All new pneumatic systems shall include duplex compressors which utilize synthetic oil or are oil free, each adequately sized to handle 100% of the anticipated peak load, with compressor alternating controls to assure equal run time, with an automatic drain piped to the floor drain and

- operated by an electric solenoid valve, with a pneumatic tank sized to provide minimum storage capacity of 30 minutes in the event of power loss and with a mechanical filter dryer system capable of reducing the dew point temperature of the air to +20°F at a pressure of 25 PSIG. Air compressors shall be sized for 30% - 40% run time on an alternating circuit. An investigation of the existing building's air system shall be completed and assessed prior to the addition of new components. No pneumatic tubing shall be installed exposed to the elements or where it could be subject to freezing. Connection to existing control air source air must be approved by a University representative and designing engineer. These systems shall include duplex reducing stations with the appropriate manual valves to provide isolation for servicing.
- 8.0 All pneumatic tubing shall be run in Type "L" (high pressure) hard copper with soldered joints (95-5 solder). Compression type connections are permitted at connections to equipment only. Minimum tubing size shall be 1/4"0.025" wall thickness. Tubing shall be run in open conduits with a minimum of 20% available for spares. Tubing shall be identified at panel drops and end devices. Copper tubing connections to end devices shall utilize barb connections to plastic tubing.
- 9.0 All control valves (chilled water, condenser water, hot water, and steam) shall be of the throttling plug (water service), V-port (chilled water choke valve service) repacking type, or globe valves (steam service). Valves 2" and smaller shall have threaded brass bodies. Valves shall have unions installed before and after for service. Valves above 2" shall be flanged and have cast iron bodies. All valves shall be provided with stainless steel stems and trims, seats, plugs, etc. Plug types as follows:
- A. Steam - Linear characteristic – 1/3-2/3 for capacities 1,200 lbs/hr or greater. [Consider the use of V-port ball valves for steam service with no 1/3, 2/3 arrangement (300:1 rangeability)]
  - B. Modulating chilled water service for hydronic coils - Equal percentage plug.
  - C. Modulating hot water service for hydronic coils - Equal percentage plug.
  - D. Mixed water application service (non-coils) - linear characteristic.
  - E. Two position - Flat seat/quick opening.
- 10.0 Each project shall provide control panels in the quantities and locations necessary to properly access and house all control equipment. Panels shall be provided with hinged covers and key operated locks. Top conduit access to any panels is prohibited. Panel shall be located in a dry location and accessible from the floor level. All control panels locations shall be pre-approved by a representative of Facilities Operations. All control panels shall be located on the project coordination drawings. Refer to *Section 23010*. The A/E shall indicate all control panel power requirements on the contract drawings. All control panels shall be fed from a dedicated power source (emergency/UPS if applicable). All control panels shall have an electrical breaker and an available duplex outlet. All control panels shall have the appropriate primary and secondary circuit protection.
- 11.0 Prior to the design of the integration of the BAS into the SCADA, the A/E shall arrange a meeting with the University Engineering Department to discuss and resolve the following:
- A. Minimum required control points list and the points monitored and/or controlled by SCADA at the Operations Control Center (OCC).
  - B. Available capacity of existing DDC panels and nodes for connection to SCADA system.
  - C. The Owner required ATC/P&ID diagrams. Review of design shall be conducted via a meeting with the University Engineering Department prior to the final bid issue. A/E shall review BAS shop drawing submittals for compliance to the final bid issue design. The University Engineering Department shall approve the BAS shop drawings.

- D. How the respective system dynamic information is reported back via SCADA to the campus Operations Control Center (OCC). For new installations only, a network connection into the building subnet along with IP address, hostname, net mask address and default route address shall be provided by the University. These are required to get the system data from the new location to OCC.
- 12.0 The drawings and specifications shall, as a minimum, include the following requirements:
- A. General system description, system architecture, including sequence of operations, point listing, description and type, engineering units, device range, point alarm parameters, control panel locations, sensor locations, etc.
- B. Shop drawing submittal requirements, including the following:
1. Contractor shall provide as a minimum an individual drawing for each system.
  2. Drawings shall show all system hardware, control panels, field devices, electrical work as well as all BAS work with each drawing containing the following information:
    - a) Wiring type and method of installation.
    - b) Control tubing information.
    - c) Point numbers and termination numbering for each control panel.
    - d) Detailed Bill of Material with appropriate reference to section where product data is presented.
    - e) Sequence of operation. Including P&ID (Control) diagrams.
    - f) Hardwired, Calculated and Logical Point database listing, software addresses following nomenclature in appendix, wiring numbering, control/alarm, setpoints, and termination locations.
  3. Hardware Product Data:
    - a) The Contractor shall furnish complete documentation pertaining to hardware and all other equipment supplied including power requirements per control panel and end devices.
    - b) Contractor shall document all point connections at the control panels. Include all pertinent wiring, field device, hardware, termination modules and software data. Control panels are to be located by the A/E with final approval coordinated with the University.
    - c) Contractor shall document all I/O modules and communication cards installed in control panels. Include all pertinent data, including firmware/software versions, switch settings, and calibration data.
  4. Software:

Provide the following information pertaining to BAS software:

    - a) All programs pertinent to project and backup format with software used to create backup.
    - b) Operating system software on acceptable digital data media.
    - c) All software, hardware and licenses required to operate, maintain and modify the system controls. The University of Pennsylvania shall be specified as owner.
    - d) A list of systems requiring graphics. A written narrative shall detail the systems graphics requirements.
    - e) Indicate the BAS software that shall execute at the BAS panel/s independent of the SCADA system, the transmission link to the SCADA system or other BAS panel/s.
    - f) Table of Contents of routines that the Contractor shall use to implement the sequence of operations specified.

- g) A written narrative shall be detailed and include definitions of each variable and instruction contained in the line code.
- h) A list of the software points to be used to implement each setpoint and control PID tuning parameters, and any other software points used.
- i) A list of all variables and their meaning.
- j) A list of the routines provided in each control panel and their storage requirement.
- k) A written narrative showing the interaction of routines in each control panel including variables being transferred from routine to routine.
- l) Implementation of energy management routines.
- m) Wireless System Requirements (not preferred - allowed where approved)

5. Description of Points:

- a) Provide table(s) listing all points with item number as shown and the following:
- b) Respective control panel card/slot for each control panel and/or data gathering.
- c) Provide for all software points the following:
  - (1) Point name.
  - (2) Point function (shall include calculated points and also logical (virtual) points available through a digital interface (not hardwired).
  - (3) Alarm limits.
  - (4) Engineering Units
  - (5) Device range in engineering units

6. Field Devices:

- a) Specification data sheets including accuracy, calibration, and servicing information and quantities for all field devices.
- b) Tabulated information showing point number, field device, and data sheets reference for all points.
- c) Drawings of all local control panels including panel face layouts.

7. Electrical Work:

- a) Submit data sheet on each type of wire to be used and its specific job application (e.g. Signal Wiring, Communication, Data Communication, etc.).

13.0 Electrical Work Requirements:

A. General:

- 1. Wiring of all field devices and electrical devices to control panels. Panels shall not have top penetrations.
- 2. All communication wiring from existing SCADA system to new control panels.
- 3. All wiring of control panels including but not limited to EP's, I/P's, DPTs, pilot lights, relays, transformers and other miscellaneous devices as shown and specified.
- 4. All power wiring of field devices as required.
- 5. All end device control wiring as required.
- 6. All field devices, indoor and outdoor, except Room Temperature Transmitters shall have conduit connections made to them from junction boxes, with a minimum of 18 inches and a maximum of 36 inches of flexible metallic conduit ("Greenfield") (liquid tight for devices outdoors or otherwise exposed to moisture) with sufficient slack to allow for removal and/or servicing.

B. Signal Wiring:

1. All signal wiring shall be point to point wiring. No splices, terminal strips, or terminal blocks shall be permitted.
2. Signal wiring to all analog field devices, including but not limited to temperature transmitters (TT) , resistance temperature detectors (RTD), humidity transmitters (HT), current to pneumatic (I/P) transducers, shall be twisted, 100% shielded pair, minimum 18 gauge wire with PVC cover Belden #8760 or Advanced Digital Cable (ADC) part number 21802TSD. Wires are to be separate from any other wiring above 30 volts and shall be run in conduit.
3. Signal wiring to 3-wire RTDs shall be three (3) conductors Belden #8770 or Advanced Digital Cable (ADC) part number 21803TSD.
4. Signal wiring to digital field devices (for circuits of 30 VAC or less) shall be as specified herein for Low Voltage Control Wiring.
5. Signal wiring shield shall be grounded at control panel end only.

C. Communication Wiring:

1. Communication wiring shall be minimum three individually 100% shielded pairs (i.e. six conductors), minimum 18 gauge cable with overall PVC cover Belden #9773 or equivalent product approved by the University product of other manufacturers, run in conduit with no splices, separate from all wiring over 30 volts. Shield shall be terminated as recommended by control panel manufacturer. Contractor shall notify Owner/Engineer in writing within 60 days after award of contract if this is in conflict with shield termination recommended by the SCADA system or control panel manufacturer. The contractor may use fiber Optic cable or other type of wiring after review and approval by the University Engineering Department.
2. In addition to the requirements specified above, all communication wiring cables shall include a 100% redundancy shielded pair (two conductors) as unused spare conductors.
3. All PennNet network cabling shall be by Penn ISC.
4. Install repeaters in locked control panels and secure from unauthorized entry to the PennNet System.
5. All LAN cabling from BAS to SCADA nodes shall be high bandwidth cabling as approved by the University of Pennsylvania Engineering Department.

D. All wiring shall be provided in rigid metal conduit in exterior locations, in mechanical/ electrical rooms, and in utility areas up to 8 feet A.F.F. All other interior wiring shall be in electrical metallic tubing (EMT – compression type). All devices and equipment shall be mounted in minimum NEMA 1 enclosures and NEMA 4 for mechanical rooms. All control conduits shall be labeled appropriately as to control voltage. Conduit fill shall not exceed 40% capacity.

E. Low Voltage Control Wiring (30 VAC or Less):

1. Low voltage control wiring shall be minimum 16 gauge, twisted pair, 100% shielded with PVC over Belden #9316 or equivalent product approved by the University of other manufacturers run in conduit with no splices, separate from any wiring above 30 volts.
2. Any changes in wiring methods or materials must be approved by the University of Pennsylvania Engineering Department.

14.0 Field Devices:

A. Temperature Transmitters (TT):

1. All temperature transmitters shall be resistance temperature detectors (RTD 4-20 mA) with 2-wire or 3-wire circuitry. However, wall mounted thermostats can be thermistor type or RTD. Wall mounted thermostats shall be sealed and insulated to prevent false readings. RTDs shall be platinum type (100 ohm at 32° F) or nickel-iron type (1,000

ohm at 70° F) as manufactured by Minco, and calibrated for the operating range of the measured variable.

2. Bendable averaging type RTDs are preferred over duct mounted insertion type.
3. Duct mounted insertion type RTDs ("RTD Duct Probe") shall be rigid area averaging type, and shall include the sensing probe, holder, utility box and gasket to prevent air leakage and vibration noise. Minimum insertion depth shall be 80% of duct.
4. Bendable area averaging type RTDs ("RTD Duct Avg.") shall include the averaging sensor, utility box and gasket to prevent air leakage and vibration noise, and shall be used, as a minimum, in all air handling unit device applications. The mounting of the averaging RTDs shall be sufficient to cover the free area top to bottom. Each pass shall not exceed 12 in. from the previous pass.
5. Fluid immersion-type RTDs ("RTD Pipe Well") shall be used for all hot, glycol, chilled, condenser water sensing points or any other fluid and shall include RTD probe, thermo wells, and temperature transmitters. Connection head probe and connection head shall be removable without breaking fluid seal or removing any equipment or piping. Fluid immersion RTDs shall be installed on the top of the pipe in horizontal runs and at a positive slope on vertical runs to prevent condensation from flowing to connection head. Small bore pipe shall have thermo-wells installed at the elbows. All thermo wells shall be bottom third filled with heat conductive grease as manufactured by Dow Chemical. Thermo well shall be constructed of stainless steel and shall penetrate pipe 2/3 of the pipe diameter and the associated sensor shall match the thermo well size.
6. End-to-end (i.e. measured temperature at field devices versus displayed valued in engineering units at control panel operator terminals and as displayed at SCADA system operator terminals) minimum accuracy of all TT's shall be +/-1.0°F over 100 °F span, +/-0.5 °F over any selected 20 °F span and +/-0.25 °F over any selected 10 °F span.
7. Temperature transmitter sensing elements shall be provided in stainless steel case, epoxy sealed for moisture resistance (Minco model TT211, no exceptions).
8. All control sensing devices shall be installed to be accessible from the outside of the air stream, (AHU, etc.) served. Accessibility of all devices shall be verified during the shop drawing review.
9. Temperature transmitters shall have the following ranges:
 

a) AHU (air only)	0 to 100°F.
b) Chilled Water	30 to 80°F.
c) Condenser Water	30 to 100°F.
d) Hot Water Systems	32 to 250°F.
e) Steam Systems	100 to 500°F.
10. Mount RTDs as per manufacturer's requirements with insulated mounting brackets. Mounting RTDs with wire ties is strictly prohibited.
11. Provide NEMA 4 enclosures for devices mounted outdoors.

B. Transducers:

1. Pressure Transducers (I/P, E/P) - ("Cur/Press Tran, Volt/Press Trans"):
2. Pressure transducers: Bellofram Type 1000, Control Air Inc., or equivalent pre-approved by University Engineering Department.
3. Pressure transducers shall have the following performance and application criteria:
 

a) Supply Pressure	18 to 100 psig
b) Output Pressure	3 to 15 psig
c) Input Signal	4 to 20 mA (I/P), 2-10 VDC (E/P)
d) Independent Linearity	+ 1% F S
e) Terminal Based Linearity	+ 1% F.S.
f) Ambient Temperature	20°F. to 140°F.
g) Hysteresis & Repeatability	1/4% F S

- h) Maximum Air Consumption 0.100 SCFM
- i) Maximum Output Capacity 4.00 SCFM

C. Humidity Transmitters (HT):

1. Units shall be suitable for duct or wall (room) or outdoor mounting.
2. Unit shall be 2-wire transmitter with humidity sensor and shall operate on power requirements of 24V DC nominally unregulated. Unit shall produce linear continuous output of 4 to 20 mA for percent relative humidity (% RH). Sensors shall have the following performance and application criteria:
  - a) Input Range: 0 to 100% RH
  - b) Output Range: 4-20 mA
  - c) Accuracy (% RH): + 2% between 0 - 95% RH at 25°C.
  - d) Sensor Operating Range: -58°F to 185°F; (Maximum operating temperature for wall mounted unit: 150°F).
  - e) Minimum zero and span adjustments of + 15% of full scale.
  - f) Vaisala model or equivalent pre-approved by University Engineering Department.
  - g) Provide radiation shield for outdoor mounting applications.

D. Differential Pressure Switches:

1. Differential pressure switches (for 2 psi) and below shall be diaphragm operated with minimum 3-1/2" diaphragm to actuate single pole double throw (SPDT) or double pole double throw (DPDT) as shown and required. DPS shall be UL listed with minimum 3% repetitive accuracy. DPS shall have setpoint screw adjustment with stainless steel calibration spring. DPS shall be Dwyer Series 1910 (SPDT Type) or 1627 (DPDT Type) or approved equivalent product of other manufacturer.
2. For waterside systems provide DPS with isolation valves on both input lines (high and low).
3. Status Inputs for Fans: Differential-pressure switch with pilot-duty rating and with adjustable range of 0-5" W.C. – Cleveland. Exceptions: For fans below 1 HP utilize DC current switches in lieu of differential pressure switches. For induced radial dilution high plume exhausters of any HP rating utilize DC current switches in lieu of differential pressure switches.
4. Status Inputs for Pumps: Differential-pressure switch with pilot-duty rating and with adjustable pressure-differential range of 8 to 60 psig, piped across pump – United Electric. Exception: For pumps below 1 HP utilize DC current switches in lieu of differential pressure switches.

E. Low Temperature Sensor: Solid state low temperature cutout and an averaging resistance temperature sensor. Snap-acting, single-pole, double-throw, manual reset switch that trips if temperature sensed across any 12 inches of bulb length is equal to or below setpoint. Setpoint factory preset to 38°F and adjustable from 30°F to 44°F. Johnson Controls model A70HA-1C or approved equal.

1. Bulb Length: Minimum 20 feet.
2. Quantity: One sensor for every 20 square feet of coil surface.

F. Current Transmitters (Status Inputs for Electric Motors): Comply with ISA 50.00.01, current-sensing fixed- or split-core transformers with self-powered transmitter, adjustable and suitable for 175 percent of rated motor current.

G. Current Switches: Self-powered, solid-state with adjustable trip current, selected to match current and system output requirements.



- H. Flow Switch (Hydronic): Mount per manufacturer's requirements including upstream and downstream diameters required.
- I. Electrical Interface Devices:
1. Control Relays:
    - a) All control relays shall be UL listed with contacts rated for the application and mounted in minimum NEMA I enclosure.
    - b) Control relays for use on electrical systems of 120 Volts or less shall be Potter Brumfield Model KRPA or approved equivalent by UED.
    - c) Relays used for across the line control (start/stop) of 120V motors, 1/4 HP and 1/3 HP shall be rated to break a minimum 10 amp inductive load. Relays shall be Honeywell Model R4222D or approved equivalent product other manufacturers. [Verify model numbers – use A/B, PB, FD]
    - d) Control relays for use on electrical systems greater than 120 volts shall be rated for 600 volts and shall be Allen Bradley Bulletin 700, Type N or approved equivalent by the University Engineering Department.
    - e) No relays mounted inside MCC.
  2. Control Transformers:
    - a) Furnish and install control transformers as required.
    - b) Transformer loading shall not exceed 60% of capacity. All control transformers shall include primary and secondary circuit protection.
    - c) Maintain enclosure environmental temperature within transformer operating range as recommended by transformer manufacturer.
- 15.0 The project specification section shall define the provision for all drivers, gateways, and systems graphics necessary for complete system monitoring and operation. The project specification section shall identify the minimum system interface and interoperability expected between specific equipment controls and the DDC/PLC for each type of project, as well as the minimum number of graphic displays for each type of system.
- Provide as a minimum at least one system graphic for each major system (i.e. AHU, Hot water system, chilled water system) and at least one control graphic and one trend graphic for each system.
- 16.0 University Campus Operations Control Center (OCC) – SCADA System:
- The SCADA system via interface to BAS systems and other local control systems provides monitoring and control of all buildings on the University campus as well as chiller plants and power substations. The SCADA operators interact with all BAS and local control systems through an Iconics system using a windows platform. This operator interface package communicates with all of the different local systems and presents information from each in a unified form to the operators. The operators manipulate controlled variables for any local system from the SCADA through an integrator approved by the University Engineering Department. The following are approved Iconics Integrators:
- A. Applied Control Engineering, Inc. (302)738-8800
  - B. e-magic, Inc. (905)313-1025
  - C. G7 Automation LLC (609)325 6133

- D. Harris Control Panels, L.L.C. (610)274-8148
- E. O&M Engineering, Inc. (443)325-0400
- F. Thermo Systems, L.L.C. (609)371-3300
- G. Trijay Systems, Inc. (215)997-5833

The following table shows the current local control hardware and communication protocol in use at the University which integrates to the SCADA:

<b>Device</b>	<b>Protocol</b>
Allen Bradley PLC5 / KT Card	DH+
Allen Bradley PLC5E	Ethernet (DH485)
Allen Bradley LOGIX	DH+
Carrier / RS-232	Proprietary
GE 90 70 PCIM	Proprietary
Siemens Building Technologies / RS-232	Open System Protocol (OSP)/BACnet
Moore APACS	MBUS
Johnson Controls Inc. (NCM350)/NAE1	N1 Ethernet/BACnet
Schneider-Electric Andover Continuum	BACnet
Schneider-Electric I/A Series	BACnet
Automated Logic WebCTRL	BACnet
American Automatrix	PUP
LONworks	BACnet

- G. All new systems shall integrate to the SCADA via OPC protocol.
- H. All BAS or local control system contractors shall include the services of an Iconics SCADA system integrator within their bids to complete the systems integration to the SCADA in accordance with the SCADA Integration Specification Handbook (located at end of Instrumentation and Integration Control standard). All SCADA system integrators must be approved by the University Engineering Department.
- I. It is the responsibility of the system integrator to configure system graphics and control graphics for the new systems in accordance with the SCADA Integration Specification Handbook (please see Appendix 2 at the end of this standard). Alarms to be configured into the system are defined in the sequence of operation as well as in the Alarm Standards for SCADA System Interface. Historical trending of all key analog data is to be provided.

17.0 Sequences of Operation – “General Operation”

- A. All new BAS systems shall include all time-of-day scheduling to ensure that they are not

dependent on communications to the SCADA.

- B. ASHRAE 90.1 Compliance: Airside and Waterside systems shall be controlled in accordance with ASHRAE Standard 90.1-2016 sections 6.5.3 and 6.5.4.
- C. Sequence of Operation for AHU with Return Air
  1. System Off Mode: Supply fan off; return fan off; outdoor air damper(s), smoke/fan isolation damper(s), and relief air dampers closed; return air damper open. Humidifier control valve, reheat coil control valve, and chilled water cooling coil control valve closed (If preheat coil discharge air temperature or mixed air temperature is below 45°F, chilled water cooling coil control valve shall open). Preheat coil control valve shall modulate to maintain preheat coil discharge air temperature at preheat coil discharge air temperature setpoint (adj.).
  2. The BAS shall provide an associated time-of-day schedule that shall include an adjustable occupied start time and an adjustable occupied stop time for the air handling unit. The BAS shall provide optimal start/stop control with associated adjustable minimum/maximum morning warm-up/cool-down duration setpoints. The SCADA system shall have priority control over the BAS such that the above mentioned functions can be overridden by the SCADA system.
  3. Depending on the season, warm-up or cool-down modes may precede normal operation where the system operates on 100% recirculation mode until it reaches the preset temperature limit and then attains minimum outdoor air and relief air damper positions.
  4. The supply fan shall be started by the BAS (or by manual intervention through SCADA system). When supply fan is started the associated return fan shall start. Upon start command, minimum outdoor air damper shall open and if there is no minimum outdoor air damper, the economizer damper shall modulate to maintain outdoor airflow at the minimum outdoor airflow setpoint (adj.). The return air damper and the relief air damper shall take corresponding positions.
  5. The BAS shall linearly reset the air handling unit discharge temperature target between minimum and maximum discharge air temperature setpoints as the outdoor air dry bulb temperature varies between minimum and maximum outdoor air dry bulb temperature setpoints (adj.). On a rise of discharge temperature above discharge air temperature target, the economizer damper shall modulate open and the chilled water cooling coil control valve shall modulate open. When discharge air temperature falls below target the reverse shall occur. If outdoor air wet bulb temperature is greater than the return air wet bulb temperature, the outdoor air dampers shall maintain minimum position and the chilled water cooling coil control valve shall modulate to maintain discharge air temperature at the discharge air temperature target.
  6. Outdoor air damper shall also be modulated by a mixed air low limit controller. When mixed air temperature falls below the low limit mixed air temperature setpoint (adj.), the supply air controller shall be overridden and the outdoor air damper shall modulate closed and return air damper shall modulate open to maintain the mixed air temperature at the low limit mixed air temperature setpoint. The chilled water cooling coil control valve shall modulate to maintain discharge setpoint.
  7. Supply fan VFD shall start at minimum speed (if the system is variable volume). Supply fan VFD shall maintain a static pressure setpoint (adj.) via static pressure probes located 2/3 down duct. (Designer to select best sensors locations per duct configuration to avoid measurement errors due to turbulence)
  8. Return fan VFD shall be started at minimum speed and ramped up to maintain a CFM that is calculated by measuring supply fan CFM minus a fixed CFM offset or the return fan VFD shall maintain an adjustable percentage of supply fan CFM.
  9. Preheat Coil Valve Control: The preheat coil control valve shall modulate to maintain the preheat coil discharge air temperature at the preheat coil discharge air temperature setpoint at all times.

10. Preheat Coil Pump Control: The glycol/hot water main circulator keeps running at all outdoor air temperatures below 45°F (adj.) to maintain flow. When the outdoor air temperature falls below 45°F (adj.), the local preheat coil circulator pump starts. The pump shall shut off at outdoor air temperature above 50°F.
11. The supply air relative humidity target shall be reset to maintain the return air relative humidity at the return air relative humidity setpoint. The supply air relative humidity target shall not be permitted to exceed a high limit setpoint of 90% relative humidity (adj.). The humidifier control valve shall modulate to maintain the supply air relative humidity at the supply air relative humidity target. An airflow switch hardwired to the humidifier control valve shall close the humidifier control valve on loss of airflow. The airflow switch shall report status to the BAS. A humidity high limit controller hardwired to the humidifier control valve shall close the humidifier control valve on high limit humidity conditions (setting of 85% relative humidity, libraries only). The humidity high limit controller shall also report status to the BAS. For non-library applications, the supply air humidity sensor shall act as the humidity high limit controller described above (software only).
12. Freeze Protection: A duct mounted low temperature sensor mounted on the face of the cooling coil shall trip on low temperature and signal an alarm to the BAS. The low temperature sensor is hard wired to shut down the supply and return fans, open the return air damper and cooling coil control valve and close the outdoor air and relief air dampers on a trip.
13. Smoke Detection: Smoke detectors located in the supply and return air ducts signal an alarm, stop the supply and return fans through hard wired interlock, close outdoor air and relief air dampers, and open the return air damper when products of combustion are detected.
14. Engineer shall document the air handling unit shutdown sequence and describe all other safeties such as high/low static pressure safeties, duct smoke detectors, and low limit temperature switches (or low temperature sensors). Additional safety devices may be required to maintain and shut down the AHU to protect system from a catastrophic failure.
15. All safeties shall be hardwired to its associated control components such as the supply/return fans, outdoor air/return air/relief air/smoke/isolation dampers, control valves, circulator/freeze protection pumps to take their respective failsafe positions on safety alarms (exception: preheat coil control valve). All safeties shall protect the equipment whether the associated motor controls, such as motor starters and/or VFDs, are in the "Hand" or "Auto" position.

C. Sequence of Operation for Single Zone Classroom

1. System Off Mode: Supply fan off; return fan off; outdoor air damper(s), smoke/fan isolation damper(s), and relief air dampers closed; return air damper open. Humidifier control valve, reheat coil control valve, and chilled water cooling coil control valve closed (If preheat coil discharge air temperature or mixed air temperature is below 45°F, chilled water cooling coil control valve shall open). Preheat coil control valve shall modulate to maintain preheat coil discharge air temperature at preheat coil discharge air temperature setpoint (adj.).
2. The BAS shall provide an associated time-of-day schedule that shall include an adjustable occupied start time and an adjustable occupied stop time for the air handling unit. The BAS shall provide optimal start/stop control with associated adjustable minimum/maximum morning warm-up/cool-down duration setpoints. The SCADA system shall have priority control over the BAS such that the above mentioned functions can be overridden by the SCADA system.
3. Depending on the season, warm-up or cool-down modes may precede normal operation where the system operates on 100% recirculation mode until it reaches the preset temperature limit and then attains minimum outdoor air and relief air damper positions.

4. Supply-Fan Control: Scheduled occupancy program starts fan to run continuously during occupied periods. The supply fan shall be started by the BAS (or by manual intervention through SCADA system).
  - a) A differential pressure switch across each fan shall be used to determine the fan running status. If any fan fails to start, an alarm shall be issued to the BAS.
  - b) A low static pressure switch at the inlet of each fan and a high static pressure switch at the discharge of each fan are hardwired to shut down both fans if a static setpoint is exceeded. If a static pressure switch trips, a signal shall be issued to the BAS indicating which fan has exceeded the static pressure limit (for units 8,000 CFM and above).
  - c) When the supply fan is started, the return fan shall start and continue to run until the supply fan is stopped. Upon receipt of a signal from the Fire Alarm System (FAS), it shall be possible to run the return fan alone with all dampers in the system closed except for the relief air damper, which shall open. The interlock with the FAS shall be wired by others to a digital input on the BAS DDC controller. The control of the fans and dampers in smoke mode shall be through software command and shall not be hardwired.
5. Freeze Protection: A duct mounted low temperature sensor mounted on the face of the cooling coil shall trip on low temperature and signal an alarm to the BAS. The freeze sensor is hard wired to shut down the supply and return fans, open the return air damper and cooling coil control valve and close the outdoor air and relief air dampers on a trip.
6. Smoke Detection: Smoke detectors located in the supply and return air ducts signal an alarm, stop the supply and return fans through hard wired interlock, close outdoor air and relief air dampers, and open the return air damper when products of combustion are detected.
7. Outdoor air damper shall also be modulated by a mixed air low limit controller. When mixed air temperature falls below the low limit mixed air temperature setpoint (adj.), the supply air controller shall be overridden and the outdoor air damper shall modulate closed and return air damper shall modulate open to maintain the mixed air temperature at the low limit mixed air temperature setpoint. The chilled water cooling coil control valve shall modulate to maintain discharge at setpoint.
8. Mixed-Air Control: When the outdoor air enthalpy is lower than the return air enthalpy, the unit shall operate in economizer mode as follows: the return air, relief air, and outdoor air dampers shall modulate to control the discharge air temperature at the discharge air temperature setpoint (adj.). There shall also be a mixed air temperature controller to modulate dampers to maintain the mixed air temperature at the low limit mixed air temperature setpoint. When the unit is not in economizer mode the mixing dampers shall modulate to the minimum outdoor air position required to maintain return air CO<sub>2</sub> levels. Dampers shall modulate to maintain discharge air temperature with mixed air temperature controller being a low limit controller.
9. Filters: A differential pressure switch installed across the filter shall signal an alarm to the BAS when the filter differential pressure exceeds setpoint.
10. Preheat Coil Valve Control: The preheat coil control valve shall modulate to maintain the preheat coil discharge air temperature at the preheat coil discharge air temperature setpoint at all times.
11. Preheat Coil Pump Control: The glycol/hot water main circulator keeps running at all outdoor air temperatures below 45°F (adj.) to maintain flow. When the outdoor air temperature falls below 45°F (adj.), the local preheat coil circulator pump starts. The pump shall shut off at outdoor air temperature above 50°F.
12. Chilled Water Cooling Coil Valve Control: During occupied periods, when the fan is running the normally, the chilled water cooling coil control valve shall modulate to maintain chilled water cooling coil discharge air temperature at the chilled water cooling coil discharge air temperature setpoint. When in economizer mode, outdoor air damper

shall open first; then the chilled water cooling coil control valve shall modulate to maintain the chilled water cooling coil discharge air temperature at the chilled water cooling coil discharge air temperature setpoint.

- a) During shutdown periods, when the fan is off, the chilled water cooling coil control valve shall be closed.
- b) During occupied periods, CO<sub>2</sub> control shall be considered.

13. Hot Water Reheat Coil Control:

- a) During occupied periods, when the fan is running, the reheat coil control valve shall be modulated to maintain the reheat coil discharge air temperature at the reheat coil discharge air temperature setpoint. The space temperature sensor shall be used to reset the reheat coil discharge air temperature setpoint.
- b) When the unit is cooling and the return air relative humidity rises above setpoint, the chilled water cooling coil control valve shall modulate open and the reheat coil control valve shall modulate to maintain space temperature at the space temperature setpoint.
- c) During unoccupied periods, when space temperature falls below the space temperature setpoint, start fan and modulate reheat coil control valve to maintain the space temperature at the space temperature setpoint.

D. Sequence of Operation for 100 percent Outdoor AHU

1. System Off Mode: Supply fan off, dampers return to normal positions. Chilled water cooling coil control valve closed (If the preheat coil discharge air temperature is below 45°F, the chilled water cooling coil control valve shall open). Humidity control valve closed. Preheat coil control valve shall modulate to maintain the preheat coil discharge air temperature at the preheat coil discharge air temperature setpoint. (adj.). Glycol preheat system shall maintain glycol preheat supply temperature via a schedule to ensure at startup the unit shall not trip the low temperature sensor.
2. The supply fan shall start by the BAS (or by manual intervention through SCADA system). Upon a start command the outdoor air damper shall open first. After proof of outdoor air damper open, supply fan and associated exhaust fan shall start. AHU shall maintain discharge air temperature by using preheat coil control valve and chilled water cooling coil control valve. If discharge temperature is above target, the preheat coil control valve shall modulate closed and the chilled water cooling coil control valve shall modulate open. If discharge temperature is below target, the chilled water cooling coil control valve shall modulate closed and the preheat coil control valve shall modulate open. Preheat coil control valve shall also modulate to maintain preheat coil discharge air temperature at a minimum preheat coil discharge air temperature setpoint (adj.)
3. Preheat Coil Pump Control: The glycol/hot water main circulator keeps running at all outdoor air temperatures below 45°F (adj.) to maintain flow. When the outdoor air temperature falls below 45°F (adj.), the local preheat coil circulator pump starts. The pump shall shut off at outdoor air temperature above 50°F.
4. Freeze Protection: A duct mounted low temperature sensor mounted on the face of the cooling coil shall trip on low temperature and signal an alarm to the BAS. The low temperature sensor is hard wired to shut down the supply and return fans, open the return air damper and cooling coil control valve and close the outdoor air and relief air dampers on a trip.
5. Exhaust fan-off position isolation and smoke dampers closed. Upon rotation of fan the dampers shall open.
6. Supply fan VFD shall start at minimum speed (if the system is variable volume). Supply fan shall modulate to maintain supply duct static pressure to the supply duct static pressure setpoint. (adj.).

7. Exhaust fan VFD on startup shall modulate to maintain exhaust duct static pressure at the exhaust duct static pressure setpoint (adj.) (if the system is variable volume).
  8. The supply air relative humidity target shall be reset to maintain the exhaust air relative humidity at the exhaust air relative humidity setpoint. The supply air relative humidity target shall not be permitted to exceed a high limit setpoint of 90% relative humidity (adj.). The humidifier control valve shall modulate to maintain the supply air relative humidity at the supply air relative humidity target. An airflow switch hardwired to the humidifier control valve shall close the humidifier control valve on loss of airflow. The airflow switch shall report status to the BAS. The supply air humidity sensor shall also act as a humidity high limit controller to close the humidifier control valve on high limit humidity conditions.
  9. Smoke detectors shall stop the supply and reduce the exhaust fan operation to maintaining building safety.
- E. Sequence of Operation for Hot Water Radiation System (Constant Volume, Variable Temperature)
1. Hot water radiation pumps shall start when solar compensated outdoor air temperature falls below 55°F (adj.). Upon proof of hot water flow, the steam control valve or mixing valve shall modulate to maintain the hot water radiation supply temperature as determined by a schedule as follows; at 60°F solar compensated outdoor air temperature, hot water radiation supply temperature = 100°F (adj.) and at 0°F solar compensated outdoor air temperature, hot water radiation supply temperature = 180°F (adj.).
  2. When solar compensated outdoor air temperature is above 60°F (adj.), the pump shall be stopped and the steam control valve shall close.
- F. Sequence of Operation for Hot Water Reheat System (Variable Volume, Variable Temperature)
1. The hot water reheat pump shall run continuously. Upon proof of hot water flow, the steam control valve shall modulate to maintain the hot water supply temperature as determined by a schedule as follows; at 60°F outdoor air temperature, hot water supply temperature = 140°F (adj.) and at 0°F outdoor air temperature, hot water supply temperature = 180°F (adj.).
  2. Differential pressure transmitter shall control pump variable frequency drive to maintain the hot water reheat system differential pressure at the hot water reheat system differential pressure setpoint (adj.).
- G. Sequence of Operation for Building Chilled Water System
1. Secondary Chilled Water Return Temperature Target: The secondary chilled water return temperature target shall be reset to maintain a 12°F differential temperature between the primary chilled water supply temperature and the secondary chilled water return temperature.
  2. Chilled Water Choke Valve Control: On a rise in differential temperature between the primary chilled water supply temperature and the secondary chilled water return temperature above the 12°F setpoint, the building chilled water choke valve shall modulate open. On a fall in differential temperature between the primary chilled water supply temperature and the secondary chilled water return temperature below the 12°F setpoint, the building chilled water choke valve shall modulate closed.
  3. The building chilled water choke valve shall modulate closed when the building chilled water system ( $\Delta P$ ) is 18 PSIG (adj.).
- H. Sequence of Operation for Building Chilled Water Pump

1. Chilled water pump shall be started and stopped via operator command and/or automatically as follows: On a fall in building chilled water differential pressure 4 PSID below the building chilled water differential pressure setpoint, start chilled water pump. On a rise in building chilled water differential pressure 2 PSID above setpoint with the building chilled water pump VFD at its minimum speed setting, stop chilled water pump.
  2. Pump shall start at minimum speed and via a differential pressure sensor vary pump speed to maintain secondary chilled water system differential pressure at the secondary chilled water system differential pressure setpoint (adj.).
- I. Sequence of Operation for VAV Systems
1. On a fall in space temperature, space temperature sensor operating through DDC controller shall modulate closed the air volume damper to minimum position and modulate open the reheat coil control valve. Maintaining a temperature space setpoint.
  2. On a rise in space temperature the reverse of the above shall occur.
  3. Dual technology occupancy sensors shall be utilized to reset the associated VAV terminal unit's minimum airflow to 50% of the scheduled minimum airflow setpoint when the associated occupancy sensor(s) indicates no occupants are present in the zone.
- 18.0 Project Closeout Requirements
- A. Before control and monitoring systems are closed out a point-to-point verification, from the field devices to OCC shall take place. The system controls shall be tested at each unit level, AHUs, VAV/CAV terminal units, hydronic systems, etc. Components failed and replaced during the warranty period shall repeat point to point check out.
- B. There shall be a verification test of blackout startup of the system. Also operation under abnormal conditions, as emergency power, etc.
- C. The contractor shall submit three binders and electronic copies for each project including the following:
1. P&ID diagram for each system.
  2. Point listing, by system, with variable acronym, software address, point type, and engineering units.
  3. Logic step diagram system.
  4. Wiring diagrams by system including termination nomenclature, location and wiring identification.
  5. Calibration sheet (minimum 3-point calibration) for each device identified in the design as requiring calibration certificate, indicating calibration date and model number. Include equipment calibration certifications for calibration standards.
  6. Final tune-up list of parameters for each PID loops, including a time graph showing response to a disturbance of a 15%.
  7. All software, hardware and licenses necessary to operate, maintain, update modify the system. Including a final version of the software operating the building.
  8. Statement indicating all systems graphics are complete and accurate.
- D. Confirmation in writing by the controls contractor that:
1. All construction Requests for Information (RFIs) are resolved.
  2. All shop drawings, as built and submittals are completed.
  3. All required training is completed.
  4. All Testing, Adjusting and Balancing and commissioning activities are completed - Refer to Selections 23010 and 23990.



- E. OCC Graphics Sign-off sheet procedure:
1. Once the controls contractor has completed the graphics with the SCADA integrator, including a point to point, as well as reviewing them in person at the operator terminal in OCC, and feel that they are complete, they are responsible for creating a sign-off sheet with project description, Penn PM listed, and a location for the consultant, Facilities, and commissioning agent to sign off.
  2. The sign off sheet shall be sent to the Penn PM, and it is their responsibility to obtain the proper signatures from FRES, Consultant Engineer (if applicable), and the commissioning agent (if applicable). Any deviations identified will be attached to the form and sent back to the controls contractor for the contractor to address.

Appendix 1: Exhibit C: Cyber Security Policy



## Exhibit C: Cyber Security Policy

### Division of Facilities and Real Estate Services

#### 1. Introduction

This Cyber Security Policy (“Policy”) is a formal set of rules applicable to Vendor/Service Providers, including their agents and subcontractors as well as the employees of each of them (each a “User”) who have access to the cyber secure network controlled by the University’s Division of Facilities and Real Estate Services. This Policy (i) describes the technology and information assets that must be protected, (ii) identifies many of the threats to those assets and (iii) informs Users of (a) requirements for protecting the cyber secure network, including its technology and information, (b) the User’s responsibilities and privileges, (c) the acceptable uses of those assets, (d) the rules regarding Internet access, (e) limitations on a User’s access privileges, (f) the process for addressing violations of the policy, and (g) procedures for responding to incidents that threaten the security of the University’s computer systems and network. Failure to comply with this Policy is a basis for termination of the Vendor/Service Provider’s contract.

#### 2. What we are protecting

All Users shall protect the technology and information assets of the University from unauthorized access, theft and destruction. The technology and information assets of the University include the following components:

- Computer hardware, CPU, Email, web and application servers.
- System Software including operating systems, database management systems, and backup and restore software, communications protocols.
- Application Software used by the various departments within the University. This includes custom written software applications, and commercial off-the-shelf software packages.
- Communications Network hardware and software including: routers, routing tables, hubs, switches, firewalls, private lines, and associated network management software and tools.

These elements are collectively referred to in this policy as “Technology and Information Assets”

#### 3. User Responsibility

When making use of the University’s Technology and Information Assets, Users are required to comply with the University Policies on Acceptable Use of Electronic Resources, <http://www.upenn.edu/computing/policy/aup.html>.



Key provisions of the policy include the following:

- User accounts on University computer systems may be used only for business of the University and not for personal activities. Unauthorized use of the system may be in violation of the law, constitutes theft and may give rise to both criminal and civil liability.
- Users are responsible for protecting all confidential information used and/or stored on their accounts. This includes logon IDs and passwords. All Users are prohibited from making unauthorized copies of such confidential information and/or distributing it to unauthorized persons.
- Users shall not use the University's Technology and Information Assets to purposely engage in activity with the intent to: harass other users; degrade the performance of the system; divert system resources to the User's own use; or gain access to University systems for which the User does not have authorization.
- Users shall report any breaches in the University's computer security, any incidents of misuse of the University's Technology and Information Assets or violations of this policy to their immediate supervisor, who shall report it to the University's Facilities and Real Estate Services IT designee.

### **3.1. Use of the Internet**

If a User gains access to the Internet through the University's Technology and Information Assets, such access shall be used only in connection with providing contracted services to the University. Permissible uses include communicating via electronic mail with suppliers and business partners, obtaining information relevant to, or other purposes relevant to, the User's services to the University.

Internet service may not be used for transmitting, retrieving or storing any communications (i) of a discriminatory or harassing nature (ii) which are derogatory to any individual or group, (iii) that are obscene or pornographic, (iv) that are defamatory or threatening in nature, or (v) that constitute "chain letters". In addition, the Internet is not to be used for any illegal purpose or for personal gain.

### **3.2. Monitoring Use of Computer Systems**

The University has the right and capability to monitor electronic information created and/or communicated by persons using University computer systems and networks, including but not limited to e-mail messages and usage of the Internet. It is not the University policy or intent to



continuously monitor all computer usage by Users of the University computer systems and network. However, Users should be aware that the University may monitor usage, including, but not limited to, patterns of usage of the Internet (e.g. site accessed, on-line length, time of day access), and User's electronic files and messages to the extent necessary to ensure that the Internet and other electronic communications are being used in compliance with the law and with University policy.

#### 4. Access Control

A fundamental component of the Policy is controlling access to the critical information resources that require protection from unauthorized disclosure or modification. The fundamental meaning of access control is that permissions are assigned to individuals or systems that are authorized to access specific resources. Access controls exist at various layers of the system, including the network.

Each individual User is required to have a unique logon ID and password in order to gain access to the University's Technology and Information Assets. The User's password is to be kept confidential and MUST NOT be shared with any third party, including management or supervisory employees. All Users must comply with the following rules regarding the creation and maintenance of passwords where technically feasible:

- Password must not be found in any English or foreign dictionary. That is, do not use any common name, noun, verb, adverb, or adjective. These can be easily cracked using standard "hacker tools".
- Passwords should not be posted on or near computer terminals or otherwise be readily accessible in the area of the terminal.
- Password must be changed every 90 days.
- User accounts will be locked after 4 failed logon attempts.
- Passwords must contain a minimum of eight (8) characters
- The password must contain characters from at least three of the following four categories:
  - English uppercase characters (A - Z)
  - English lowercase characters (a - z)
  - Base 10 digits (0 - 9)
  - One special character ex: !@#



Users are not permitted to access password files on any network infrastructure component. Password files on servers will be monitored for access by unauthorized users. Copying, reading, deleting or modifying a password file on any computer system is prohibited.

Users are not permitted to logon as a System Administrator. Users who need this level of access to production systems must request a Special Access account as outlined elsewhere in this document.

Each User shall be required to fill out and sign a SCADA Access Authorization and Briefing Form in order to receive User Logon IDs and passwords. User Logon IDs and passwords will be deactivated as soon as possible upon expiration or termination of a Vendor/Service Provider's contract or if a User is terminated, fired, suspended, placed on leave, or otherwise leaves the employment of the University or Vendor/Service Provider.

A Vendor/Service Provider's Supervisors / Managers shall immediately and directly contact the University IT Manager to report change in user status that requires terminating or modifying employee logon access privileges.

Users who forget their password must call the University's Facilities and Real Estate Services IT designee to have a new password assigned to their account. The User must identify himself/herself by name, User ID and the name of its Vendor/Service Provider employer, to the University's Facilities and Real Estate Services IT designee.

Users will be responsible for all transactions occurring during logon sessions initiated by use of the User's password and ID. Users shall not logon to the University's electronic resources and then allow another individual to use the logged on device or otherwise share access to the University's systems. Passwords that are shared by Users will be deactivated.

#### **4.1. Connecting to Third Party Networks**

This policy is established to ensure a secure method of connectivity between Penn and all third-parties required to electronically exchange information with the University.

“Third-party” refers to Vendors/Service Providers (including the User), consultants and business partners doing business with the University, and other partners who have a need to exchange information with the University. Third-party network connections are to be used only by the employees of the third-party and only for purposes related to performing a Vendor/Service Provider's responsibilities under its contract with the University. The third-party will ensure that only authorized Users will be allowed to access University information. The third-party will not allow Internet traffic or other private network traffic to flow into the University's network. This policy applies to all third-party connection requests and any existing third-party connections.



## 4.2. Connecting Devices to the Network

Only authorized devices may be connected to the University network(s) on a case by case basis with approval from FRES IT. Authorized devices include but is not limited to PCs, workstations, and all other devices attached to the network that comply with the computer configuration guidelines of the University.

Users shall not attach devices to the network that are not authorized, owned and/or controlled by University. Users are not authorized to attach any device that would alter the topology characteristics of the Network or any unauthorized storage devices, e.g. thumb drives and writable CD's. All devices must comply with the latest patches and virus definitions as applicable, and will be considered unauthorized unless so complying.

## 4.3. Remote Access

Only authorized persons may remotely access the University network. Remote access is provided only to those employees, contractors and business partners of the University who have demonstrated a legitimate business need to exchange information with University systems through a secure ID. Users may not install software which provides remote access to the University's Technology and Information Assets unless authorized to remotely access the University network.

## 5. Data Privacy

Users shall use University data only for the purpose of fulfilling contractual duties. Users shall not share such data with or disclose them to any third party without the prior written consent of the University or as otherwise required by law. By way of illustration and not of limitation, User will not use such data for User's own benefit and, in particular, will not engage in "data mining" of University or end-user data or communications, whether through automated or human means, except as specifically and expressly required by law or authorized in writing by the University. All University or end-user data will be stored on servers, located solely within the Continental United States.

Vendors/Service Providers shall provide access to University data only to those employees and subcontractors who need to access the data to perform contractual obligations. Vendor's/Service Providers will ensure that employees and subcontractors who perform work under agreements with the University have read, understood, and received appropriate instruction as to how to comply with the data protection provisions of this Policy, and have undergone appropriate background screening and possess all qualifications required by the University prior to being granted access to the University or end-user data.



Vendors/Service Providers shall ensure that post-interview or post-offer, pre-employment background checks are conducted as to all employees (i) performing any services at locations on the University's campus or (ii) who would have access to the University's technology and information assets, University data or end-user data. These checks shall include a federal criminal background check, state or county of residence criminal background checks for all jurisdictions where the individual has lived for the past seven (7) years, and a previous residential address search. The criminal background check shall include any criminal convictions as well as any periods of judicial oversight occurring within the last seven (7) years.

Background checks shall include social security number trace and verification. Vendors/Service Providers shall review all background checks and shall exclude from participation in the performance of the Services any dishonest, dangerous or otherwise unqualified person.

Pre-employment background checks for any User shall be available to the University upon the University's request along with information regarding the analysis that Vendor/Service Provider performed when considering the information included in the background checks. The University will observe all relevant privacy laws in the handling and review of the reference and background checks. To the extent authorization is required from the employee in order to share reference and/or background checks with the University, Service Provider shall be responsible for obtaining such authorization. In discharging its responsibilities under this section, Vendor/Service Provider shall comply with and abide by all applicable laws including, but not limited to, the Fair Credit Reporting Act, Title VII of the Civil Rights Act of 1964 and the Philadelphia Fair Criminal Records Screening Standards Ordinance.

## **6. Data Security and Integrity**

All facilities used to store and process University data will employ commercial best practices, including appropriate administrative, physical, and technical safeguards, to secure such data from unauthorized access, disclosure, alteration, and use. Such measures will be no less protective than those used to secure Vendor's/Service Provider's own data of a similar type, and in no event less than reasonable, taking into account the type and nature of the data involved. Without limiting the foregoing, Vendor/Service Provider warrants that all University data will be encrypted in transmission (including via web interface) at no less than 128-bit level encryption. To the extent that Vendor/Service Provider records, including records of its services, (such as work orders) include University data, Vendor/Service Provider shall securely store such data in accordance with this section.

This Policy is intended to meet the NIST 800-53 series of standards, including the best practices for information security management, and standards for the establishment, implementation, control, and improvement of the information security management systems, and is more fully





expressed in the following University policy directives, copies of which are available to Vendor/Service Provider from the University's Facilities and Real Estate Services IT designee:

- Policy Directive on Access Authentication and Authorization
- Policy Directive on Audit and Accountability
- Policy Directive on Configuration Management and Change Control
- Policy Directive on Maintenance
- Policy Directive on Media Protection
- Policy Directive on Incident Response Plan

Users acknowledge that the User's compliance with this Policy is intended to meet these standards and directives, and Users shall not knowingly or negligently deviate from these standards and directives. User will provide to the University's employees and consultants, information reasonably requested by the University regarding Vendor's/Service Provider's security practices and policies. Vendor/Service Provider will use industry-standard and up-to-date security tools and technologies such as anti-virus protections and intrusion detection methods in providing Services under this Agreement. Vendor/Service Provider will implement commercially reasonable measures, including regular data integrity audits, to protect University data against deterioration or degradation of data quality and authenticity.

Vendor/Service Provider will at its own expense conduct or have conducted at least annually an audit in compliance with audit standard SSAE 16 SOC 2 of Vendor/Service Provider's security policies, procedures and controls resulting in the issuance of a Service Auditor's Report Type II.

Vendor/Service Provider will provide the University upon request the results of the above audits, scans and tests, and will promptly modify its security measures as needed based on those results in order to meet its obligations under this Agreement

## 7. Auditing

In addition to providing results of the tests and procedures described above, the Vendor/Service Provider shall also submit to audits conducted by University personnel or by third parties engaged by the University for any other reasonable purpose as determined by University, including audits of:

- Practices and systems
- General controls and security practices and procedures,
- Disaster recovery and back up, procedures
- The Vendor/Service Provider's practices in complying with regulatory requirements,
- Any certification made by the Vendor/Service Provider.

The Vendor/Service Provider shall provide full cooperation to such auditors, inspectors, regulators, and representatives, including the installation and operation of audit software.



## 8. Training

The Vendor/Service Provider shall provide training to all Users with respect to each User's responsibilities relative to cyber security. Such training must be sufficient to ensure each User's competence in cyber security to a level commensurate with his or her assigned job functions. Cyber security training may be obtained free of charge from the FBI and from the Department of Homeland Security via their respective websites.

## 9. Response to Legal Orders, Demands or Requests for Customer Data or End User Data

Except as otherwise expressly prohibited by law, Vendor/Service Provider will:

- Immediately notify University of and provide to the University a copy of any subpoenas, warrants, or other legal orders, demands or requests received by Vendor seeking University Data and/or End User Data;
- Consult with University before providing a response;
- Cooperate with University's reasonable requests in connection with efforts by University to intervene and quash or modify the legal order, demand or request; and upon University's request, provide University with a copy of its response.

If the University receives a subpoena, warrant, or other legal order, demand or request seeking University Data or End User Data maintained by Vendor and not accessible by the University, the University will promptly provide a copy to Vendor/Service Provider. Vendor/Service Provider will promptly supply the University with copies of data required for the University to respond, and will cooperate with the University's reasonable requests in connection with its response.

## 10. Data Compromise Response


Immediately upon becoming aware of a data compromise, or of circumstances that could have resulted in unauthorized access to or disclosure or use of University Data, Vendor/Service Provider will notify the University, fully investigate the incident, and cooperate fully with the University's investigation of and response to the incident. Vendor/Service Provider shall immediately take all reasonable steps to mitigate the consequences of the Data Compromise and shall promptly take all corrective action necessary to prevent a future Data Compromise or creation of circumstances that could result in unauthorized access to or disclosure of University Data. Except as otherwise required by law, Vendor/Service Provider will not provide notice of the incident directly to the persons whose data were involved, regulatory agencies, or other entities, without prior written permission from University.

Notwithstanding any other provision of this agreement, and in addition to any other remedies available to University under law or equity, Vendor/Service Provider will reimburse University



in full for all costs incurred by University in investigation and remediation of such Data Compromise, including but not limited to providing notification to third parties whose data were compromised and to regulatory agencies or other entities as required by law or contract; the offering of 12 months' credit monitoring to each person whose data were compromised; and the payment of legal fees, audit costs, fines, and other fees imposed by regulatory agencies or contracting partners as a result of the Data Compromise.

## Appendix 2: SCADA Integration Specification Handbook



# SCADA Integration Specification Handbook

---

*University of Pennsylvania*

This document specifies the conventions that should be adopted by SCADA integrators for any SCADA integration as well as information required to be provided by SCADA integrators for any integration work done within university. Many images are provided so that integrators could be consistent in the look and feel of the application.

---

1/1/2016

---

## Table of Contents

Introduction .....	4
Purpose .....	4
Background .....	4
Design Goals.....	4
Definitions .....	5
SCADA System Architecture.....	6
Architecture Components.....	6
Network Topology.....	7
SCADA Server Hardware Specifications .....	14
ICONICS AssetWorX/Tagnames .....	16
Graphics .....	18
HyperHistorian and Historical Trends.....	18
AlarmWorX and Smart Alarms.....	19
Unified Data Manager(UDM).....	20
OPC Servers.....	20
Utility Meters .....	20
Conventions .....	21
Scope.....	21
AssetWorX Structure for Real-Time Tags.....	21
AssetWorX Structure for FrameWorX Servers(MT1 & MT2) .....	22
AssetWorX Structure for Alarm Enter and Exit Conditions.....	22
AlarmWorX Server Structure for Alarm Triggers and Alarm Areas.....	24
UDM Structure for Variable Ages .....	25
UDM Structure for Smart Alarm Tags .....	26
HyperHistorian Structure .....	28
Graphics Structure .....	30
BACnet Structure .....	32
Access to Graphics and Navigation through Graphics.....	33
Introduction .....	33
Graphical Symbols.....	36
Color Standards.....	36

Graphics Navigation, Types and Functionality..... 38

Alarms ..... 54

    AlarmWorX Viewer ..... 54

    Types of Alarms..... 55

System Setpoints, Time Schedules, and Holiday Schedules ..... 67

    System set points ..... 67

    Time schedules..... 67

    Holiday schedules ..... 67

Override of Control Hardware Outputs ..... 68

    BACnet (Johnson Controls, Siemens, Andover, Automated Logic, Carrier)..... 68

    Gyrec (Siemens – Open System Gateway)..... 68

    Ethernet/IP CIP (Allen-Bradley Rockwell) ..... 68

    Metasys (Johnson Controls)..... 68

Operator Log On Procedures for Gen64 SCADA ..... 69

    OCC Operator Log On Procedure ..... 69

## Introduction

### Purpose

The intent of this document is to specify the conventions that should be adopted by SCADA integrators for any SCADA integration as well as information that should be provided to university for subsequent maintenance. It is intended to be read in conjunction with any supplementary documents that may be specific to a SCADA integration project.

This document makes extensive use of illustrations so that integrators could meet the standard look and feel of the University's SCADA application. It is not intended to stifle the creativity of the integrator.

The conventions has been made to be specific for the University Iconics GENESIS64 SCADA software.

This document describes the current installation of the Iconics SCADA software and its ultimate goal is to have a common standard that will be applied across the campus despite different SCADA projects being done by different integrators concurrently or at different times.

**This document assumes that the reader is competent in the use of Iconics GENESIS64 SCADA software.**

Any deviation from this standard for any SCADA integration will have to be approved by the University and be documented and incorporated as a revision to this document.

The goal is to standardize any future SCADA application implementation practice by following the already approved SCADA practice of the current SCADA at the University.

### Background

In 1993, the University selected ProcessVision from Comdale Technologies Inc. as replacement software to the DGS SCADA system. At that time, ProcessVision represented an innovative approach to SCADA software. It had many advantages over other SCADA packages. Some of these advantages included:

- A. It fully supported a distributed network architecture
- B. It was control hardware independent
- C. It was a modular, robust, redundant scalable system which ran on a real-time operating system (a high performance Operating System vs MS Windows).
- D. It was capable of using PennNet as a communication backbone, rather than requiring the installation of another communications infrastructure.

The distributed nature and hardware independence of the Comdale system have been the key factor to enable the University to continuously integrate different building control systems successfully into the same SCADA system in a cost effective and robust manner.

In 2014, the University commenced a project to migrate the existing ProcessVision SCADA to the Iconics GENESIS64. The migrated application is intended to be identical to the original ProcessVision system. e-Magic Inc. was contracted to perform the migration of the existing configuration. The application is being migrated in 4 Phases.

### Design Goals

The ensuing criteria are the basis of the design for the new Penn SCADA system with Iconics' GENESIS64 Software:

The New SCADA system shall incorporate the philosophy of the existing System as follows:

1. The system shall remain distributed



- a) Each SCADA Server shall run autonomously for monitoring, alarming, data collection and control of the local building automation systems.
  - b) The central monitoring control workstation shall be capable of overseeing the SCADA of the entire campus.
  - c) Clusters of critical areas shall have redundant systems.
2. The storing of historical data shall be centralized with redundant servers.
3. The SCADA system shall employ a higher level of security to protect the SCADA system from external malicious attacks and threats.
4. Each of the clusters shall have the ability to buffer historical data in the case of a communication interruption between the cluster and the historical data servers.  
This allows minimizing the loss of historical data should the PennNet network connection be down for any reason.
5. The communications between each cluster and the historical servers shall be secured via PennNet and the established firewalls.
6. The design of the SCADA system adheres to open system standards such as OPC to facilitate the following:
- a) Allow a bigger selection of third parties products.
  - b) Allow easy third party integration.
  - c) Cost effective way to access real-time data and historical data.

## Definitions

A	ACL	Access Control List
B	Alarms Workstation	ASCADAClient
C	BAS	Building Automation System
D	Domain	Name of local network
E	Domain Controller	A computer that allows the access to the SCADA at different operational levels, based on user name and password.
F	DNS	Domain Name Server
G	Engineering Workstation	A computer used by SCADA Maintenance Personnel to update and maintain the SCADA system.
H	Historian Data Server	A computer where desired data is archived for future retrieval.
I	Middle-Tier FrameWorX Server for Web SCADAClients	A computer load balancing the access to the SCADA system by Web SCADA Client as well as hosting a Web site that allows remote access to SCADA system by delivering web pages and data files to remote authorized browsers.

J	Middle-Tier FrameWorX Server for SCADA Clients	A computer load balancing the access to the SCADA system by Operator Workstation and Alarms Workstation as well as running report generator.
K	OCC	Penn Operations Control Center, located at 3101 Walnut Street.
L	Operator Workstation	A SCADA Client.
M	Public Web Server	A computer hosting a Web site that provides general operating information such as energy usage among buildings in the campus. The intended audience is general public and students.
N	SCADA Client	A computer that connects to one or more SCADA Servers and provides monitoring and control functions for the SCADA system. Operator Workstation and Alarms Workstation are SCADA Clients.
O	SCADA Server	A computer referred to as a SCADA Server that runs SCADA to monitor and control a manageable subset of building automation systems within a large set of building automation systems.
P	SCADA System	Both the SCADA configuration and hardware combined to provide the functionality of a SCADA.
Q	UDM	Iconics Unified Data Manager.
R	VLAN	Virtual Local Area Network.
S	Web SCADA Client	A computer that connects to one or more SCADA Servers and provides monitoring and limited control functions for the SCADA system via Internet Explorer browser.

## SCADA System Architecture

### Architecture Components

The following software hardware components together with PennNet constitute the Penn SCADA architecture. Please see the SCADA Architecture Diagram at the end of this section

- A. Domain controller is setup in a domain called "GENESIS". All computers under the trusted VLAN (See Network Topology below) are assigned to the Penn SCADA domain.
- B. DNS role was added to the Domain controller. This allows computers within the domain to find each other by name.
- C. Domain controller was configured with user/password and user/group via Active Directory for user within Windows Server 2012.
- D. SCADA Servers shall be distributed across the campus and shall be connected locally to the Building Automation Systems to obtain BAS data as well as to provide access of monitoring and controlling of the BAS from the Operations Control Center (OCC).
- E. Operator Workstations allow the operator to remotely monitor and control all the Building Automation Systems on campus.

- F. Alarm Workstations allow the operator to remotely monitor and acknowledge any alarms of all the Building Automation Systems on campus.
- G. Historian Data Server(HIST1 & HIST2) was setup to centralize the collection of data from each SCADA Server as well as to centralize the logging of alarm messages.
- H. Middle-Tier FrameWorX Server(s) acts as a load balance communication agent among the SCADA Servers, Hyper Historian and SCADA Clients. The main purpose of load balancing is to distribute the communication workload across multiple Middle-Tier FrameWorX Server so as to achieve optimal resource utilization, maximum throughput, minimize response time and avoid overload.
- I. Middle-Tier FrameWorX Server(s)(MT1 &MT2) was setup as part of the overall SCADA System Architecture. The communication channels can be increased by simply adding more load balancing Middle-Tier FrameWorX Servers when existing communication channels are overloaded. No change in configuration will be required by both SCADA Clients and Servers.
- J. SCADA Web Server was setup within the Middle-Tier FrameWorX Server. The SCADA Web Server will allow authorized remote users to access the SCADA via Internet Explorer browser. Such authorized users who use the Web to access the SCADA are called Web SCADA Clients.
- K. Report Server was setup within Middle-Tier FrameWorX Servers in the trusted VLAN. The Report Server will generate reports according to a predefined schedule.
- L. Engineering Workstation(ENGWKSTN1 & ENGWKSTN2) was setup for Penn SCADA Operations' Personnel to configure, modify and test any new SCADA configuration prior to production release. It also acts as a file server to provide a location to store and keep all the revisions of SCADA configuration for the entire SCADA network as well as to provide a read-only shared storage for the entire SCADA network with the current production revision of SCADA application.
- M. Public Web Server was setup in the DMZ. The purpose is to provide a subset of SCADA data to the public such as energy consumption among buildings on the campus.
- N. All critical SCADA Servers are setup with redundant SCADA Servers.
- O. The redundancy of the entire infrastructure at OCC was setup in MOD7 in case the OCC connection to the Penn SCADA goes down.

## Network Topology

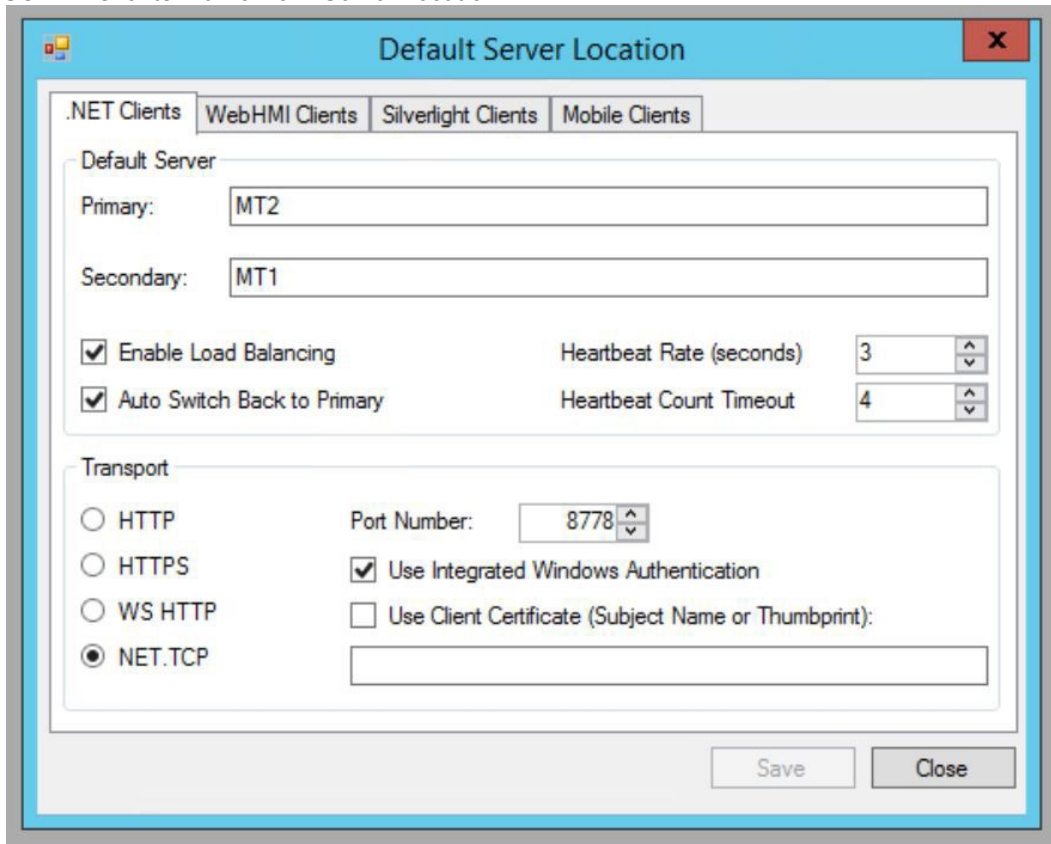
At the University, there are approximately 150 buildings on campus. These buildings are grouped into clusters. There are approximately 54 clusters. Each cluster has a local SCADA Server which communicates with the equipment in the buildings in that cluster. These servers also communicate with the redundant HyperHistorian Servers and FrameWorX Servers which are located at the OCC and MOD7 Building. Note that OCC and MOD7 have infrastructure for redundancy of operation.

For further clarity, the system works as follows:

Each SCADA Server in the field manages the affairs of a cluster. Each cluster manages multiple buildings. Each SCADA server runs the OPC servers required to communicate with the field devices. They also run collectors for historical data.

For real-time operation the Local FrameWorX server on the cluster communicates over PennNet with the redundant FrameWorX servers at OCC and MOD7. All client machines in OCC(including Engineering WorkStations) get their realtime data from MT1 or MT2(depending on which is active). Each client machine needs to be configured for these redundant real-time FrameWorX servers.

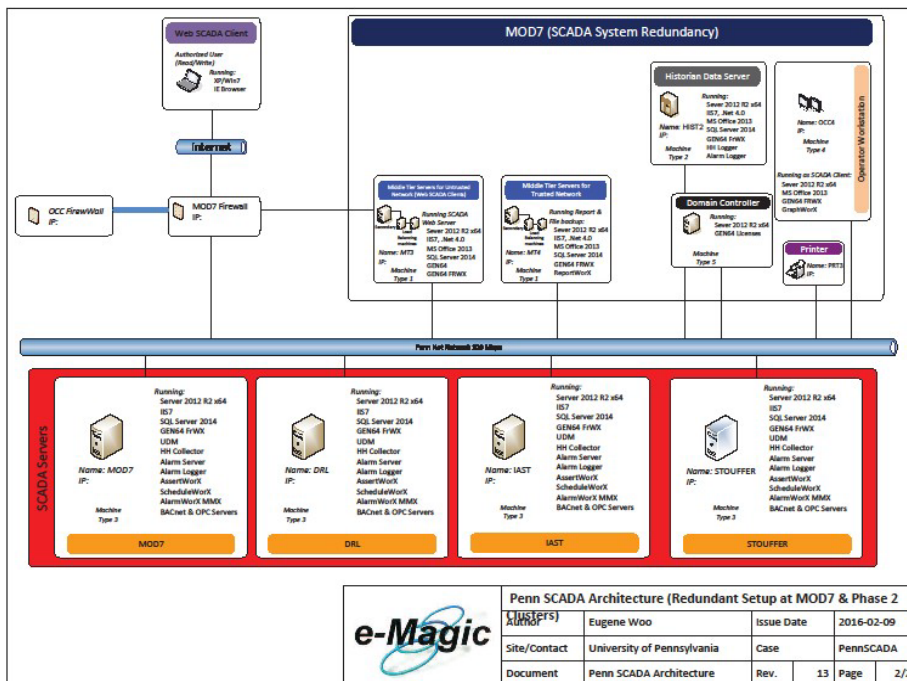
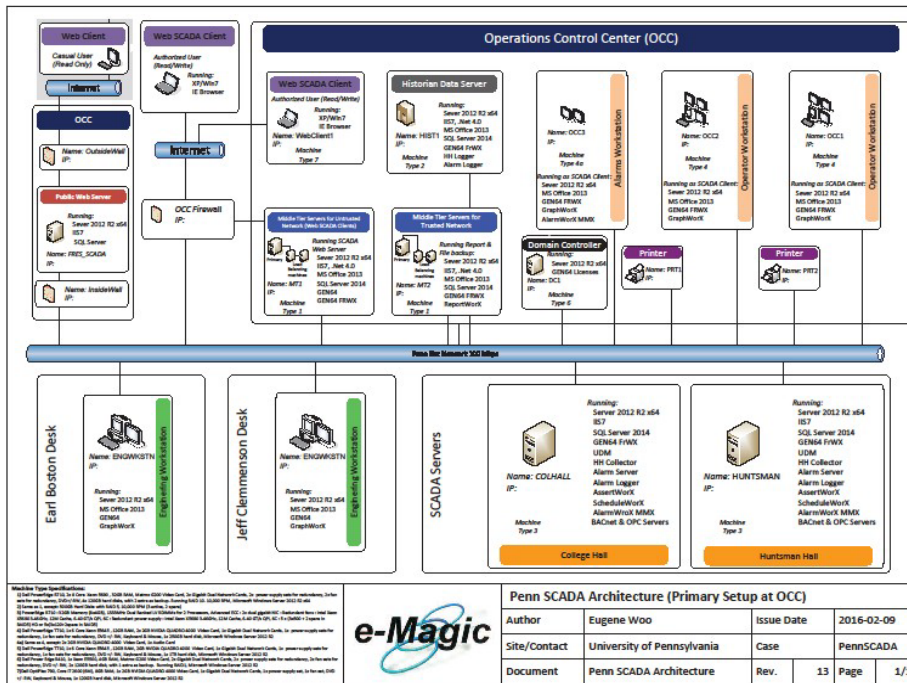
SCADA Clients FrameWorX Server Location

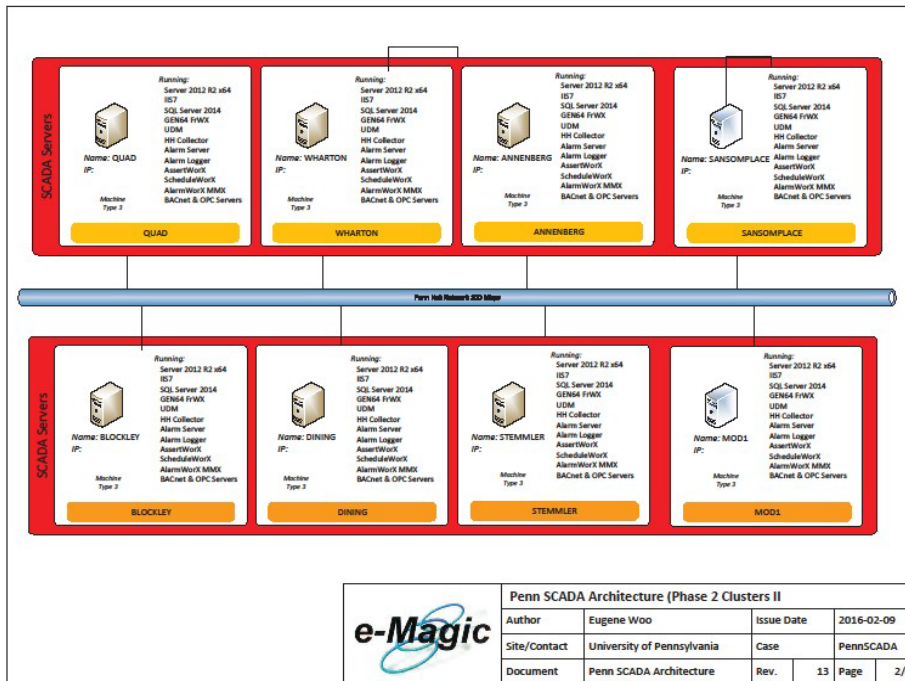
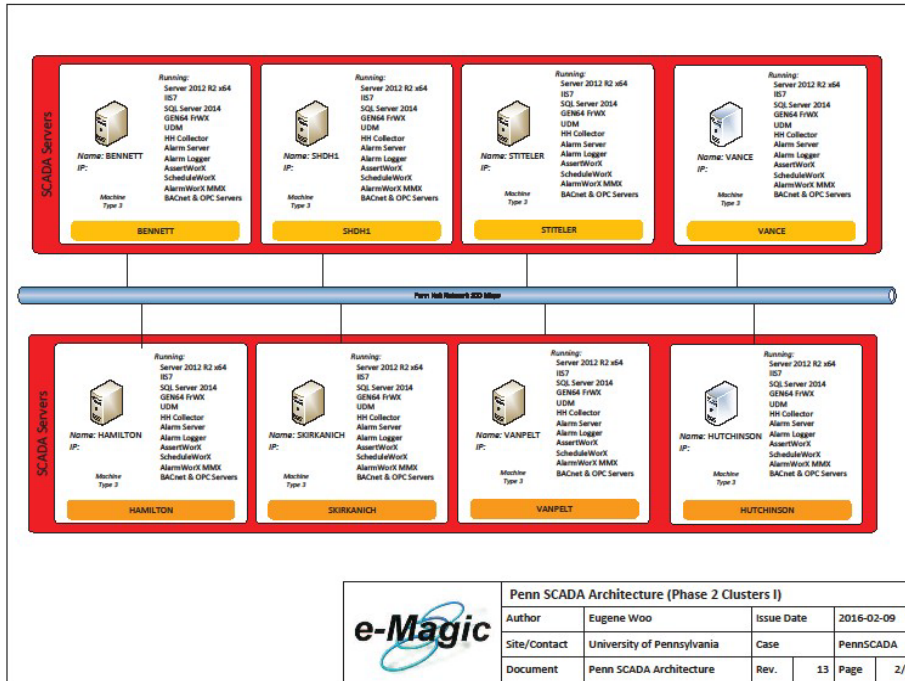


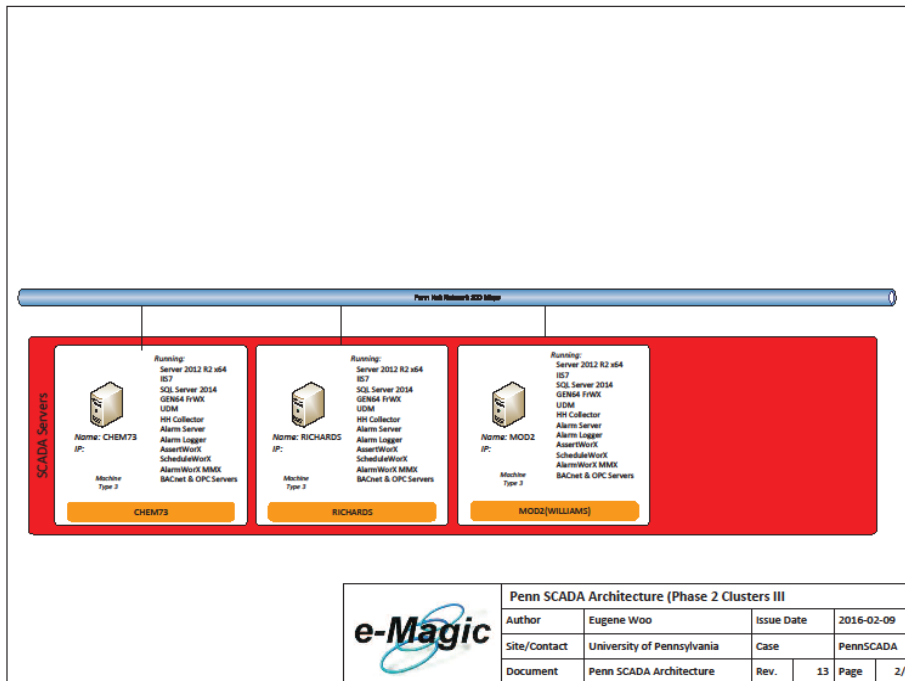
For historical information, the collectors in the field send their data to the redundant HyperHistorians, HIST1 and HIST2. Any client that needs historical information, will get it from HIST1 or HIST2 directly. Client application DataSources reference an alias HIST which is configured on MT1 and MT2 to allow redundant access to historical data.

**Note that each SCADA server must be configured to be able to monitor and control the buildings in their cluster even if they lose connectivity with MT1, MT2, HIST1 and HIST2.**

Penn SCADA Architecture Diagram







P. Virtual Local Area Networking

1. A Virtual LAN (VLAN1) was setup as a protected and private LAN for the SCADA system within PennNet. All servers in this LAN are trusted. ISC closet Switches are configured with ACL to route traffic only among pre-defined servers.
2. A second Virtual LAN (VLAN2) was setup as a DMZ (DeMilitarized Zone) within PennNet. The purpose is to separate the external network from directly referencing an internal network, hence it limits the exposure of the internal network (VLAN1) to the outside, untrusted environment.
3. An untrusted environment can be the internet and PennNet beyond the DMZ.

Q. Firewall

1. A firewall was installed between the DMZ and the untrusted network. It is set to allow only HTTP traffic.
2. A firewall was installed between the trusted and DMZ. It is set to allow only FrameWorX server traffic to communicate with the SCADA Servers and with the Hyper Historian.
3. The purpose of the firewall is to heighten the security for the SCADA system by exposing services that are required. Hence, this reduces the possible attack space.

R. Virtual Private Network (VPN)

1. VPN is the only entrance from the Internet or outside of the DMZ to PennSCADA.
2. SCADA administrators with appropriate credentials will be able to remote in to the Engineering Workstation to maintain the SCADA System if SCADA Administrator could successfully log onto the VPN.

3. VPN shall be setup to authenticate web-based SCADA Clients to access PennSCADA with a secure, encrypted tunnel via Network Access Server (NAS). NAS will authenticate the user and only permit the connection to SCADA Web Server within Middle-Tier FrameWorX Server in DMZ if the user is authorized and his/her computer is up-to-date with firewall, virus scan, OS service pack and Internet Explorer.
  4. NAS is available through by ISC LAN.
- S. Securing the SCADA System
1. Using ACL to route traffic only among pre-defined servers, this restricts any computer to be part of the private SCADA VLAN.
  2. By separating the trusted private SCADA VLAN from the outside (PennNet and Internet) with DMZ, it significantly increases the security.
  3. The firewalls are configured to allow only essential services required for any inbound traffic to the VLAN.
  4. VPN ensures that the connected Web based SCADA Client machines are healthy, free from any virus and with sufficient security measures. All VPN authorized users, except the VPN authorized SCADA Administrator can only access servers in the DMZ. This further secures the underlying SCADA system on the trusted private SCADA VLAN from attacks.
  5. All servers or computers within the trusted and DMZ should meet the security guidelines by Penn ISC
  6. All hosts shall be able to meet the following Penn ISC standards:
    - a) Devices connected to PennNet shall have all relevant security patches applied, or the associated vulnerabilities shall be otherwise effectively eliminated on a timely basis. Patches for Critical Vulnerabilities shall be applied to, or the associated vulnerabilities shall be otherwise effectively eliminated from: servers immediately, but within, at most, ten days of availability, desktop and workstation computers within two business days of availability, and all other PennNet-connected devices within two business days of availability. This includes, but is not limited to, routers, printers, and special purpose devices connected to PennNet. Note that security patches to devices such as printers are very rare.
    - b) When software vendors package fixes for Critical Vulnerabilities together with numerous other fixes to repair non-critical problems (such as Microsoft Service Packs), the risk of the combined fix introducing new problems is considerably higher. Consequently, systems administrators are not required to apply such "roll-up" software fixes in the timeframes outlined above, but rather are strongly encouraged to first consult with other technical staff at Penn and elsewhere to determine whether sufficient testing has been done. Penn ISC will work with software vendors to try to ensure that fixes for critical vulnerabilities are distributed as discrete fixes, independent of large, roll-up software fixes.
    - c) The operating system network shall be capable of VPN tunneling and IP SEC encryption.
    - d) All access shall use Strong Passwords and shall use Strong Authentication, and passwords shall not be stored in cleartext.
    - e) For operating systems for which Penn owns site-licensed anti-virus software, there shall be a regular program of maintaining current virus signatures and real-time scanning, consistent with software vendor recommendations.



- f) All critical host servers storing Operational Data shall implement a routine program of data backup and regular recovery testing.
- 7. All Critical Host servers shall meet the following additional Penn ISC standards:
  - a) Shall be scanned or examined for common security vulnerabilities by ISC monthly. Any serious vulnerability – those that allow a remote or local user to gain full privileges on the system shall be corrected within two business days. Critical hosts located behind hardware firewalls shall be scanned from inside the firewall by the system owner subject to ISC providing supporting security scanning training, and a for-fee scanning service.
  - b) Implement a process to ensure that user accounts are promptly disabled when users no longer require access.
  - c) Servers shall be housed in a locked, physically secure area accessible only by those requiring access.
- 8. SPIA Participate in the University's Security and Privacy Impact Assessment (SPIA) program, which provides a framework and support for inventorying confidential data, assessing risks to data, and identifying appropriate steps to remediate those risks.
- E. All Critical Host servers storing Confidential University Data shall meet the following additional standards.
  - 1. Provide at least two independent mechanisms to ensure that only network traffic expected inbound and outbound are allowed. Examples include, but are not limited to, eliminating un-needed services on the Critical Host, host-based or external firewalls, a program of regular port-scanning. This provision is subject to ISC providing a recommended supported firewall product, for-fee firewall consulting, recommended firewall training, and recommended firewall consulting vendors.

## SCADA Server Hardware Specifications

The hardware specifications of the SCADA server for each cluster are:

Number of Server Units	1 or multiple if redundancy is required
Chassis	DELL PowerEdge T630 or better
Processor	2 x Intel XEON E5-2609 v2 <ul style="list-style-type: none"> <li>• 8 core total</li> <li>• 2.5 GHz</li> <li>• 10M Cache</li> <li>• 6.4 GT/s QPI</li> </ul>
RAM	32 GB <ul style="list-style-type: none"> <li>• 1600 MHz RDIMMs</li> </ul>
Hard Disk Drive	4 x 600 GB <ul style="list-style-type: none"> <li>• 1.2 TB effective total</li> <li>• 10k RPM</li> <li>• SAS 6Gbps</li> <li>• 2.5 in Hot-plug</li> <li>• RAID 10</li> </ul>
Ethernet	2 x Broadcom 5719 QP 1Gb <ul style="list-style-type: none"> <li>• 8</li> <li>• Ports total</li> </ul>
Graphics	NVidia Quadro K2000 <ul style="list-style-type: none"> <li>• 2GB VRAM</li> <li>• 2 x Display Port 1.2 connectors</li> <li>• Supports up to 4 monitors</li> </ul>
DVD drive	2 x DVD +/- RW <ul style="list-style-type: none"> <li>• SATA</li> </ul>
Power Supply	1100 W dual hot plug redundant power supplies
Power Cord	2 x power cords
KVM Switch	1 x Space (1.75") Rack mount 17" LCD KVM c/w 8 port switch
Display port cables	1 x 6ft Display port cables
UPS	1 x APC Smart UPS 2200VA RM 120V 2U LCD

### Software

The SCADA Server will have the following software specifications:

Operating System	Microsoft Windows Server 2012 R2 Standard Edition, including IIS7
Microsoft SQL Server	Microsoft SQL Server 2014 Standard w/10 CALs
Microsoft Office	Microsoft Office 2013 Standard

### **ICONICS Software on Cluster SCADA Servers**

- AssetWorX
- GEN64 FrameWorX
- UDM
- HyperHistorian Collector
- AlarmWorX Server
- AlarmWorX Logger
- AlarmWorX MMX
- ScheduleWorX
- BACnet
- OPC Servers

**It is required that the Integrator purchase all ICONICS software and SupportWorX for that software directly from ICONICS so that they may receive the University pricing for those products and services.**

**Note that ICONICS software must be installed with the Iconics\_admin user name.**

### **KVM Switches**

- 1 Space (1.75") rack mount 17" LCD KVM c/w 8 port switch  
Model No.: RM-KB-LCD17X8KVM

### **UPS**

- APC Smart UPS **2200VA RM 120V 2U LCD** - Rack mount

### **Cabinets**

- Floor mounted
- 6 inches off the floor

## ICONICS AssetWorX/Tagnames

The Iconics GENESIS64 SCADA application at the University is based on using AssetWorX. AssetWorX enables users to organize all enterprise and equipment data into reusable equipment (asset) classes that can be easily instantiated for all like assets to construct a system. Pumps, heat exchangers, well heads, gas fields, turbines, chillers, buildings, building zones, manufacturing cells and plants can all be defined as Asset Classes. The AssetWorX approach greatly reduces engineering efforts needed to configure a system and delivers a very consistent system organization. Assets are defined in an ISA S95-compliant asset tree, constructed to represent the enterprise.

The University implementation of AssetWorX takes advantage of the concept of distributed AssetWorX which means that you can merge multiple independent AssetWorX trees into one global AssetWorX tree. It is now easy to provide a view of your multi-site organization to central management while keeping the maintenance of the individual sites on local levels.

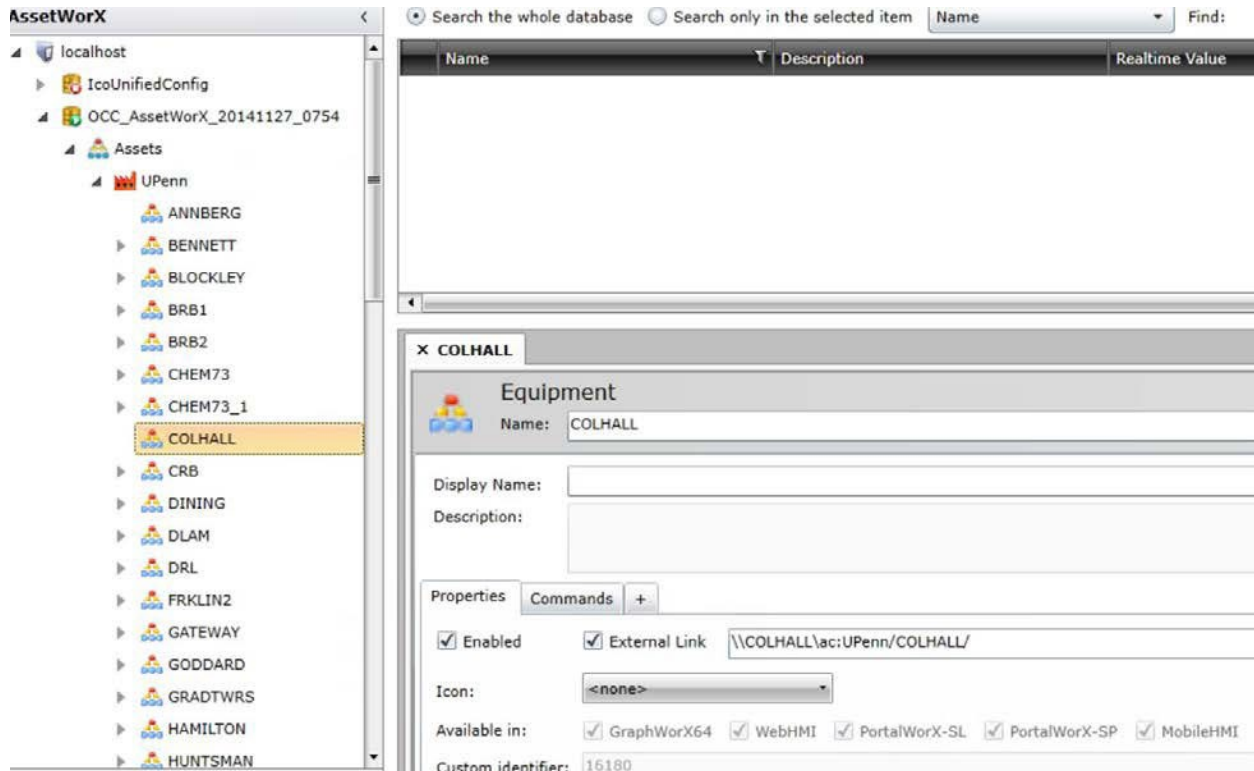
See Iconics application note on Scalable Distributed S95 Asset Architecture here;

[http://support.elmark.com.pl/iconics/10.8/10\\_8/AssetWorX%20-%20Scalable%20Distributed%20S95%20Asset%20Architecture.pdf](http://support.elmark.com.pl/iconics/10.8/10_8/AssetWorX%20-%20Scalable%20Distributed%20S95%20Asset%20Architecture.pdf)

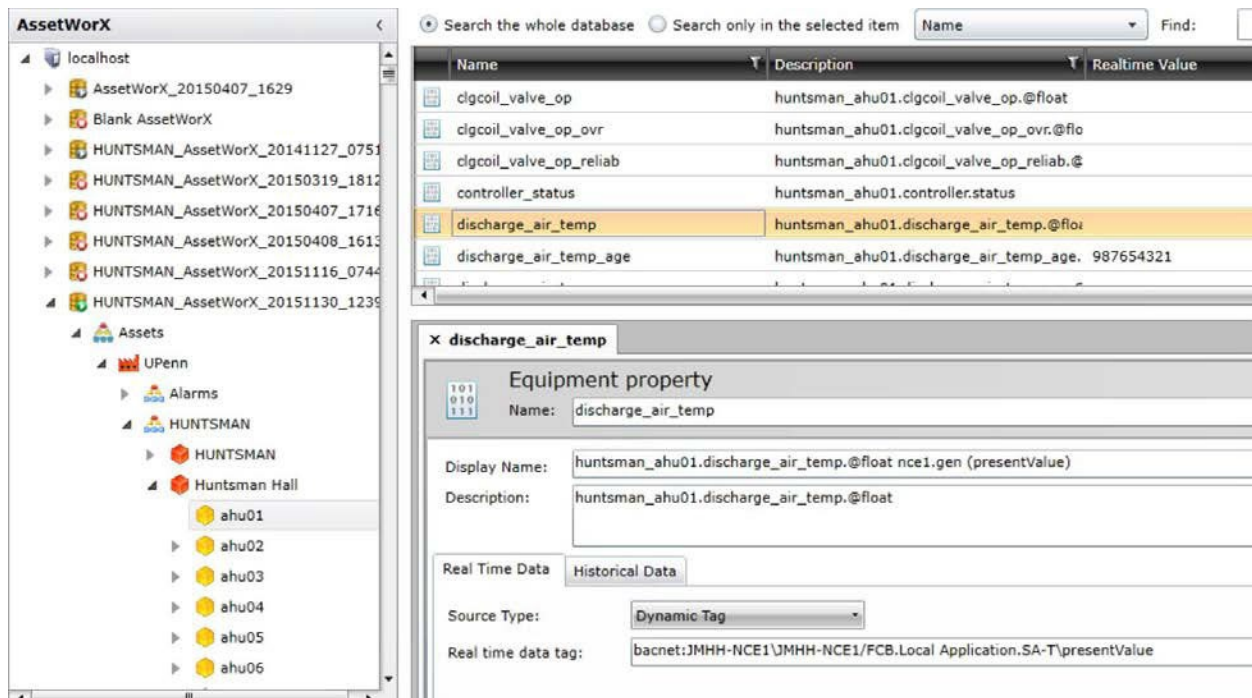
Each Cluster has a SCADA server(e.g. HUNTSMAN) with an AssetWorX tree for its Buildings, Equipment and Equipment Properties. The AssetWorX trees in the redundant MT1 and MT2 are linked to the AssetWorX trees on the local SCADA cluster servers.

See examples of the AssetWorX trees below:

### AssetWorX Tree at MT1



AssetWorX Tree at HUNTSMAN



**It is imperative that AssetWorX be used for any Iconics GENESIS64 application at the University.**

A naming standard promotes consistency throughout a project or multiple projects. It simplifies maintenance of the SCADA configuration. It helps to convey useful information of the system in a consistent manner and makes it easier for users to quickly identify the information. Hence, it reduces user training.

At the University, tagnames in the Asset tree is structured as follows:

```

AssetWorX
  Assets
    UPenn
      Cluster(e.g. HUNTSMAN)
        Building(e.g. Huntsman Hall)
          Equipment(e.g. AHU01)
            Equipment Property(e.g. return air temperature)
    
```

Thus,

ac:UPenn/HUNTSMAN/Huntsman Hall/ahu02/return\_air\_temp

is an example of a tagname that is used universally as a DataSource in GraphWorX64, AlarmWorX, TrendWorX(for real-time trends, see section on trends for information on historical trends), UDM, OPC Servers, etc.

Each local cluster server has an AssetWorX database that manages the buildings in that cluster. The redundant FrameWorX Servers MT1 and MT2 have AssetWorX databases for the entire campus because they are linked to the local AssetWorX databases.

## Graphics

Graphics( Iconics .gdfx files) for each cluster SCADA server are kept on the C:\UPenn drive of that server. Graphics for Engineering Workstations and Operator View stations in OCC and the redundant location at MOD7 are on the C:\UPenn drive of each of those computers.

## HyperHistorian and Historical Trends

The HyperHistorian(HH) runs on the redundant servers HIST1 and HIST2 with are located at OCC and MOD7. These servers receive their data for the HH Collectors that run on the Cluster SCADA Servers. MT1 and MT2 are configured with an alias HIST which points to HIST1 as primary and HIST2 as secondary historical data servers.

*HH aliasing configuration on MT1*

The screenshot shows the 'Platform Services' configuration window. The left pane shows the 'Project Explorer' with 'FrameWorX Server' expanded to 'Platform Services'. The main window title is 'FrameWorX Server Platform Services'. Below the title bar, there is a text box: 'This is the configuration of redundant platform services. Specify the machine name of your Back-End servers on the network.' Below this is a table with the following data:

	Server Name	Primary Machine Name	Secondary Machine Name
▶	HIST	HIST1	HIST2
*			

The screenshot shows the 'OPC UA and OPC.NET Servers' configuration window. The left pane shows the 'Project Explorer' with 'FrameWorX Server' expanded to 'OPC UA/.NET Servers'. The main window title is 'FrameWorX Server OPC UA and OPC.NET Servers'. Below the title bar, there is a text box: 'This is the configuration of OPC UA and OPC.NET servers (they could be redundant). For each server specify the primary server URI , and optionally the secondary server URI.' Below this is a table with the following data:

	Server Name	Server Type	Endpoint URI	Secondary Endpoint URI
▶	HIST	OPC UA	http://HIST1:80/Hyperhistorian	http://HIST2:80/Hyperhistorian
*				

Historical trend pens DataSource are configured to refer to HIST. They retrieve data directly from the active HH.

An example of an Historical trend pen DataSource is:

ua:HIST\Configuration\UPenn\HUNTSMAN\Huntsman Hall\ahu02\return\_air\_temp

The HH logs data at 1 or 5 minute intervals. Fast changing data at 1 minute and slower at 5 minute intervals. The HH maintains historical data files for a minimum of 365 days. These files are archived after this time.

## AlarmWorX and Smart Alarms

Smart alarms are implemented using AssetWorX, AlarmWorX Server and UDM on the local cluster SCADA server. Alarms are also logged locally by the cluster-based AlarmWorX Logger.

Operators in OCC view alarms in the AlarmWorX Viewer. Real-time alarms come from the cluster-based AlarmWorX Server. Historical alarms are retrieved from the cluster-based AlarmWorX Logger.

Alarm messages are categorized and could be filtered by categories.

Alarm message categories are:

- Critical - Alarms for the Operators
- Control - Alarms for Control Engineers
- ChillWater - Chill Water related Alarms
- Steam - Steam related Alarms
- Electrical- Electrical related Alarms
- PM - Preventative Maintenance Alarms
- Maintenance - Maintenance Alarms
- General - General Alarms
- Cluster - The Cluster that the alarm comes from
- Building - The Building that the alarm comes from
- Equipment - The Equipment that the alarm comes from

The Iconics Alarms Area feature is used to label alarms with categories.

Alarms and faults are also viewed in the graphics. Variables known as smart alarms are set to predefined values when an alarm is true. Based on the value of these variables graphical objects such as symbols are made to change their color.

Smart alarms are not simply limit and deviation alarms. They could be quite complex, involving multiple conditions and expressions.

Smart Alarms are implemented as follows:

- AssetWorX expressions are used to trigger enter and exit conditions. This will set a digital point. This enables use of complex algebraic expressions as entry and exit conditions.
- The AlarmWorX Server monitors the above digital point with delay, etc. and sends Messages to AlarmWorX Viewer if the delay requirement is satisfied. This allows the integrator to only present an alarm to the operator if it persists for the delay period.
- Messages are categorized using multiple Iconics Area labels.
- AlarmWorX Multimedia is used to send email & SMS.
- UDM expressions are used to monitor the AlarmWorX server variables and UDM registers are used to set smart alarm variable values.
- These smart alarm variables are used for high granularity graphics objects color change. e.g graphics objects can be set to change their color based on the values of these smart alarm variables.
- AlarmWorX Logger is used to store alarm messages
- AlarmWorX Viewer is used by operators to view real-time and historical alarms.

## **Unified Data Manager(UDM)**

The UDM is primarily used to:

- Calculate the last time that a tag value was changed(age of variables) - UDM expressions
- To assign values to OPC Tags( age , smart alarm variables) - UDM registers

## **OPC Servers**

OPC Servers are used to connect AssetWorX tags to field devices as required.

It is the responsibility of the control company or installer of specified equipment to provide an OPC Server and appropriate software licenses so that that equipment could be interfaced to the ICONICS GENESIS64 SCADA.

Available OPC Servers include:

- BACnet
- Modbus TCP
- Allen Bradley PLC5 - Ethernet
- Allen Bradley PLC5 - Serial
- Allen Bradley CIP
- GE Fanuc 9070 Ethernet

## **Utility Meters**

Utility meters will communicate via the University ISC network to the server that is used for that building.



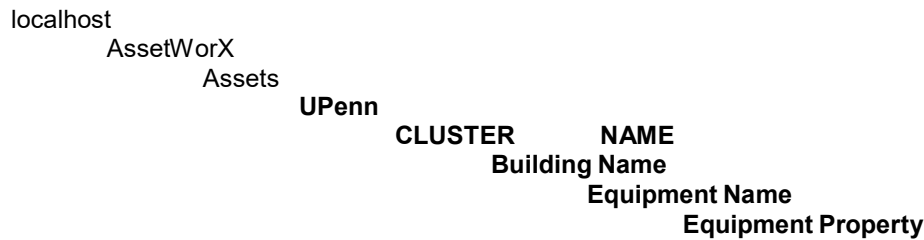
## Conventions

### Scope

The scope of this part of this document is to specify in more detail the convention that should be used in configuring an operator interface relating to SCADA integration. This includes naming conventions, graphical standards, alarms standards, trends, logging and security.

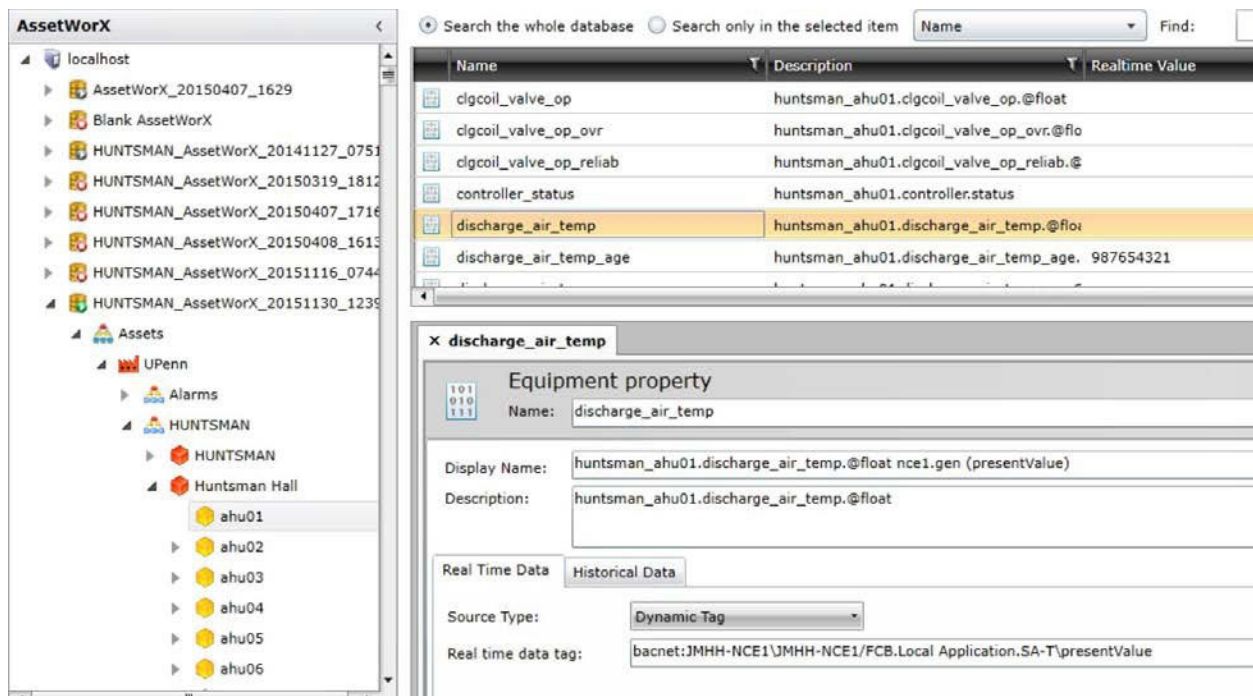
### AssetWorX Structure for Real-Time Tags

AssetWorX tree structure for the local clusters is:



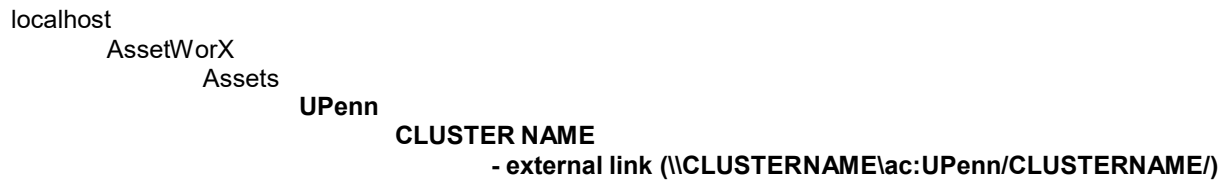
All **bold** branches are added by the integrator.

AssetWorX tree for HUNTSMAN

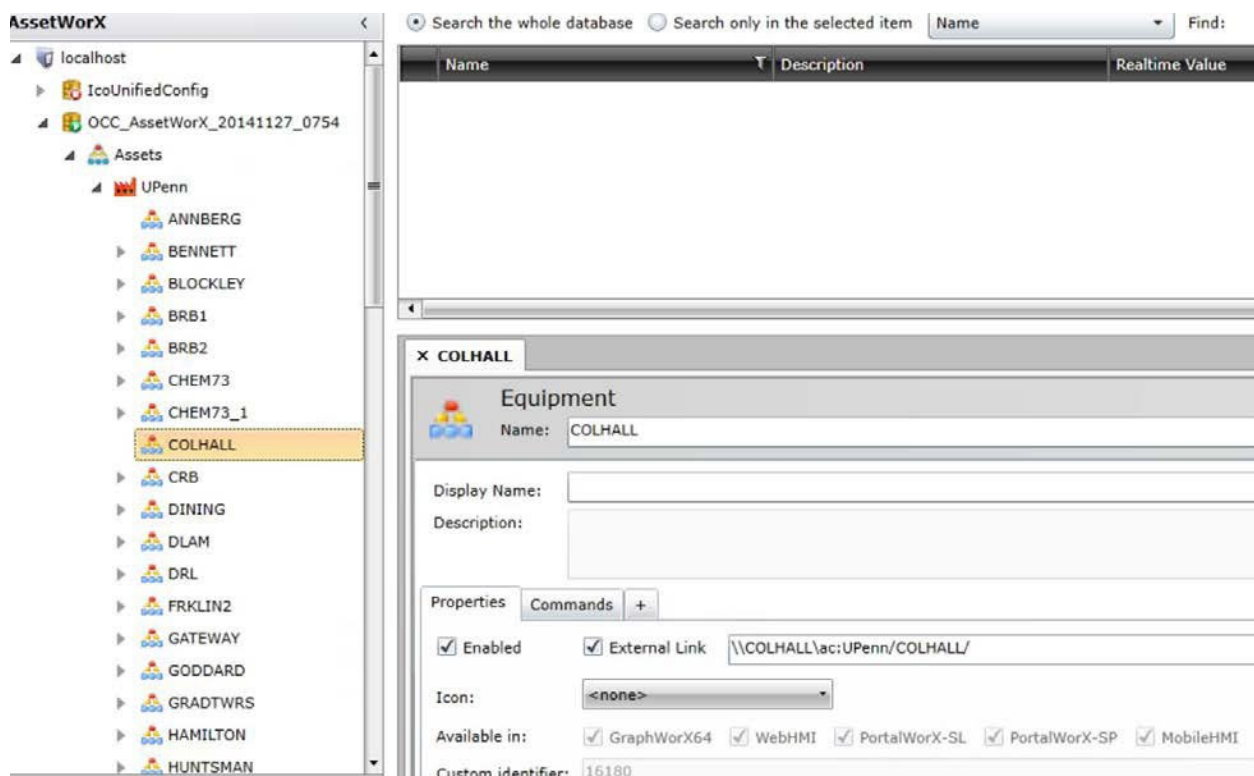


## AssetWorX Structure for FrameWorX Servers(MT1 & MT2)

AssetWorX tree structure for MT1 and MT2 is:

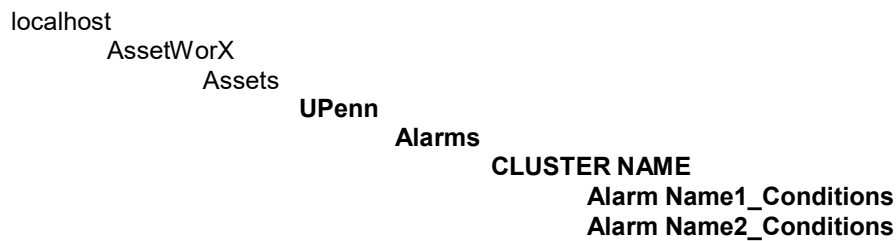


AssetWorX tree for MT1



## AssetWorX Structure for Alarm Enter and Exit Conditions

The AssetWorX Tree structure for each local cluster also has a branch for handling Alarm entry and exit conditions.



Note that each alarm condition has a name and is appended with **\_Conditions**. See section below on Alarm Configuration for a walk through of how smart alarms are implemented using AssetWorX, AlarmWorX Server and UDM.

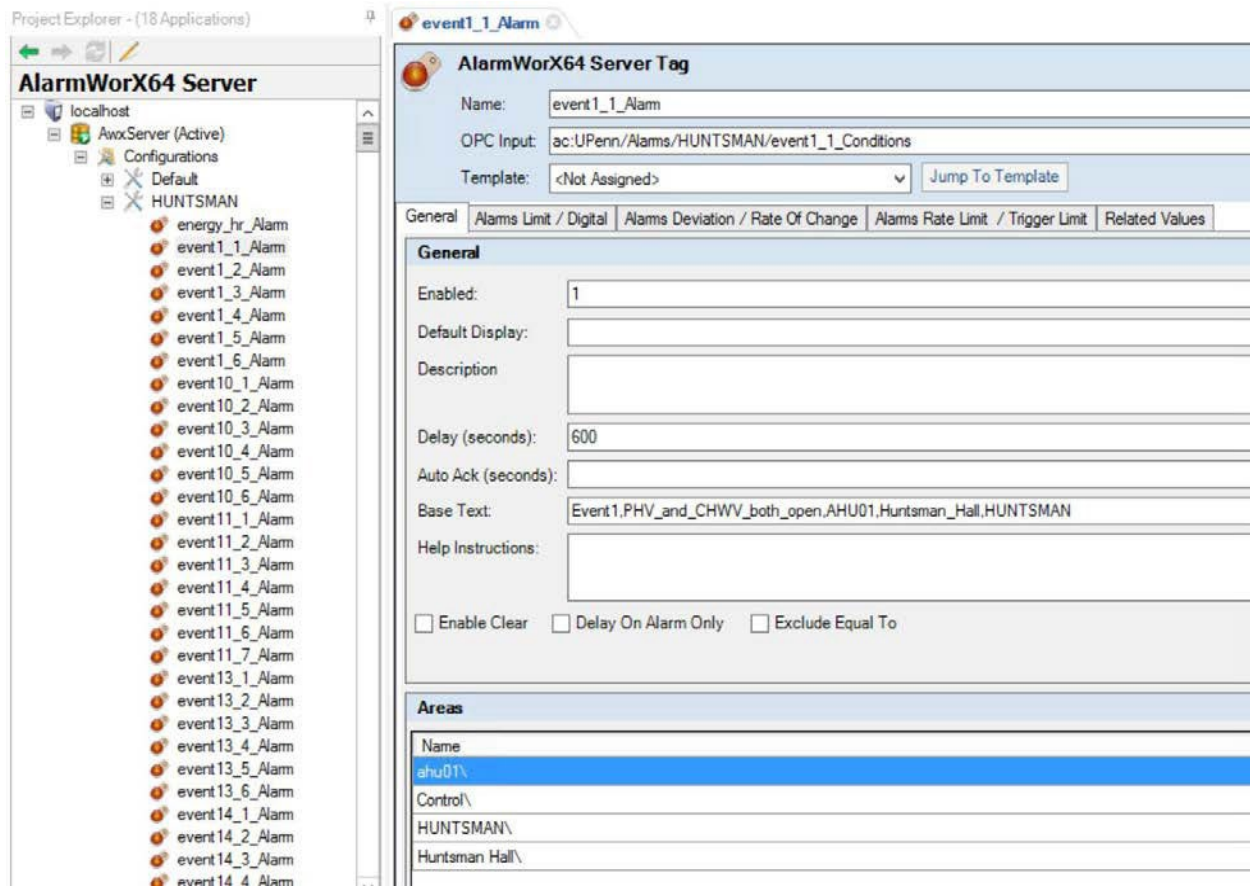
AssetWorX Tree for Smart Alarm Entry and Exit Conditions

The screenshot displays the AssetWorX software interface. On the left is a tree view under 'localhost' containing several 'AssetWorX' folders and an 'Assets' folder. The 'Assets' folder is expanded to show 'UPenn', which contains 'Alarms' and 'HUNTSMAN'. 'HUNTSMAN' is further expanded to show 'HUNTSMAN', 'LAW', 'NANOTECH', and 'TOWNE1'. Below the tree are tabs for 'AlarmWorX64 Logger', 'AlarmWorX64 Server', 'AssetWorX', and 'BACnet'. The main window on the right shows a search bar and a table of conditions. The table has columns for 'Name', 'Description', and 'Realtime Value'. The first row, 'hhah1dathi\_Conditions', is selected. Below the table is a configuration window for 'hhah1dathi\_Conditions' with the following fields:

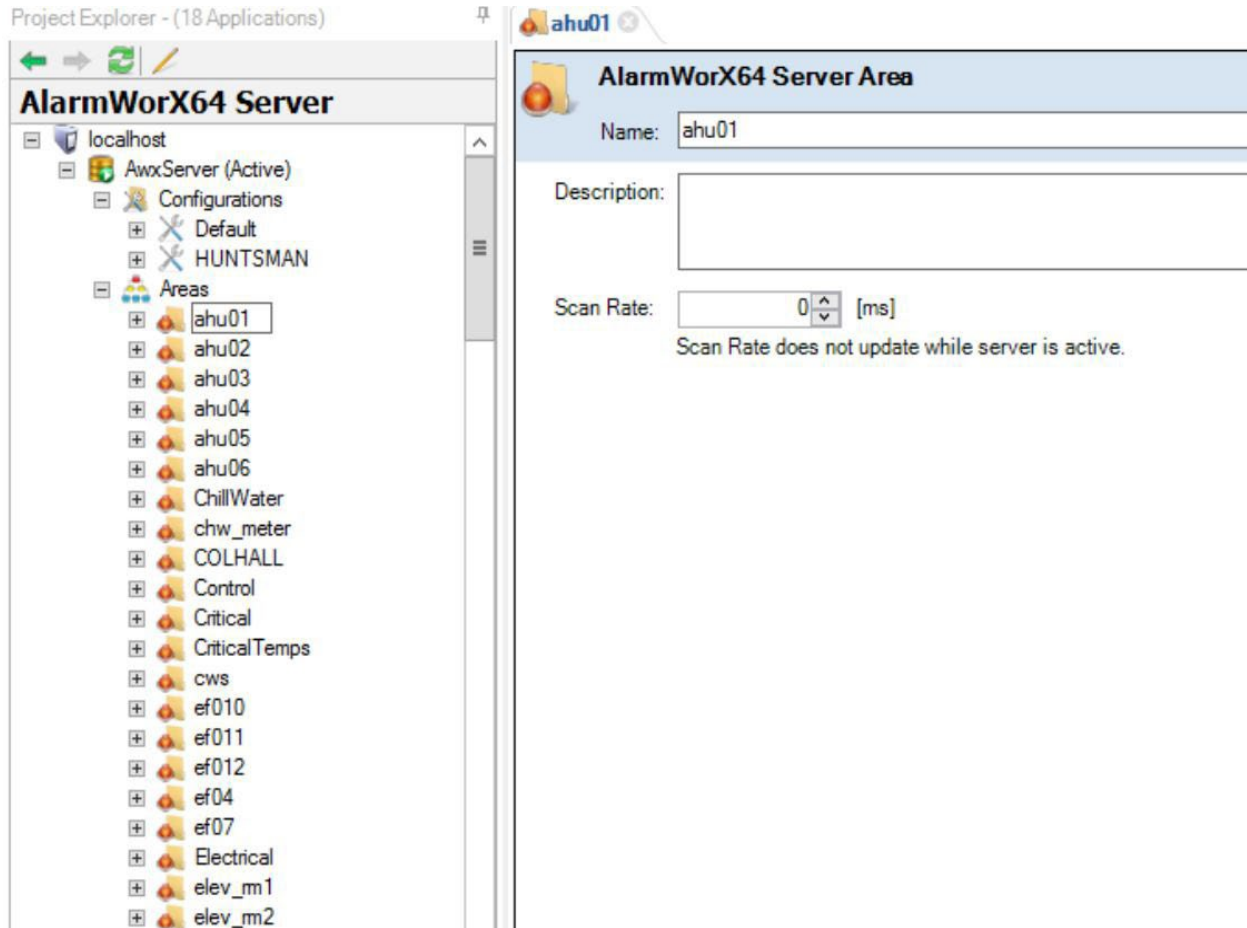
- Name: hhah1dathi\_Conditions
- Display Name: [Empty field]
- Description: [Empty field]
- Real Time Data / Historical Data tabs
- Source Type: Expression
- Data Type: Boolean value
- Read Expression: x=IF ({{{ac:UPenn/HUNTSMAN/Huntsman Hall/ahu01/sfana\_di\_status}} || {{a
- Write expression enabled
- Real time data tag: [Empty field]

## AlarmWorX Server Structure for Alarm Triggers and Alarm Areas

### AlarmWorX Server Tree for Monitoring Alarm Conditions and Generating Messages

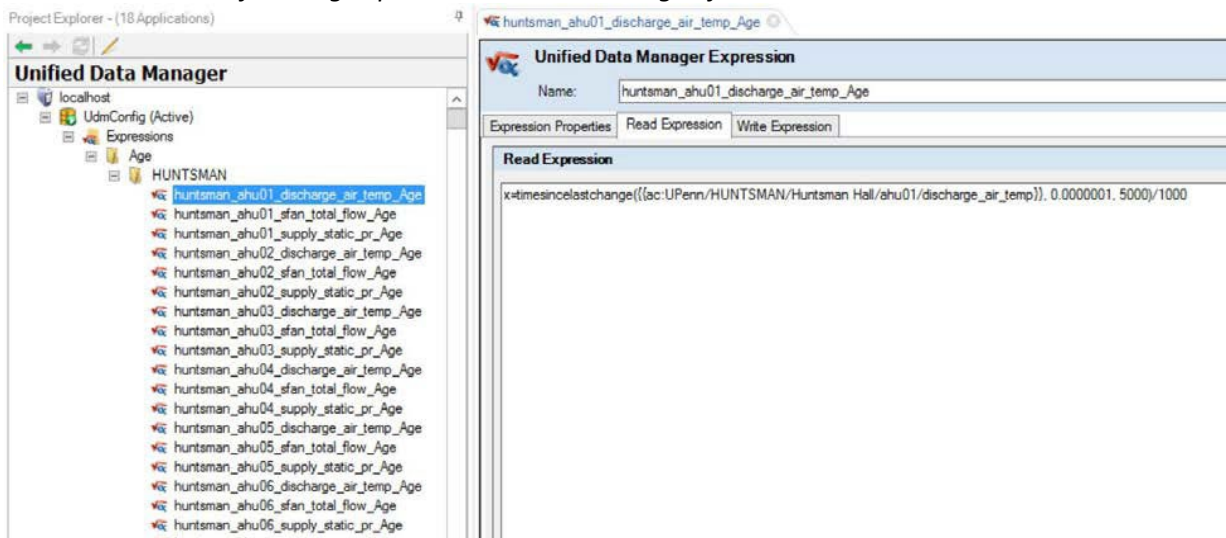


AlarmWorX Server Tree for Alarm Areas



UDM Structure for Variable Ages

UDM Tree Structure for using Expressions to Calculate Age of Variables



UDM Tree for using Registers for Assigning Calculated Age to tagnames

The screenshot shows the Unified Data Manager interface. On the left is a tree view of the database structure, including 'Registers' and 'Age' categories. The main area displays a table of registers with columns for Name, Scan Rate, and Input Tag. Below the table, a detailed view for the 'huntsman\_ahu01\_discharge\_air\_temp\_Age\_Register' is shown, including its properties and input/output configurations.

Name	Scan Rate	Input Tag
huntsman_ahu01_discharge_air_temp_Age_Register	50	@exp64:Age.HUNTSMAN.hunts
huntsman_ahu01_sfan_total_flow_Age_Register	50	@exp64:Age.HUNTSMAN.hunts
huntsman_ahu01_supply_static_pr_Age_Register	50	@exp64:Age.HUNTSMAN.hunts
huntsman_ahu02_discharge_air_temp_Age_Register	50	@exp64:Age.HUNTSMAN.hunts
huntsman_ahu02_sfan_total_flow_Age_Register	50	@exp64:Age.HUNTSMAN.hunts
huntsman_ahu02_supply_static_pr_Age_Register	50	@exp64:Age.HUNTSMAN.hunts
huntsman_ahu03_discharge_air_temp_Age_Register	50	@exp64:Age.HUNTSMAN.hunts

**Register Configuration: huntsman\_ahu01\_discharge\_air\_temp\_Age\_Register**

**Properties**

- Input OPC Tag:**  Enable
- OPC Tag: @exp64:Age.HUNTSMAN.huntsman\_ahu01\_discharge\_air\_temp\_Age.Value
- Requested Data Type: FLOAT
- Scan Rate: 50 milliseconds
- Delay: 50 milliseconds

**Input String**

- Use Initial Value

**Output OPC Tag:**  Enable

- Output Tag: ac:UPenn/HUNTSMAN/Huntsman Hall/ahu01/discharge\_air\_temp\_age
- Refresh output every: 1 seconds

UDM Structure for Smart Alarm Tags

UDM Tree Structure for using expressions to calculate smart alarm values

The screenshot shows the Unified Data Manager interface with a tree view of expressions. The main area displays the configuration for the 'event1\_1\_EnterDo' expression, including its name and the read expression code.

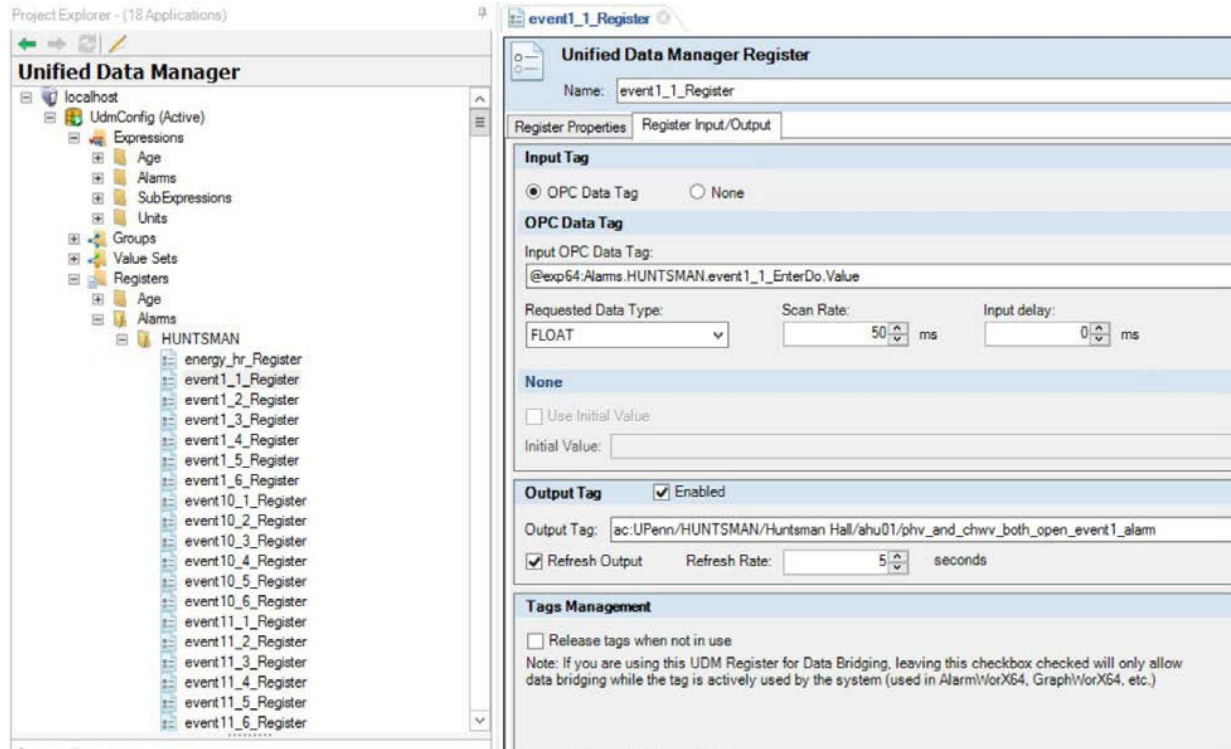
**Unified Data Manager Expression**

Name: event1\_1\_EnterDo

**Read Expression**

```
x=IF({@ICONICS.AlarmSvr_1\event1_1_Alarm.DIG_Active.Value}) == 1 THEN 1 ELSEIF ({{{@ICONICS.AlarmS
```

UDM Tree for using Registers for Assigning Calculated Values to Smart Alarm Variables



## HyperHistorian Structure

### HyperHistorian Tree Structure for Collector

Project Explorer - (12 Applications)

Collects every 1 minute

#### Hyper Historian Collector Group

Name:

#### Collector

Select Collector:

Collector overwrites SourceTimestamp of data with its actual UTC time

#### Collection Parameters

	Hours	Minutes	Seconds	MilliSeconds
Data collection rate:	0	1	0	0
<input checked="" type="checkbox"/> Force refresh rate:	0	1	0	0
Calculation period:	0	1	0	0

#### Collecting Condition

Collect On Condition

#### Info

Description:

#### Hyper Historian

- localhost
  - Hyper Historian
  - UPenn\_HistConfig
  - UPenn\_HH
  - UPenn\_HH\_Test
  - UPenn Hyper Historian
  - Hyper Historian 20150119 2244 (Active)
    - Data Collections
      - UPenn
        - COLHALL
        - HUNTSMAN
      - Groups
        - COLHALL Period-365 days
          - Collects every 1 minute
          - Collects every 5 minutes
        - COLHALL Period-90 days
        - HUNTSMAN Period-365 days
        - HUNTSMAN Period-90 days
        - Logging Group
      - Loggers
        - COLHALL 365 Days Logger
        - COLHALL 90 Days Logger
        - Data Logger
        - HUNTSMAN 365 Days Logger
        - HUNTSMAN 90 Days Logger
        - Snapshot Logger
      - Node Setup and Redundancy
        - Local Logging Server
        - COLHALL Collector
        - HUNTSMAN Collector
        - Local Collector
    - System Administration
    - Calculation Functions
    - Calculation Triggers
    - SPC Distribution Rules



HyperHistorian Tree Structure for Loggers

Project Explorer - 12 Applications

- Hyper Historian
  - localhost
    - Hyper Historian
      - UPenn\_HistConf.g
        - UPennHH
          - UPenn\_HH\_Test
            - UPenn Hyper Historian
  - Hyper Historian 20150119 2244 (Active)
    - Data Collections
      - UPenn
        - COLHALL
          - HUNTSMAN
      - Groups
        - COLHALL Period-365 days
          - Collects every 1 minute
          - Collects every 5 minutes
          - COLHALL Period-90 days
            - HUNTSMAN Period-3&5days
            - HUNTSMAN Period-90 days
          - logging Group
        - loggers
          - COLHALL 3&5 Days logger
          - COLHALL 90 Days logger
          - Data logger
          - HUNTSMAN 365 Days logger
          - HUNTSMAN 90 Days logger
          - Snapshot logger
        - Node Setup and Redundancy
        - Local logging Server
          - COLHALL CoRector
            - HUNTSMAN Collector
            - Local Collector
            - System Administration
          - Calculation Functions
          - Calculation Triggers
            - SPC Distribution Rules

COLHALL 365 Days logger Hyper

**Historian Logger** Name:

icolHALL 365 Days logger

---

**loggerSelect-**

Logger Type: Disk Logger

---

**File Storage Informalim**

Storage Mode: Universal Mode

Data Store Directory: Ic:\PennSCADA-HistoricalData\COLHALL\

Time zone:  Use local server time  Use UTC

Recurrence type: Time interval " || Preview |

Starting at: Thursday, 01-January-2015 18:02:00; 0 - |

Recur every: 365 Days 0 Hours 0 Mins 0 Sees

---

**Archiving Inbnillioo**

Storage Unit

Condition: Minimum Time Extent

Min time extent: = Days 0 Hours

Max total size: 10240 Mega Bytes

Check condition:  Every = Mns 0: Sees

On Event

Action

Take action: Archive older files

Data Archive Directory: L



## Graphics Structure

All GraphWorX64 .gdfx files for each cluster is kept in the local cluster server. The directory structure is:

C:\UPenn\Cluster Name\\*.gdfx. e.g. C:\UPenn\HUNTSMAN\AHU01.gdfx

For View stations such as OCC1, OCC2 & OCC3, Graphics files for all clusters are located on each.

### HUNTSMAN Server Graphics Files Directory

Name	Date modified	Type	Size
huntsman_4mer_exh	4/2/2015 11:24 AM	GraphWorX64 Display	74 KB
huntsman_4mer_exh_ctl	6/15/2015 10:14 AM	GraphWorX64 Display	50 KB
huntsman_ahu01	11/19/2015 1:56 PM	GraphWorX64 Display	1,059 KB
huntsman_ahu01_ctl	11/19/2015 1:58 PM	GraphWorX64 Display	1,553 KB
huntsman_ahu01_trnd	9/28/2015 1:47 PM	GraphWorX64 Display	127 KB
huntsman_ahu02	11/17/2015 4:37 PM	GraphWorX64 Display	1,061 KB
huntsman_ahu02_ctl	11/17/2015 4:35 PM	GraphWorX64 Display	1,559 KB
huntsman_ahu02_trnd	9/28/2015 1:49 PM	GraphWorX64 Display	128 KB
huntsman_ahu03	11/17/2015 4:39 PM	GraphWorX64 Display	1,055 KB
huntsman_ahu03_ctl	11/17/2015 4:41 PM	GraphWorX64 Display	1,559 KB
huntsman_ahu03_trnd	9/28/2015 1:50 PM	GraphWorX64 Display	129 KB
huntsman_ahu04	11/17/2015 4:45 PM	GraphWorX64 Display	1,083 KB
huntsman_ahu04_ctl	11/17/2015 4:43 PM	GraphWorX64 Display	1,585 KB
huntsman_ahu04_trnd	9/28/2015 1:53 PM	GraphWorX64 Display	130 KB
huntsman_ahu05	11/17/2015 4:48 PM	GraphWorX64 Display	1,086 KB
huntsman_ahu05_ctl	11/17/2015 4:47 PM	GraphWorX64 Display	1,590 KB
huntsman_ahu05_trnd	9/28/2015 1:54 PM	GraphWorX64 Display	131 KB
huntsman_ahu06	11/17/2015 4:51 PM	GraphWorX64 Display	919 KB
huntsman_ahu06_ctl	11/17/2015 4:50 PM	GraphWorX64 Display	1,305 KB
huntsman_ahu06_trnd	9/28/2015 1:56 PM	GraphWorX64 Display	105 KB
huntsman_chw_sys	11/13/2015 2:12 PM	GraphWorX64 Display	403 KB
huntsman_chw_sys_ctl	11/13/2015 2:14 PM	GraphWorX64 Display	419 KB
huntsman_chw_sys_trnd	9/28/2015 2:01 PM	GraphWorX64 Display	61 KB
huntsman_chw_trnd	9/28/2015 2:02 PM	GraphWorX64 Display	45 KB
huntsman_emp01	11/18/2015 7:50 AM	GraphWorX64 Display	625 KB
huntsman_emp01_trnd	9/28/2015 2:03 PM	GraphWorX64 Display	37 KB
huntsman_emp02	11/18/2015 8:16 AM	GraphWorX64 Display	625 KB
huntsman_emp02_trnd	9/28/2015 2:05 PM	GraphWorX64 Display	36 KB
huntsman_fire_panel	4/2/2015 12:09 PM	GraphWorX64 Display	704 KB
huntsman_fir2_crmvav_ctl	6/15/2015 10:40 AM	GraphWorX64 Display	1,426 KB
huntsman_fir2_crmvav_trnd	9/28/2015 2:17 PM	GraphWorX64 Display	121 KB

OCC1 Graphics Files Directory

Name	Date modified	Type	Size
COLHALL	1/11/2015 12:27 PM	File folder	
HUNTSMAN	2/9/2016 10:01 AM	File folder	
AlarmWorX Config - COLHALL	4/17/2015 5:24 PM	Workbench Alarm	46 KB
AlarmWorX Config - HUNTSMAN	4/17/2015 5:24 PM	Workbench Alarm	42 KB
AlarmWorX Config - UPenn	12/1/2015 9:30 AM	Workbench Alarm	45 KB
AlarmWorX Viewer - COLHALL	4/17/2015 5:22 PM	GraphWorX64 Display	15 KB
AlarmWorX Viewer - HUNTSMAN	4/17/2015 5:20 PM	GraphWorX64 Display	24 KB
AlarmWorX Viewer - UPenn	12/1/2015 9:42 AM	GraphWorX64 Display	25 KB
bldg_group_6	11/18/2015 7:19 PM	GraphWorX64 Display	70 KB
bldg_group_7	11/18/2015 7:17 PM	GraphWorX64 Display	7 KB
bldg_group_8	11/18/2015 7:16 PM	GraphWorX64 Display	6 KB
bldg_group_9	11/18/2015 7:14 PM	GraphWorX64 Display	9 KB
bldg_power	11/18/2015 7:12 PM	GraphWorX64 Display	201 KB
bldg_steam_sys	11/18/2015 7:11 PM	GraphWorX64 Display	23 KB
bldgs_overview	11/18/2015 7:09 PM	GraphWorX64 Display	1,051 KB
brb1start	11/18/2015 7:01 PM	GraphWorX64 Display	8 KB
bridge_stat	11/18/2015 6:59 PM	GraphWorX64 Display	107 KB
campus_chw_overview	11/18/2015 6:57 PM	GraphWorX64 Display	1,170 KB
campus_chw_piping	11/18/2015 6:56 PM	GraphWorX64 Display	3,582 KB
campus_chw_piping1	11/18/2015 6:54 PM	GraphWorX64 Display	6 KB
campus_chw_piping2	11/18/2015 6:52 PM	GraphWorX64 Display	2,674 KB
campus_chw_pump_new	11/18/2015 6:50 PM	GraphWorX64 Display	993 KB
campus_chw_pumps	11/18/2015 6:48 PM	GraphWorX64 Display	992 KB
campus_chw_quad1	11/18/2015 6:46 PM	GraphWorX64 Display	1,277 KB
campus_chw_quad2	11/18/2015 6:44 PM	GraphWorX64 Display	936 KB
campus_chw_quad3	11/18/2015 6:42 PM	GraphWorX64 Display	1,124 KB
campus_chw_quad4	11/18/2015 6:41 PM	GraphWorX64 Display	645 KB
campus_lighting	11/18/2015 6:40 PM	GraphWorX64 Display	296 KB
campus_lighting_hw	11/18/2015 6:38 PM	GraphWorX64 Display	351 KB
campus_steam_ne_piping	11/18/2015 6:37 PM	GraphWorX64 Display	122 KB
campus_steam_nw_piping	11/18/2015 6:34 PM	GraphWorX64 Display	137 KB

161 items

## BACnet Structure

### HUNTSMAN BACnet Tree Structure

The screenshot displays a BACnet configuration interface. On the left is a tree view of the BACnet structure, and on the right is a detailed view of a selected object.

**BACnet Tree Structure:**

- localhost
  - BACnet
    - HUNTSMAN\_BACnet
      - Devices
        - Network 1
          - JMHH-NAE10 (510)
            - AnalogInput Objects
            - AnalogOutput Objects**
            - AnalogValue Objects
            - BinaryInput Objects
            - BinaryOutput Objects
            - BinaryValue Objects
            - Device Objects
            - MultistateOutput Objects
            - Program Objects
            - TrendLog Objects
            - JMHH-NAE11 (509)
            - JMHH-NAE19 (507)
            - JMHH-NCE1 (501)
            - JMHH-NCE2 (502)
            - JMHH-NCE3 (503)
            - JMHH-NCE4 (504)
            - JMHH-NCE5 (505)
            - JMHH-NCE6 (506)
          - Network 5
          - Ports

**AnalogOutput Objects Table:**

Name	Property	Polling Rate	Priority
JMHH-NAE10/N2-1.DX10-200.CHP1-VFD (7194932)			
JMHH-NAE10/N2-1.DX10-200.CHP1Setp (7194949)			
JMHH-NAE10/N2-1.DX10-200.CHP2-VFD (7194939)			
JMHH-NAE10/N2-1.DX10-200.CHW-BYPV (7194957)			
JMHH-NAE10/N2-1.DX10-200.CHWV-VLV (7194953)			
JMHH-NAE10/N2-1.DX10-200.CHWSSWPT (7194958)			
JMHH-NAE10/N2-1.DX10-200.Delta-SP (7194946)			
JMHH-NAE10/N2-1.DX10-200.SecRetSP (7194944)			
JMHH-NAE10/N2-1.DX10-200.Sel-DPT (7196982)			

**Object Type: AnalogOutput Objects**

Selected Object: JMHH-NAE10/N2-1.DX10-200.CHP1-VFD (7194932)

Group	List
<b>Basic / Object</b>	
Description	CHP-1 VFD Speed Control
Object Type	Analog Output
Present Value	0
<b>Basic / Status</b>	
Reliability	No Fault Detected
Out Of Service	<input type="checkbox"/>
<b>Advanced / Engineering Values</b>	
Relinquish Default	0.00000
Min Value	0.00000
Max Value	105.00000





Buttons: Apply, Close, Refresh, Reset

## Access to Graphics and Navigation through Graphics

### Introduction

The HMI application should be developed with GraphWorX64. The application will allow users to view status, alarms and trend information for various equipment. All graphics screens should be configured for 1920x1080 with true color support. The Font Family used for graphics is Arial.

#### Runtime and other properties of Graphics

<b>Runtime</b>	
ZoomEnabled	True
PanEnabled	True
ScanRate	<b>100</b>
DesiredFrameRate	Automatic
ReleaseOutOfViewData	False
CachePriority	Normal
ShowControlCursor	True
ShowControlFocus	True
DisableControlWhenReadOnlyData	True
DisableControlWhenSecurityDenied	True
UseDisabledColors	<b>False</b>
DisabledFillColor	 192, 192, 192
DisabledLineColor	 128, 128, 128
UsePointFailColors	True
PointFailFillColor	 <b>255, 255, 224</b>
PointFailLineColor	 128, 128, 128
UsePointFailText	True
PointFailText	*
SpecifyRuntimeWindowProperties	True
RuntimeWindowProperties	
DisplayTabs	
LocalAliases	<b>(Collection)</b>
GlobalAliases	
ResolveAliasesInDragDropDataSources	True
Transition	None
SafeTouchZoneWarningDuration	Infinite
<b>Runtime - Compatibility</b>	
DisableControlWhenAnyRelatedDynamicsDisabled	False
HideDynamicActiveWhenPointFailure	False
StateFieldDropDownUsesSystemColors	False

RuntimeWindowProperties

SpecifyWindowLocation	True
SpecifyWindowSize	True
SpecifyWindowStyle	True
SpecifyCommandingOptions	True
StartLocation	CJ Manual
Left	0
Top	0
Width	1220.42980902695
Height	767.246189376443
WindowState	Normal
TitleBarVisible	True
Text	.....sman\huntsman_hw_sys_ctl
ControlBox	True
MinimizeBox	True
MaximizeBox	True
OuterBorder	True
Resizable	True
ToolWindow	False
InnerBorder	True
InnerBorderBrush	D 160.160.160
InnerBorderThickness	E1 1
HorizontalScrollBarVisible	fitJ.to
VerticalScrollBarVisible	fitJ.to
SpecifyScrollBarColors	False
RibbonVisible	False
MenuVisible	False
NavigationBarVisible	False
StatusBarVisible	False
ShowContextMenu	True
TopMost	False
CommandingEnabled	True
DragAndDropCommandingEnabled	True
CommandingName	
CommandingDisplayName	
MaxCommandScope	Process
OverridePreviousDisplay	False

▷ RuntimeWindowProperties	
▷ DisplayTabs	
LocalAliases	<b>(Collection)</b>
GlobalAliases	
ResolveAliasesInDragDropDataSources	True
Transition	None
SafeTouchZoneWarningDuration	Infinite
▣ <b>Runtime - Compatibility</b>	
DisableControlWhenAnyRelatedDynamicsDisabled	False
HideDynamicActiveWhenPointFailure	False
StateFieldDropDownUsesSystemColors	False
▣ <b>Script</b>	
References	(Collection)
Namespaces	(Collection)
▣ <b>ToolTip</b>	
ShowToolTips	True
IncludeObjectDescription	True
IncludeDynamicDescription	True
IncludeDataSourceName	True
IncludeDataSourceValue	True
IncludeErrorInformation	True
▣ <b>Visual Quality</b>	
SnapsToDevicePixels	False
EdgeMode	Default
BitmapScalingMode	Unspecified



The purpose of this section is to describe the graphical interface for the Physical Plant’s Building Automation Control (BAC) at the University of Pennsylvania. The graphical interface provides the user a real life graphical look of the BAC system on campus from the Operations Control Center (OCC). The main screen is the University Buildings Overview Screen. Clicking on an individual building brings up the Building Overview Screen. This screen provides a summary of the HVAC conditions within a building. From this screen further detail on the conditions and distribution network within a building or information regarding the operation of equipment involved in the conditioning of the air supplied to the building can be obtained by selecting subsequent screens. Clicking on the blinking “SERVER” box (blinking identifies active and operational) will bring up hardware summary screens. These hardware summary screens show the communication status for all communication interfaces for each server.

**Graphical Symbols**

All symbols should be created according to ISA Standard S5.1 Instrumentation Symbol Specification.

The figure below shows the graphical symbols used in the University SCADA.



**Color Standards**

**Screen Background Colors**

Equipment view	light grey
Overview, plan view	light green
Trend screens	light green and black
Point control	black

*ON/OFF Equipment Color Changes*

Item	ON	OFF	ON FAIL	OFF FAIL	NOT AVAILABLE
Pumps	Green	Red	Blinking red	Blinking green	Yellow
Fans	Green	Red	Blinking red	Blinking green	Yellow
Chillers	Green	Red	Blinking red	Blinking green	Yellow
Electric heat	Green	Red	Blinking red	Blinking green	Yellow
Unit heaters	Green	Red	Blinking red	Blinking green	Yellow

*OPEN/CLOSE Equipment Color Changes*

Item	Fully Open	Modulating/Modulating	Fully Closed
Dampers	Yellow	Green	Red
Valves	Yellow	Green	Red
VAV/Reheat Boxes	Yellow	Green	Red

*Status of Equipment*

Equipment	Normal	Alarm
Smoke detector	Cyan	Flashing red
Filter	Cyan	Flashing red
Freezestat	Cyan	Flashing red

*Miscellaneous - I/O Devices and Circuit Breakers*

DDC control units & I/O Devices	Communicating	Not communicating
	Green	Red
Circuit breakers	CLOSED/ENERGIZED	OPEN/NON ENERGIZED
	Green	Red

*Process / Field Values*

Item	Color
Numeric value	cyan
Alarm box under numeric value if alarmed <ul style="list-style-type: none"> <li>• LO LO</li> <li>• LO</li> <li>• HI</li> <li>• HI HI</li> </ul>	Blinking red Red Yellow Blinking yellow
Point control windows (faceplate) <ul style="list-style-type: none"> <li>• process value</li> <li>• setpoint</li> <li>• control output</li> </ul>	cyan light yellow grey

**Fluids - General Color Code**

Fluid	Color	System
Glycol	Light blue	Air handling unit (AHU)
Hot water	Light blue	Air handling unit (AHU)
chilled water	Dark blue	Air handling unit (AHU)
Steam	White	All
Condenser water	Dark green	Chillers

**Exceptions**

*MOD III Chiller 1:* Refrigerant - cyan, pink, red, depending on temperature and whether liquid or gas

*MOD VI Glycol*

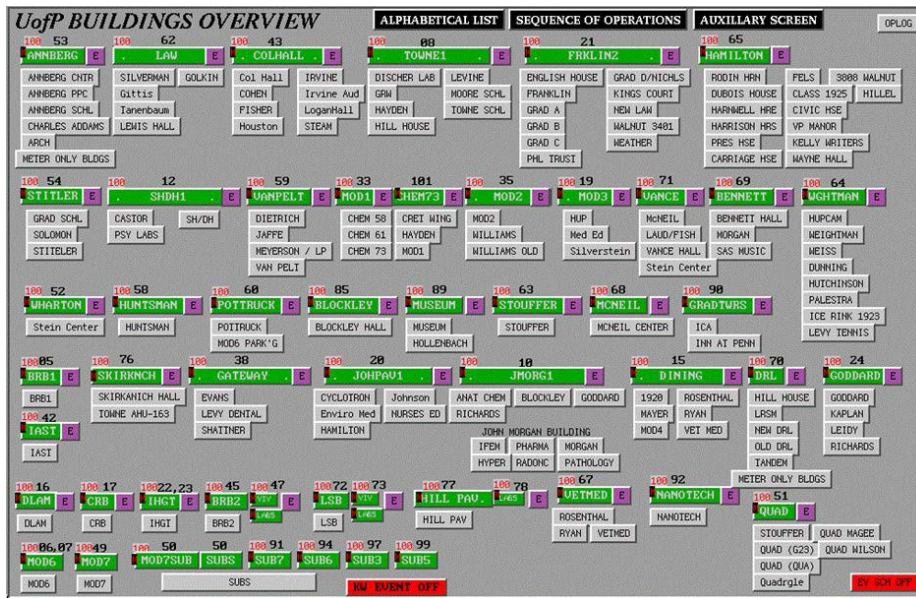
inactive	black
chw via ch4-6	light blue
ice melt	yellow
ice build	white

**Graphics Navigation, Types and Functionality****Click Actions**

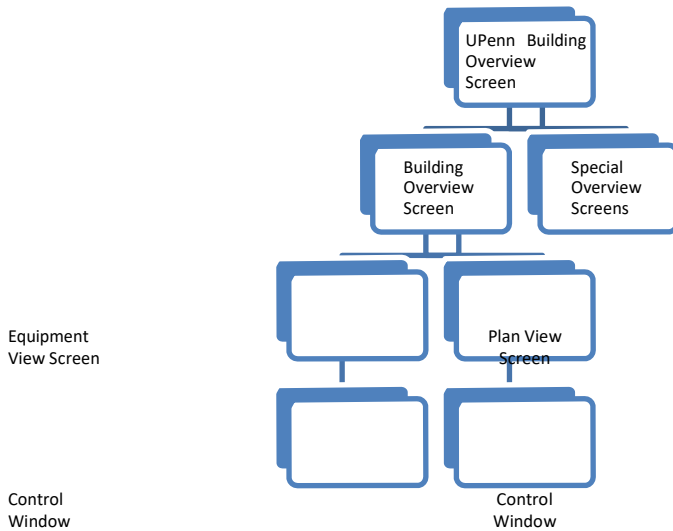
Item/Symbol	Action
Box with text in it e.g. <div style="border: 1px solid black; display: inline-block; padding: 2px 10px; margin: 5px 0;">CHWS</div>	Connect systems. In the example on the L.H.S., a click on the box goes to the system supplying the fluid
Control element e.g. pump, valve, etc	Goes to control windows
GO TO button	Selects graphic/system to go to
TREND Button	Goes to trend of selected system
Tag display	Display or hide instrument tags used in description of sequence of operations

**University Buildings Overview Screen**

This is the screen that opens when the ICONICS Gen64 SCADA starts. The screen displays all the server computers on campus and the buildings under each. The server name box at the top of the list of buildings flashes (green/dark grey) as a heartbeat signal to show that the graphics are link to the server. Also, clicking of the server name box which brings up a hardware overview screen that shows the control hardware connected to that server.



Graphical Interface Flow Chart



Building Overview Screens

A Building Overview Screen provides a summary of the current operational state of the equipment within that building. It also provides an alarm summary for the smart alarms present in the building. The following table shows the items that can be selected from a Building Overview Screen.

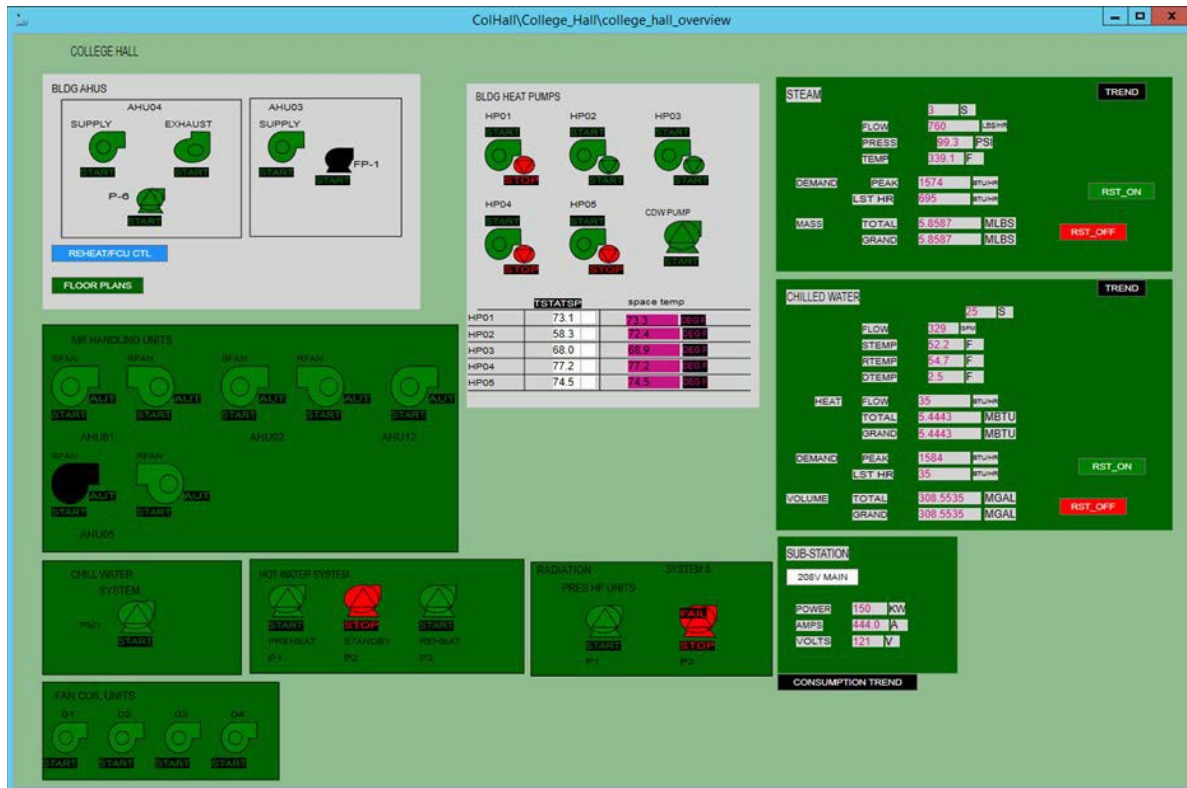
Table 0-1: Click actions on Building Overview Screens

Item Selected	Resultant Screen
---------------	------------------

Any of the HVAC equipment shown on the Building Overview Screen.	Equipment View containing the piece of equipment that was clicked on.
DETAIL PLAN	Plan View Screen

TREND button brings up window with a list of all the summary trends for HVAC systems within the building	Trend View
HARDWARE button (some overviews)	Hardware Overview

*Building Overview Screen (Non-Animal Facility)*



Building Overview Screen (Animal Facility) (Legacy Screen Shown- To be Updated)

ihgt/ihgt\_overview

(Close) (Cancel) (Print) (Help...)

### JM3 - ULAR VIVARIUM (AUTOMATRIX) (PREVIOUSLY IHGT)

**PLAN VIEW**

**ANIMAL ROOMS** TREND

341	71.0 F	53.8 %RH	+ve	→	-ve	342	69.5 F	46.8 %RH	+ve	→	-ve
342	69.5 F	46.8 %RH	+ve	→	-ve	343	70.2 F	52.8 %RH	+ve	→	-ve
343	70.2 F	52.8 %RH	+ve	→	-ve	344	70.5 F	38.8 %RH	+ve	→	-ve
344	70.5 F	38.8 %RH	+ve	→	-ve	345	71.0 F	48.8 %RH	+ve	→	-ve
345	71.0 F	48.8 %RH	+ve	→	-ve	346	70.6 F	51.8 %RH	+ve	→	-ve
346	70.6 F	51.8 %RH	+ve	→	-ve	349	73.1 F	57.8 %RH	+ve	→	-ve
349	73.1 F	57.8 %RH	+ve	→	-ve	352	72.1 F	43.8 %RH	+ve	→	-ve
352	72.1 F	43.8 %RH	+ve	→	-ve	353	70.2 F	48.8 %RH	+ve	→	-ve
353	70.2 F	48.8 %RH	+ve	→	-ve	354	71.8 F	54.8 %RH	+ve	→	-ve
354	71.8 F	54.8 %RH	+ve	→	-ve						

**NON ANIMAL ROOMS** TREND

348	72.2 F	CORR 2	-30. F
344A	23 CFM	368	77.2 F
347	71.9 F	371	75.9 F
348	25 CFM	372	78.2 F
CORR 1	70.8 F	LOCK	74.7 F
350	70.5 F	VEST	71.9 F
351	71.9 F	375	66.2 F
CORR 2A	73.2 F	CORR 3	71.5 F
370	281 CFM	374	74.2 F
		376	

=Procedure room

**AHU01**

SA-1A SA-1B  
STOP START

COND. UNIT  
EL. HUMID

GLYCOL PUMPS  
 P1 P2  
OK NO FLOW

EL. PREHEAT

**CORRIDOR PROG CTL**

**EXHAUST FANS**

EF-1 EF-2  
START STOP

**EMERGENCY MODE -- NORMAL**

**ATC COMP** Procedure Room  
 PRESSURE NORMAL RM 341

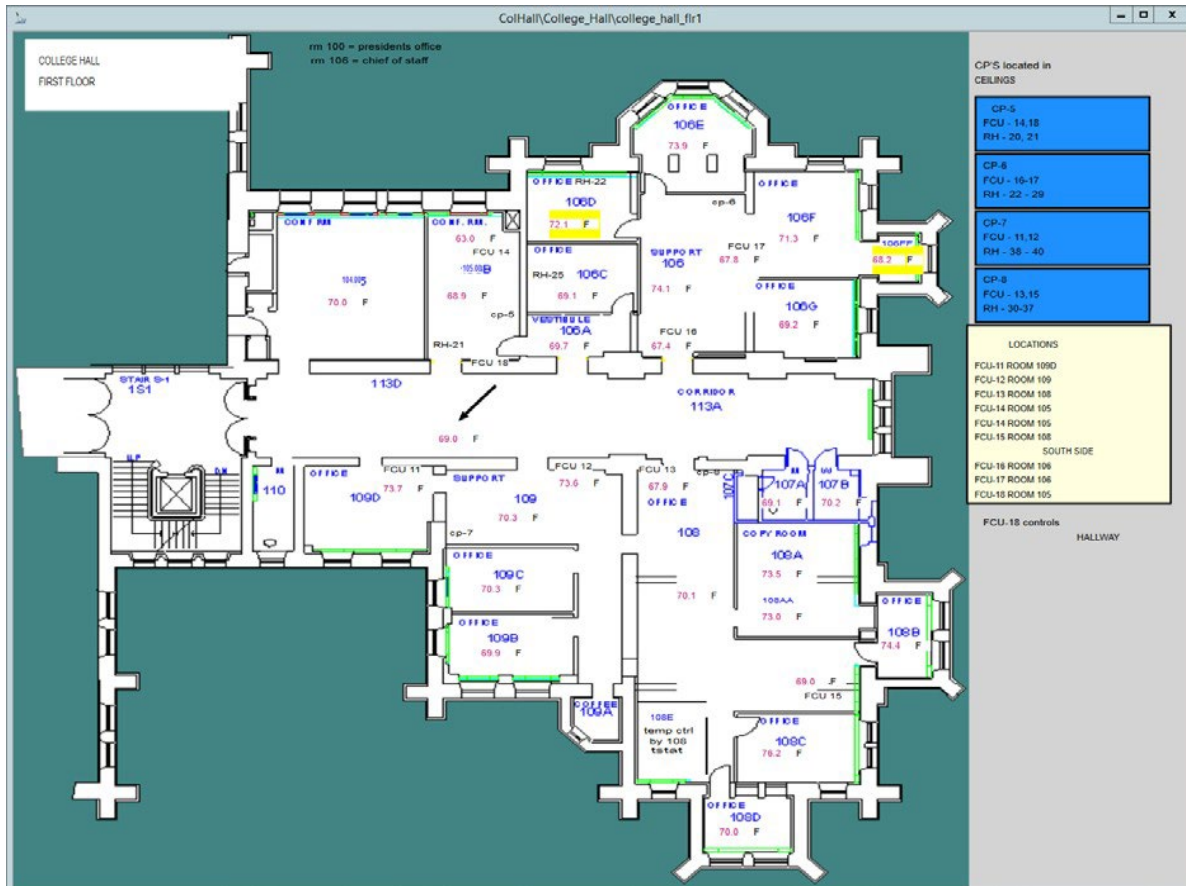
**SUMMARY OF ALARMS**

CLASS	#	MSG
FIRE	0	MSG
ENERGY	0	MSG
ANIMAL	887	MSG
HVAC	24	MSG
COMM.	0	MSG

**Plan View Screen (Not currently available for all buildings)**

The purpose of the Plan View Screen is to provide a more detailed view of the HVAC elements located on a particular floor. Temperatures and humidities are shown in the approximate location where the reading is being taken within the room.

Each temperature and humidity has an alarm box that changes colors as described earlier. Clicking on temperature or humidity brings up the control window or the trend for that room.

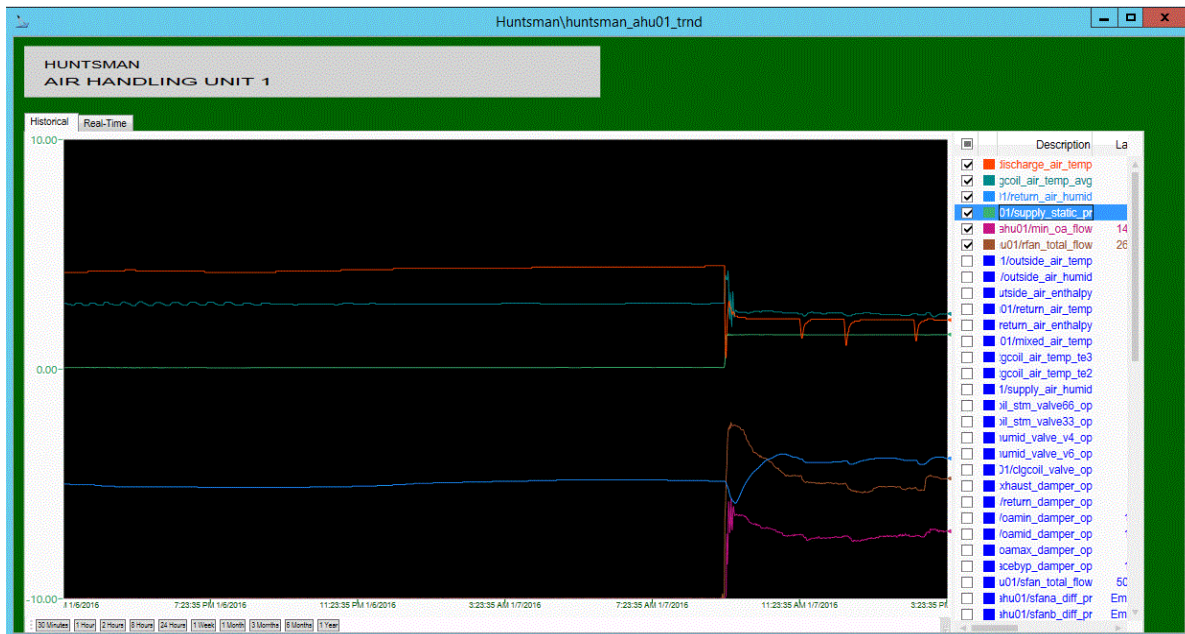


**Trend View Screen**

The purpose of the trend screen is to get a historical view of critical process values - useful in trouble shooting HVAC systems. The historical information is stored on HIST1 and HIST2 and using the trend tool box one can go back in time to view historical values. The screen can also be used to view real-time process values. Using the trend tool box which appears by double clicking anywhere on the trend screen, the time scale (display time), trend colors, variables and ranges (low/high limits) to display in the trend window can be changed.

The trends should have Historical and Real-Time Tabs for realtime and historical trends as shown below.





Real time trend pen DataSource example is:

ac:UPenn/HUNTSMAN/Huntsman Hall/ahu02/return\_air\_temp

Historical trend pen DataSource example is:

ua:HIST\Configuration/UPenn/HUNTSMAN/Huntsman Hall/ahu02/return\_air\_temp

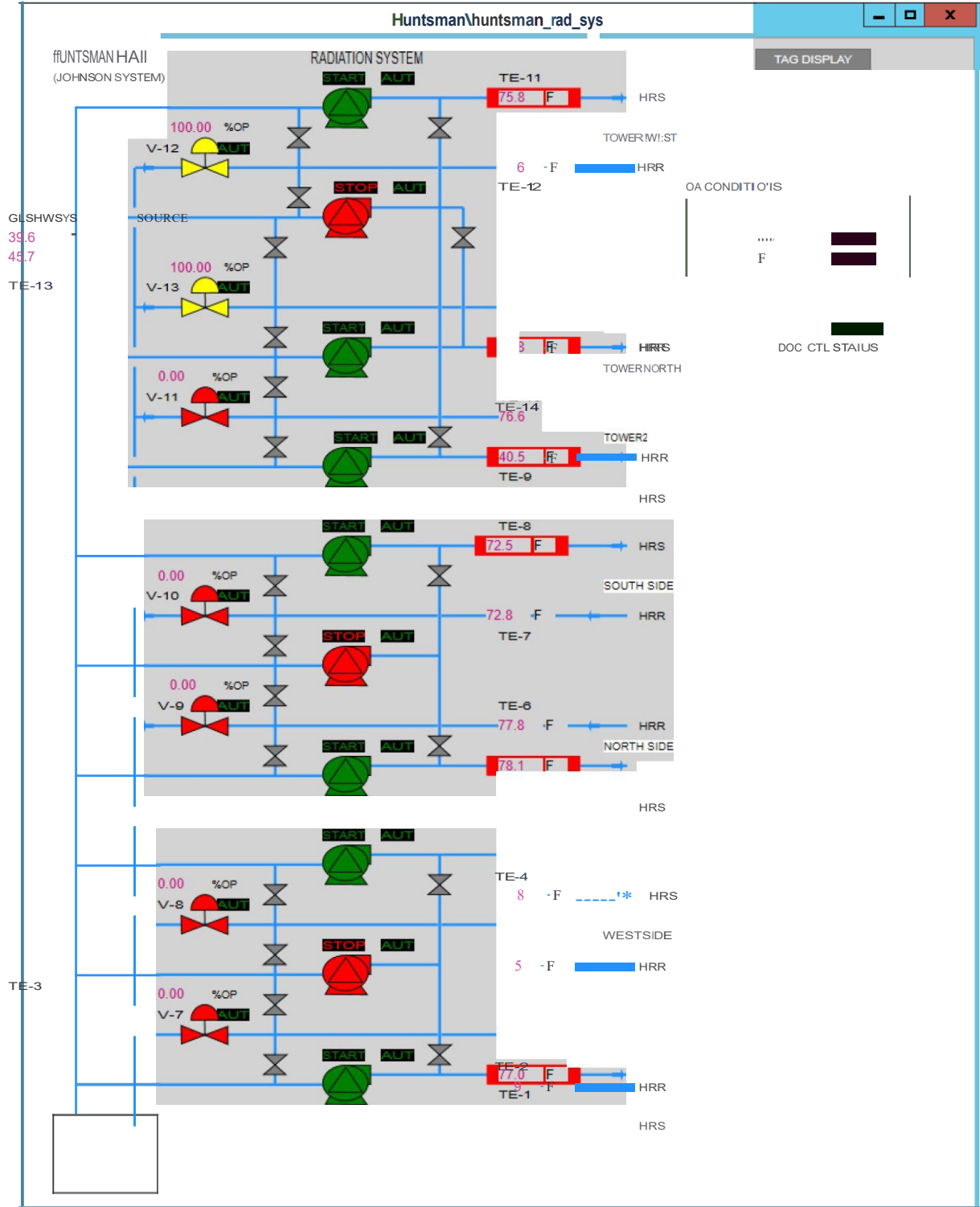
### HVAC Equipment View Screen

HVAC equipment view screens provide a P&ID style screen representing the operation of the equipment group / HVAC system the equipment is part of. The purpose of the HVAC Equipment Screen is to show the real time operation of the HVAC system or equipment group. From this view, motors can be started or stopped, valves can be opened or closed, and setpoints can be adjusted through a Point Control Window (Faceplate). Critical process values such as discharge air temperatures on this screen have an associated alarm box that changes color as described earlier.

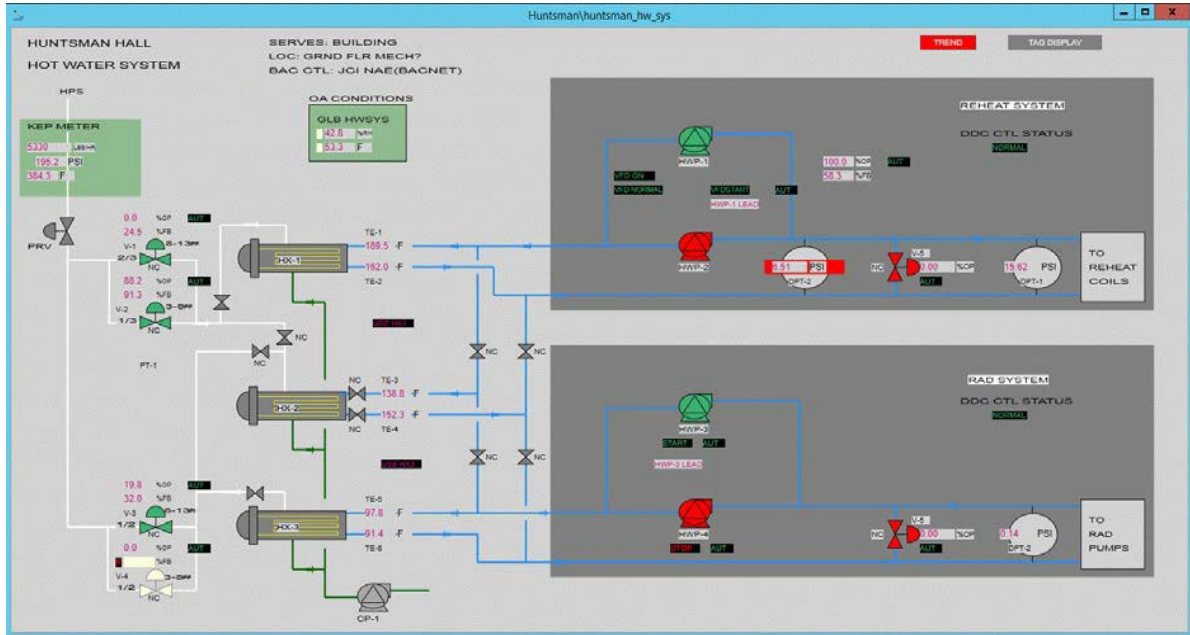
Selectable Items	Resultant Screen
Any control element such as valves, dampers, pumps, fans, vav boxes, fan coil units, etc.	Control Window
Box that identifies supply or return piping	Equipment View of the associated system and will bring up the overview of that system.
TREND button	Trend View for the that particular system



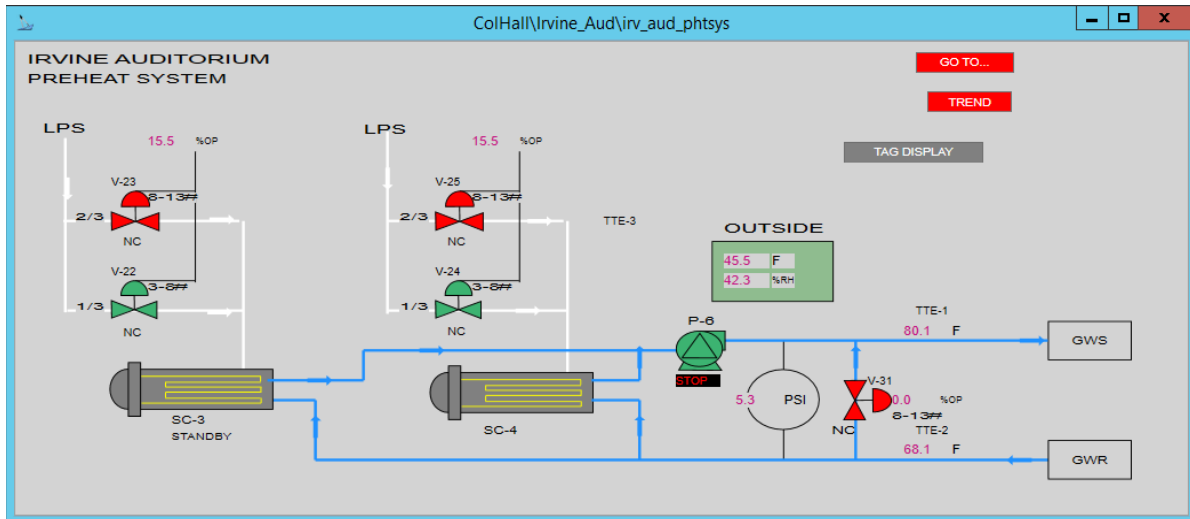
HVAC Equipment View Screen (Radiation System)



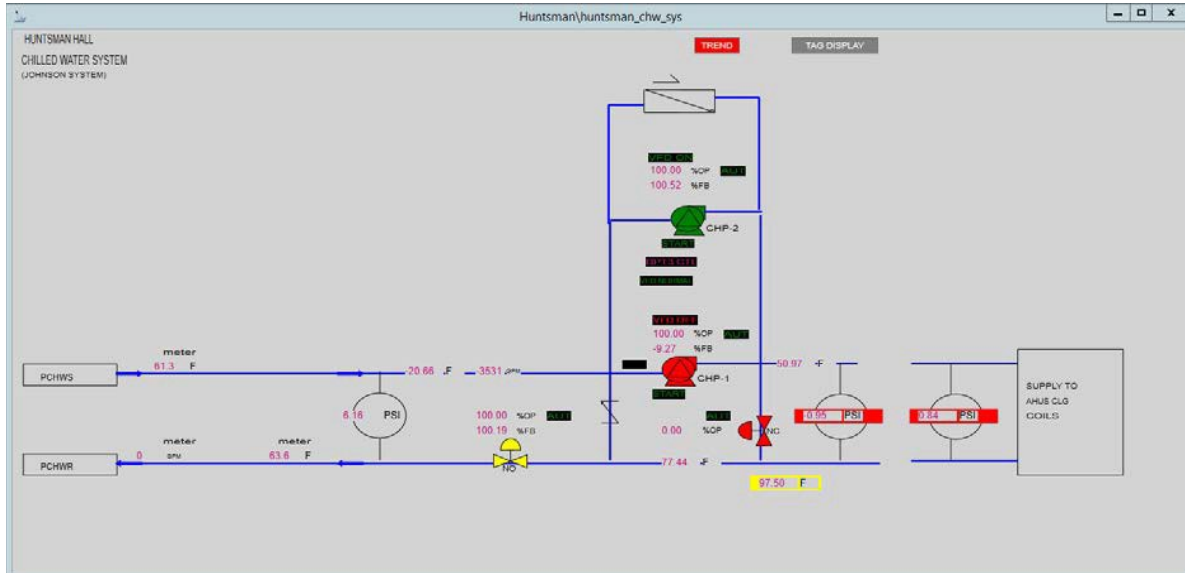
*HVAC Equipment View Screen (Reheat/Rad System)*



*HVAC Equipment View Screen (Preheat System)*



**HVAC Equipment View Screen (Building Chilled Water System)**



**Control Window**

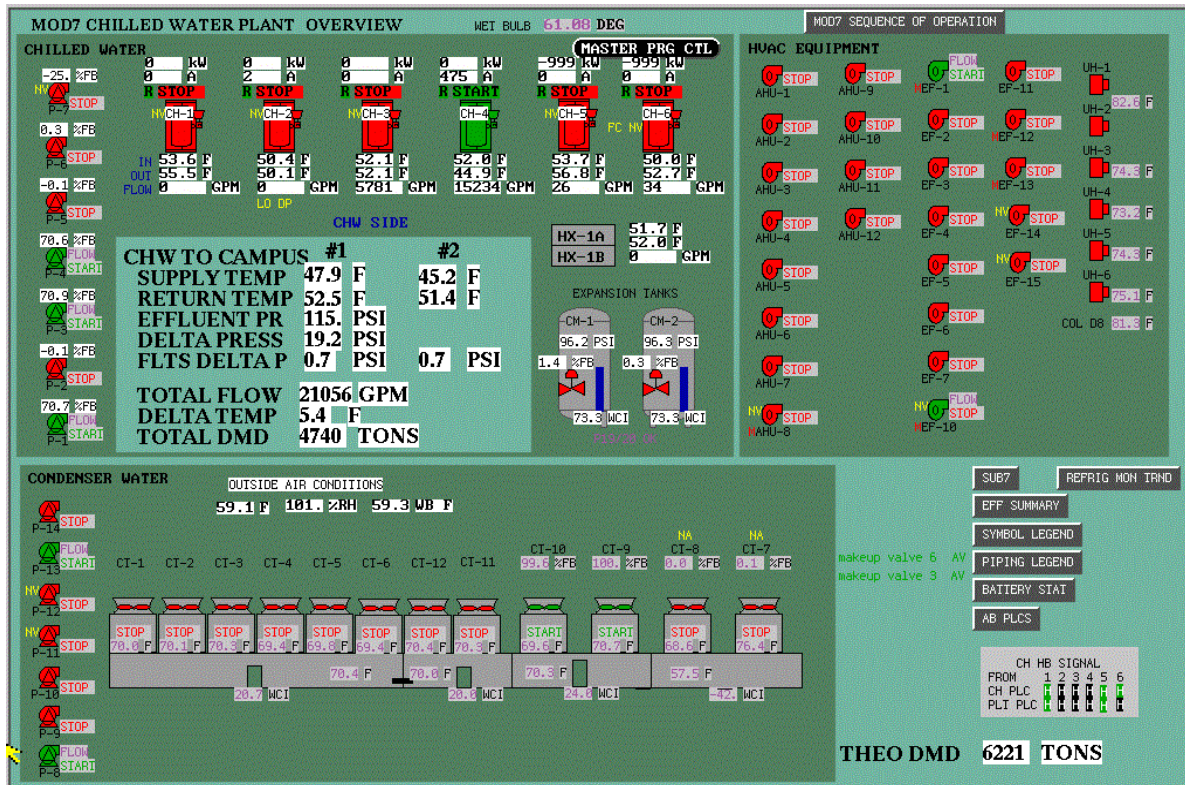
This window provides a way to control the system selected. Selecting any control element from the equipment view screen will bring up the control screen. From this operator can change setpoints, start/stop equipment, and open/close valves.

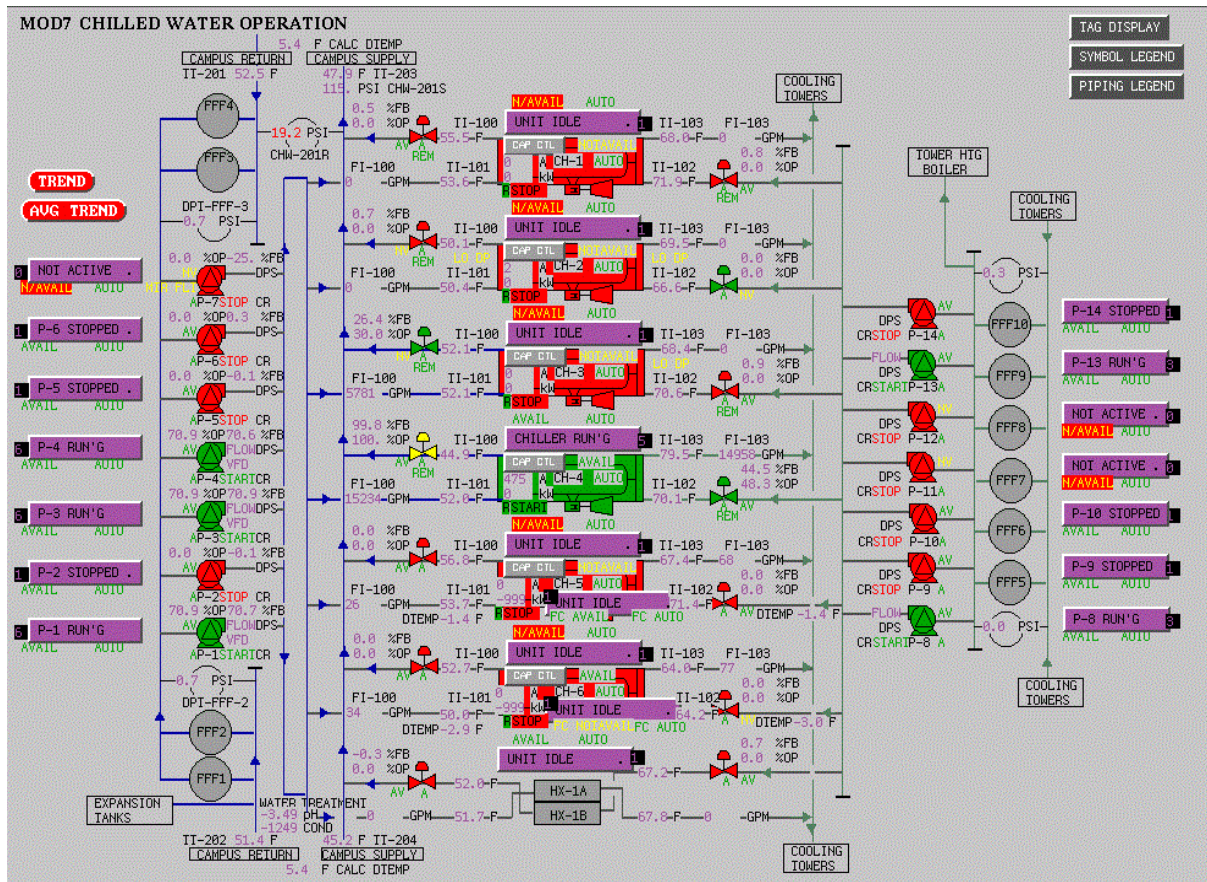
**Chiller Plant View Screen (Legacy Screen Shown - To be Updated)**

Chiller Plant View Screens provide a P&ID type screen that represent the operation of the plant. To depict the chiller plant operation graphically may require more than one screen. If the chiller plant view involves several screens, the operator will be able to page forward and backward between these screens.

The purpose of this screen is to view the real time operation of the chiller plant. From this view, motors can be started or stopped, valves can be opened or closed, and setpoints can be adjusted, all through the Control Window which can be accessed by clicking on the control object.

Selectable Items	Resultant Screen
Any control element such as valves, dampers, pumps, fans, vav boxes, fan coil units, etc.	Control Window
Box that identifies supply or return piping	Continuation of Chiller Plant or Chilled Water System Overview
GO TO button	Equipment View for Chiller Plant Sub-systems
TREND button	Trend View for Chiller Plant Sub-system





**Campus CHW Piping Screen (Legacy Screen Shown - To be Updated)**

The purpose of this screen is to show which chiller plant is feeding a particular building. The following process values are shown:

Chiller plants    influent/effluent temperature, delta pressure, influent/effluent pressure

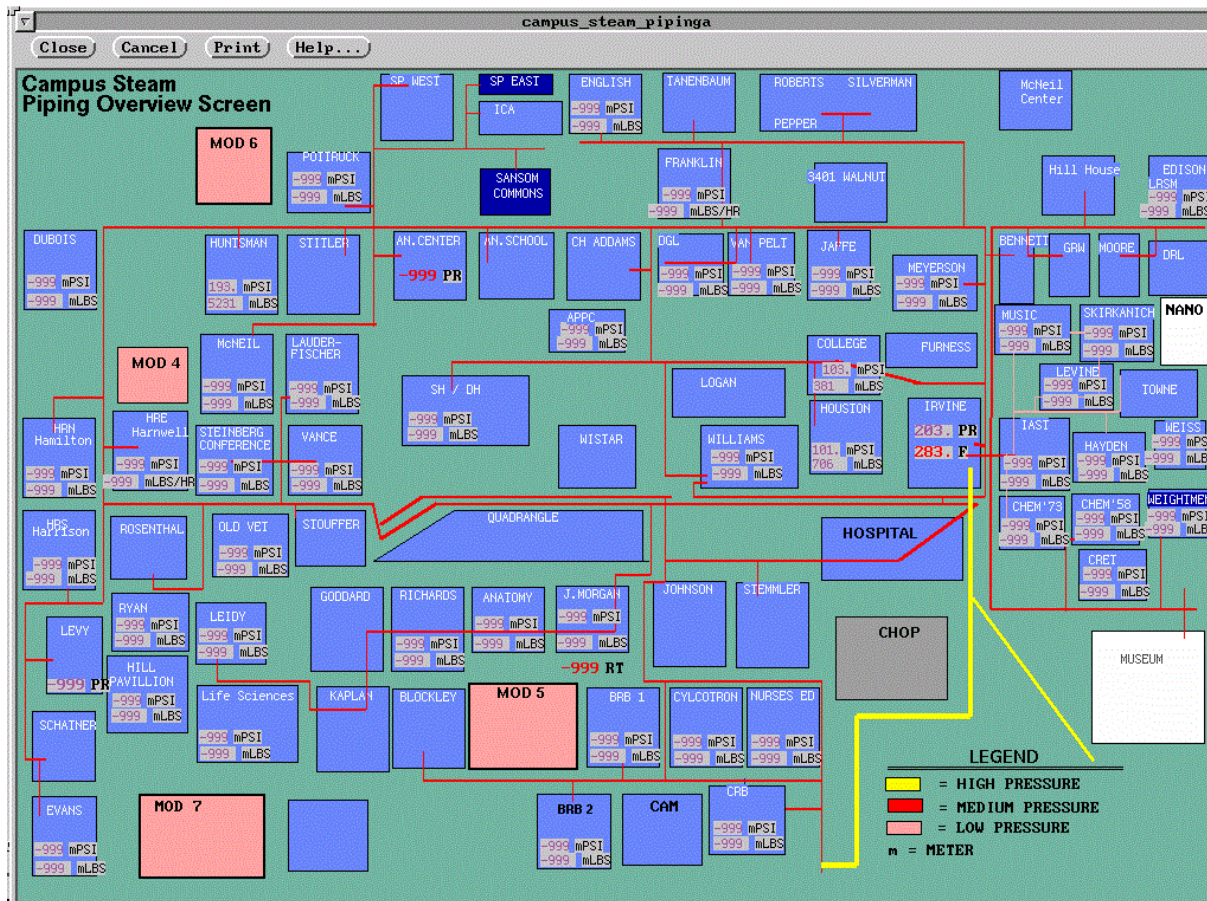
Building CHW supply    influent/effluent temperature, delta pressure, influent/effluent pressure

*Campus Steam Piping Screen (Legacy Screen Shown - To be Updated)*

The purpose of this screen is to show the steam being fed to each building. The following process values are shown:

Building Steam supply    delta pressure, steam flow





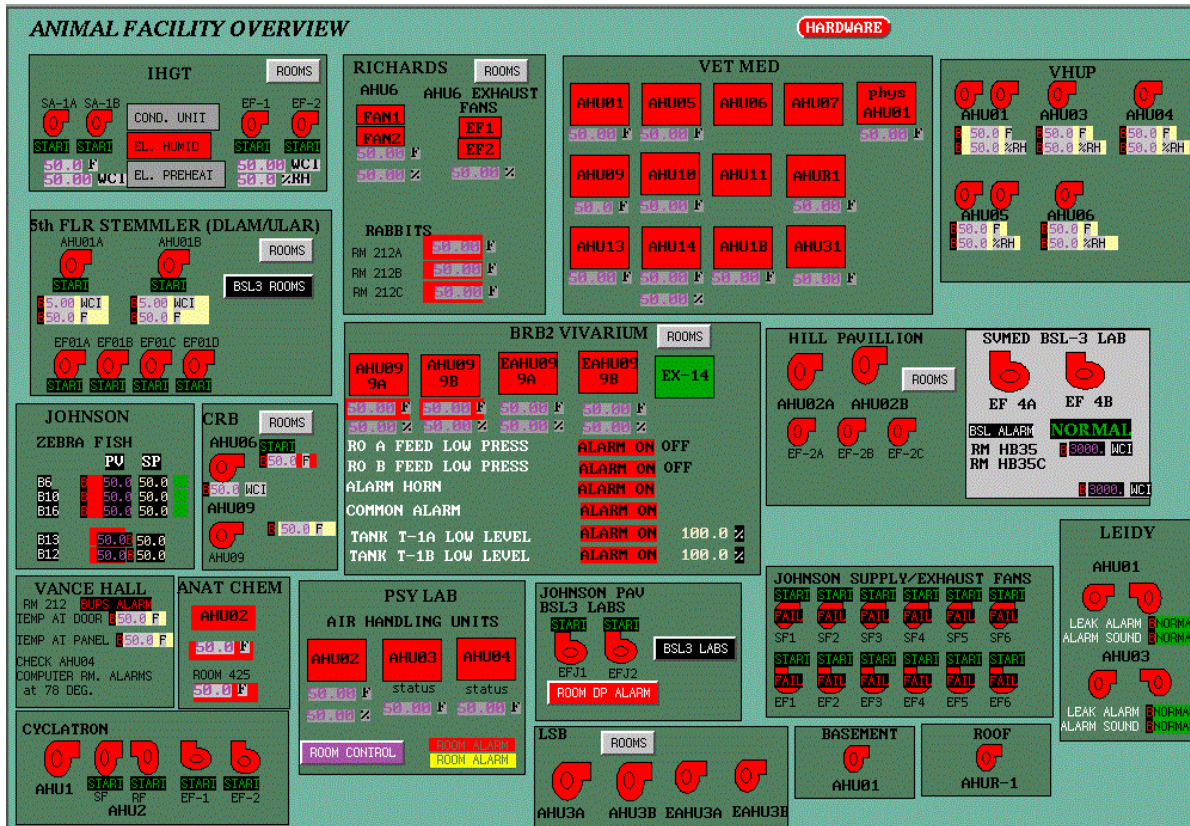
**Communication Drivers Screen**

This screen provides a summary of all the communication interfaces on a server. It shows whether the communication interface is active and, in most cases, shows whether the communication interface is functioning properly by display whether values are changing.

- blinking red NOT Communicating
- green Communicating
- grey Blank

***Animal Area Overview (Legacy Screen Shown - To be Updated)***

This provides a summary screen for all Animal areas. Equipment status and critical process values for each Animal Area is shown. Clicking on equipment symbols brings up the equipment screen for that Animal Area.



## Alarms

### AlarmWorX Viewer

The system should show real-time and historical alarms in separate tabs as shown below.

### All Alarms

Time / Date	Description	Area	Qual	Type
1/7/2016 2:55 PM	HIGH Discharge Air Temp - AHU03 PRESIDENT'S OFFICES - COLHALL In Alarm	ahu03; COLHALL; College Hall; Control; Maintenance	Good	Digi
1/7/2016 2:54 PM	HIGH Return Air Humid - AHU04 FISHER FINE ARTS - COLHALL Out Of Alarm	ahu04; COLHALL; Control; Fisher Fine Arts; Maintenance	Good	Digi
1/7/2016 2:34 PM	LOW Supply Temp - HWS02 FISHER FINE ARTS - COLHALL Out Of Alarm	COLHALL; Control; Fisher Fine Arts; hws02; Maintenance;...	Good	Digi
1/7/2016 2:04 PM	HIGH Building Differential Pressure DPT-2 - CWS HUNTSMAN - HUNTSMAN In Alarm	cws; HUNTSMAN; Huntsman Hall; Maintenance; ChillWater	Good	Digi
1/7/2016 1:12 PM	HIGH Space Air Temp - HP03 PRESIDENT'S OFFICES - COLHALL In Alarm	COLHALL; College Hall; Control; hp03	Good	Digi
1/7/2016 12:48 PM	Event13,Outside Air Temp < 50 and CHW Valve > 10%,AHU01,Fisher,COLHALL In Alarm	ahu01; COLHALL; Control; Electrical; Fisher Fine Arts; global	Good	Digi
1/7/2016 11:34 AM	LOW Return Air Humid - AHU01 FISHER FINE ARTS - COLHALL Out Of Alarm	ahu01; COLHALL; Control; Fisher Fine Arts	Good	Digi
1/7/2016 10:49 AM	RH-42 (RM 205C) OFF Temperature Setpoint - COLLEGE HALL - COLHALL Out Of Alarm	COLHALL; College Hall; Control; Maintenance; rh42	Good	Digi
1/7/2016 10:15 AM	HIGH Building Differential Pressure DPT-3 - CWS HUNTSMAN - HUNTSMAN Out Of Alarm	cws; HUNTSMAN; Huntsman Hall; Maintenance; ChillWater	Good	Digi
1/7/2016 10:06 AM	Event13,Outside Air Temp < 50_and_CHW_Valve > _0%,AHU01,Huntsman_Hall,HUNTSMAN...	ahu01; Control; HUNTSMAN; Huntsman Hall	Good	Digi
1/7/2016 9:29 AM	RH-47 (RM 207) OFF Temperature Setpoint - COLLEGE HALL - COLHALL Out Of Alarm	COLHALL; College Hall; Control; Maintenance; rh47	Good	Digi
1/7/2016 9:18 AM	Supply Fan-A Fail Alarm - AHU01 HUNTSMAN - HUNTSMAN Out Of Alarm	ahu01; Control; Critical; HUNTSMAN; Huntsman Hall	Good	Digi
1/7/2016 9:18 AM	Supply Fan-B Fail Alarm - AHU01 HUNTSMAN - HUNTSMAN Out Of Alarm	ahu01; Control; Critical; HUNTSMAN; Huntsman Hall	Good	Digi
1/7/2016 9:13 AM	RH-44 (RM 205D/206) OFF Temperature Setpoint - COLLEGE HALL - COLHALL Out Of Alarm	COLHALL; College Hall; Control; Maintenance; rh44	Good	Digi
1/7/2016 8:15 AM	RH-66 (RM 308B) OFF Temperature Setpoint - COLLEGE HALL - COLHALL Out Of Alarm	COLHALL; College Hall; Control; Maintenance; rh66	Good	Digi
1/7/2016 6:46 AM	RH-45 (RM 205E) OFF Temperature Setpoint - COLLEGE HALL - COLHALL Out Of Alarm	COLHALL; College Hall; Control; Maintenance; rh45	Good	Digi
1/7/2016 6:19 AM	RH-63 (RM 305B) OFF Temperature Setpoint - COLLEGE HALL - COLHALL Out Of Alarm	COLHALL; rh63; Maintenance; College Hall; Control	Good	Digi
1/7/2016 5:57 AM	RH-67 (RM 308C) OFF Temperature Setpoint - COLLEGE HALL - COLHALL Out Of Alarm	COLHALL; College Hall; Control; Maintenance; rh67	Good	Digi
1/7/2016 12:36 AM	RH-16 (RM 8B) OFF Temperature Setpoint - COLLEGE HALL - COLHALL Out Of Alarm	COLHALL; College Hall; Control; Maintenance; rh16	Good	Digi
1/6/2016 11:29 PM	HIGH VCV-084 Space Temperature - GRND FLOOR HUNTSMAN - HUNTSMAN Out Of Alarm	Control; flrg_vcv084; HUNTSMAN; Huntsman Hall;...	Good	Digi
1/6/2016 11:21 PM	RH-64 (RM 307) OFF Temperature Setpoint - COLLEGE HALL - COLHALL Out Of Alarm	COLHALL; College Hall; Control; Maintenance; rh64	Good	Digi
1/6/2016 6:34 PM	RH-27 (RM 106F) OFF Temperature Setpoint - COLLEGE HALL - COLHALL Out Of Alarm	COLHALL; College Hall; Maintenance; rh27; Control	Good	Digi
1/6/2016 6:26 PM	RH-13 (RM 9D) OFF Temperature Setpoint - COLLEGE HALL - COLHALL Out Of Alarm	COLHALL; College Hall; Control; Maintenance; rh13	Good	Digi
1/6/2016 6:11 PM	RH-34 (RM 103) OFF Temperature Setpoint - COLLEGE HALL - COLHALL Out Of Alarm	COLHALL; College Hall; Control; Maintenance; rh34	Good	Digi
1/6/2016 5:34 PM	RH-11 (RM 9E) OFF Temperature Setpoint - COLLEGE HALL - COLHALL Out Of Alarm	COLHALL; College Hall; Control; Maintenance; rh11	Good	Digi
1/6/2016 4:55 PM	FCU-20 (RM 208,VEST) OFF Temperature Setpoint - COLLEGE HALL - COLHALL Out Of Alarm	COLHALL; College Hall; Control; fcu20; Maintenance	Good	Digi

### Critical Alarms - Filtered

Time / Date	Description	Area	Qual	Type
1/7/2016 9:18 AM	Supply Fan-A Fail Alarm - AHU01 HUNTSMAN - HUNTSMAN Out Of Alarm	ahu01; Control; Critical; HUNTSMAN; Huntsman Hall	Good	Digi
1/7/2016 9:18 AM	Supply Fan-B Fail Alarm - AHU01 HUNTSMAN - HUNTSMAN Out Of Alarm	ahu01; Control; Critical; HUNTSMAN; Huntsman Hall	Good	Digi
1/6/2016 10:07 AM	Preheat Pump P-6 Failed to Start - AHU04 COLLEGE HALL - COLHALL In Alarm	ahu04; COLHALL; College Hall; Control; Critical;...	Good	Digi
1/6/2016 10:02 AM	LOW Freezestat BELOW 40 F - AHU04 COLLEGE HALL - COLHALL Out Of Alarm	ahu04; COLHALL; Miscellaneous; Steam; Critical; Electrical;...	Good	Digi
1/6/2016 7:44 AM	Return Fan-B VFD Alarm - AHU01 HUNTSMAN - HUNTSMAN Out Of Alarm	ahu01; Control; Critical; HUNTSMAN; Huntsman Hall	Good	Digi
1/6/2016 7:44 AM	Supply Fan-A VFD Alarm - AHU01 HUNTSMAN - HUNTSMAN Out Of Alarm	ahu01; Control; Critical; HUNTSMAN; Huntsman Hall	Good	Digi
1/6/2016 7:44 AM	Return Fan-A VFD Alarm - AHU01 HUNTSMAN - HUNTSMAN Out Of Alarm	ahu01; Control; Critical; HUNTSMAN; Huntsman Hall	Good	Digi
1/6/2016 7:44 AM	Supply Fan-B VFD Alarm - AHU01 HUNTSMAN - HUNTSMAN Out Of Alarm	ahu01; Control; Critical; HUNTSMAN; Huntsman Hall	Good	Digi
1/6/2016 7:44 AM	Freezestat Alarm - AHU01 HUNTSMAN - HUNTSMAN Out Of Alarm	ahu01; Control; Critical; Electrical; HUNTSMAN; Huntsman...	Good	Digi
1/5/2016 11:08 PM	LOW Preheat Air Temperature - AHU04 COLLEGE HALL - COLHALL Out Of Alarm	ahu04; COLHALL; College Hall; Critical; Miscellaneous	Good	Digi
1/5/2016 1:58 PM	LOW Supply Air Static Press - AHU02 HUNTSMAN - HUNTSMAN Out Of Alarm	ahu02; Control; Critical; HUNTSMAN; Huntsman Hall	Good	Digi
1/5/2016 1:47 PM	LOW Supply Air Static Press - AHU01 HUNTSMAN - HUNTSMAN Out Of Alarm	ahu01; Control; Critical; HUNTSMAN; Huntsman Hall	Good	Digi
1/5/2016 1:35 PM	Return Fan-B Fail Alarm - AHU01 HUNTSMAN - HUNTSMAN Out Of Alarm	ahu01; Control; Critical; HUNTSMAN; Huntsman Hall	Good	Digi
1/5/2016 1:35 PM	Return Fan-A Fail Alarm - AHU01 HUNTSMAN - HUNTSMAN Out Of Alarm	ahu01; Control; Critical; HUNTSMAN; Huntsman Hall	Good	Digi
1/5/2016 7:05 AM	cc lon Not Communicating with LUC11-10 - COLLEGE HALL - COLHALL In Alarm	COLHALL; College Hall; Control; Miscellaneous; Critical;...	Good	Digi
1/5/2016 6:39 AM	Supply Fan-B VFD Alarm - AHU02 HUNTSMAN - HUNTSMAN Out Of Alarm	ahu02; Control; Critical; HUNTSMAN; Huntsman Hall	Good	Digi
1/5/2016 6:39 AM	Supply Fan-A VFD Alarm - AHU02 HUNTSMAN - HUNTSMAN Out Of Alarm	ahu02; Control; Critical; HUNTSMAN; Huntsman Hall	Good	Digi
1/5/2016 6:39 AM	Return Fan-A VFD Alarm - AHU02 HUNTSMAN - HUNTSMAN Out Of Alarm	ahu02; Control; Critical; HUNTSMAN; Huntsman Hall	Good	Digi
1/5/2016 6:39 AM	Return Fan-B VFD Alarm - AHU02 HUNTSMAN - HUNTSMAN Out Of Alarm	ahu02; Control; Critical; Huntsman Hall; HUNTSMAN	Good	Digi
1/5/2016 6:39 AM	Freezestat Alarm - AHU02 HUNTSMAN - HUNTSMAN Out Of Alarm	ahu02; Control; Critical; Electrical; Steam; HUNTSMAN;...	Good	Digi
1/5/2016 5:53 AM	Return Fan RF-B Failed to Start - AHU02 HUNTSMAN - HUNTSMAN Out Of Alarm	ahu02; Control; Critical; HUNTSMAN; Huntsman Hall	Good	Digi
1/5/2016 5:53 AM	Supply Fan SF-B Failed to Start - AHU02 HUNTSMAN - HUNTSMAN Out Of Alarm	ahu02; Control; Critical; HUNTSMAN; Huntsman Hall	Good	Digi
1/5/2016 5:53 AM	Return Fan RF-A Failed to Start - AHU02 HUNTSMAN - HUNTSMAN Out Of Alarm	ahu02; Control; Critical; HUNTSMAN; Huntsman Hall	Good	Digi
1/4/2016 12:27 AM	LOW Preheat Air Temp - AHU03 PRESIDENT'S OFFICES - COLHALL Out Of Alarm	ahu03; COLHALL; College Hall; Critical	Good	Digi
1/3/2016 10:40 PM	LOW Differential Temperature - CWS HUNTSMAN - HUNTSMAN In Alarm	Control; Critical; cws; HUNTSMAN; Huntsman Hall;...	Good	Digi
1/3/2016 10:16 PM	LOW Supply Air Static Press - AHU06 HUNTSMAN - HUNTSMAN Out Of Alarm	ahu06; Control; Critical; HUNTSMAN; Huntsman Hall	Good	Digi

An unacknowledged “In Alarm” message will have a bright orange color alarm row. A selected message whether in or out of alarm will change the alarm row to a pale orange. Acknowledgement of an alarm will remove the orange highlight and the message text will appear red. When the alarm is “Out of Alarm” the message row color is white. Double clicking on an alarm will acknowledge the alarm. Other ways to acknowledge alarm, right click and then can select different acknowledgement criteria.

Can change location of alarm columns by clicking and dragging to desired location

Can sort by each column by clicking on the column. Where the red arrow shows is the column that is being sort, the direction of the arrow indicates the direction of sorting.

Time / Date	Description	Area	Acknowledge
1/6/2016 10:07 AM	Preheat Pump P-6 Failed to Start - AHU04 COLLEGE HALL - COLHALL In Alarm	ahu04; COLHALL; College Hall; Control; Critical;...	Good D
1/5/2016 7:05 AM	cc Ion Not Communicating with LUC11-10 - COLLEGE HALL - COLHALL In Alarm	COLHALL; College Hall; Control; Miscellaneous; Critical; ddc;...	Good D
1/3/2016 10:40 PM	LOW Differential Temperature - CWS HUNTSMAN - HUNTSMAN In Alarm	Control; Critical; cws; HUNTSMAN; Huntsman Hall; ChillWater	Good D
12/27/2015 10:08 PM	Preheat Pump Alarm - AHU03 PRESIDENT'S OFFICES - COLHALL In Alarm	ahu03; COLHALL; College Hall; Steam; Control; Critical	Good D
12/26/2015 10:42 PM	Preheat Pump Failed to Start - AHU03 PRESIDENT'S OFFICES - COLHALL In Alarm	ahu03; COLHALL; College Hall; Control; Critical; Steam	Good D
12/23/2015 4:26 PM	Pump 4 Failed to Stop - HWS02 FISHER FINE ARTS - COLHALL In Alarm	COLHALL; Control; Critical; Fisher Fine Arts; hws02; Steam	Good D
12/23/2015 4:26 PM	Return Fan Failed to Start - AHU02 COLLEGE HALL - COLHALL In Alarm	ahu02; COLHALL; College Hall; Control; Critical	Good D
12/23/2015 4:25 PM	Supply Fan Failed to Start - AHU06 FISHER FINE ARTS - COLHALL In Alarm	ahu06; COLHALL; Control; Critical; Fisher Fine Arts	Good D
12/23/2015 4:23 PM	Return Fan Fail - AHU02 COLLEGE HALL - COLHALL In Alarm	ahu02; COLHALL; College Hall; Control; Critical	Good D
12/23/2015 4:21 PM	Clock time not changing - Automated Logic LGR - COLLEGE HALL - COLHALL In Alarm	COLHALL; College Hall; lgr; device110081; device110091;...	Good D
12/23/2015 4:21 PM	Clock time not changing - Automated Logic LGR - FISHER - COLHALL In Alarm	COLHALL; College Hall; device24110; device24111;...	Good D
12/23/2015 4:21 PM	Clock time not changing - Automated Logic LGR - COLLEGE HALL - COLHALL In Alarm	COLHALL; College Hall; Control; Critical; device110081;...	Good D
12/23/2015 4:20 PM	AGE of cc pup Broadcast variables - COLHALL In Alarm	ahu01; ahu02; ahu03; Miscellaneous; Control; Critical;...	Good D
12/23/2015 4:20 PM	AGE of cc mbustcp variables - COLHALL In Alarm	chw_meter; Cohen Hall - Claudia; COLHALL; Houston Hall;...	Good D
12/23/2015 4:20 PM	AGE of cc bacnet MBC Time variables - COLHALL In Alarm	ahu03; COLHALL; College Hall; Control; Critical; hp01;...	Good D
12/23/2015 4:20 PM	Total units up in loop2 - COLHALL In Alarm	ahu01; ahu02; ahu03; chws; COLHALL; College Hall; hws_gly;...	Good D
12/23/2015 4:20 PM	Total units up in loop1 - COLHALL In Alarm	ahu01; ahu02; ahu03; COLHALL; College Hall; Control;...	Good D
12/23/2015 4:20 PM	AGE of cc gyrec MBC Time variables - COLHALL In Alarm	COLHALL; College Hall; Control; Critical; mbc001; mbc002;...	Good D
12/23/2015 4:20 PM	AGE of string variables - COLHALL In Alarm	Control; Critical	Good D
12/22/2015 1:53 PM	LOW City Water Pressure - MISC HUNTSMAN - HUNTSMAN In Alarm	Critical; fmisc; HUNTSMAN; Huntsman Hall	Good D
12/22/2015 1:53 PM	LOW Fire Water Pressure - MISC HUNTSMAN - HUNTSMAN In Alarm	Critical; fmisc; HUNTSMAN; Huntsman Hall	Good D
12/22/2015 1:53 PM	Exhaust Fan EX-15 Failed to Start - FWCIT HUNTSMAN - HUNTSMAN In Alarm	Control; Critical; fwcit; HUNTSMAN; Huntsman Hall	Good D
12/22/2015 1:50 PM	AGE of cc_bacnet variables - JCI NCE6 AHU06 HUNTSMAN - HUNTSMAN In Alarm	ahu06; COLHALL; Control; Huntsman Hall; jmhh_nce6;...	Good D
12/22/2015 1:50 PM	AGE of cc_bacnet variables - JCI NCE5 AHU05 HUNTSMAN - HUNTSMAN In Alarm	ahu05; COLHALL; Control; Critical; HUNTSMAN; Huntsman...	Good D
12/22/2015 1:50 PM	AGE of cc_bacnet variables - JCI NCE1 AHU04 HUNTSMAN - HUNTSMAN In Alarm	ahu04; COLHALL; Control; Critical; HUNTSMAN; Huntsman...	Good D
12/22/2015 1:50 PM	AGE of cc_bacnet variables - JCI NCE3 AHU03 HUNTSMAN - HUNTSMAN In Alarm	ahu03; COLHALL; Control; Critical; HUNTSMAN; Huntsman...	Good D

## Types of Alarms

### No communication to system

There are two methods to determine if the communications are inactive between the GENESIS64 server and the HVAC equipment.

Open the hardware screen for the cluster and check if the communication driver is in alarm

Open a graphic for one of the systems. If there are pale yellow squares where data values should be, then the communications have likely failed.

### HVAC Alarms

The following is a general guide to alarms seen in most HVAC systems at UPenn. While this will cover most situations, each system is unique and its sequence of operations should be consulted. A “hardware alarm” refers to a switch, contact, or other device in the field that triggers when certain conditions are met. Often these devices lock out or shut down certain functions or aspects of a system. A “SCADA alarm” refers to an alarm programmed within AlarmWorX. These alarms are typically are for informational purposes only and do not interrupt system operations.

## *AHU Alarms*

### *Freezestat*

Viewable on: System Overview, System Control Screen. Hardware Alarm.

The freezestat is a mechanical interlock to prevent the chill water coil from freezing due to low outside air temperature. Typically, when the freezestat trips, the AHU is shut down, the chill water valve is opened 100% and the preheat valve is opened 100%.

### *Dirty Filter*

Viewable on: System Overview, System Control Screen. Hardware or SCADA Alarm.

The filters on the AHU prevent dirt and debris from entering the heating and cooling coils, and the fans, and thus become dirty with use. When the differential pressure across the filter becomes too high, the dirty filter alarm will trigger.

### *Smoke and Fire Alarms*

Viewable on: System Overview, System Control Screen

Smoke Alarms are detected by smoke detectors placed in the supply or return air duct. When triggered, the unit is shut down.

Fire alarms are typically generated by the building fire alarm system and sent to the air handling unit controller to shut the unit down.

### *High and Low Static Pressure Switches*

Viewable on: System Overview, System Control Screen. Hardware alarm.

The high static pressure switch is typically located after the fan and is a differential pressure switch used to detect if the duct after the fan has become obstructed, such as a closed damper. When the switch triggers, the unit is shut down to prevent high pressures and equipment damage.

The low static pressure switch is typically located before the fan and is a differential pressure switch used to detect if the duct before the fan has become obstructed such as a closed damper. When the switch triggers, the unit is shut down to prevent low pressures and equipment damage.

### *Low Preheat/Mixed Air Temperature Alarm*

Viewable on: System Overview. SCADA alarm.

If the temperature of the temperature sensor that is directly before the chill water coil drops below 42 °F, then a low alarm is triggered. This is typically either the preheat temperature, or the mixed air temperature, depending on system configuration.

### *Supply/Space/Return High and Low Humidity Alarms*

Viewable on: System Overview. SCADA alarm.

If there is a humidifier present in the system, typically either the supply humidity, space humidity, or return humidity is monitored and controlled, depending on the building's needs. The monitored and controlled humidity point will have a low alarm trigger when the humidity drops 10% below set point. On the air handling units that have a dehumidification process available, the monitored and controlled humidity point will have a high alarm trigger when the humidity increase 10% above set point.

### *High and Low Discharge Air Temperature Alarms*

Viewable on: System Overview. SCADA alarm.

If the air handling unit is running and the discharge temperature deviates from set point by  $\pm 5$  °F the temperature goes into high or low alarm.

#### High and Low Supply Static Air Pressure Alarms

Viewable on: System Overview. SCADA alarm.

If the air handling unit is running and the supply static pressure deviates from set point by  $\pm 20\%$  the static pressure goes into high or low alarm.

### *Fan Failure Alarms*

#### Fail to Start

Viewable on: Building Overview, System Overview, System Control Screen

When a fan is commanded to turn on, but the feedback status switch does not indicate that it has turned on, then the fan goes into alarm. The delay is 3 to 5 minutes and the fan will begin to blink red. The alarm status is cleared when the fan successfully turns on.

#### Fail to Stop

Viewable on: Building Overview, System Overview, System Control Screen

When a fan is commanded to turn off, but the feedback status switch does not indicate that it has turned off, then the fan goes into alarm. The delay is 3 to 5 minutes and the fan will begin to blink red. The alarm status is cleared when the fan successfully turns off. This alarm situation typically occurs when the equipment has been overridden at the equipment to stay on and is referred to be being “in hand”.

#### VFD Fault

Viewable on: System Overview, System Control Screen. Hardware alarm.

When an error occurs with the Variable Frequency Drive on the fan, an alarm status is triggered. Some systems require the alarm reset to be toggled to clear the alarm and allow the fan to be put back in service.

#### Fan Alarm

Viewable on: System Overview, System Control Screen. Hardware alarm.

A generic fan alarm to indicate a number of issues that may have occurred with the fan. Some systems require the alarm reset to be toggled to clear the alarm and allow the fan to be put back in service.

#### High and Low Discharge/Supply Air Temperature Alarms

Viewable on: System Overview. SCADA alarm.

When the discharge air temperature deviates from set point by  $\pm 5$  °F and the fan is running, the temperature goes into high or low alarm. If there is an unoccupied mode available, if the temperature rises 5 °F above the unoccupied cooling set point or drops 5 °F below the unoccupied heating set point then the temperature goes into high or low alarm respectively.

### *Chill Water System Alarms*

#### Pump Failure Alarms

##### *Fail to Start*

Viewable on: Building Overview, System Overview, System Control Screen

When a pump is commanded to turn on, but the feedback status switch does not indicate that it has turned on, then the pump goes into alarm. The delay is 3 to 5 minutes and the pump will begin to blink red. The alarm status is cleared when the pump successfully turns on.

*Fail to Stop*

Viewable on: Building Overview, System Overview, System Control Screen

When a pump is commanded to turn off, but the feedback status switch does not indicate that it has turned off, then the pump goes into alarm. The delay is 3 to 5 minutes and the pump will begin to blink red. The alarm status is cleared when the pump successfully turns off. This alarm situation typically occurs when the equipment has been overridden at the equipment to stay on and is referred to be being “in hand”.

*VFD Fault*

Viewable on: System Overview, System Control Screen. Hardware alarm.

When an error occurs with the Variable Frequency Drive on the pump, an alarm status is triggered. Some systems require the alarm reset to be toggled to clear the alarm and allow the pump to be put back in service.

*Pump Alarm*

Viewable on: System Overview, System Control Screen. Hardware alarm.

A generic pump alarm to indicate a number of issues that may have occurred with the pump. Some systems require the alarm reset to be toggled to clear the alarm and allow the pump to be put back in service.

*High and Low Chill Water Supply Temperature Alarms*

Viewable on: System Overview. SCADA alarm.

When the chill water supply temperature deviates from set point by  $\pm 5$  °F and the pump is running, the temperature goes into high or low alarm.

*High and Low Differential Pressure Alarms*

Viewable on: System Overview. SCADA alarm.

When the differential pressure deviates from set point by  $\pm 5$  PSI and the pump is running, the differential pressure goes into high or low alarm.

*Hot Water System Alarms (includes Preheat, Reheat, and Radiation systems)*

*Pump Failure Alarms*

*Fail to Start*

Viewable on: Building Overview, System Overview, System Control Screen

When a pump is commanded to turn on, but the feedback status switch does not indicate that it has turned on, then the pump goes into alarm. The delay is 3 to 5 minutes and the pump will begin to blink red. The alarm status is cleared when the pump successfully turns on.

*Fail to Stop*

Viewable on: Building Overview, System Overview, System Control Screen

When a pump is commanded to turn off, but the feedback status switch does not indicate that it has turned off, then the pump goes into alarm. The delay is 3 to 5 minutes and the pump will begin to blink red. The alarm status is cleared when the pump successfully turns off. This alarm situation typically occurs when the equipment has been overridden at the equipment to stay on and is referred to be being “in hand”.



### *VFD Fault*

Viewable on: System Overview, System Control Screen. Hardware alarm.

When an error occurs with the Variable Frequency Drive on the pump, an alarm status is triggered.

Some systems require the alarm reset to be toggled to clear the alarm and allow the pump to be put back in service.

### *Pump Alarm*

Viewable on: System Overview, System Control Screen. Hardware alarm.

A generic pump alarm to indicate a number of issues that may have occurred with the pump. Some systems require the alarm reset to be toggled to clear the alarm and allow the pump to be put back in service.

High and Low Chill Water Supply Temperature Alarms

Viewable on: System Overview. SCADA alarm.

When the chill water supply temperature deviates from set point by  $\pm 5$  °F and the pump is running, the temperature goes into high or low alarm. High

and Low Differential Pressure Alarms Viewable

on: System Overview. SCADA alarm.

When the differential pressure deviates from set point by  $\pm 5$  PSI and the pump is running, the differential pressure goes into high or low alarm.

### *Room Control*

#### *High and Low Space Temperature Alarms*

Viewable on: Building Floor Plan, System Control Screen. SCADA alarm.

When the space temperature deviates from set point by  $\pm 5$  °F the temperature goes into high or low alarm. If there is an unoccupied mode available, if the temperature rises 5 °F above the unoccupied cooling set point or drops 5 °F below the unoccupied heating set point then the temperature goes into high or low alarm respectively.

#### *Space High and Low Humidity Alarms*

Viewable on: Building Floor Plan, System Control Screen. SCADA alarm.

When the space humidity deviates from set point by  $\pm 10$  % relative humidity, the humidity goes into high or low alarm.

#### *High and Low Space Pressure Alarms*

Viewable on: System Control Screen. SCADA alarm.

Some areas are to be maintained at either a slightly positive or slightly negative space pressure with respect to the areas adjacent to them. Examples of slightly positive rooms are in the Krishna P. Singh Center for Nanotechnology. Examples of slightly negative rooms are the Biological Safety Level 3 (BSL-3) Suites in the Johnson Pavilion. Rooms that are to be kept under positive pressure go into low alarm when the space pressure falls below 0" water column. Rooms that are to be kept under negative pressure go into high alarm when the space pressure rises above 0" water column.

### *Phoenix Valves (Typically used for room control)*

#### *Supply and Exhaust Flow Alarm*

Viewable on: System Control Screen. Hardware alarm.

When the Phoenix Valve detects an inability to reach the flow set point, the valve triggers the flow alarm.

### Supply and Exhaust Jam Alarm

Viewable on: System Control Screen. Hardware alarm.

When the Phoenix Valve detects that the valve has jammed, the valve triggers the jam alarm.

Supply and Exhaust Flow Deviation Alarms (Applies only to Phoenix Valves)

Viewable on: Building Floor Plan, System Control Screen. SCADA alarm.

When the supply or exhaust flow deviates by  $\pm 10\%$  of the set point, the flow goes into alarm.

### High and Low Space Pressure Alarms

Viewable on: System Control Screen. SCADA alarm.

Some areas are to be maintained at either a slightly positive or slightly negative space pressure with respect to the areas adjacent to them. Examples of slightly positive rooms are in the Krishna P. Singh Center for Nanotechnology. Examples of slightly negative rooms are the Biological Safety Level 3 (BSL-3) Suites in the Johnson Pavilion. Rooms that are to be kept under positive pressure go into low alarm when the space pressure falls below 0" water column. Rooms that are to be kept under negative pressure go into high alarm when the space pressure rises above 0" water column.

### Alarm Configuration

Here is an example of a smart alarm configuration and naming conventions.

Description:

- This creates a smart alarm if the President's Office has a high space temperature

Alarm Name:

- PresHighSpaceTemp

Alarm Enter Condition:

- If ("fan is running" AND ("the space temperature" - "the space temperature setpoint")  $\geq 5$ ) OR ("the fan is not running" AND "the space temperature"  $> 80$ )
- This is configured in AssetWorX as one expression of the enter and exit conditions. The name of the AssetWorX condition is **PresHighSpaceTemp\_Conditions**.
- e.g. `x=IF ({{{ac:UPenn/COLHALL/College Hall-01/hp01/fan_di_status}}} && ({{{ac:UPenn/COLHALL/College Hall-01/hp01/space_temp}}} - {{{ac:UPenn/COLHALL/College Hall-01/hp01/tstat_temp_sp}}}  $\geq 5$ ) || (!{{{ac:UPenn/COLHALL/College Hall-01/hp01/fan_di_status}}}) && {{{ac:UPenn/COLHALL/College Hall-01/hp01/space_temp}}}  $> 80$ )) THEN true ELSEIF ({{{@ICONICS.AlarmSvr_.1\ PresHighSpaceTemp _Alarm.DIG_Active.Value}}} && ({{{ac:UPenn/COLHALL/College Hall-01/hp01/fan_di_status}}} && ({{{ac:UPenn/COLHALL/College Hall-01/hp01/space_temp}}} - {{{ac:UPenn/COLHALL/College Hall-01/hp01/tstat_temp_sp}}}  $< 4$ )) || (!{{{ac:UPenn/COLHALL/College Hall-01/hp01/fan_di_status}}}) && {{{ac:UPenn/COLHALL/College Hall-01/hp01/space_temp}}}  $< 79$ )) THEN false ELSE {{{@ICONICS.AlarmSvr_.1\ PresHighSpaceTemp _Alarm.DIG_Active.Value}}} False`

Alarm is triggered if enter condition is sustained for:

- Delay Time(seconds): 240
- This is configured in AlarmWorX Server under the name **PresHighSpaceTemp\_Alarm**

On entering this alarm:

- Display Message: HIGH Space Temperature - HP01 PRESIDENT'S OFFICE - COLHALL ; This is configured in AlarmWorX Server under the name **PresHighSpaceTemp\_Alarm**
- i.e. if ac:UPenn/Alarms/COLHALL/ PresHighSpaceTemp \_Conditions is true for 240 seconds, present message: HIGH Space Air Temp - HP01 PRESIDENT'S OFFICES - COLHALL
- Set OPC Tag: "College Hall hp01 smart alarm" = 2; this value is used to change colors of graphical objects in GraphWorX64; This is configured in UDM as an expression under the name **PresHighSpaceTemp\_EnterDo**
- e.g. UDM expression; x=IF{{{@ICONICS.AlarmSvr\_.1\PresHighSpaceTemp \_Alarm.DIG\_Active.Value}} == 1 THEN 2 ELSEIF ((({@ICONICS.AlarmSvr\_.1\PresHighSpaceTemp \_Alarm.DIG\_Active.Value}} == 0) && ({@exp64:Alarms.COLHALL. PresHighSpaceTemp \_EnterDo.Value}} == 2)) THEN 0 ELSE {{{@exp64:Alarms.COLHALL. PresHighSpaceTemp \_EnterDo.Value}}}
- e.g. UDM trigger; ac:UPenn/COLHALL/College Hall-01/hp01/space\_temp\_smart\_alarm is assigned a value equal to @exp64:Alarms.COLHALL. PresHighSpaceTemp \_EnterDo.Value. This is configured in the UDM as a trigger in the name **PresHighSpaceTemp\_Register**

Alarm Exit Condition:

- If ("fan is running" AND ("the space temperature" - "the space temperature setpoint") < 5)) OR ("the fan is not running" AND "the space temperature " < 79)
- This is configured in AssetWorX as one expression of the enter and exit conditions. The name of the AssetWorX condition is **PresHighSpaceTemp\_Conditions**
- e.g. x=IF ((({ac:UPenn/COLHALL/College Hall-01/hp01/fan\_di\_status}} && ({ac:UPenn/COLHALL/College Hall-01/hp01/space\_temp}} - {{ac:UPenn/COLHALL/College Hall-01/hp01/tstat\_temp\_sp}} >= 5)) || (!({ac:UPenn/COLHALL/College Hall-01/hp01/fan\_di\_status}} && {{ac:UPenn/COLHALL/College Hall-01/hp01/space\_temp}} > 80)) THEN true ELSEIF ({@ICONICS.AlarmSvr\_.1\ PresHighSpaceTemp \_Alarm.DIG\_Active.Value}} && ({ac:UPenn/COLHALL/College Hall-01/hp01/fan\_di\_status}} && ({ac:UPenn/COLHALL/College Hall-01/hp01/space\_temp}} - {{ac:UPenn/COLHALL/College Hall-01/hp01/tstat\_temp\_sp}} < 4)) || (!({ac:UPenn/COLHALL/College Hall-01/hp01/fan\_di\_status}} && {{ac:UPenn/COLHALL/College Hall-01/hp01/space\_temp}} < 79))) THEN false ELSE {{{@ICONICS.AlarmSvr\_.1\ PresHighSpaceTemp \_Alarm.DIG\_Active.Value}} False

On exiting this alarm:

- Display Message: Recovered from HIGH Space Temperature - HP01 PRESIDENT'S OFFICE - COLHALL
- Set OPC Tag: "College Hall hp01 smart alarm" = 0; this value is used to change colors of graphical objects in GraphWorX64; This is configured in UDM as an expression under the name **PresHighSpaceTemp\_EnterDo**
- e.g. UDM expression; x=IF{{{@ICONICS.AlarmSvr\_.1\PresHighSpaceTemp \_Alarm.DIG\_Active.Value}} == 1 THEN 2 ELSEIF ((({@ICONICS.AlarmSvr\_.1\PresHighSpaceTemp \_Alarm.DIG\_Active.Value}} == 0) && ({@exp64:Alarms.COLHALL. PresHighSpaceTemp \_EnterDo.Value}} == 2)) THEN 0 ELSE {{{@exp64:Alarms.COLHALL. PresHighSpaceTemp \_EnterDo.Value}}}
- e.g. UDM trigger; ac:UPenn/COLHALL/College Hall-01/hp01/space\_temp\_smart\_alarm is assigned a value equal to @exp64:Alarms.COLHALL. PresHighSpaceTemp \_EnterDo.Value. This is configured in the UDM as a trigger in the name **PresHighSpaceTemp\_Register**

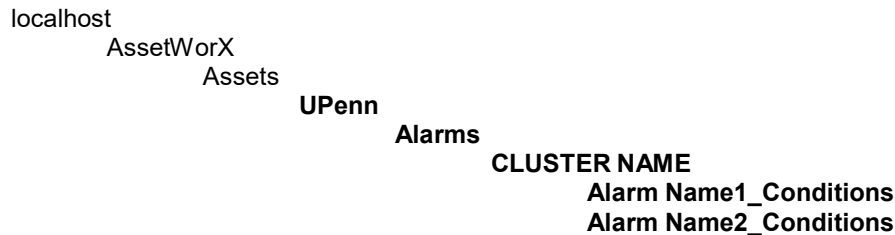
Areas to which this alarm belong:

- COLHALL - Cluster

- College Hall - Building
- Critical - For operator attention
- Control - For Control Engineers' attention
- ChillWater - Chill Water alarm
- HP01 - Equipment

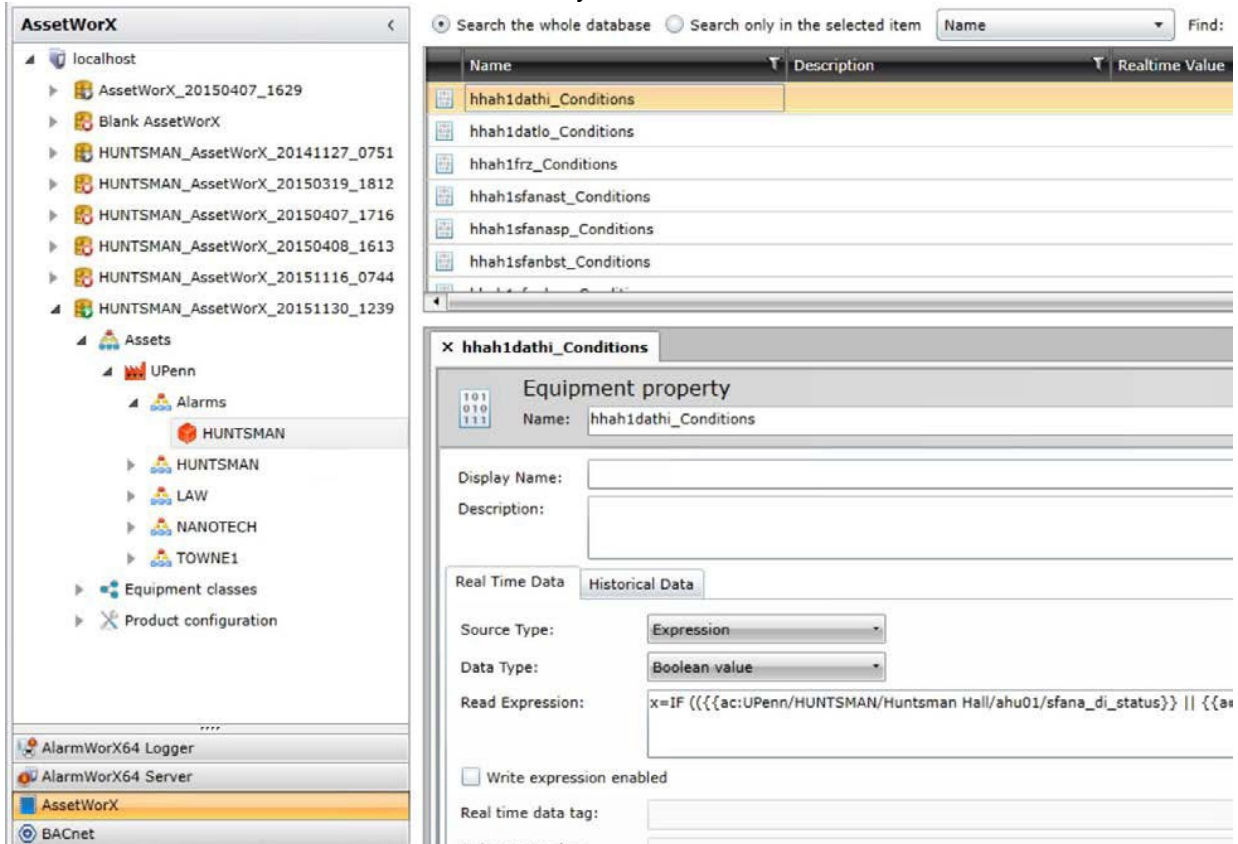
*AssetWorX and Alarms*

The AssetWorX Tree structure for each local cluster also has a branch for handling Alarm entry and exit conditions.



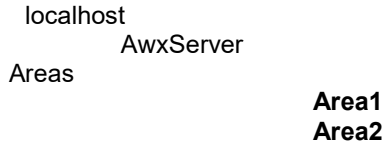
Note that each alarm has a name and is appended with \_Conditions.

*HUNTSMAN AssetWorX Server Tree for Alarm Entry and Exit Conditions*

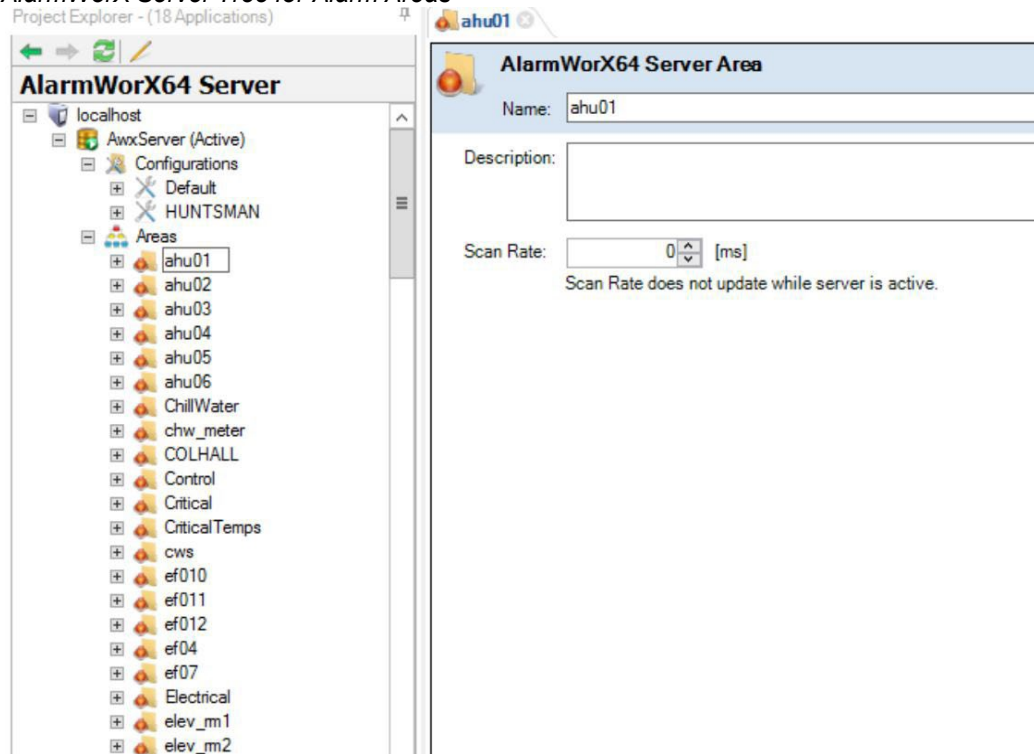


*AlarmWorX Server Areas*

The AlarmWorX Tree structure for assigning alarm messages to areas is shown below.



*AlarmWorX Server Tree for Alarm Areas*



*AlarmWorX Server and Alarm Messages*

The AlarmWorX Tree structure for monitoring Alarm Conditions, applying Delay and producing alarm messages is shown below.



Note that each alarm has a name appended with \_Alarm.

AlarmWorX Server Tree for applying Delay on Alarm Conditions and generating Messages

The screenshot displays the AlarmWorX64 Server configuration interface. On the left, a Project Explorer shows a tree view of the server structure under 'localhost'. The tree includes 'AworServer (Active)', 'Configurations', 'Default', and 'HUNTSMAN'. Under 'HUNTSMAN', a list of alarm events is shown, including 'energy\_hr\_Alarm', 'event1\_1\_Alarm', 'event1\_2\_Alarm', 'event1\_3\_Alarm', 'event1\_4\_Alarm', 'event1\_5\_Alarm', 'event1\_6\_Alarm', 'event10\_1\_Alarm', 'event10\_2\_Alarm', 'event10\_3\_Alarm', 'event10\_4\_Alarm', 'event10\_5\_Alarm', 'event10\_6\_Alarm', 'event11\_1\_Alarm', 'event11\_2\_Alarm', 'event11\_3\_Alarm', 'event11\_4\_Alarm', 'event11\_5\_Alarm', 'event11\_6\_Alarm', 'event11\_7\_Alarm', 'event13\_1\_Alarm', 'event13\_2\_Alarm', 'event13\_3\_Alarm', 'event13\_4\_Alarm', 'event13\_5\_Alarm', 'event13\_6\_Alarm', 'event14\_1\_Alarm', 'event14\_2\_Alarm', and 'event14\_3\_Alarm'.

The main configuration panel on the right is titled 'AlarmWorX64 Server Tag' and is currently displaying the configuration for 'event1\_1\_Alarm'. The configuration includes the following fields:

- Name: event1\_1\_Alarm
- OPC Input: ac:UPenn/Alarms/HUNTSMAN/event1\_1\_Conditions
- Template: <Not Assigned> (with a 'Jump To Template' button)

The 'General' tab is selected, showing the following settings:

- Enabled: 1
- Default Display: (empty)
- Description: (empty)
- Delay (seconds): 600
- Auto Ack (seconds): (empty)
- Base Text: Event1.PHV\_and\_CHWV\_both\_open.AHU01.Huntsman\_Hall.HUNTSMAN
- Help Instructions: (empty)

There are three checkboxes at the bottom of the General tab: 'Enable Clear' (unchecked), 'Delay On Alarm Only' (unchecked), and 'Exclude Equal To' (unchecked).

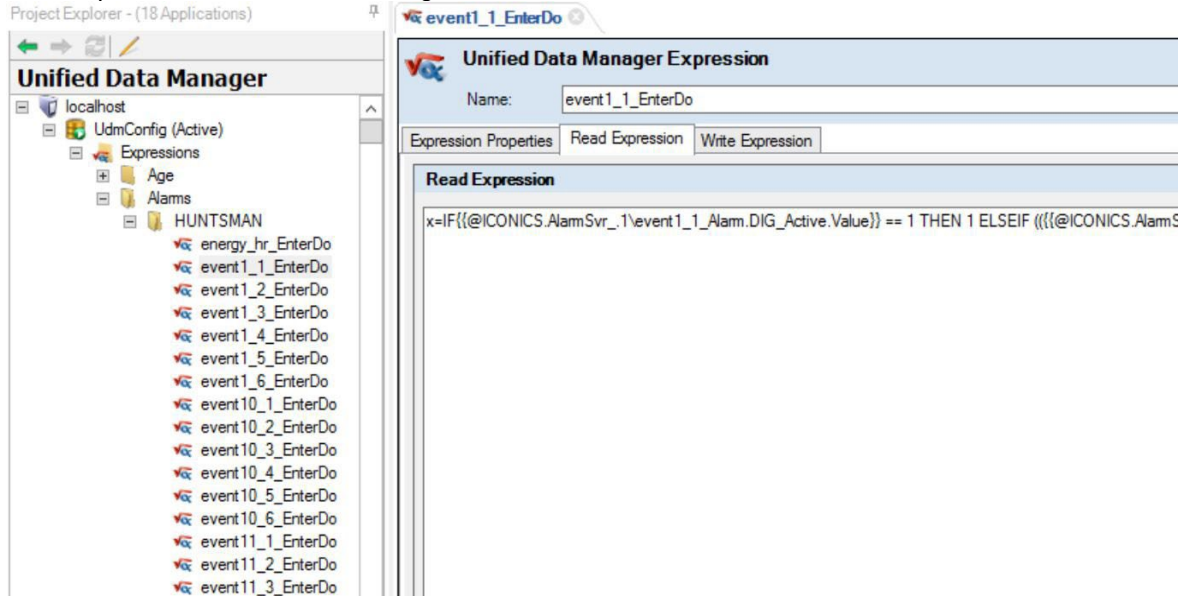
The 'Areas' section is also visible, with a table listing the areas associated with the alarm:

Name
ahu01\
Control\
HUNTSMAN\
Huntsman Hall\

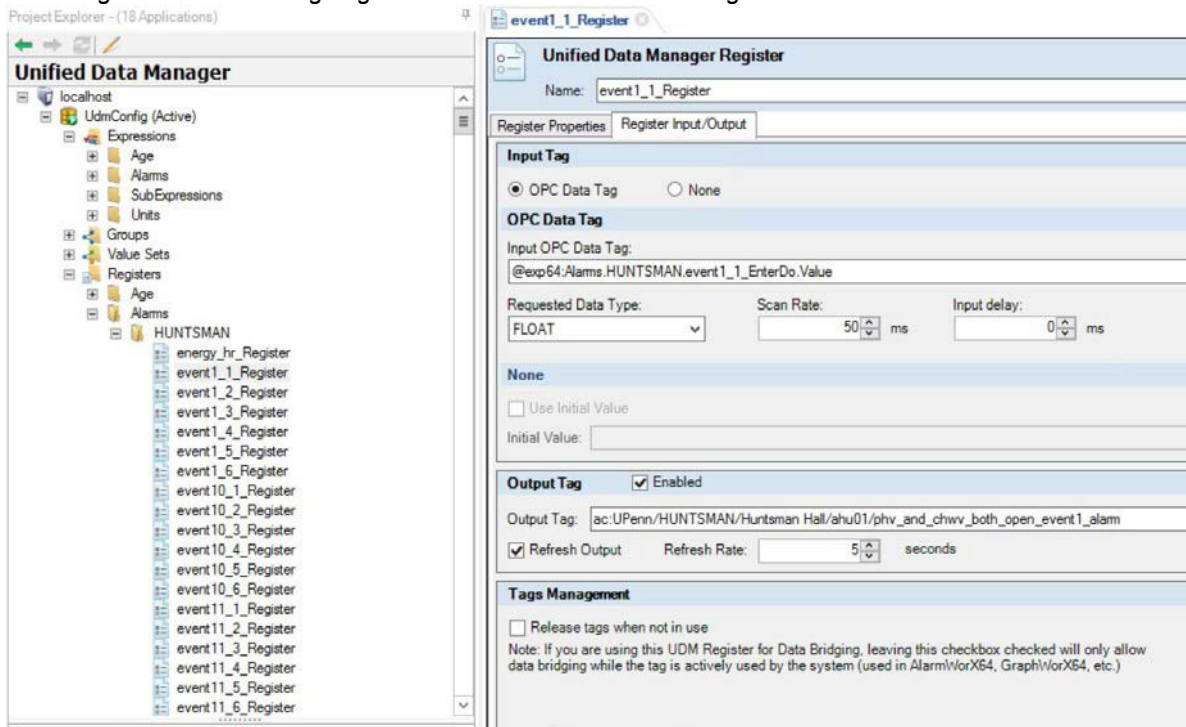
### UDM and Alarms

The UDM Tree structure for monitoring alarms and assigning smart alarm values is shown below.

#### UDM EXpressions Tree for Calculating Values of Smart Alarms when Alarms are Entered or Exited



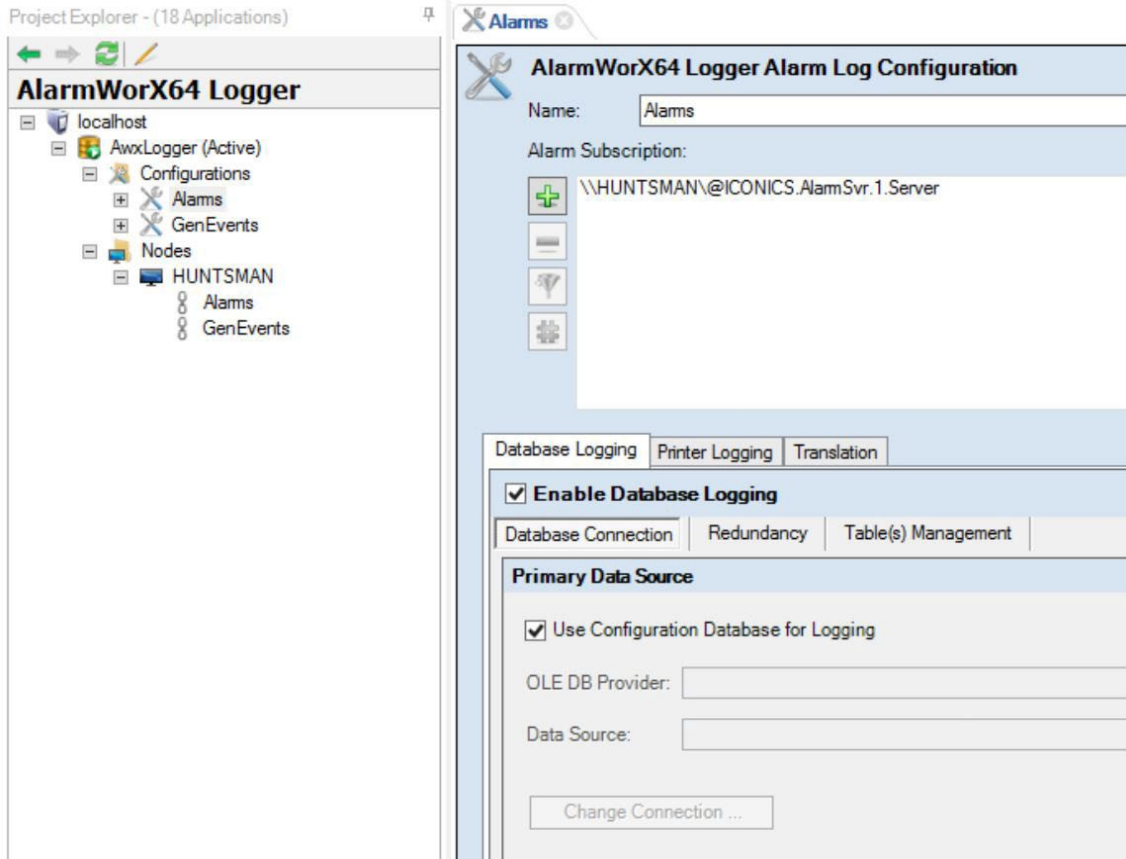
#### UDM Register Tree for Assigning Smart Alarm Values to OPC Tags when Alarms are Entered or Exited



### AlarmWorX Logger and Alarm Messages

The AlarmWorX Logger must subscribe to the AlarmWorX Server to log historical messages. These messages are retrieved in the historical alarms tab of the AlarmWorX Viewer.

#### AlarmWorX Logger Subscription to AlarmWorX Server





## System Setpoints, Time Schedules, and Holiday Schedules

### System set points

All set points are located on the system's respective Control Graphic. A set point is a value that the system attempts to meet, and is a value that is light yellow in color. A control output is a modulating piece of equipment such as a valve or damper, and has a value that is represented with a grey color. All light yellow or grey values that have a green or red override box can be changed. Most values missing the override box are typically read-only; however this is not always the case. Some controllers do not have the concept of an override built in. For instructions on how to override set points, please see section below.

### Time schedules

Some buildings have schedules for when the spaces and HVAC equipment is to be used and not used, referred to as an occupied or unoccupied mode, or in some instances as a night set back. For the buildings that do have this functionality available, typically the air handling unit has a weekday and weekend time schedule for when the building is occupied with staff and students.

When the time of day falls outside the scheduled occupied time, the equipment shuts down and goes into a "stand-by" mode and will only start up when a set point is not being met, when it is time for the equipment to be occupied again, or the equipment is overridden to be active.

The occupied schedule is located on the Control Graphic on the system. The occupancy schedule typically handled on a per-system basis instead of a global setting applied to all units in the building.

Occupancy control for individual rooms is typically found on the room control graphic. The occupancy schedule for the rooms is typically controlled by the air handling unit that supplies the rooms, though an individual room can be set to either occupied or unoccupied.

### Holiday schedules

Updated holiday schedules are to be obtained from the University of Pennsylvania and the changes applied to any affected building's occupancy schedule as described in the time schedule section.

## **Override of Control Hardware Outputs**

All set points are located on the system's respective Control Graphic. A set point is a software value that the system attempts to meet, and is a value that is light yellow in color. A control output is a modulating piece of equipment such as a valve or damper, and has a value that is represented with a grey color. All light yellow or grey values that have a green or red override box are can be changed. Most values missing the override box are typically read-only; however this is not always the case. Some controllers do not have the concept of an override built in.

### **BACnet (Johnson Controls, Siemens, Andover, Automated Logic, Carrier)**

#### ***Applicable Controls Contractors: Johnson Controls, Siemens, Radius Systems, Phoenix Systems***

- Click on the value and it should be highlighted
- Enter new value into the box
- Press the "Enter" key
- If the set point of output was in automatic mode, it should change to override in a few minutes

### **Gyrec (Siemens - Open System Gateway)**

#### ***Applicable Controls Contractors: Siemens***

- Click on the Manual/Override button
- Change mode to "Manual"
- Click on the value and it should be highlighted
- Enter new value into the box
- Press the "Enter" key

### **Ethernet/IP CIP (Allen-Bradley Rockwell)**

#### ***Applicable Controls Contractors: Automated Controls Concepts, Thermo Systems***

- Click on the Manual/Override button
- Change mode to "Manual"
- Click on the value and it should be highlighted
- Enter new value into the box
- Press the "Enter" key

### **Metasys (Johnson Controls)**

#### ***Applicable Controls Contractors: Johnson Controls***

- Click on the Manual/Override button
- Change mode to "Manual"
- Click on the value and it should be highlighted
- Enter new value into the box
- Press the "Enter" key

## Operator Log On Procedures for Gen64 SCADA

### OCC Operator Log On Procedure

Prior to having access to the SCADA system, users will be required to complete a form titled 'SCADA Access Authorization and Briefing Form'. This form is available from the FRES IT department. Once completed, FRES IT will create a Windows account on the SCADA domain. FRES IT will then provide the user with their username and a temporary password. This temporary password will need to be changed at the user's initial logon. Passwords will be need to be changed every ninety (90) days.

The selected security method for UPenn's GENESIS64 SCADA software is Single Sign-on. When a user successfully logs into Windows (on a SCADA machine), the user will automatically be logged in to GENESIS64 software. Switching users (at times of shift change for example) requires logging out of Windows so the new user can log in.

There will be three GENESIS64 SCADA workstations used at OCC and each user/operator will need to logon to each machine for their shift.

Once successful logon has occurred, a default set of SCADA screens will be displayed. This can be reconfigured and modified for all users or for individual users. See the SCADA Administrator for assistance if the default set of screens needs to be changed. The three SCADA workstations are planned to provide six monitors with the ability to support a maximum of 10 displays/monitors. Each machine will have a different set of default screens and will initially mimic the existing Comdale Environment.

For problems with Windows logon, contact the FRES IT department. For problems with access and features within GENESIS64, contact the SCADA Administrator.