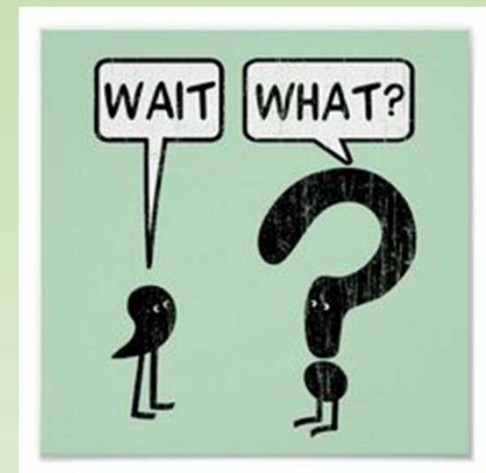


Better SCADA Terminology

Using better terminology to make
automatic control systems
easier to design, program and use

Graham Nasby, P.Eng, PMP, CAP
Water SCADA & Security Specialist
City of Guelph Environmental Services

2021 OWWA Ontario Water Conference
Apr 19 to May 5, 2021 – Ontario, Canada



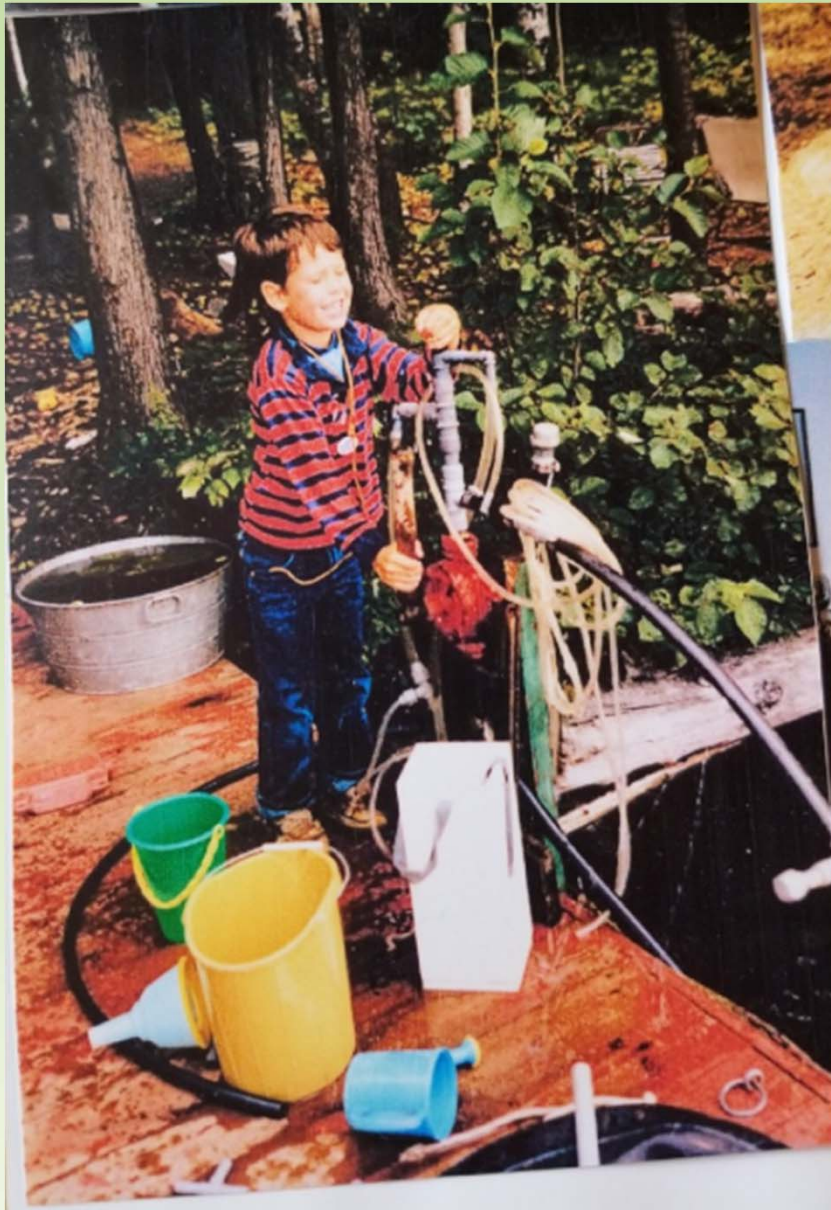
Control Schemes
Permissives
Interlocks
Alarms
Statuses

About the Speaker

Graham Nasby, P.Eng., PMP, CAP
Water SCADA & Security Specialist
City of Guelph Environmental Services



- 10 years in the consulting sector
- Joined City of Guelph Water Services in 2015
- OWWA and WEAO Member, Member of OWWA Automation Committee
- Co-chair of ISA112 SCADA Systems standards committee
- Voting member of ISA101 HMI Design and ISA18 Alarm Management committees
- Member of IEC/SCC TC65A “Industrial process measurement, control and automation”
- Member of CSA P125 “Operational Technology: Functional Safety and Security”
- Sessional instructor at McMaster University and Conestoga College
- Has published over 40 papers and articles on automation topics
- Received University of Guelph “Mid Career Achievement Award” in 2014
- Named ISA’s technical division leader of the year award in 2013.
- Contact: graham.nasby@guelph.ca



**I wanna be a
Water Guy
when I grow up!**



Presentation Outline

- SCADA Refresher
- Why Specifying SCADA functionality is hard
- The Process Control Narrative (PCNs)
- Issues with traditional PCNs
- A New Approach to PCNs
- Control Schemes, Interlocks, Permissives, Alarms
- Status vs. Alarm
- Station Control vs. Device-level Control
- Implementation Example
- The Standardized Guelph Water PCN Format
- Best Practices & Take-Aways



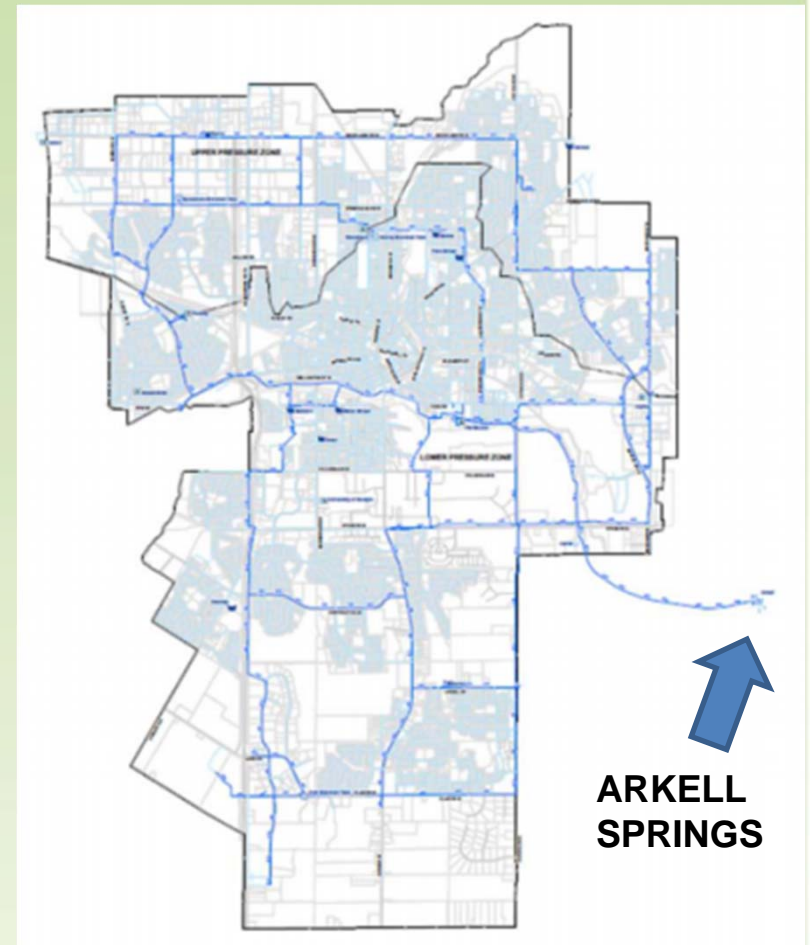
City of Guelph Water Services

- Guelph, Ontario, Canada
- 140,000 residents
- 21 groundwater wells
- 3 water towers
- 600 km of water mains
- 49,000 service connections
- 2,750 fire hydrants
- 35 unmanned facilities
- 46,000 m³/day [12 MGD]
- 60,000 m³/day peak [15 MGD]



Guelph Water Connected with SCADA

- Approx. 15km x 15km area
- 35 Facilities
 - 4 booster stations
 - 21 wells
 - 2 control chambers
 - 3 water towers
 - 5 monitoring sites
- 50 PLCs plus 2 data centers
- Redundant Data-Logging
 - Traditional SCADA data-logging
 - QuickPanels with store/forward
 - DNP3 Data-loggers with store/forward
- High availability SCADA network
 - Primary: private fibre optic
 - Secondary: private wireless backup, with 45 second auto-failover

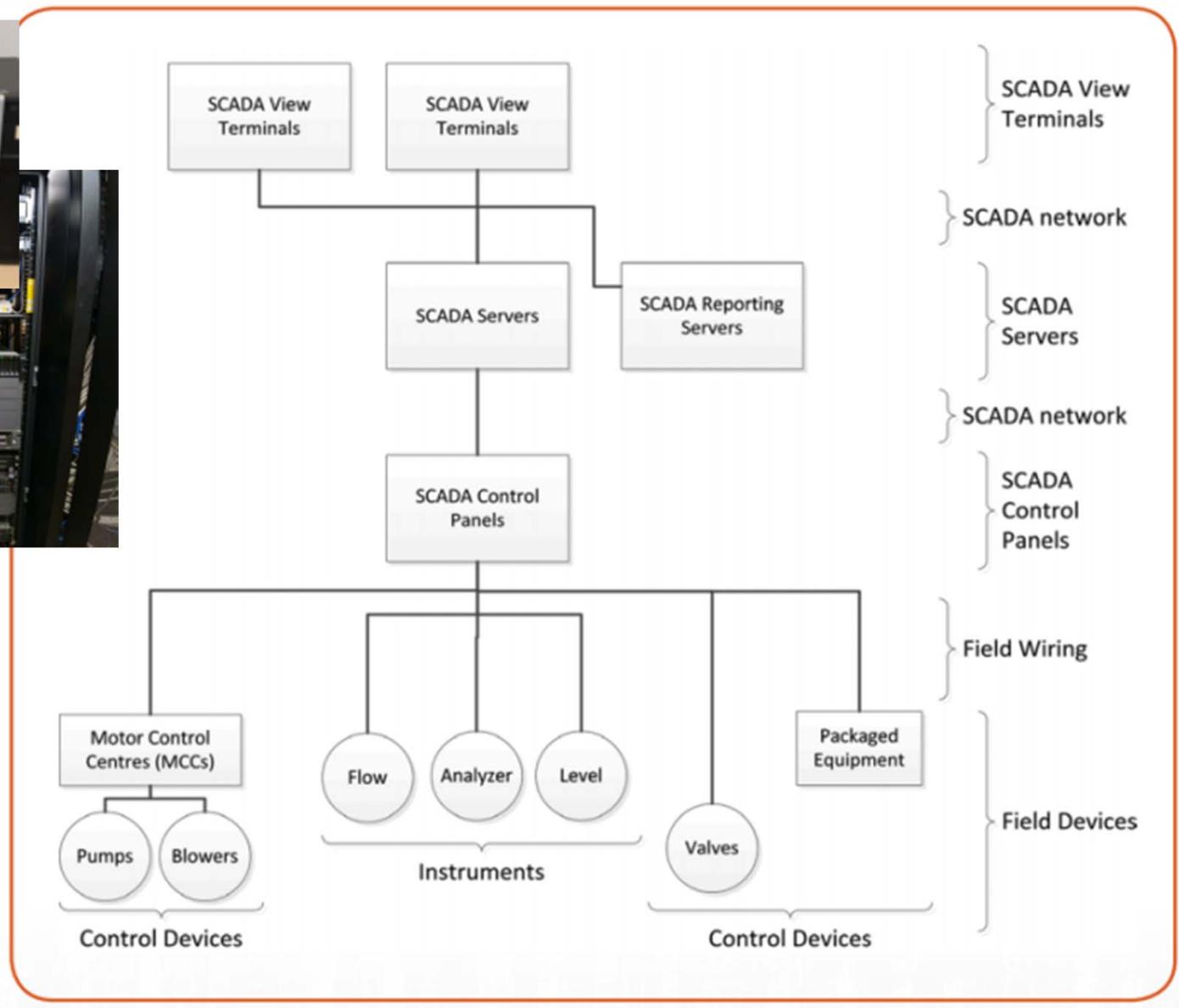


What is SCADA?



SCADA = Supervisory Control and Data Acquisition

Typical SCADA Architecture



Why Defining SCADA Functionality is Hard



Why Defining SCADA Functionality is Hard

CAUSE AND EFFECT CHART									
rev 4.2 7/21/06									
<div> <div>Questionable</div> <div>Modified</div> <div>Local Control</div> </div>									
Process Component						Device ID			
ID	Service	ID	#	SAC#	In	PLC			
H2S	H2S/SO2 Detectors	OSH	15	H2S	X4	5	X	X	
		OSH	5	SO2	X13	5	X	X	
		OAL	10/2	both	X14	5		X	
LEL	Combustible Gas Detectors	ASH	45%		X15	5	X	X	
		AAL	20%		X21	5	X		
	Purge Alarms	PAL			X51	var	X	X	
	Amine Plant (from local panel)	SD			X52	5	X	X	
		ALM			X53	5	X	X	
GO	Gross Oil Header WR 1, 2	PSH	205A		X56	5	X	X	
		PSL	205A		X57	5	X	X	
GO	Gross Oil Header WR 3, 4	PSH	206A		X60	5	X	X	
		PSL	206A		X61	5	X	X	
OS	Oil Pipeline	PSH			X62	5	X	X	
		PSL			X63	5	X	X	
		FAL	Waugh		X64	5	X	X	
		PAL			v1413	2	X	X	
GS	Gas Pipeline	PSH			X65	5	X	X	
		PSL			X66	5	X	X	
H2S	Sales Gas H2S Detectors	QAH			v1407	3	X	X	
SSV	Pneumatic System Well Room 1	PAL			X331	5	X	X	
SSV	Pneumatic System Well Room 2	PAL			X332	5	X	X	
SSV	Pneumatic System Well Room 3	PAL			X333	5	X	X	
SSV	Pneumatic System Well Room 4	PAL			X334	5	X	X	
SSSV	Hydraulic System Well Room 1 & 2	PAH			X306	5	X	X	
		PAL			X307	5	X	X	

Pg 3 of 29

Date Printed 01/03/2008

Why Defining SCADA Functionality is Hard

Excerpt from a very long specification document...

An ultrasonic level sensing device is used to measure the contact chamber water level. The device generates an analog signal (variable) that is monitored by the local P.L.C. Based on programmed contact chamber level set points, the P.L.C. controls the start / stop cycles of the Well and Booster pumps. The contact chamber floor is at 0 m.

During normal “Automatic” operations, the Booster pump runs continuously to provide a consistent pressure and supply to the distribution system. To achieve this, the Well pump flow rate is set 2 to 5 L/sec above the Booster flow rate and operates on start and stop set points based on reservoir level.

Well and Booster Start/Stop setpoints can be manually entered in SCADA iFix by selecting 'Well Site Number 1' on the 'Main System Overview' home page; then selecting 'Station Setpoints' Other available setpoint options with respect to Well Site No.1 Booster are as follows:

- Start / stop setpoints for can be entered in relation to the Primary Tower level.
- A Booster Discharge Pressure Start Setpoint that ensures a minimum pressure in the distribution system at the station discharge (this setpoint overrides the setpoints based on the Primary Tower level – if necessary).
- Time of Day Start/Stop Setpoints can be entered as a means of storage control during periods of low system demand.
- There is a stop set point for the Booster pump to protect it from running dry under abnormal conditions.

The raw water is chlorinated using 12 % sodium hypochlorite. The liquid chemical is stored in a plastic container which sits inside a second spill containment tank. The sodium hypochlorite tank is located on a weigh scale so that sodium hypochlorite consumption and dosage records can be maintained.

A chemical feed pump is located above the sodium hypochlorite tank which processes sodium hypochlorite through a feed line to a chlorination point where Well water enters the contact chamber. The pump is “flow-paced” and will adjust its dosage rate in response to a variable 4 to 20 mA signal from the PLC based on the raw water flow rate. The pump is set to deliver a specific finish free chlorine residual in the treated water discharged from the facility. A continuous free chlorine analyzer monitors the finish residual. Manual adjustments to the output volume of the chemical feed pump (based on raw water flow rate) can be made via the on site QuickPanel or remotely through SCADA.....

Why Defining SCADA Functionality is Hard

Excerpt from another very long specification document...

With the selector switch in Auto position an operator can set the Control Software to operate in one of the following modes:

Control on Command – (manual control from Woods PS or Well local HMI screens). The well pump start will allow the well pump to start. This feature provides manual control from Woods PS or Well local HMI screens and will start/stop if all pre-conditions have been satisfied. All inputs to the PLC are still monitored, and alarm conditions are indicated.

The following pre-conditions must be set before a start will be allowed:

- Well Pump must be available (level OK, pump not in local)
- Well Pump must be in Remote

The following conditions must occur for the equipment to remain on after a start is complete:

- no low flow alarm
- no low/high pressure alarm

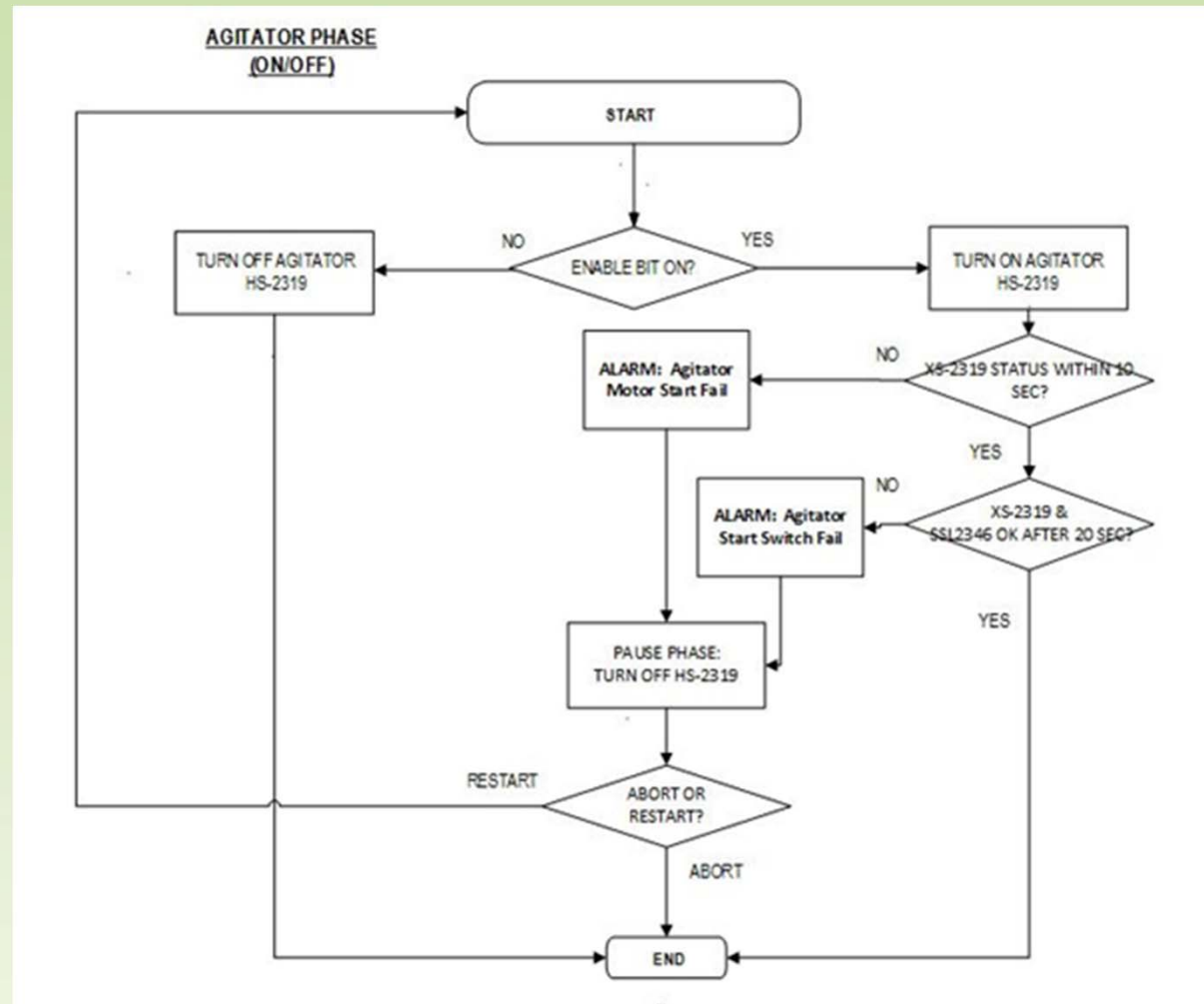
Automatic – The control software is in the automatic mode. The well system will request an automatic start of a duty pump. This allows the well pumps to start/stop as directed by the SCADA system. All inputs to the PLC are still monitored, and alarm conditions are indicated. Same pre, mid, and post conditions in manual start still apply.

Alarms are indicated both at Well local HMI screens and at Woods PS Station Central Control. All alarms will remain indicating until they are both acknowledged and cleared.

Alarms:

- Pump Fail to Start/Stop
- Well System General Alarm
- Low Well Pump Flow
- High Well Pump Flow
- Well Motor Overload
- Power Failure
- Well Low/high Pressure
- Well Level Low Low

Why Defining SCADA Functionality is Hard



Process Control Narratives

Process control narratives are written for a number of reasons. They reveal the design engineer's overall control philosophy and objectives. They **should simply and clearly state** how the control systems are expected to function, so everyone—suppliers, contractors, and operators—will understand. (Source: WEF MoP 21)

However, many control narratives end up being:

- Very long (100+ pages not unusual)
- Difficult for operations staff to read and understand
- Use a large number of confusing terms the user has to remember as they read it
- Are sprinkled with many, many cryptic tags and jargon, including weird “SCADA Tags”
- Structured in such a way to make design coordination checks very difficult
- Not defining what the expected normal operating ranges for process values should be
- Not clearly defining the operating targets (and limits) for the automatic control system
- Setpoint values that are not shown in context
- How the system should (or should not) handle various problems is not clearly defined
- Details needed by the programmer / system integrator are often left out
- Often results in many time-consuming questions from the system integrator
- **Don't clearly define what the control system is supposed to be doing (or not do)**

Process Control Narratives

Complexity is your enemy.
Any fool can make
something complicated. It is
hard to ***keep things simple.***
-Richard Branson



A New Simpler Way (and Better Terminology)

Station-Level Control

- Station Permissives
- Station Mode (e.g., Just Run, Tower-level, Pressure)
- Run Enable/Disable

Station Sequencer

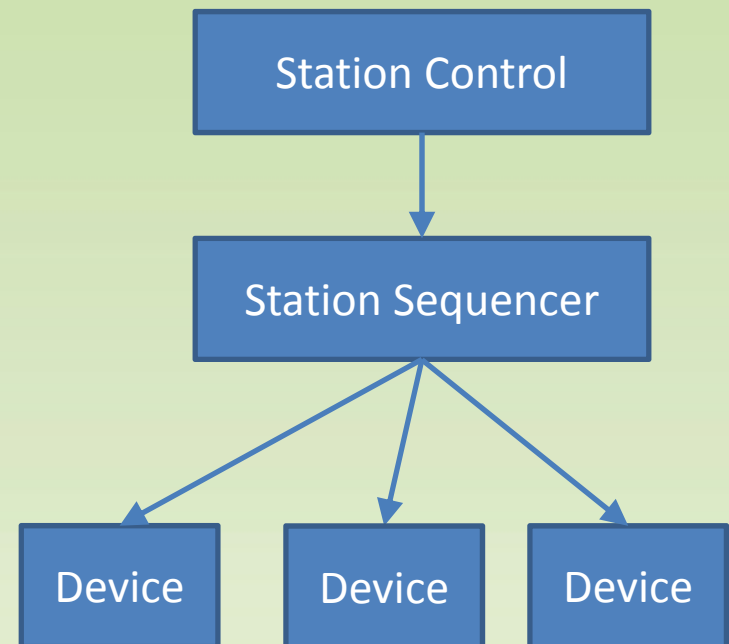
- Automated start-up
- Automated shut-down
- Re-start after power outage

Device-Specific Control

- Control Scheme (e.g., fill based on level)
- Permissives
- Interlocks
- Alarms

Analog Value Alarms

Other Alarms



Device = a Pump or a Controlled Valve

New Terminology – Interlocks, Permissives & Alarms

Station Permissives

- Conditions that must be true for entire station to be able to start (and continue running)
- Programmed as numbered station permissives (01, 02, 03, etc.) with description for each one
- Station will shutdown if one or more station permissives are lost
- **Station can auto-restart** once all station permissives are met (and if no devices are interlocked)

Device Control Scheme

- The normal automatic control scheme for a device (e.g. start-on-low-level, stop-on-high-level)
- Does not cover exceptions / problems

Each device will have its own device-specific numbered lists of:

- **Device Permissives (01, 02, 03, etc.)**
 - Conditions that must all be OK for the pump to run (or valve to open)
 - If a permissive is lost, pump will stop; but pump will auto-restart once condition resolves
- **Device Interlocks (01, 02, 03, etc.)**
 - If an interlock is activated when the pump is off, the pump will be prevented from starting
 - If an interlock is activated when the pump is on, it will shutdown pump and latch in place, and trigger a “shutdown on interlock” alarm – it must be now be reset by an operator
- **Device Alarms (01, 02, 03, etc.)**
 - Numbered alarms that are specific to that pump (or controlled valve)

New Terminology – Interlock vs. Alarm

Alarm

- Notifies an operator that a response is required
- Not used for shutting down any equipment
- Can be adjusted and enabled/disabled by operators

Interlock

- Prevents a device from running (or starting) in the case of a bad condition
- Also used to automatically shutdown a device (pump or valve) due to undesirable condition
- Does not trigger an alarm, instead is separate “shutdown on interlock” alarm for each device
- If interlock occurs and device is not running, no notification to operator (since it doesn’t matter)
- Interlocks cannot be modified or enabled/disabled without a change control process

Interlock = will shut down a running device if triggered. After a shutdown, operator reset required.

Permissive = required for a device to run. A device can auto-restart if its permissives are satisfied.

From IEC-62682 “Management of Alarm Systems for the Process Industries” and ISA18.2”:

Alarm: audible and/or visible means of indicating to the operator an equipment malfunction, process deviation, or abnormal condition requiring a timely response.

New Terminology – Alarm vs. Status

Status

- The raw unfiltered / unmodified status of a signal coming into the PLC from the field
- Used for showing the status of devices and instruments on SCADA screens
- Shows the “current truth” to operators of what is going on

Alarms

- An alarm is a notification of a condition that requires a timely operator response/action.
- Unlike a raw status, an alarm will often have trigger delay, masking or logic filtering:
 - e.g., building flood switch with a 5 second “de-bounce” delay to prevent nuisance alarms
 - e.g., when a pump starts, and associated low flow alarm is masked for the first 2 minutes
 - e.g., a reservoir low level float switch alarm would be filtered if a station is out of service

For I/O points, there will always be a separate statuses and (if needed) separate alarms

From IEC-62682 “Management of Alarm Systems for the Process Industries” and ISA18.2”:

Alarm: audible and/or visible means of indicating to the operator an equipment malfunction, process deviation, or abnormal condition requiring a timely response.

New Terminology – Station Control vs. Device Control

Station-Level Control

- Station Permissives
- Station Mode (e.g., Just Run, Tower-level, Pressure)
- Run Enable/Disable

Station Sequencer

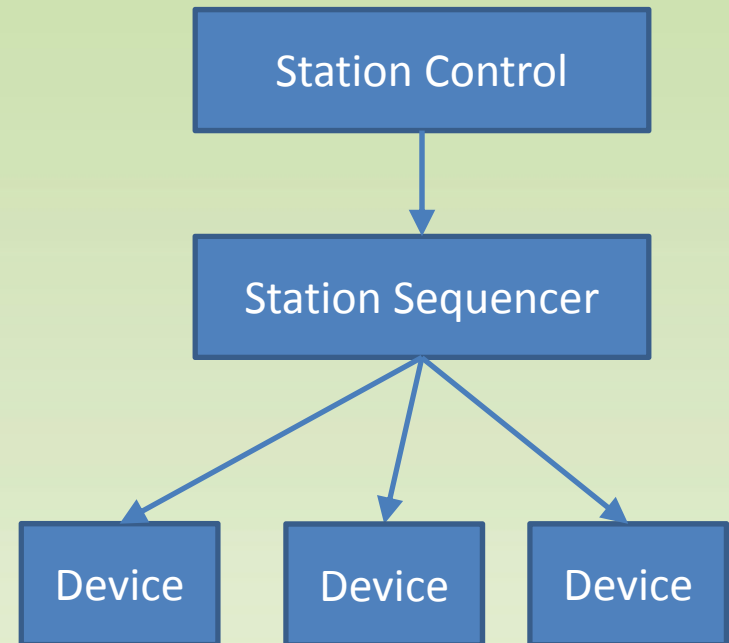
- Automated start-up
- Automated shut-down
- Re-start after power outage

Device-Specific Control

- Control Scheme (e.g., fill based on level)
- Permissives
- Interlocks
- Alarms

Analog Value Alarms

Other Alarms



Device = a Pump or a Controlled Valve

Station Control

Controls when station as a whole is called to run
Could be “Just Run” or be based on a Tower Level

Device Control

Receives commands from Station Sequencer
Looks after the control of just that specific device

Device Permissive, Interlock and Alarm Tables

EXAMPLE: CHEMICAL FEED PUMP (HYPO PUMP)

Control Scheme

- If well pump is running, run the chemical feed pump
- Chemical feed pump speed = $\text{DoseSetpoint} * \text{FlowRate} * 0.03 / \text{PumpSize} * 100 * \text{Factor}$

Permissives Table

Permissives – Required to Run. Auto Restart Possible			Applies to			Other
#	Name	Description, Logic, Setpoints, Timers	SCADA Manual	SCADA Auto	Local	
01	Facility Power Ok	- Facility Power must be online for at least 2 minutes	X	X	X	
02	Hypo Pump Power	- Pump Power Feed must be good for at least 1 minute	X	X	X	Based On Pump Speed Feedback
Plus	No Interlock Conditions are True	- None of the interlocks in the following table can be active	X	X	--	

Interlocks Table

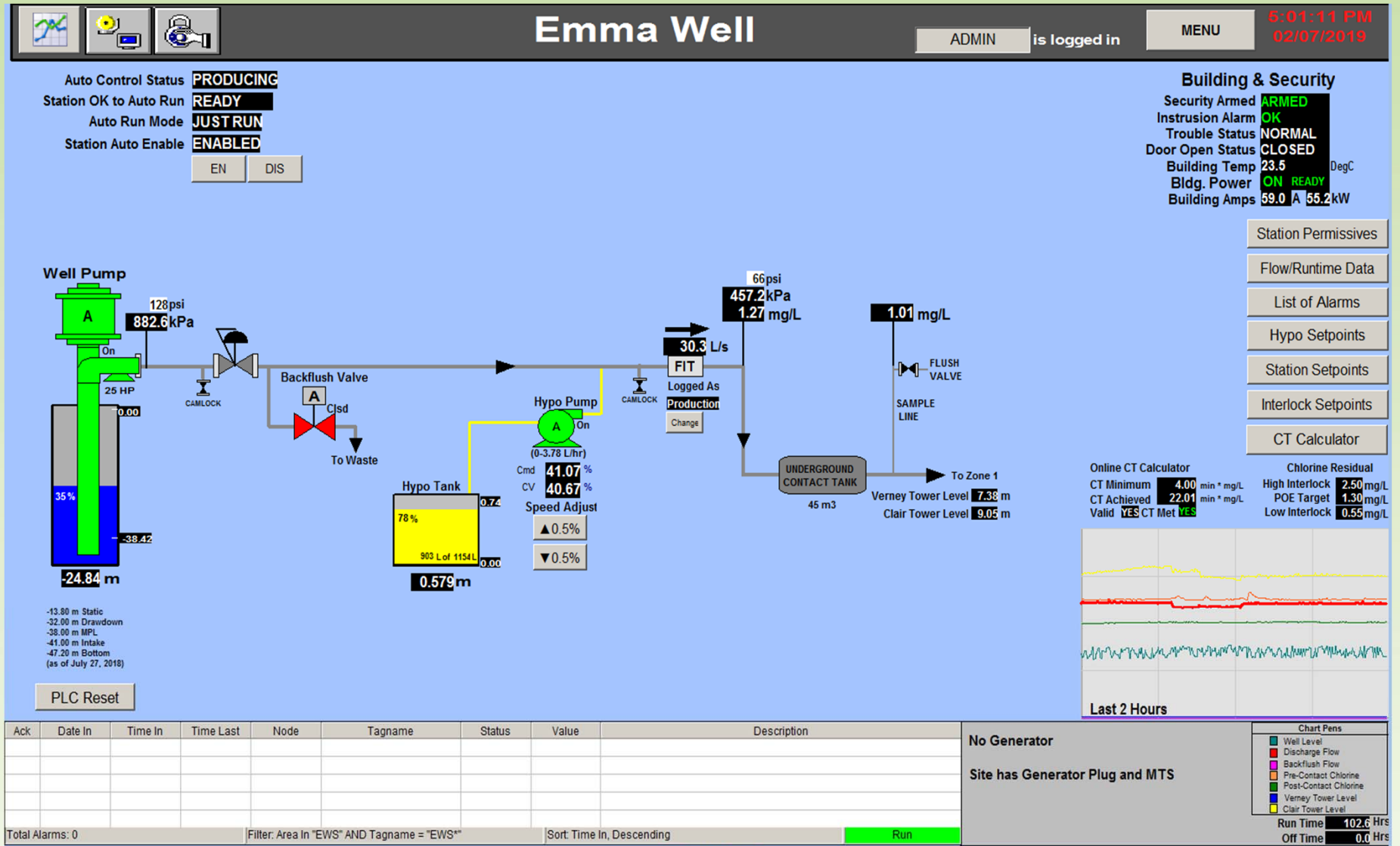
Interlocks – Stops the Pump, Manual Reset Necessary			Applies to			Reset Type		Other
#	Name	Description, Logic, Setpoints, Timers	SCADA Manual	SCADA Auto	Local	Via button on HMI	via physical reset button	
01	Hypo Pump Fault	- Hypo Pump fault signal (digital input) for 5 sec	X	X	--	--	X	Mask if facility power outage
02	Hypo Pump Tube Leak Fault	- Hypo Pump tube leak fault signal (digital input) for 5 sec	X	X		--	X	Mask if facility power outage
03	Hypo Pump Feedback Signal Bad	- Feedback signal outside of 4-20mA Range for 10 sec	X	X	--	X	--	Mask if facility power outage
Plus	Hypo pump Virtual alarms	- Hypo pump fail to start, fail to stop, Uncommanded start, Uncommanded stop, Speed Deviation	X	X	--	X	X	Mask if facility power outage

Device Permissive, Interlock and Alarm Tables

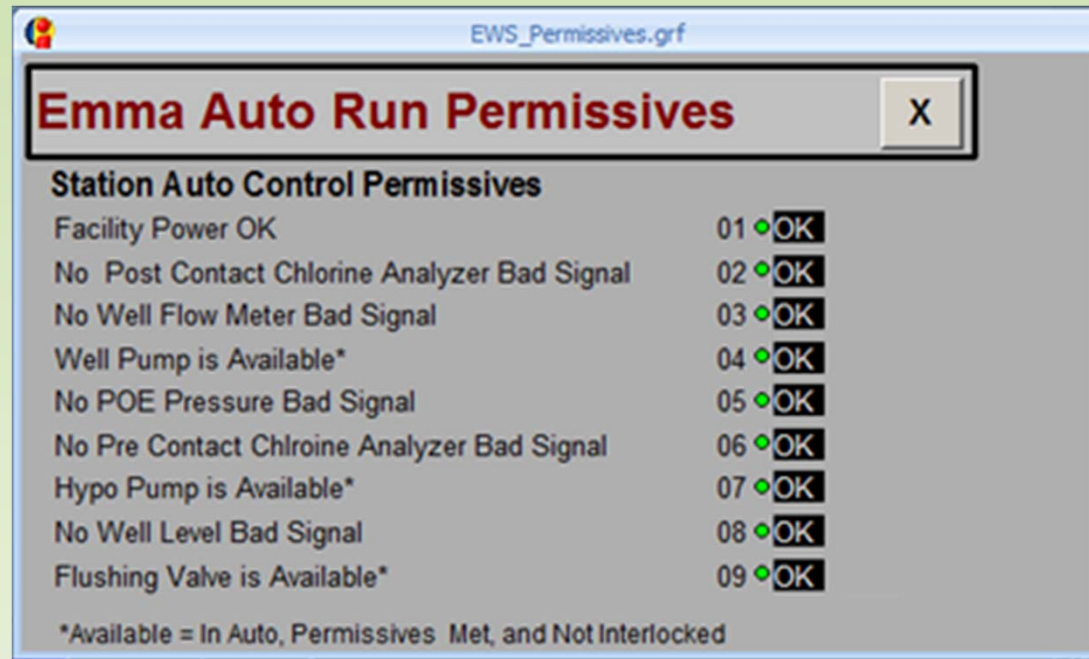
Alarms Table

#	Alarm Description	Alarm Logic	Purpose	Consequence if Ignored	Operator Action	Time to Respond
01	Fail to Start	Standard alarm logic (see SCADA standards)	Acts as interlock	Possible malfunction, station not able to operate without hypo pump (loss of production capacity)	Investigate on site	2 hrs
02	Fail to Stop	Standard alarm logic (see SCADA standards)	Acts as interlock	Possible malfunction, station not able to operate without hypo pump (loss of production capacity)	Investigate on site	2 hrs
03	Uncommanded Start	Standard alarm logic (see SCADA standards)	Acts as interlock	Possible malfunction, station not able to operate without hypo pump (loss of production capacity)	Investigate on site	2 hrs
04	Uncommanded Stop	Standard alarm logic (see SCADA standards)	Acts as interlock	Possible malfunction, station not able to operate without hypo pump (loss of production capacity)	Investigate on site	2 hrs
05	Emma Hypo Pump Speed Deviation	Setpoint vs. Feedback more than 10% different for 75 seconds (to allow for 60 second prime button)	Acts as interlock	Possible malfunction, station not able to operate without hypo pump (loss of production capacity)	Investigate on site	2 hrs
06	Emma Hypo Pump Fault	Hypo pump fault (digital input) for 5 seconds	Hypo pump not working properly	Low chlorine alarm, well pump shutdown, low chlorine water in reservoir	Visit site	2 hrs
07	Emma Hypo Pump Tube Runtime HI	Tube Runtime above HI Setpoint	Hypo Pump Tube Runtime HIHI	Tube Runtime above HI Setpoint 2500 hrs	Warn that tube needs to be replaced soon	Tube breakage will eventually occur soon
08	Emma Hypo Pump Tube Runtime HIHI	Tube Runtime above HIHI Setpoint	Hypo Pump Tube Runtime HI	Tube Runtime above HIHI Setpoint 3500 hrs	Warn that tube needs to be replaced	Tube breakage will occur soon
09	Emma Hypo Pump Tube Leak Fault	Hypo pump tube leak fault (digital input) for 5 seconds	Hypo pump not working properly	Low chlorine alarm, well pump shutdown, low chlorine water in reservoir	Visit site	2 hrs
10	Hypo Pump Left Running in Local 5 min	Pump left in local for 5 minutes	Remind operator to place in auto	No automatic control of station, possible improper dosing	Place pump into Remote-Auto	1 hour
11	Hypo Pump Left Running in Manual 5 min	Pump left in manual for longer than 5 minutes	Remind operator to place in auto	No automatic control of station, possible improper dosing	Place pump into Remote-Auto	1 hour
12	Hypo Pump Shutdown on Interlock	Pump Shutdown due to interlock	interlock needs to be reset, to return pump back to service	Possible malfunction, station not able to operate without hypo pump (loss of production capacity)	Investigate on site	2 hrs

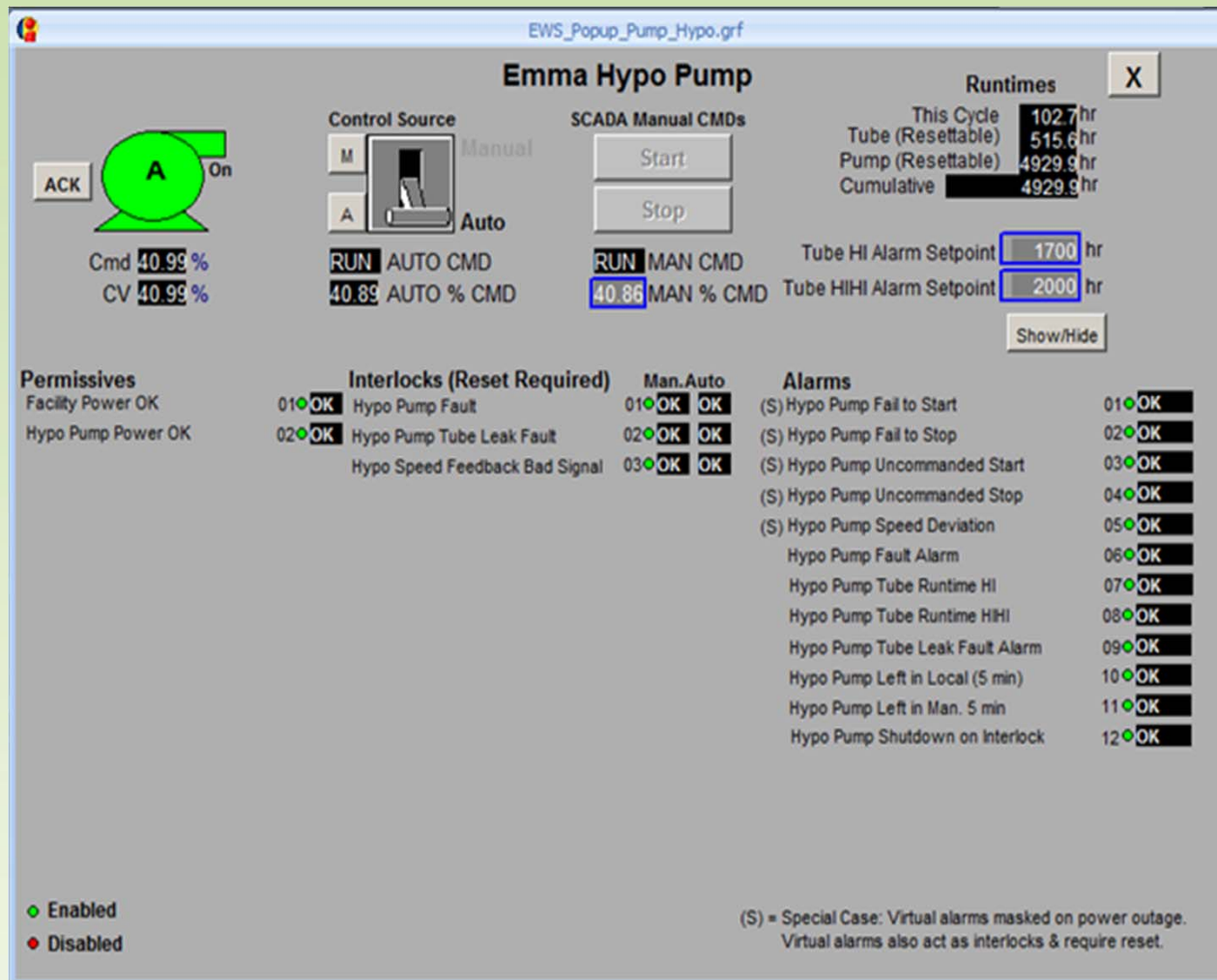
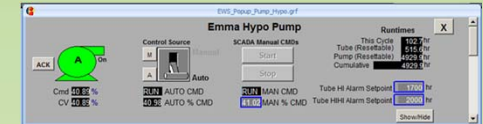
New SCADA Terminology - Example



New SCADA Terminology - Example



New SCADA Terminology - Example



New SCADA Terminology - Example



EWS_Popup_Pump.grf
X

Emma Well Pump

ACK

Control Source

M Manual

A Auto

RUN AUTO CMD

SCADA Manual CMDs

Start

Stop

RUN MAN CMD

Runtimes

This Run Cycle 102.6 hr

Motor (Resettable) 4928.5 hr

Pump (Resettable) 1018.8 hr

Cumulative 4,928.46 hr

Volume Today 1824 m3

Volume Yesterday 2619 m3

Show/Hide

Permissives

Facility Power OK

Well Pump Starter Power OK

Interlocks (Reset Required)

01	OK	Well Level Below MPL
02	OK	Well Pump Flow Rate Above Permit
		Well Pump Daily Flow Total Above Permit
		Well Pump Starter Fault
		Hypo Pump Interlocked
		Hypo Pump Did Not Start In 5 Sec
		Well Pump No Flow (<5 L/s, 30 s)
		Global Chlorine Interlock
		Well Level Bad Signal
		Well Pump E-Stop Pressed

Man. Auto

01	OK	OK
02	OK	OK
03	OK	OK
04	OK	OK
05		OK
06		OK
07		OK
08	OK	OK
09	OK	OK
10	OK	OK

Alarms

(S) Well Pump Fail to Start Alarm

(S) Well Pump Fail to Stop Alarm

(S) Well Pump Uncommanded Start Alarm

(S) Well Pump Uncommanded Stop Alarm

Well Pump Starter No Power

Well Pump Starter Fault Alarm

Well Pump Left In Local For 30 min

Well Pump MPL Warning Alarm

Well Daily Flow Total Near Permit Alarm

Well Flow Rate Near Permit Alarm

Well Pump Shutdown on Interlock Alarm

Well Pump E-Stop Pressed Alarm

● Enabled

● Disabled

(S) = Special Case: Virtual alarms masked on power outage. Virtual alarms also act as interlocks & require reset.

New SCADA Terminology - Example

WWS_Analog_Popup.grf


Well Level

Value **-24.01** m (-38.8 to 0) Raw Signal: **OK**

Alarm Setpoints:

	EN	DIS	Enabled?	ALARM
HIHI: 0.00	<input type="checkbox"/>	<input type="checkbox"/>	• Disabled	OK
HI: 0.00	<input type="checkbox"/>	<input type="checkbox"/>	• Disabled	OK
LO: 0.00	<input type="checkbox"/>	<input type="checkbox"/>	• Disabled	OK
LOLO: 0.00	<input type="checkbox"/>	<input type="checkbox"/>	• Disabled	OK
Bad Signal	<input type="checkbox"/>	<input type="checkbox"/>	• Enabled	OK

Last 24 Hours

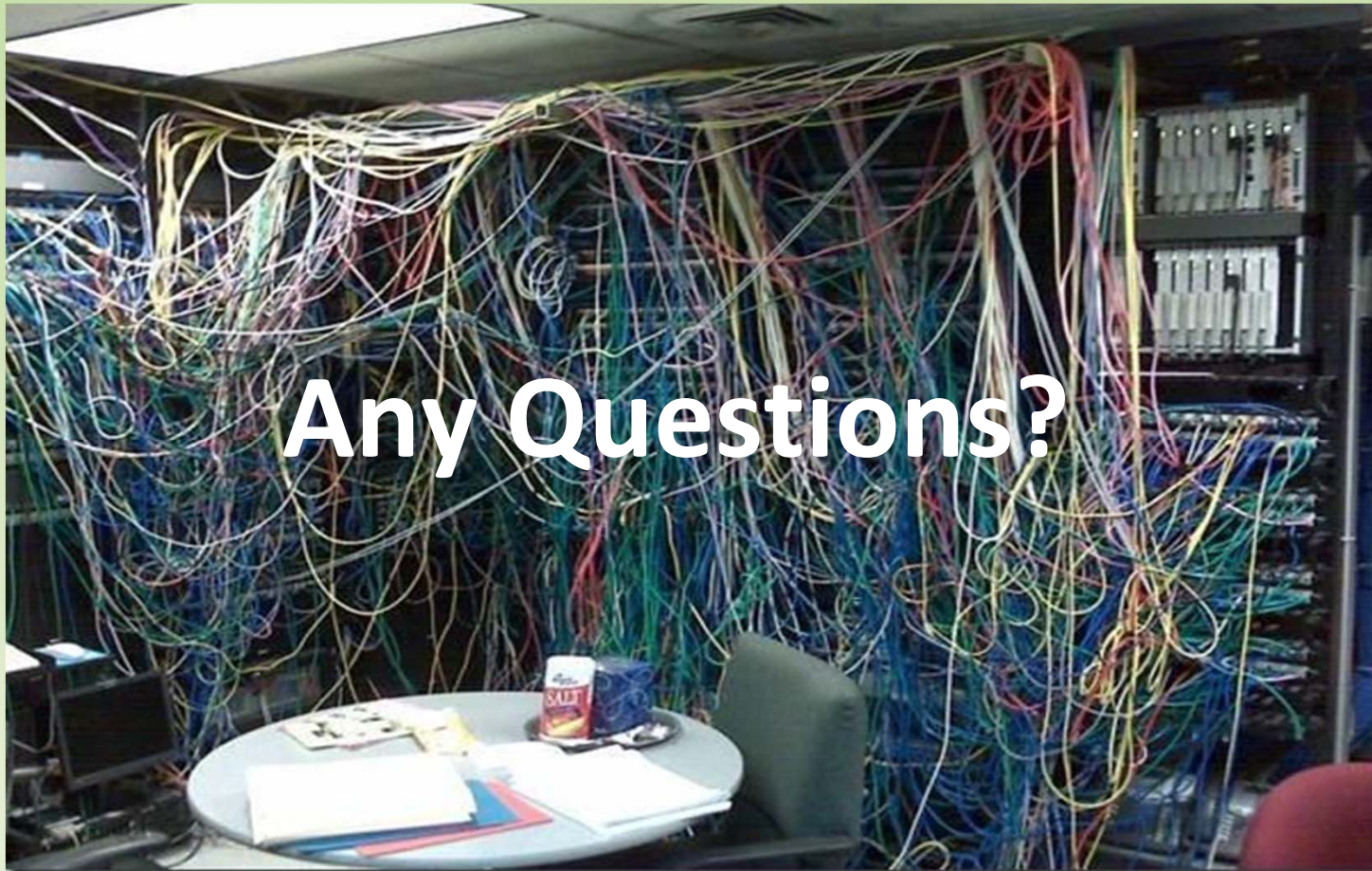


	MINIMUM	MAXIMUM	AVERAGE
TODAY	-24.72	-21.83	-23.44
YESTERDAY	-24.24	-12.01	-17.26

ACK

Guelph Water New Standardized PCN Format

1	Facility Overview	15	Device Control Module
1.1	Facility Description	16	Device Control Module
1.2	Process Block Diagram	17	Device Control Module
		18	Etc.
2	General Information		
3	Equipment Summary	27	Flow Totalization
3.1	Devices	28	Device Runtimes
3.2	Instruments	29	Online CT Calculator (if applicable)
3.3	Packaged Equipment	30	PLC-to-PLC Communications
3.4	Measurements from PLC-to-PLC Message	31	PLC Panel Functions and PLC Pilot Lights
3.5	Calculated measurements	32	Electrical Equipment
3.6	PLC Panel Devices	33	Building Services Equipment
3.7	Electrical Equipment	34	Fault Conditions and Responses
3.8	Building Services		
3.9	Miscellaneous SCADA Equipment		
3.10	Other		
			Appendices
4	Operating Strategy	A:	Facility P&ID Drawing
5	Regulatory Limits	B:	Facility Layout Drawing
6	Regulatory Data Logging Requirements	C:	Main PLC I/O List
7	Primary Disinfection Calculation for Well: CT Calc (Info)		
8	Secondary Free Chlorine Residual Requirements (Info)	D:	PLC Messaging – Digital Power Monitor
9	Operating Targets & Limits	E:	PLC Messaging – Outboxes for SCADA Statistics PLC
10	Automatic Control Summary	F:	PLC Messaging to/from Other Sites
		G:	Data Points to be Logged by SCADA Historian
11	Control Modes	H:	PLC Outboxes/Inboxes for QuickPanel
12	SCADA Conventions	I:	I/O List for Backup Data Logger
13	Software & Device Control Modules Hierarchy	J:	SCADA Screen Design
14	Station Control Module	K:	Master List of Alarms
15	Station Sequencer Module		



Any Questions?

* Not a High Performance SCADA System

Graham Nasby, Water SCADA & Security Specialist

graham.nasby@guelph.ca