Current Trends in SCADA Systems

Situational Awareness
Alarm Management
Data Availability
System Robustness/Redundancy

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

OWWA Total Water Solutions Workshop
Tuesday, Oct 3, 2017 – Timmins, Ontario, Canada

About the Speaker

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

- 10 years in the consulting sector
- Joined 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 standards committee
- Voting member of ISA18 Alarm Management standards committee
- Named Canadian Expert on IEC/SCC-TC65 with Standards Council of Canada

- Has published over 30 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

City of Guelph Water Services

- Guelph, Ontario, Canada
- 130,000 residents
- 21 groundwater wells
- 3 water towers
- 549 km of water mains
- 49,000 service connections
- 2,750 fire hydrants
- 46,000 m^3/day [12 MGD]

Presentation Outline

- Review of what SCADA is
- State of Most SCADA Systems

- Situational Awareness
- High Performance HMI
- Alarm Management
- Data Redundancy – making it easier
- SCADA communication networks
- Cyber Security
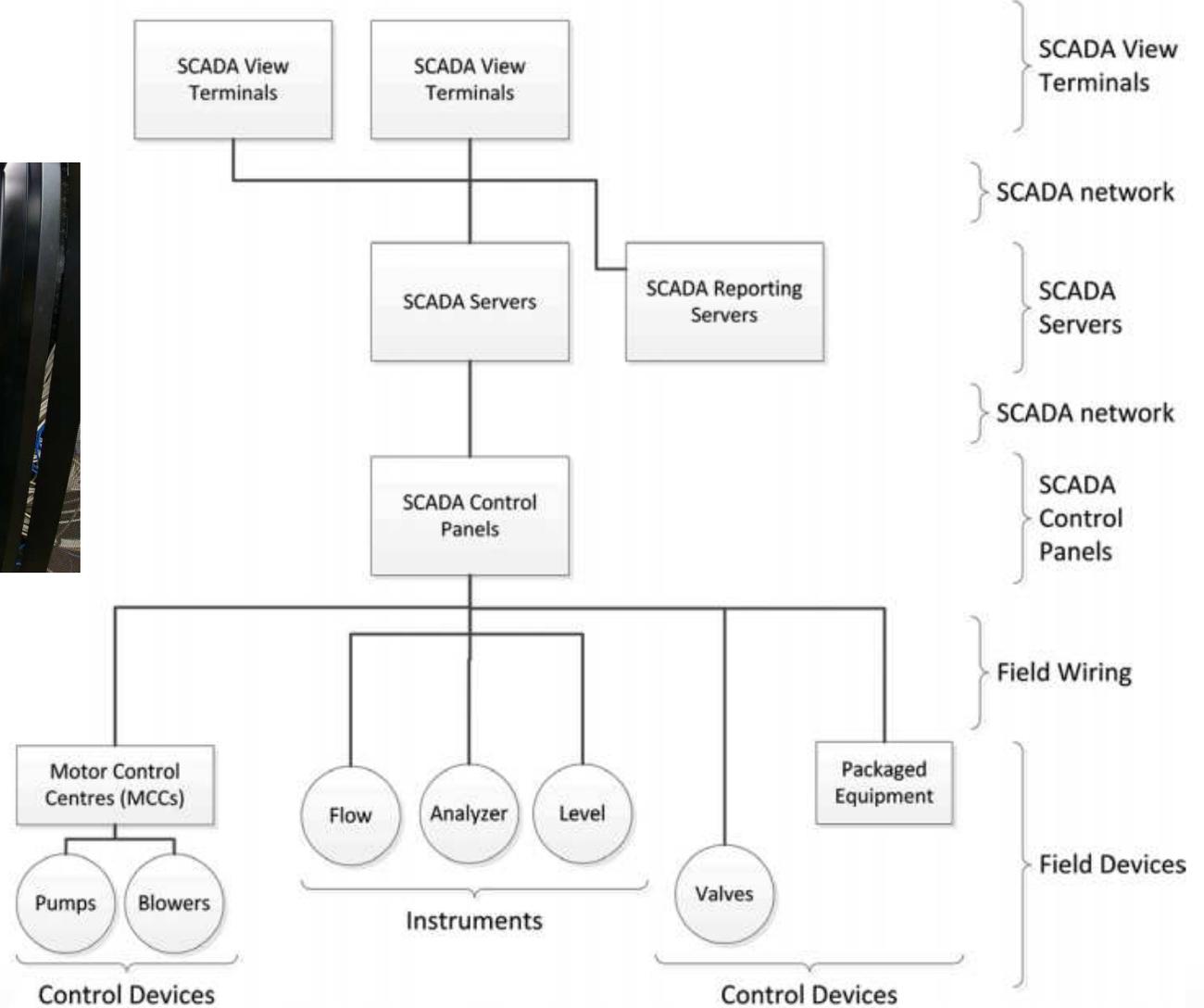- Planning for SCADA Upgrades: building on what you have

Review:
What is SCADA?

**SCADA = Supervisory Control and Data Acquisition**

Typical SCADA Architecture
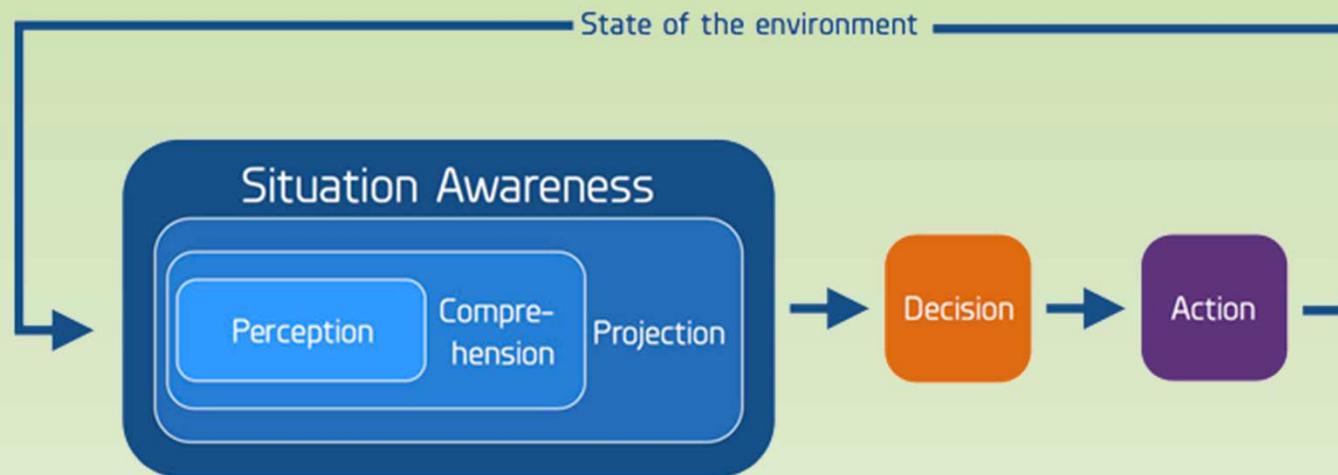
Why we have SCADA systems

- Unattended automatic control of water facilities
- Logging of critical control parameters
  - Chlorine Residuals (e.g., 5 minute recording intervals)
  - Turbidity
  - Well Flow Rates & Daily Flow Totals
  - POE Flow Rates & Daily flow Totals
  - Tower Levels & Pressure

- Provides "visualization" of water facilities to Operators
- Enables remote monitoring and control by Operators
- Triggering and Annunciation of Alarms
- Automated responses (increase chlorine dose, shutdown, etc.)
- Reporting based on logged process data

What's new in SCADA?
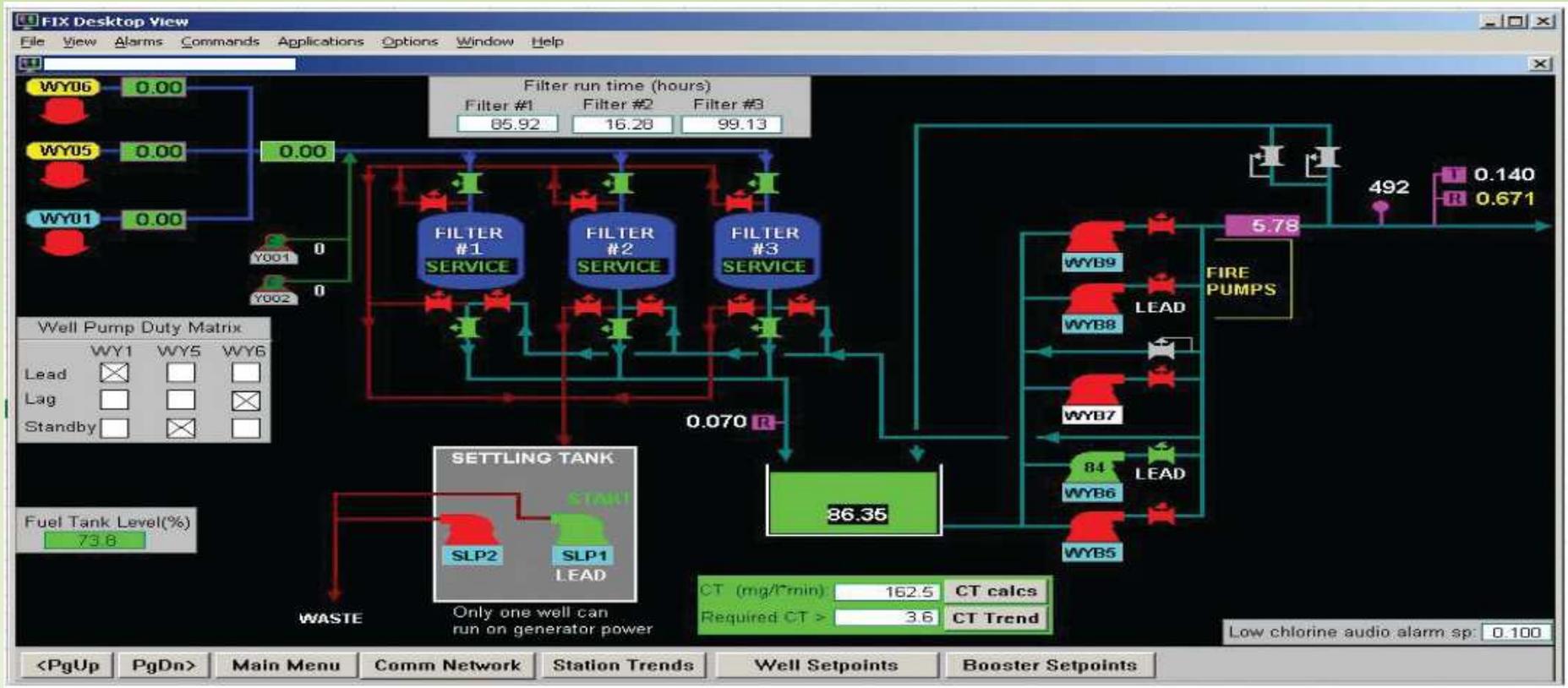
- What is running?

- What if your are colour blind?

- Is the process running well?

- Is anything abnormal?

SCADA: Situational Awareness

To be an effective operator

–

you have to be aware of what your plant is doing
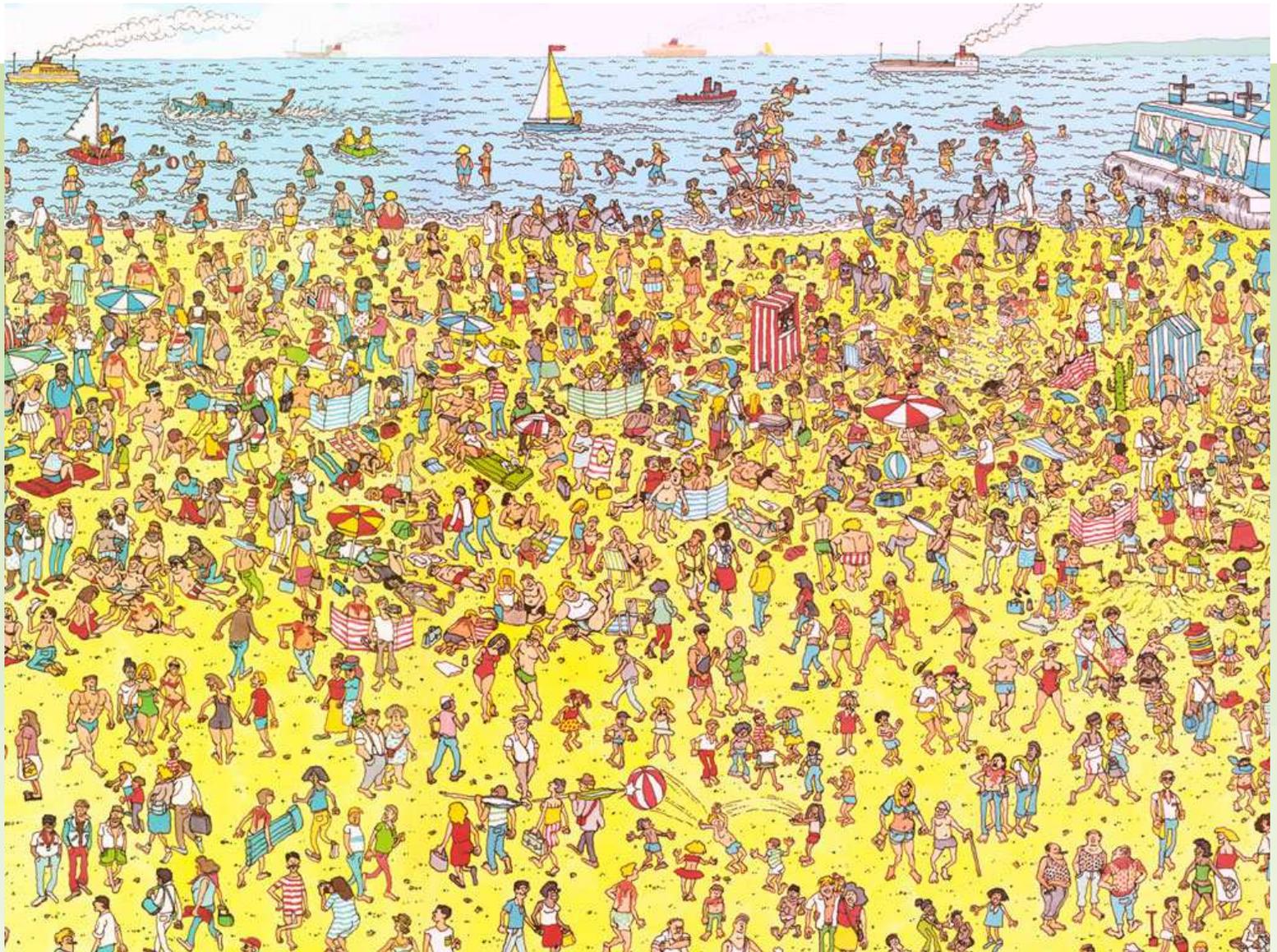
Common SCADA problem

In some SCADA systems….
You can't see the whole picture

Common SCADA problem

What your SCADA system may not be showing you

CAN

YOU

FIND

THE

PROBLEM

ON THE

SCADA

SCREEN?

Friendly
SCADA Guy

Situational Awareness

- **To be able to react to a problem,
  Operators <u>need to be aware</u> of the problem**

- Old way operating "by alarm" (reactively)

- New approach: Present data to operators so they can proactively respond to problems as they develop

- Reserve alarms only for events that require immediate action

- High Performance HMIs (Human Machine Interfaces)

- Alarm Management (better designed alarm systems)
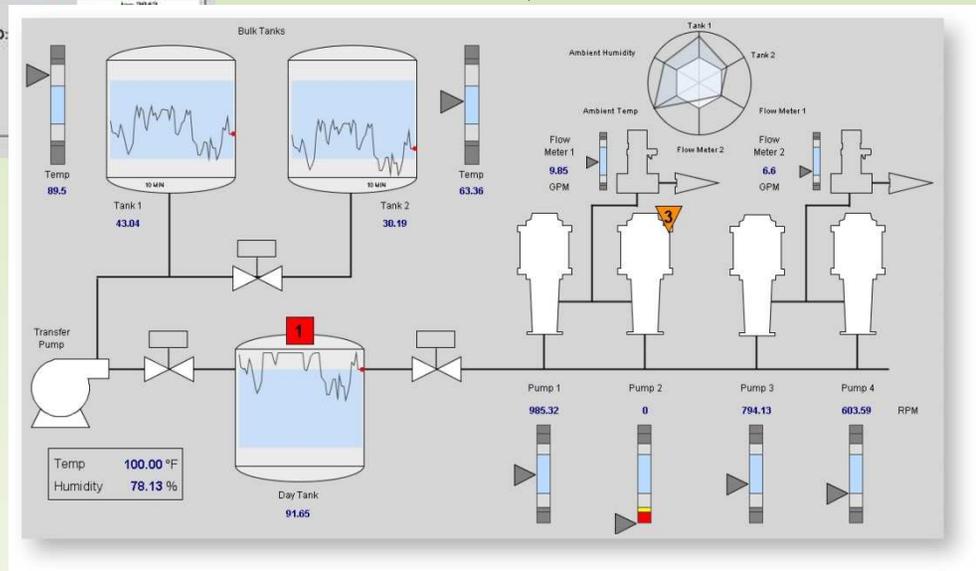
High Performance HMIs

High Performance HMIs
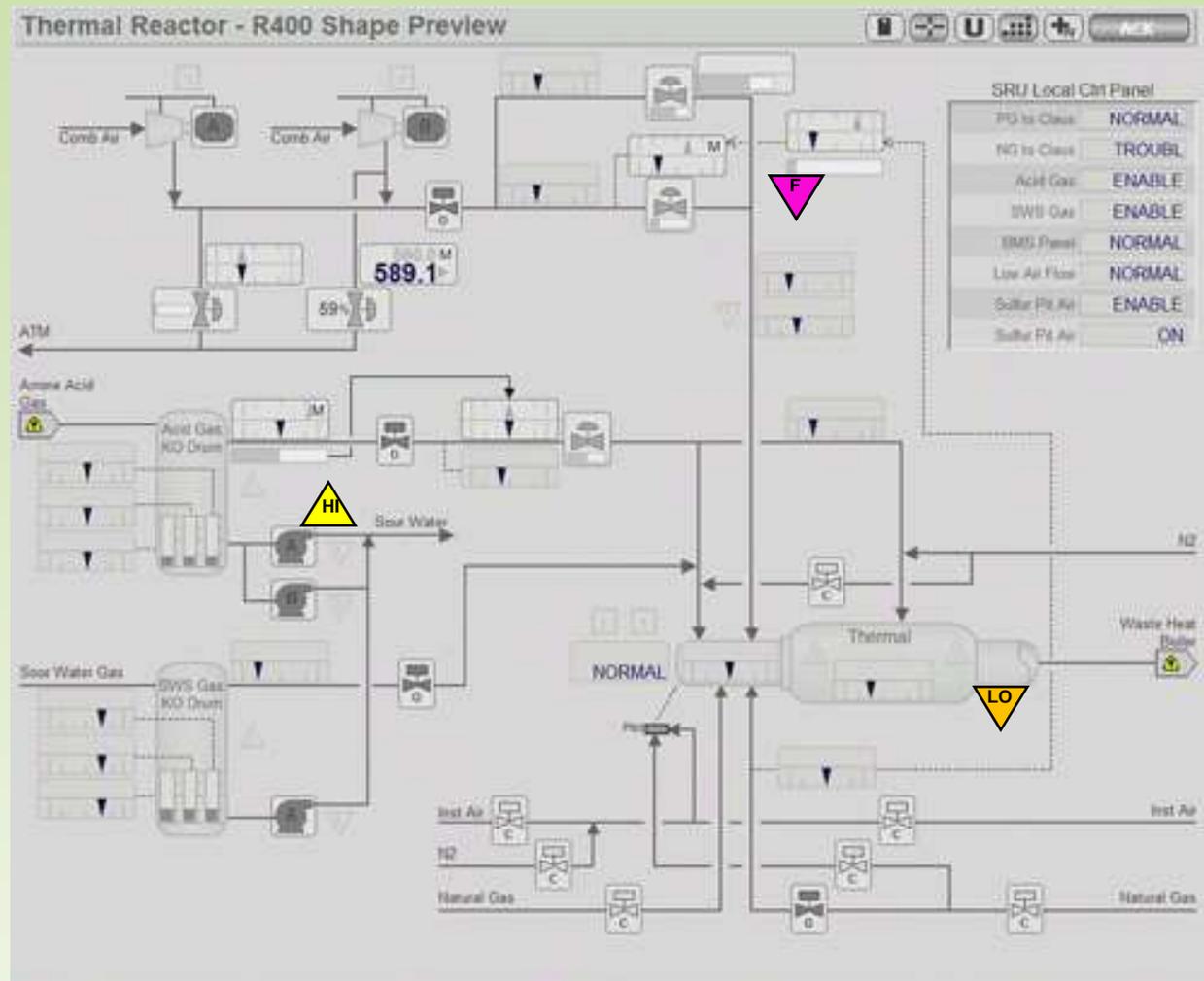
HMI = Human Machine Interface (computer screen)

High Performance HMI
Colour scheme
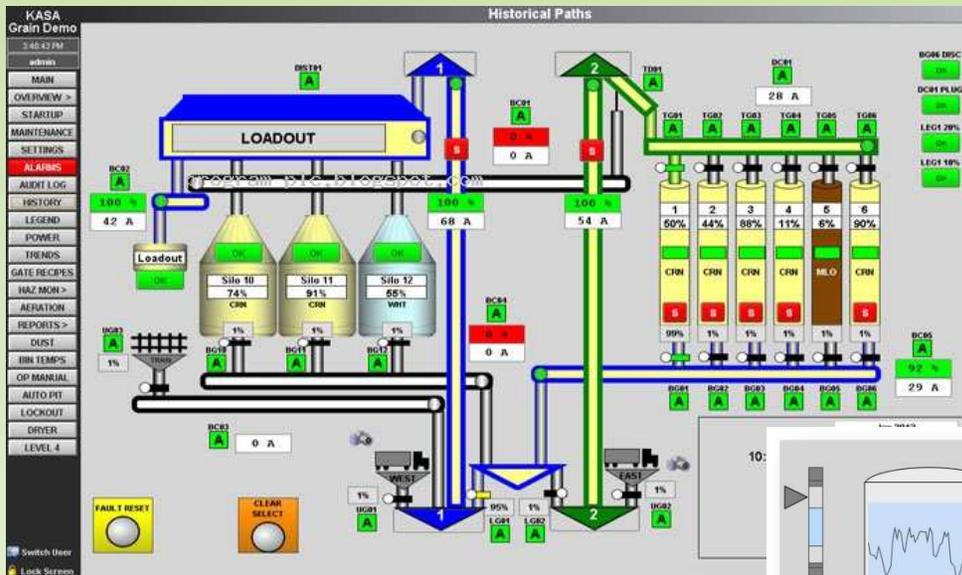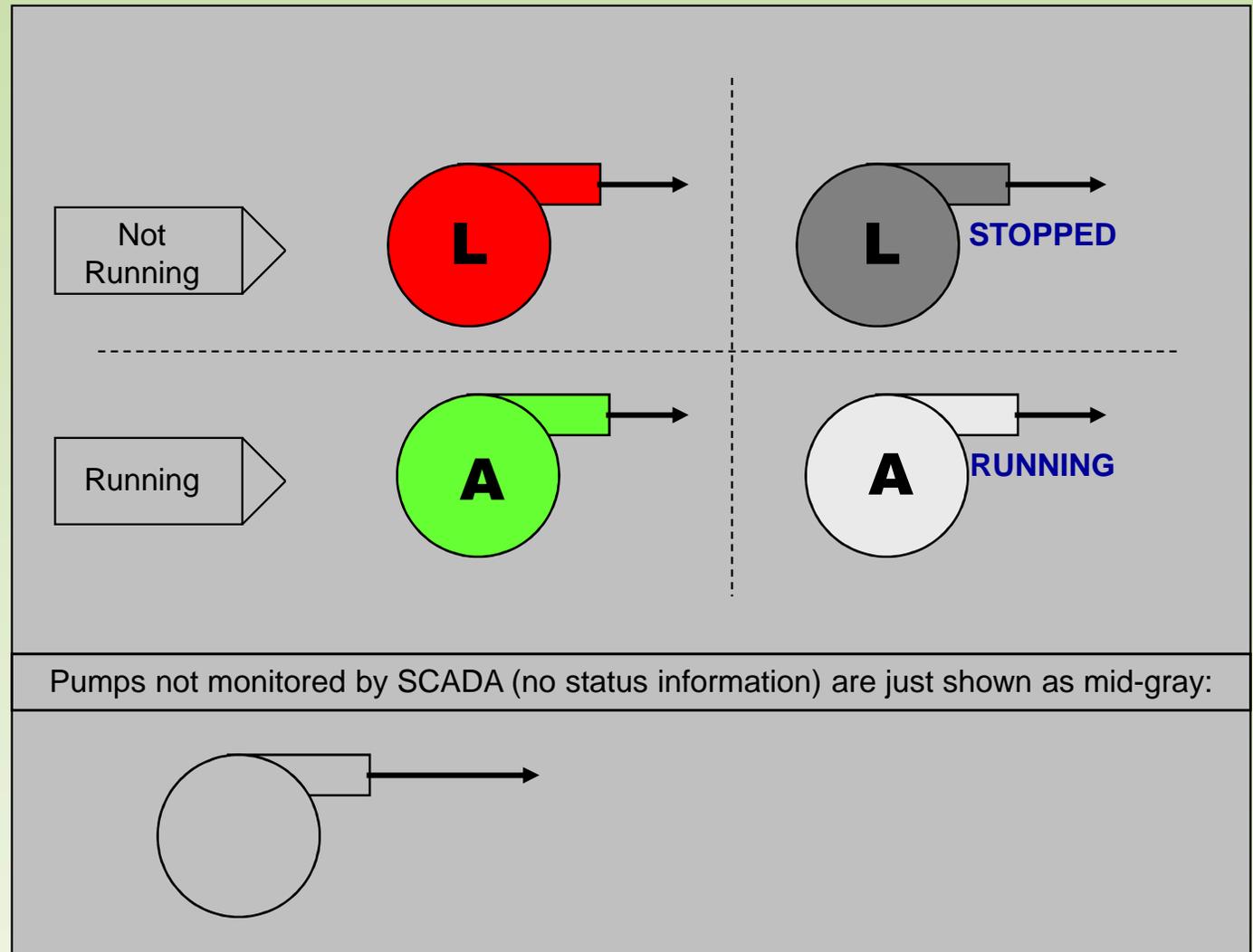
Poor Colour Scheme

High Performance HMI – Plant Running Normally

Notice the Lack of Colour

High Performance HMI – Showing Pump Statuses

Red/Green

for status

vs.

Greyscale & redundant coding

Not Running

Running

L

L **STOPPED**

A

A **RUNNING**

Pumps not monitored by SCADA (no status information) are just shown as mid-gray:

High Performance HMI – Analog Values

Often Seen	480.1 psi	No Alarm Indication	480.1 psi		Only a Colour Change!

Better

480.1 psi	480.1 psi	480.1 psi	480.1 psi
Diagnostic Priority	Priority 3	Priority 2	Priority 1

Betterer

480.1 psi	480.1 psi	480.1 psi	480.1 psi
Diagnostic Priority	Priority 3	Priority 2	Priority 1

Best!

4 480.1 psi	3 480.1 psi	2 480.1 psi	1 480.1 psi	S 480.1 psi
Diagnostic Priority	Priority 3	Priority 2	Priority 1	Suppressed Alarm

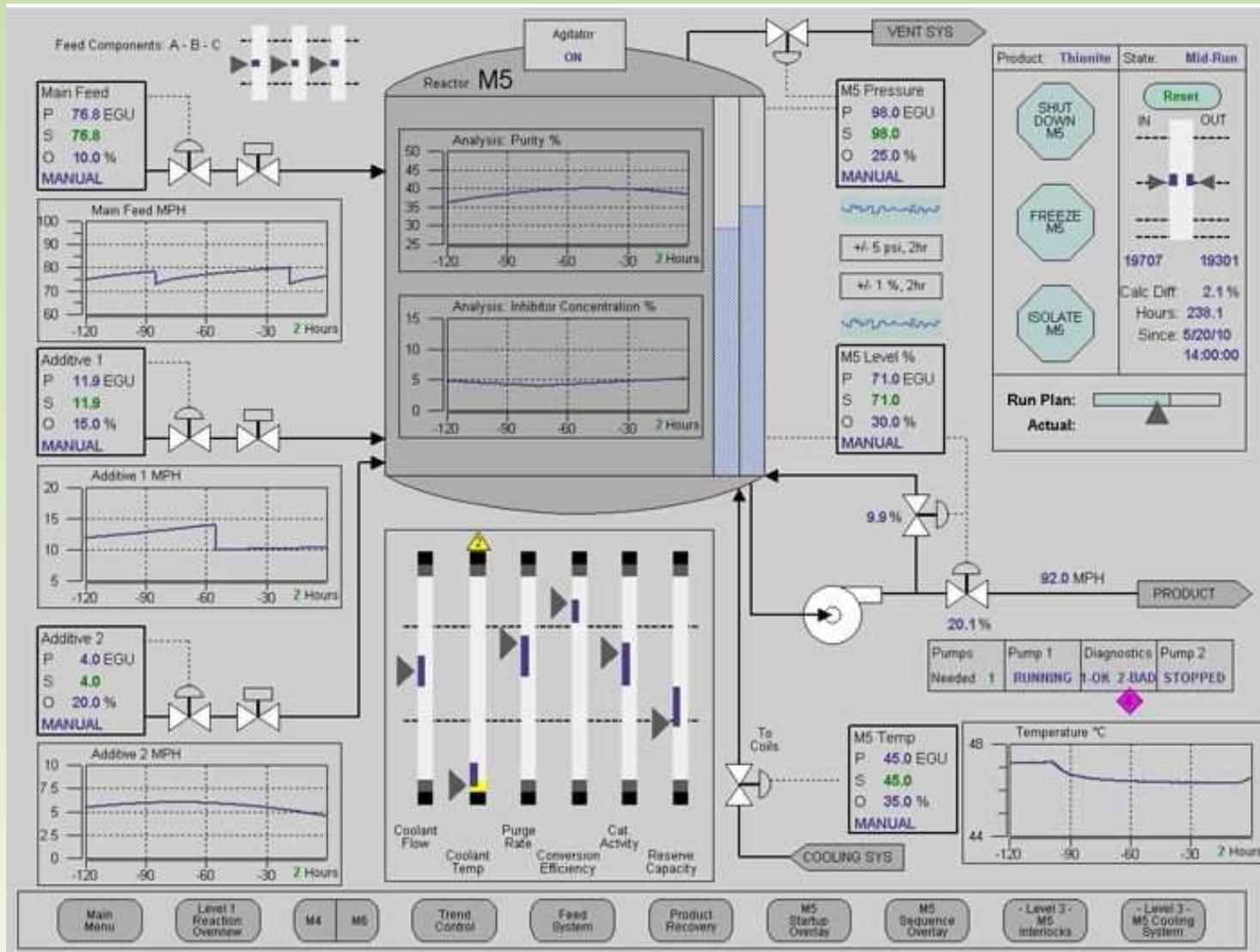Show alarms in multiple ways: Colour, Shape, Text ("redundant coding")

High Performance HMI – Analog Values Another Way

High Performance HMI – Tank Levels Depiction
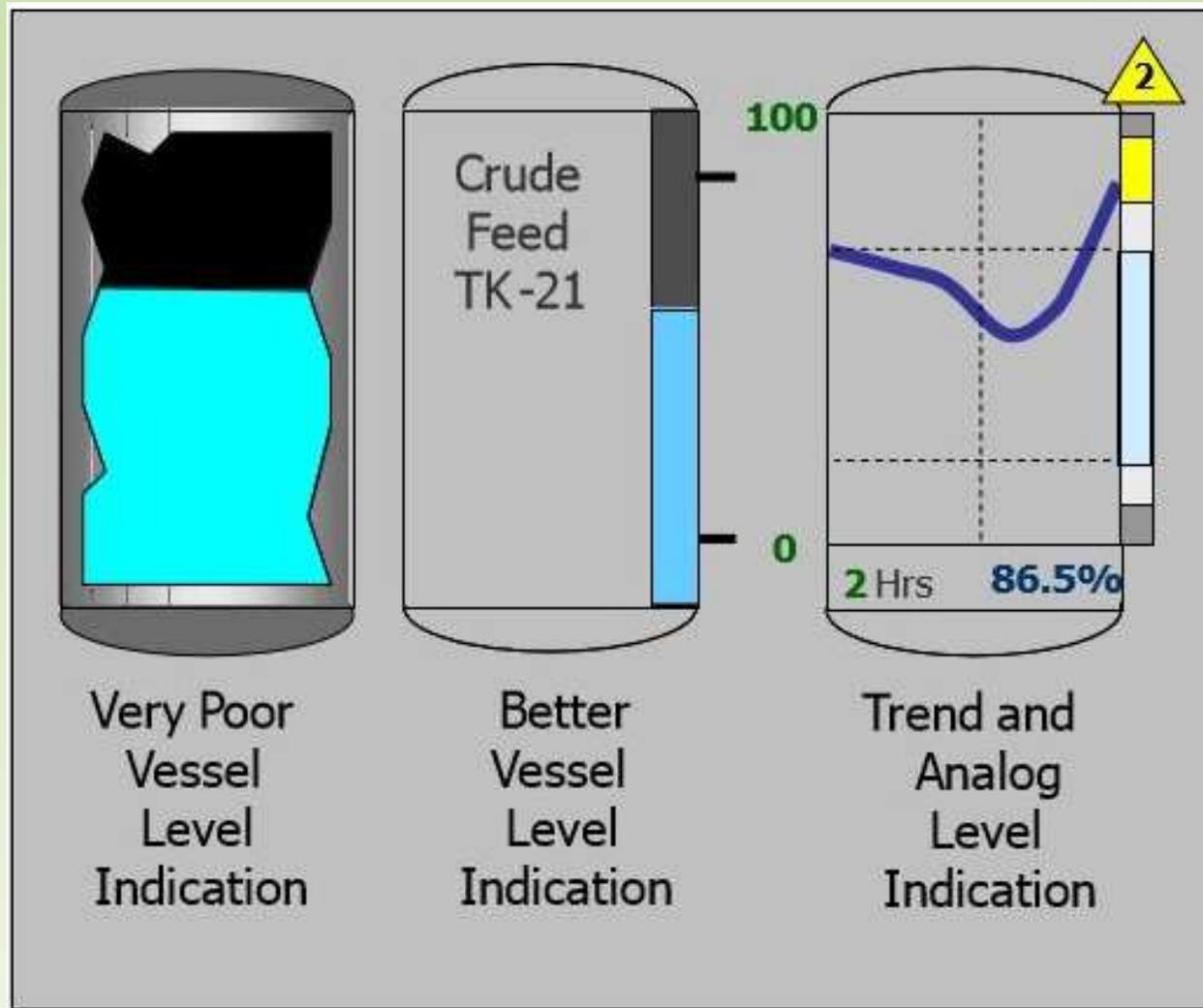
High Performance HMI – Embedding Trends
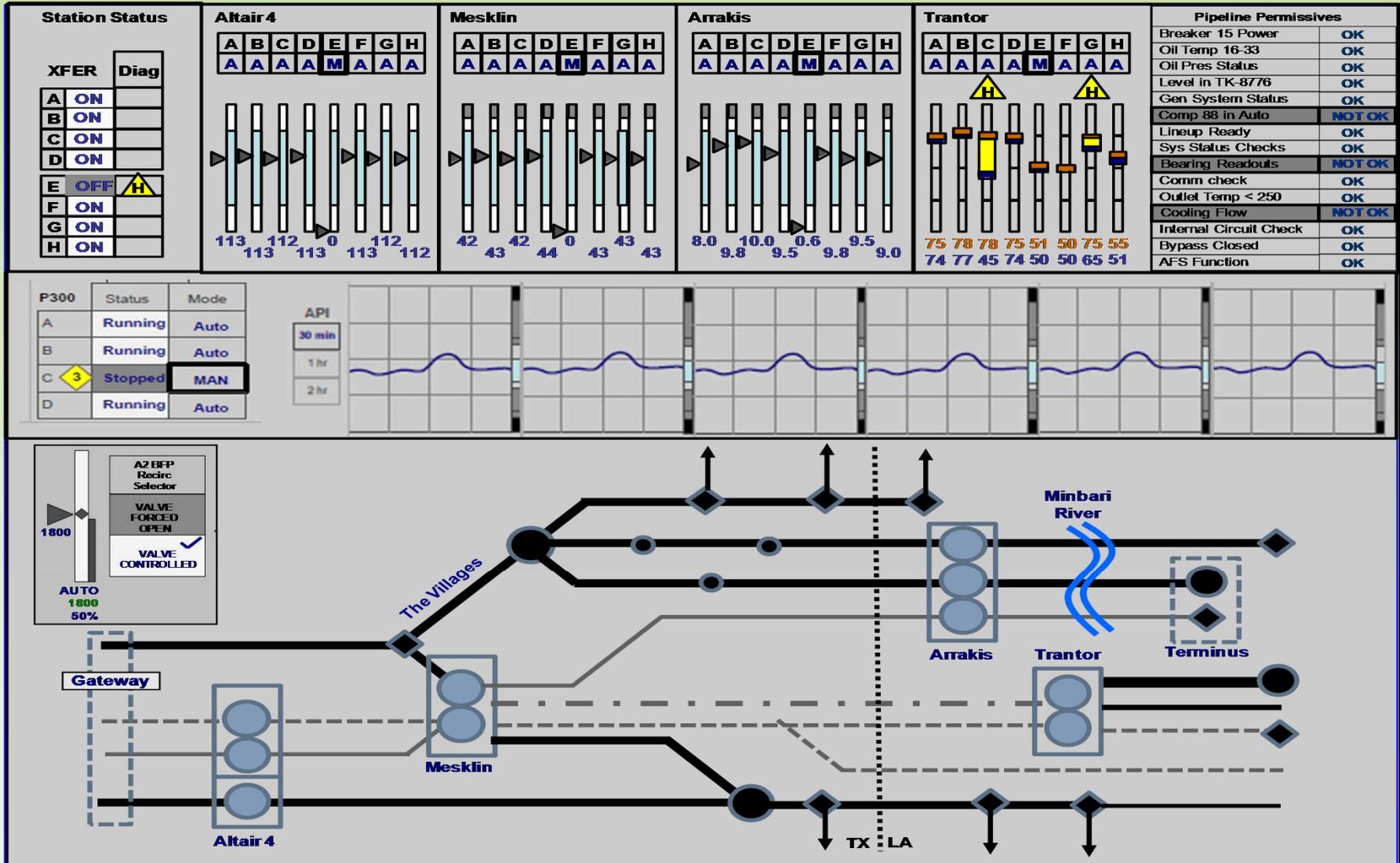

Source: High Performance HMI Handbook

High Performance HMI – Display Hierarchy

- HIERARCHY for Displays:
- Level 1 – Plant or Entire System Overview
  - Entire Operator Span of Control. "Single-Glance"
- Level 2 – Sub-Process Overview
  - More details than a Level 1 display, smaller area
- Level 3 – Equipment or Details Screen
  - Specific details about part of the process or control
- Level 4 – Specific Task or Diagnostic Screen
  - Very detailed screen, only used for diagnostics
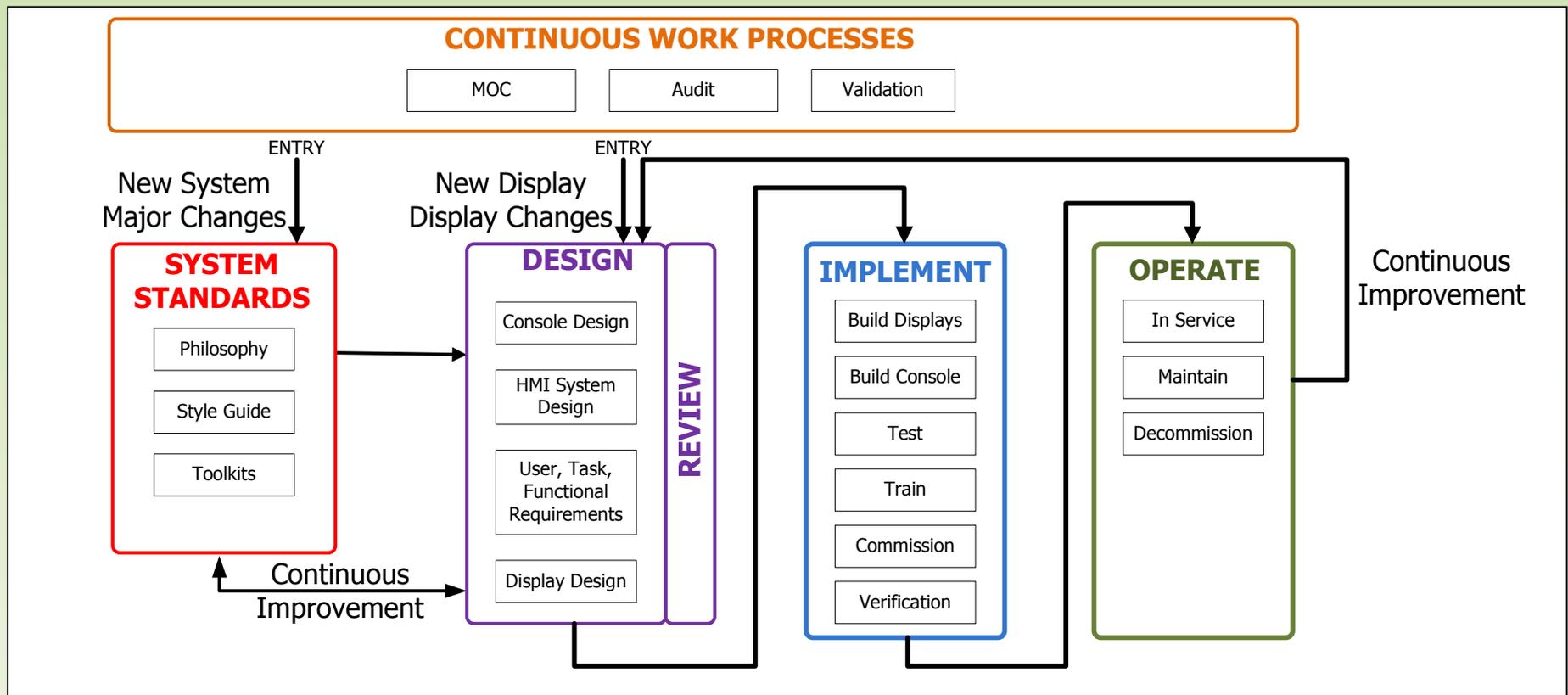
CITY OF
Guelph
Making a Difference

High Performance HMI – The old way
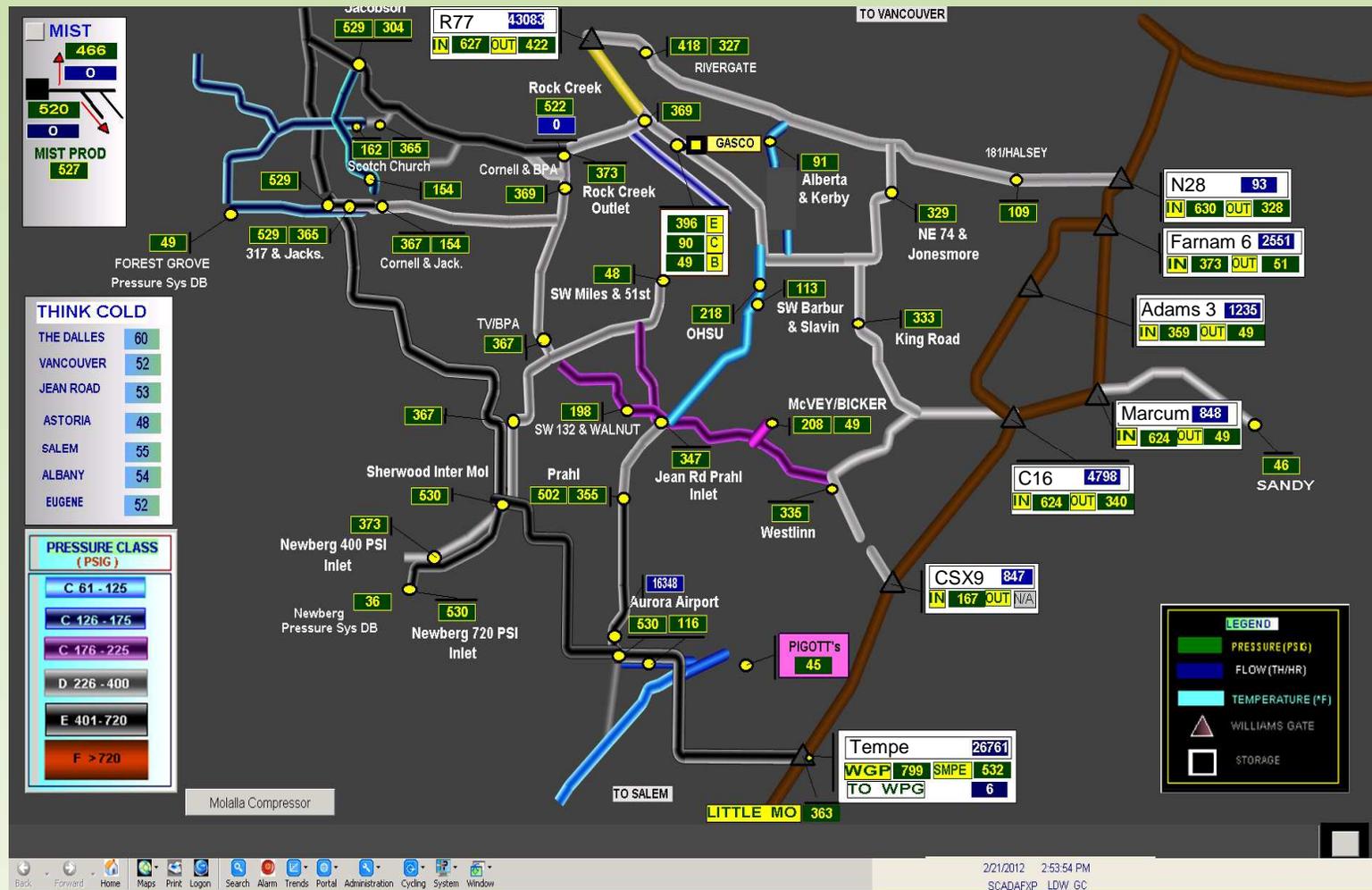
High Performance HMI – Proper Level 1 Display

Source: High Performance HMI Handbook

High Performance HMI – ISA101 Standard

CONTINUOUS WORK PROCESSES

| MOC | Audit | Validation |

ENTRY — New System Major Changes

ENTRY — New Display Display Changes

Continuous Improvement

SYSTEM STANDARDS
- Philosophy
- Style Guide
- Toolkits

Continuous Improvement

DESIGN
- Console Design
- HMI System Design
- User, Task, Functional Requirements
- Display Design

REVIEW

IMPLEMENT
- Build Displays
- Build Console
- Test
- Train
- Commission
- Verification

OPERATE
- In Service
- Maintain
- Decommission

Alarm Management

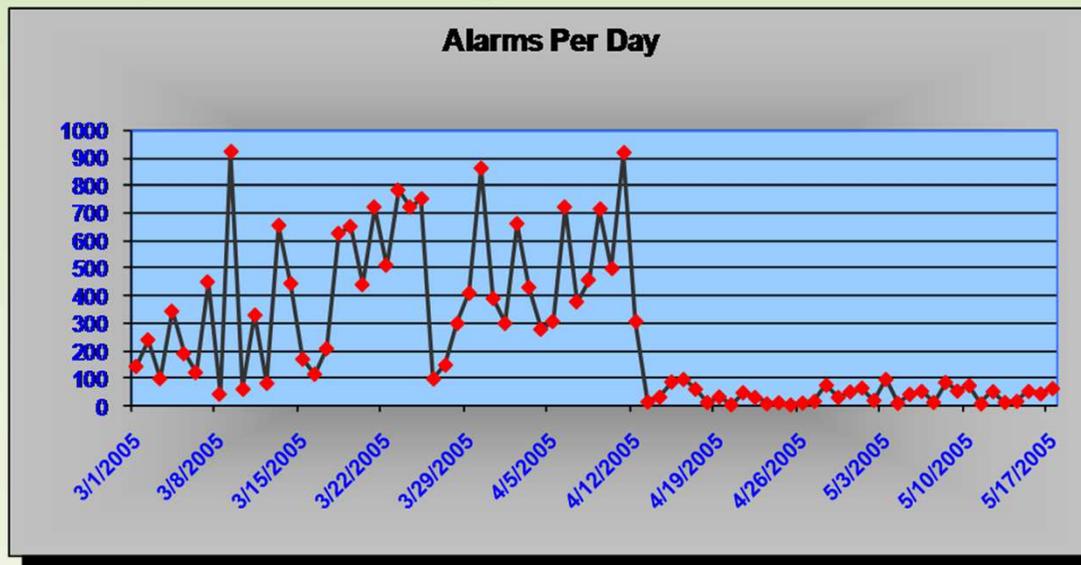# Alarm Management: ISA18.2

ANSI/ISA-18.2-2016 *

Management of Alarm Systems for the Process Industries

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

Methodology for identifying, rationalizing and designing alarms to be a powerful tool for operations, and eliminating non-useful alarms


Typical example of results of 18.2 being implemented (showing before/after)

*originally published as ISA-18.2-2009, now also IEC-62682

Alarm Management: ISA18.2

ANSI/ISA-18.2-2016,
Management of Alarm Systems for the Process Industries

-Addresses the development, design, installation, and management of alarm systems in the process industries

-Defines the terminology and models to develop an alarm system – and the work processes to effectively maintain it throughout its lifecycle

-Six technical reports available to explain specific applications in greater detail

-Based on work by the ISA18 committee, which has been active since 2003.

-First version of ISA18.2 standard published in 2009, became IEC-62682 in 2015, and updated version published in 2016.

Alarm Management: ISA18.2 Alarm Mgmt. Lifecycle
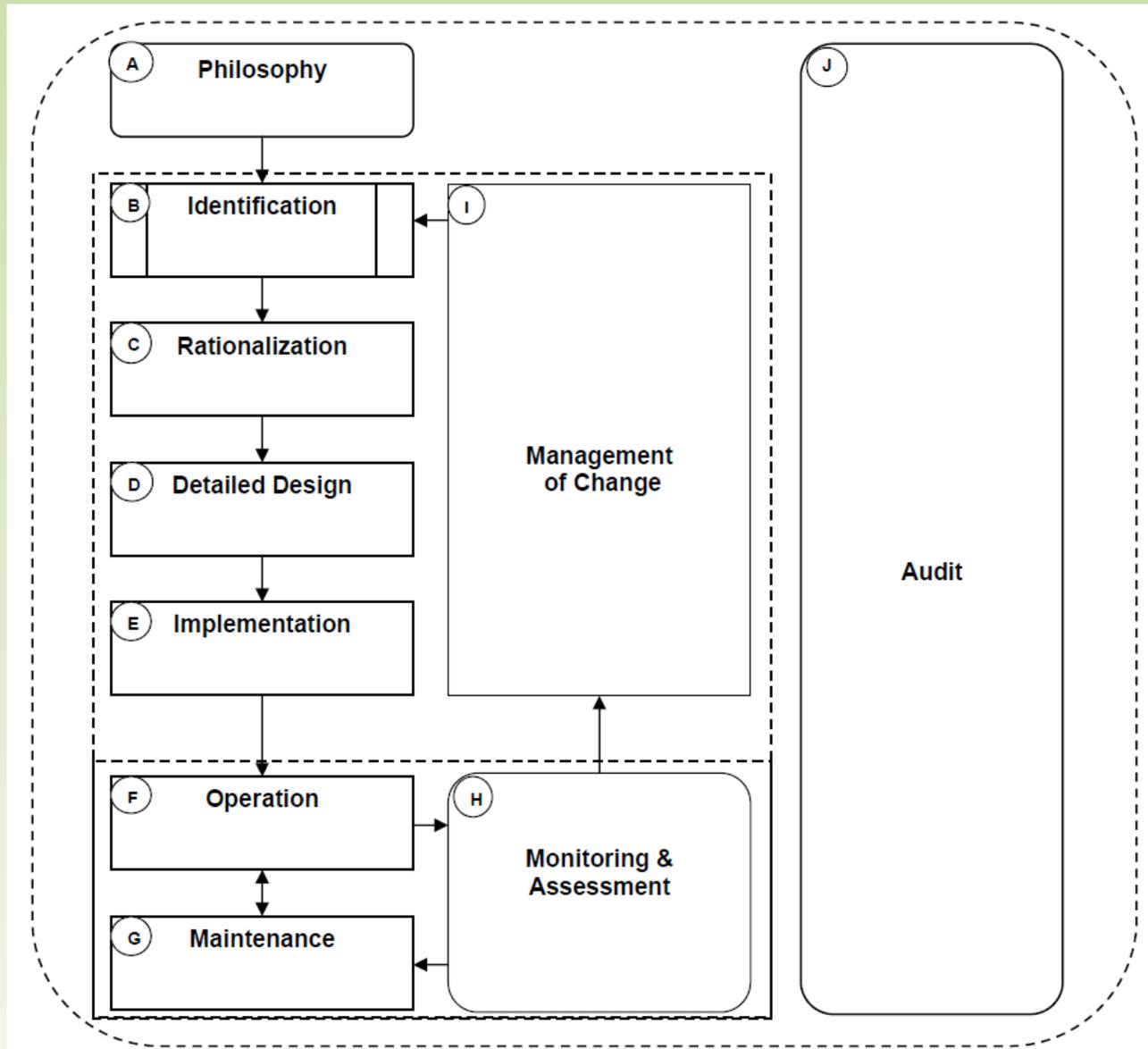
Alarm Management: Master Alarm Database

- ## MADB

  – ## Central repository of approved alarms and their configuration

Tag	Priority	Desc.	Condition	Consequence If Ignored	Consequence Severity	Expected Operator Response	Time to Respond
P1-380-LAH-201	LOW	Aeration 1 High Level	High Level Switch Activated for 10sec	Overflows in Secondary clarifiers.	MINOR	Check Level Controller	2 hours
P1-380-AAL-102	MED	Aeration 1 Low DO	DO below 3ppm for 30min	Loss of Biological Action, Risk of Damage to Biological Mass	MAJOR	Investigate and turn on additional blowers	1 hour
P1-380-PALL-456A	LOW	Aeration 1 Air Pres. Low Low	Less than 15psi for 5min	Loss of Energy if Air Leak, Poor Aeration (Note: there is a low DO alarm)	MINOR	Check pressures in air distribution system via HMI, check valves in field	4 hrs

Alarm Management: Master Alarm Database

- **Alarm Tag**

- **Alarm Description** (full description & what is shown on HMI)

- **Identification:** Trigger Condition, Purpose

- **Rationalization**:
  - Consequence & Severity if Ignored
  - Expected Operator Response, Time to Respond
  - Alarm Priority & Alarm Class
  - Justification for having this alarm configured!

- **Design:** Trigger Condition, On/Off Delays, Additional Filtering Logic, Setpoints, Routing/grouping information for the HMI

- **Operation:** When put into service, If Periodic Testing is required

Alarm Management: Key SCADA Features

- Master Alarm Database

- Ability to create non-alarm messages and logged events

- Support for Alerts, Prompts, and Maintenance Messages

- HMI Alarm Summary Display Screen

- Alarm Sorting, Filtering, Routing

- Alarm Areas/Grouping

- Alarm Priorities

- Alarm Classes

Alarm Management: Key SCADA Features cont'd

- Standardizing Alarm Features with Function Blocks

- On-Delay, Off-Delay, Deadband

- Conditional Alarming: base condition plus additional logic

- Alarm Shelving Method with Authorization / Logging

- Alarm Out of Service

- Change Control – Permissions, Setpoints, Configuration

- Configuration Change Logging

- Alarm Setpoint/Attribute verification & enforcement

Alarm Management: Non-Alarms

HMI: Alarms, Events and Notifications

- SCADA Systems can have multiple types of notifications

Operator notification types	Operator is expected to take an action	Operator might need to be aware but is not required to take action *(Action might be expected from someone other than the operator.)*
Arises from an abnormal process or equipment situation	Alarm	Alert
Arises from a normal situation	Prompt	Status

Figure 6 – Sample criteria for notification types from an alarm philosophy

- SCADA systems should have support for:
  - Alarms
  - Other notifications: alerts, prompts, maintenance messages
  - Event messages
  - Logged-only events

Guelph
CITY OF
Making a Difference

Alarm Management: Dedicated Alarm Display

- Dedicated screen for displays alarms – only alarms
- Ideally on its own dedicated monitor in multi-monitor setup

Alarm Management: Programming Best Practices

- Use a standardized function block in your PLC for all alarms
- Key Features:
  - Raw Status vs. Alarm Bit
  - Condition Inversion
  - Logic-Based Suppression
  - ON-Delay
  - OFF-Delay
  - Shelving / Out of Service support (if required at PLC-level)
- Additional Features for Analog/Value Alarms
  - Deadband
  - Alarm Masking if Signal is Bad
  - Masking of Lesser Alarms (L vs. LL)
  - Rate of Change

Data Redundancy

Data Redundancy: Logging Data

- O.Reg. 170 requires us to log chlorine residuals every 5 minutes

- SCADA Systems are not perfect: unit failures and network outages do happen
- Best Practice is to have redundant data logging
  - Main SCADA System logging data
  - Data loggers at sites

- Existing Practice
  - Redundant data loggers. Data must be gathered or imported manually into reporting system
  - Custom programming often needed to implement backup data logging in PLCs
- New Developments
  - New data loggers and operator terminals that do store/forward data logging
  - Reporting systems and historians that can accept data from multiple sources
  - Networking Protocols, e.g., DNP3, that have built-in time-stamping & store/forward logging

Data Redundancy: Logging Data
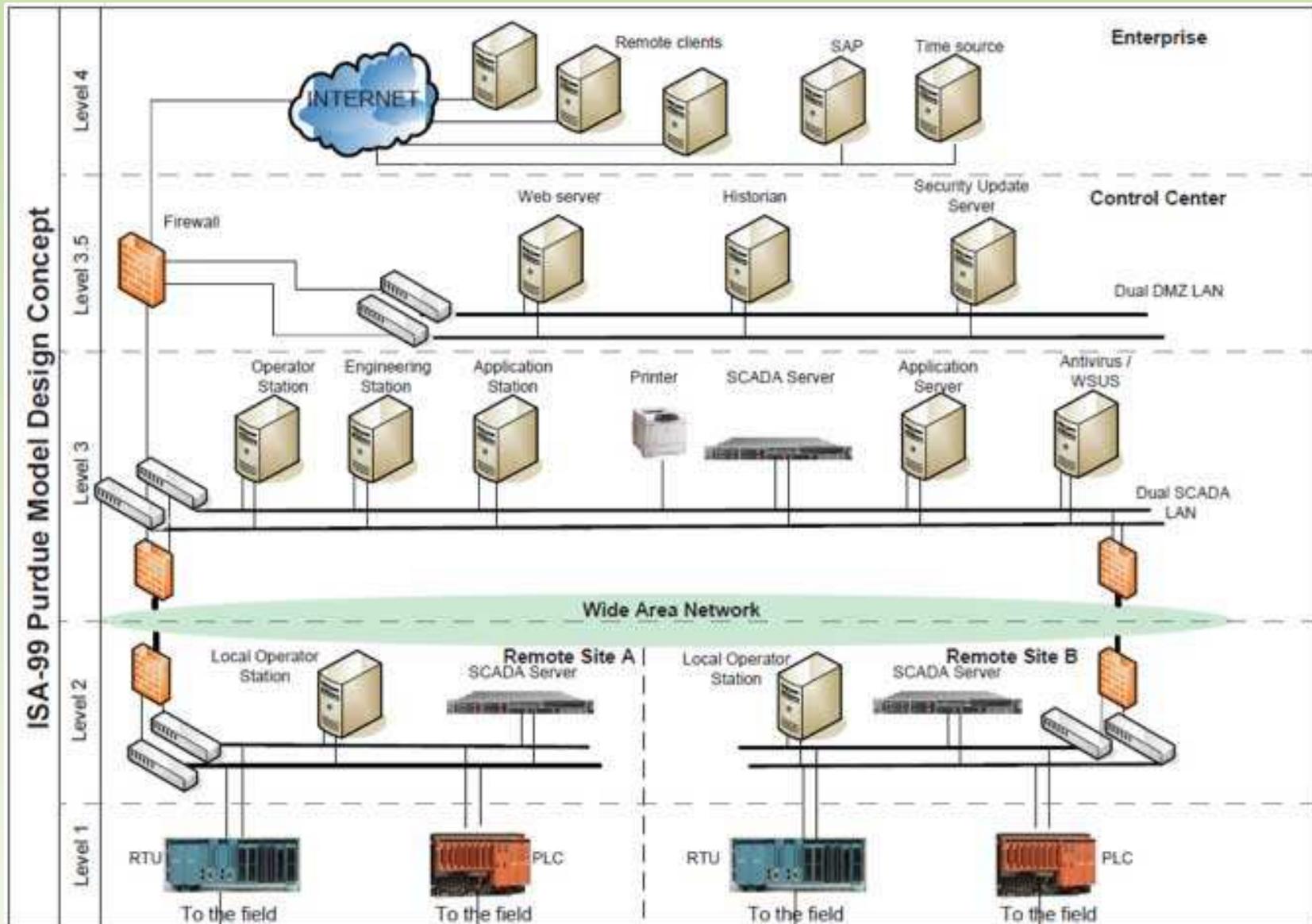
SCADA Network Redundancy

SCADA Network Redundancy

- SCADA is critical to operations
  - Data Logging,
  - Situational Awareness,
  - Remote Control by Operators,
  - Automatic Control,
  - Alarms,
  - Reporting

- SCADA relies on its process control network to stay online
  - In-plant Ethernet networks
  - Wide Area Networks (WAN) to remote sites

- Without the SCADA network, the SCADA system cannot operate
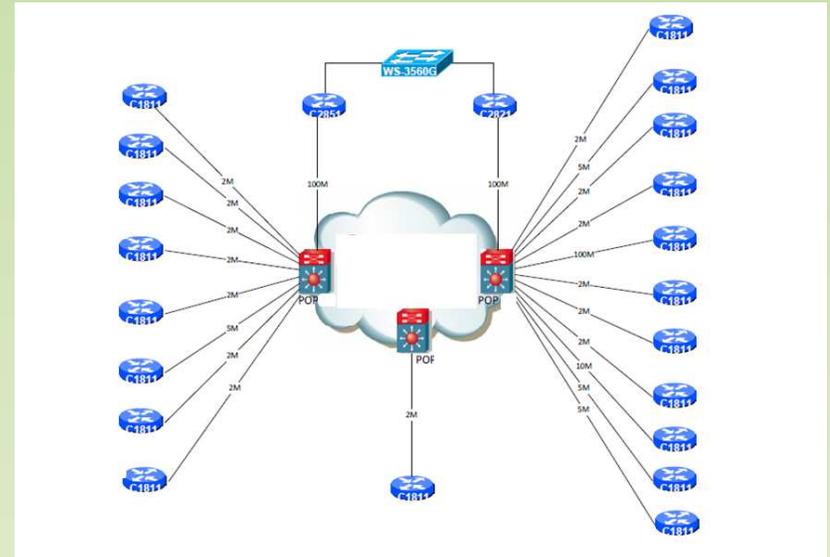
SCADA Network Redundancy

- **O.Reg. 170 – Drinking Water Systems**
- Free Chlorine Residuals Must be Logged Minimum Every 5 minutes
- Low chlorine alarms must be communicated promptly

- **Very challenging to meet this uptime for a SCADA network**
- SCADA system must be online 24/7, 365 days/year
- Less than 5 min downtime/year = 99.9995% uptime
- Most IT Systems only reach 95 to 99% uptime (outages at night ok)
- SCADA system has to be **10,000 X more reliable** than an IT system

SCADA Network Redundancy

- **SCADA Network Technologies**
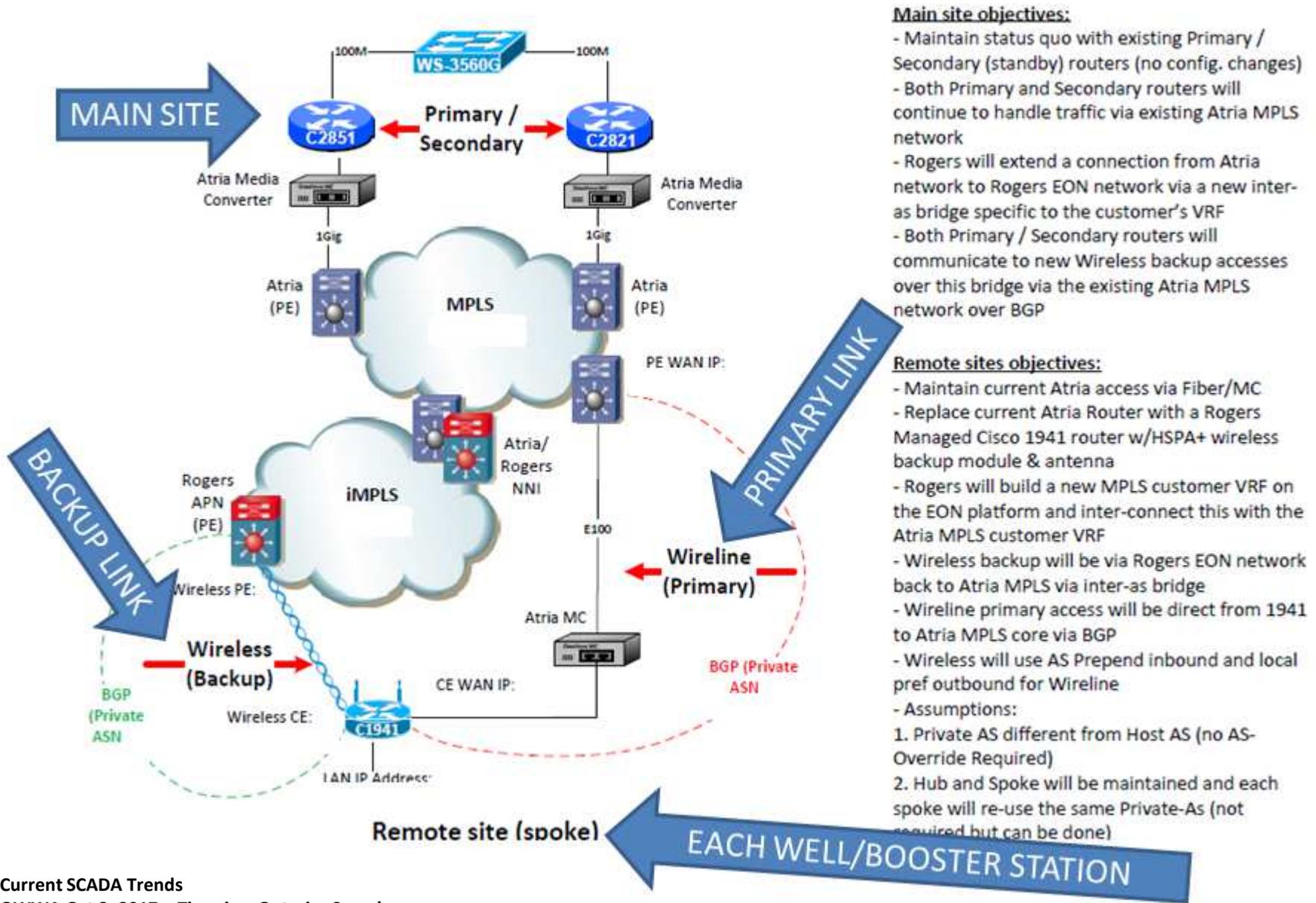 - **Fibre optic (public)***
  - **Fibre optic (MPLS)**
  - **Fibre optic (utility owned)**
  - **Cellular / Wireless***
  - **DSL (private or public)***
  - **Radios – licensed***
  - **Radios – unlicensed***
  - **Bell Lines**
  - **Private Cables**
  - **?**

*these approaches usually require extra VPN routers/firewalls be used

SCADA Network Redundancy: One Solution

Main site objectives:
- Maintain status quo with existing Primary / Secondary (standby) routers (no config. changes)
- Both Primary and Secondary routers will continue to handle traffic via existing Atria MPLS network
- Rogers will extend a connection from Atria network to Rogers EON network via a new inter-as bridge specific to the customer's VRF
- Both Primary / Secondary routers will communicate to new Wireless backup accesses over this bridge via the existing Atria MPLS network over BGP

Remote sites objectives:
- Maintain current Atria access via Fiber/MC
- Replace current Atria Router with a Rogers Managed Cisco 1941 router w/HSPA+ wireless backup module & antenna
- Rogers will build a new MPLS customer VRF on the EON platform and inter-connect this with the Atria MPLS customer VRF
- Wireless backup will be via Rogers EON network back to Atria MPLS via inter-as bridge
- Wireline primary access will be direct from 1941 to Atria MPLS core via BGP
- Wireless will use AS Prepend inbound and local pref outbound for Wireline
- Assumptions:
1. Private AS different from Host AS (no AS-Override Required)
2. Hub and Spoke will be maintained and each spoke will re-use the same Private-As (not required but can be done)

Last of all: Cyber Security

SCADA Cyber Security

- **You need to protect your SCADA system for unauthorized access**
- **In the past this was difficult to do**
- **Requires multipronged approach**
  - **People**
  - **Process**
  - **Technology**

- **There is guidance now available on how to do this**
  - **ISA/IEC-62443 (formerly known as ISA-99)**
  - **AWWA GW430**
  - **NIST Cyber Security Framework**

SCADA Cyber Security: ISA/IEC-62443

General

ISA-62443-1-1	ISA-TR62443-1-2	ISA-62443-1-3	ISA-TR62443-1-4
Terminology, concepts and models	Master glossary of terms and abbreviations	System security compliance metrics	IACS security lifecycle and use-case

Policies & procedures

ISA-62443-2-1	ISA-TR62443-2-2	ISA-TR62443-2-3	ISA-62443-2-4
Requirements for an IACS security management system	Implementation guidance for an IACS security management system	Patch management in the IACS environment	Installation and maintenance requirements for IACS suppliers

System

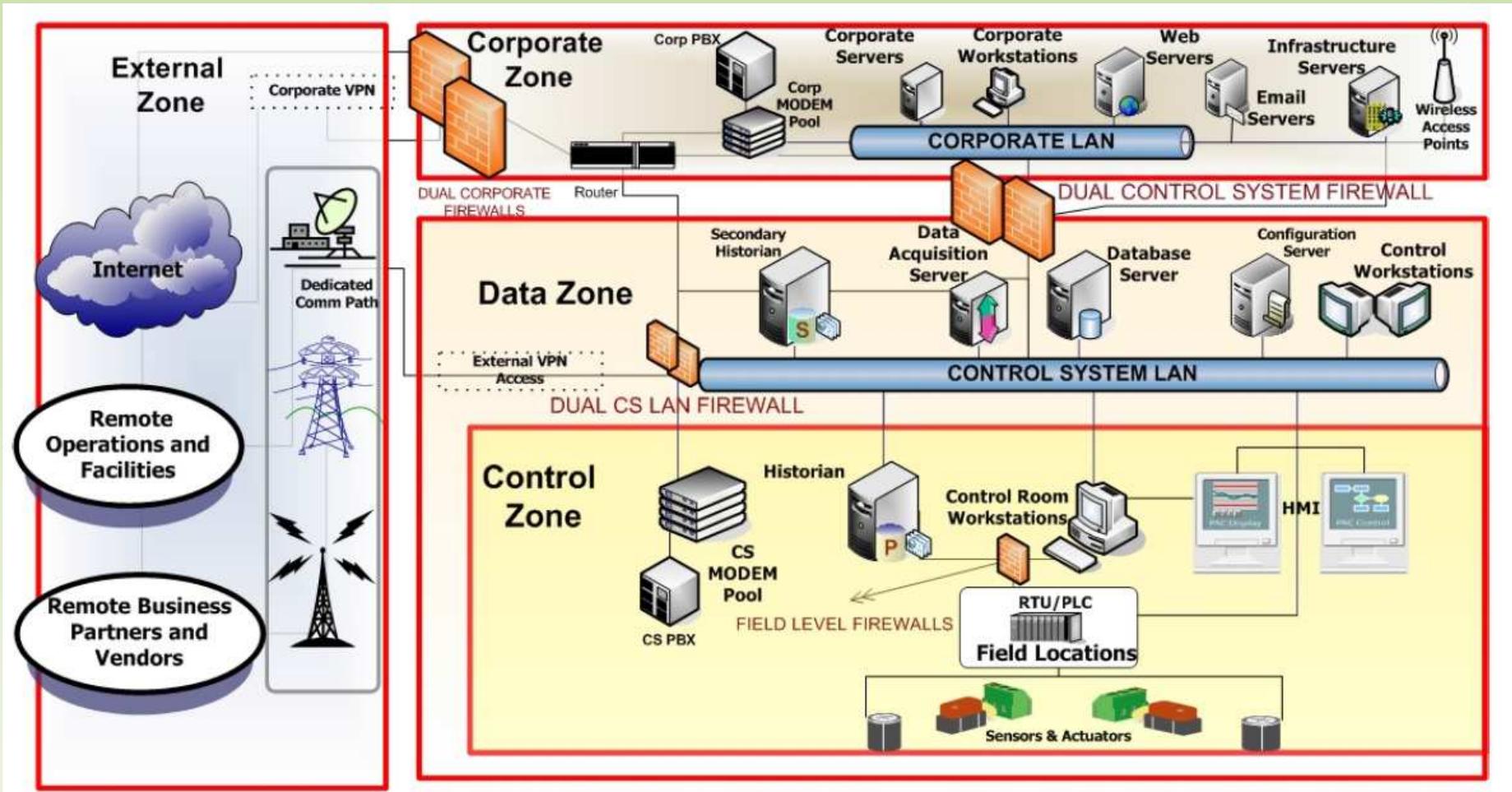| ISA-TR62443-3-1	ISA-62443-3-2	ISA-62443-3-3
Security technologies for IACS	Security levels for zones and conduits	System security requirements and security levels

Component

ISA-62443-4-1	ISA-62443-4-2
Product development requirements	Technical security requirements for IACS components

Making a Difference

SCADA Cyber Security: ISA/IEC-62443

Wrapping Up

- **SCADA is essential for both Operations and Compliance**

- **Operators Need Situational Awareness to Operate Effectively**
- **Use the SCADA HMI to show the whole picture to operators**
- **SCADA Alarms systems must be rationalized/documented**

- **Pay attention to data integrity by investing in data redundancy**
- **SCADA networks are key to robust SCADA systems**
- **Cyber Security is requires a multi-pronged approach**

- **When upgrading SCADA systems, leverage what you have.**
- **Take advantage of new technology and ideas.**