OAK RIDGE National Laboratory

Alarm System Guidelines

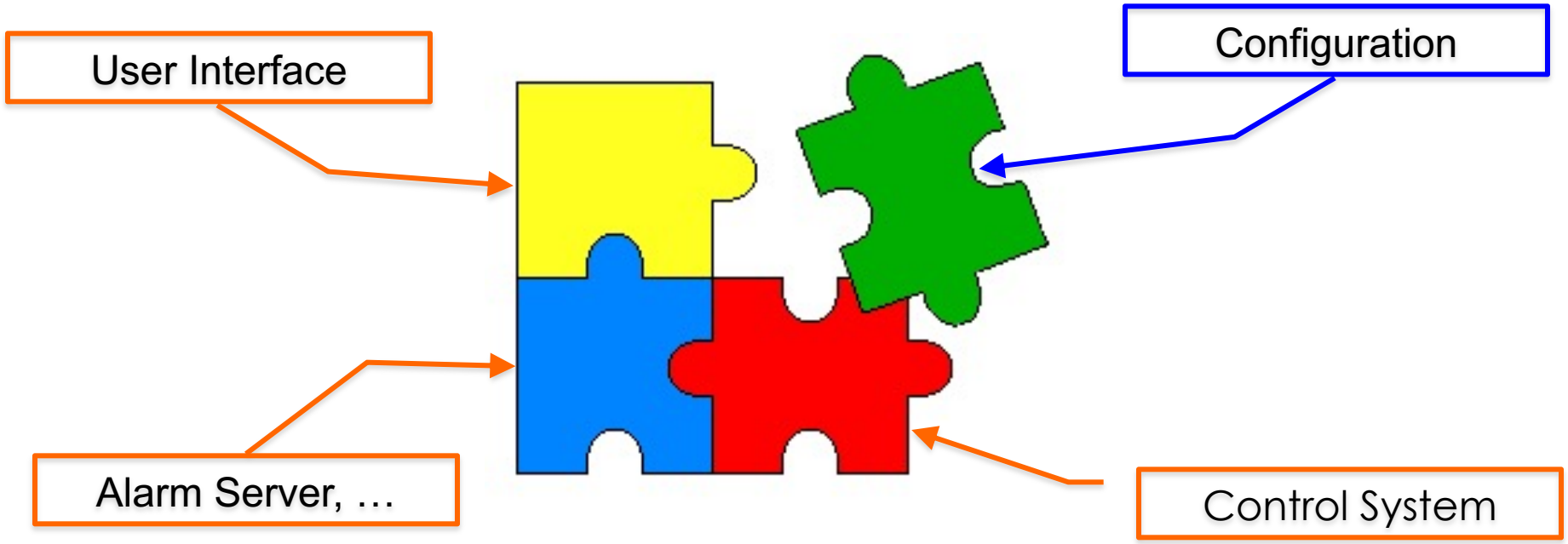
Kay Kasemir

Feb. 2022

ORNL is managed by UT-Battelle, LLC for the US Department of Energy

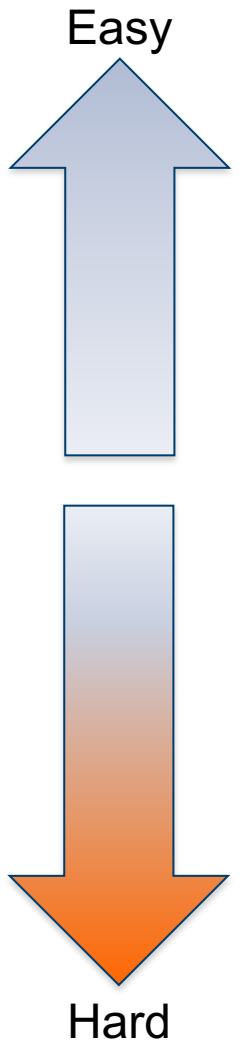
U.S. DEPARTMENT OF ENERGY

Alarm System Components

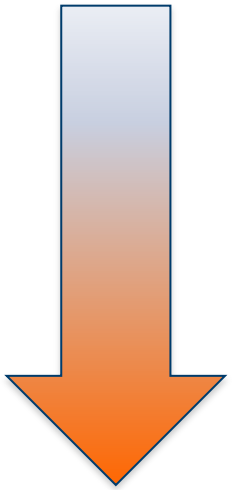


Levels Of Complexity

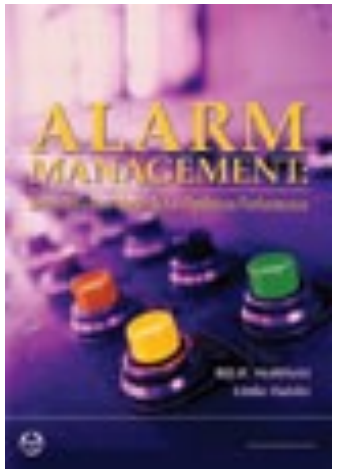
- Use the Alarm System
  - Control Room operator
- Configure the Alarm System
  - Certain operators, IOC engineers
- Alarm System Setup
  - CS-Studio maintainer for site
- Coming up with a good configuration
  - Everybody



Creating a good Alarm Configuration



Hard



B. Hollifield, E. Habibi,
"Alarm Management:
Seven Effective Methods
for Optimum Performance", ISA, 2007

Alarm Philosophy

Goal:

Help operators take correct actions

- Alarms with guidance, related displays
- Manageable alarm rate (<150/day)
- Operators will respond to every alarm
  (corollary to manageable rate)

What's a valid alarm?

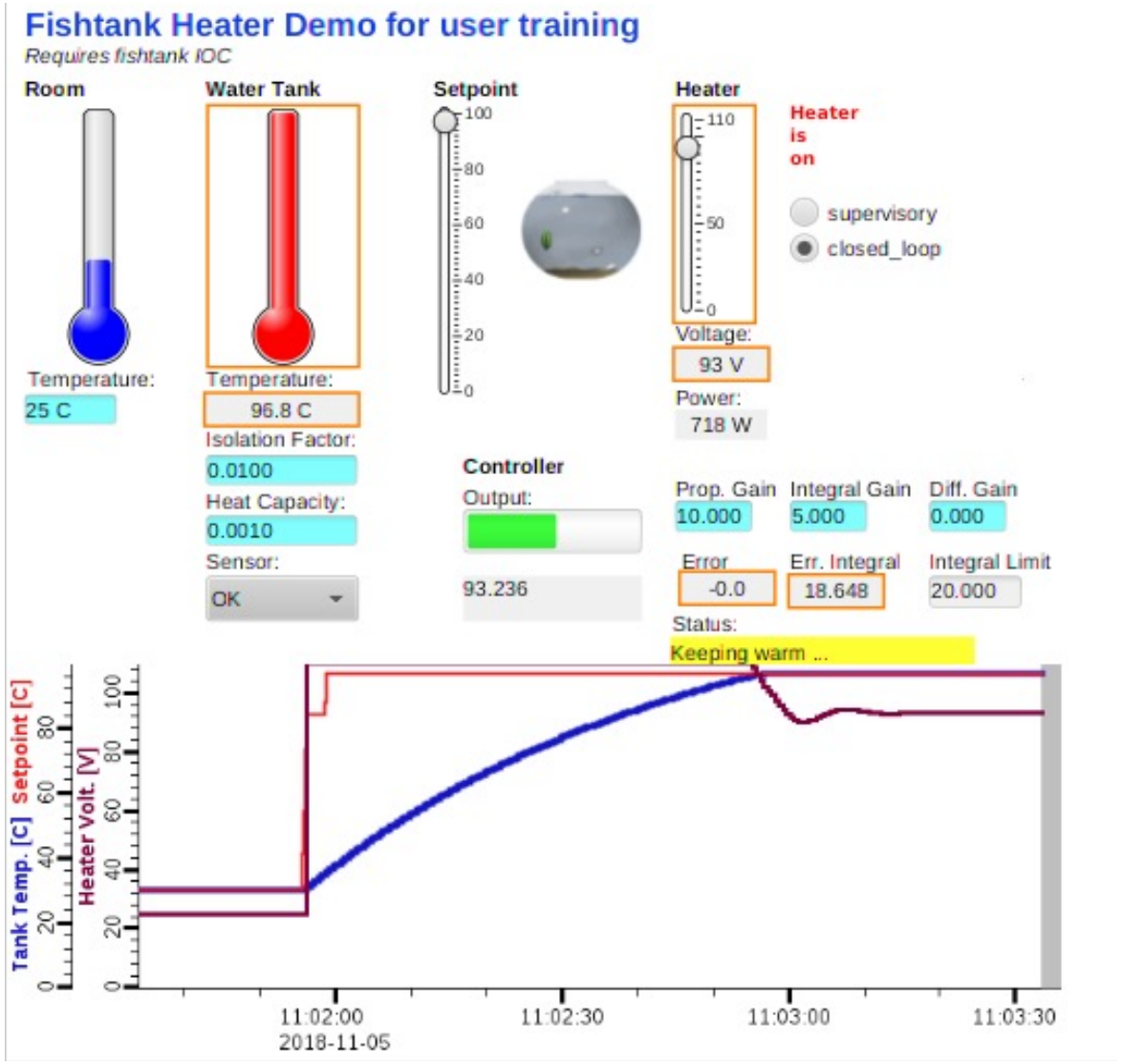
DOES IT REQUIRE
IMMEDIATE OPERATOR ACTION?

- What action? Alarm guidance!
  - Not "make elog entry", "tell next shift", …
- Consequence of not reacting?
- How much time to react?

Fishtank Example

- Heater Voltage alarms at high PID drive
- Tank Temperature alarms at
  70 (MINOR) and
  100 (MAJOR)

Which one is a good alarm trigger PV?



How are alarms added?

- Alarm triggers: PVs on IOCs
  - But more than just setting HIGH, HIHI, HSV, HHSV
  - HYST is good idea
  - Dynamic limits, enable based on machine state,...

    Requires thought, communication, documentation
- Added to alarm server with
  - Guidance: How to respond
  - Related screen: Reason for alarm (limits, …), link to screens mentioned in guidance
  - Link to rationalization info (wiki)

Example: Elevated Temp/Press/Res.Err./…

- Immediate action required?
  - Do something to prevent interlock trip
- Impact, Consequence?
  - Beam off: Reset & OK, 5 minutes?
  - Cryo cold box trip: Off for a day?
- Time to respond?
  - 10 minutes to prevent interlock?

- MINOR? MAJOR?
- Guidance: “Open Valve 47 a bit, …”
- Related Displays: Screen that shows Temp, Valve, …

Avoid Multiple Alarm Levels

- Analog PVs for Temp/Press/Res.Err./…:
  - Easy to set LOLO, LOW, HIGH, HIHI
- Consider:
  - Do they require *significantly different* operator actions?
  - Will there be a lot of time after the HIGH to react before a follow-up HIHI alarm?
- In most cases, HIGH & HIHI only double the alarm traffic
  - Set only HSV to generate single, early alarm
  - Adding HHSV alarm assuming that the first one is ignored only worsens the problem

Water Tower, Bad Example

- Level < 30%: Minor/Low Alarm
  "Try to raise water level"

- Level <25%: Major/LoLo Alarm
  "Really, try to raise the water level NOW"

➔ Nearly same reason and guidance, should be one alarm

Water Tower, Better Example

- Level < 50%: Minor/Low Alarm
  "Check if auto-topup pumps which should keep water level above 50% are running. If they are, try to reduce water consumption by disabling unnecessary users like lawn sprinkler and guest house water feature. If they aren't, call Fred @ 567-987"

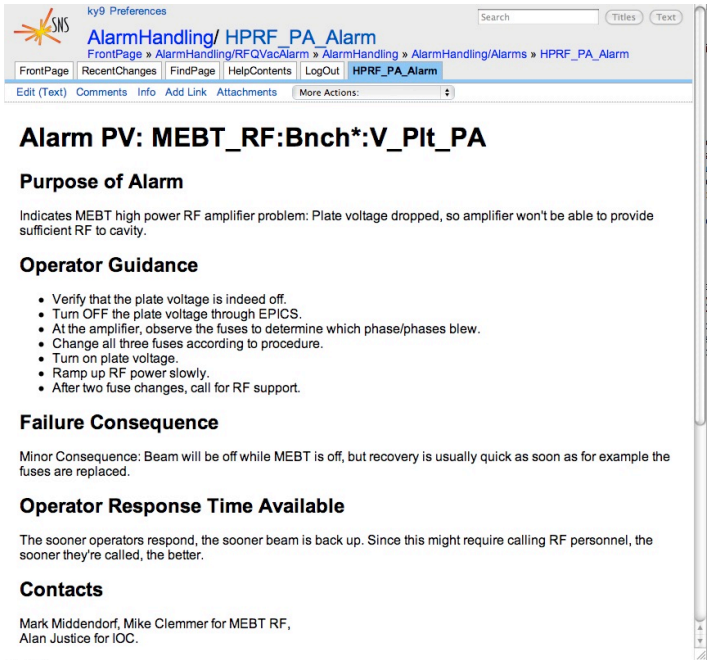
- Level <25%: Major/LoLo Alarm
  "Water level is approaching minimum required for fire suppression systems. Perform fast machine shutdown, procedure 4812, and inform operations leader."

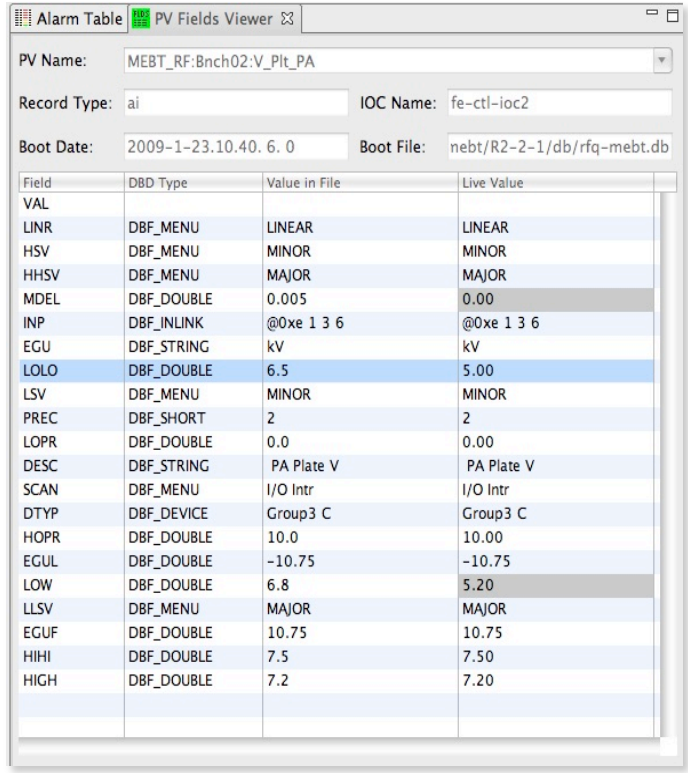
Bad Example: Old SNS 'MEBT' Alarms

- Each amplifier trip:
  3 quasi identical alarms,
  no guidance
- Rethought w/ subsystem engineer, IOC programmer and operators: 1 better alarm

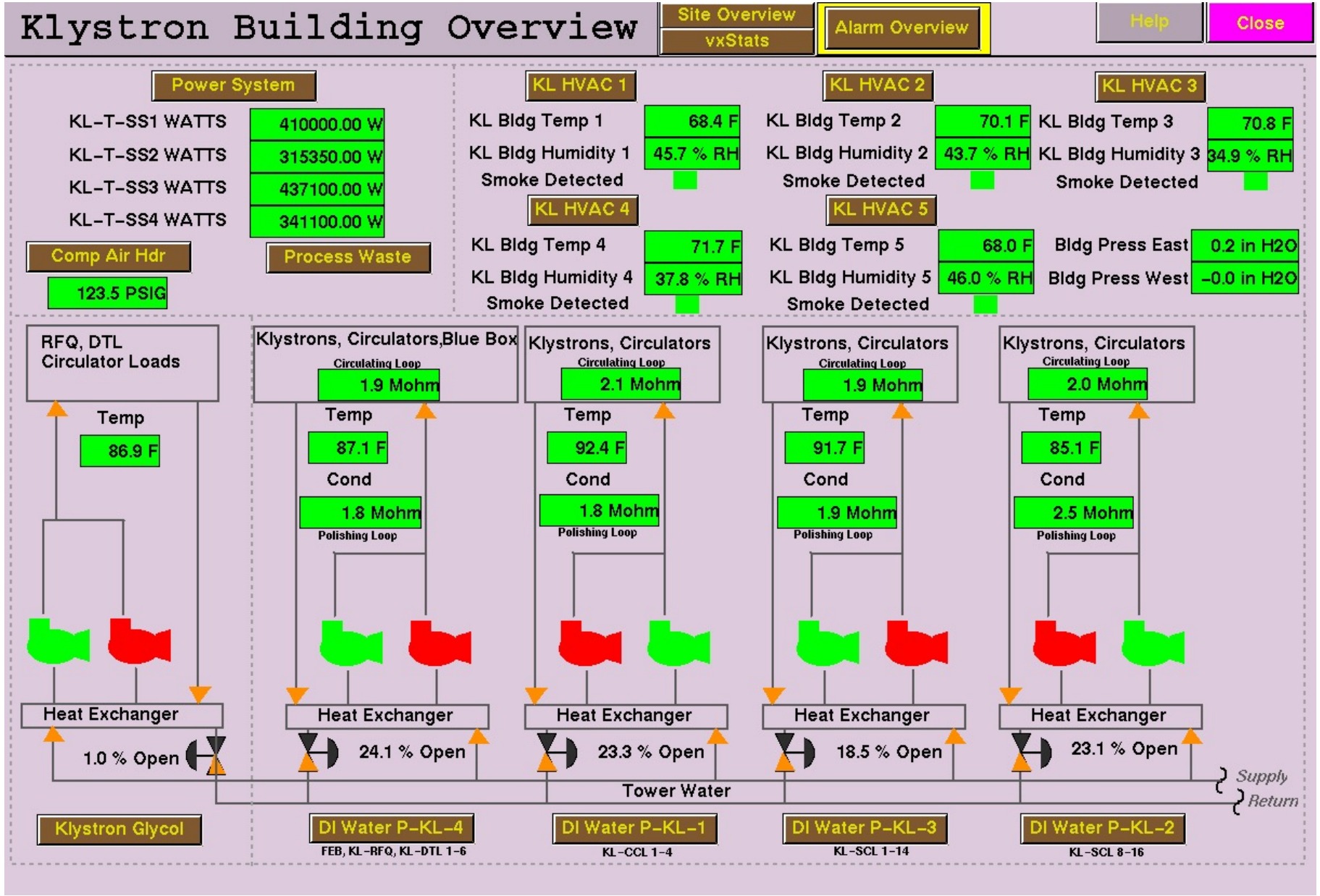
#	Date	Type	Name	Severity	TEXT
1	2009-03-16 13:46:20.255	talk		MAJOR	MAJOR alarm: MEBBIT two power amplifier trip
2	2009-03-16 13:46:19.962	talk		MINOR	MINOR alarm: MEBBIT two power amplifier trip
3	2009-03-16 13:45:56.241	talk		MAJOR	MAJOR alarm: S C L 18 modulator in standby
4	2009-03-16 13:45:25.963	talk		MAJOR	MAJOR alarm: MEBBIT two power amplifier trip
5	2009-03-16 13:45:25.891	talk		MINOR	MINOR alarm: MEBBIT two power amplifier trip
6	2009-03-16 13:45:25.884	talk		MAJOR	MAJOR alarm: MEBBIT two power amplifier trip
7	2009-03-16 13:23:09.202	talk		MINOR	MINOR alarm: DTL 3 RCCS CV one valve open limit is exceeded

MEBT_RF:Bnch02:V_Plt_PA	MEBBIT two power amplifier trip
MEBT_RF:Bnch02:V_Fil_PA	MEBBIT two power amplifier trip
MEBT_RF:Bnch02:I_Plt_PA	MEBBIT two power amplifier trip

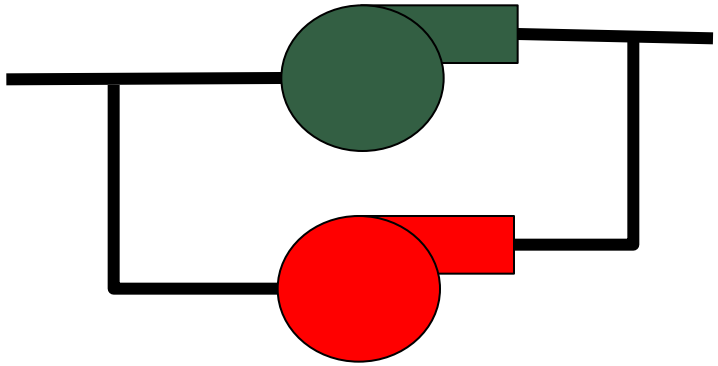




Alarms for Redundant Pumps



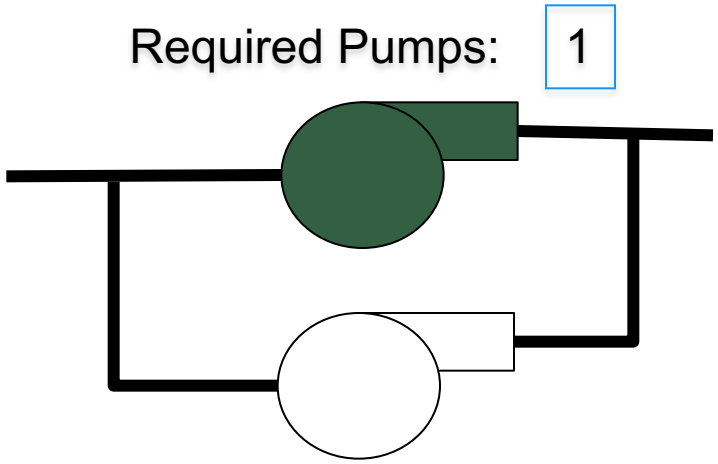
Alarm Generation: Redundant Pumps the wrong way



- Control System
  - Pump1 on/off status
  - Pump2 on/off status

- Simple Config setting: Pump Off => Alarm:
  - It's normal for the 'backup' to be off
  - Both running is usually bad as well
    - Except during tests or switchover
  - During maintenance, both can be off

Redundant Pumps



- Control System
  - Pump1 on/off status
  - Pump2 on/off status
  - Number of running pumps
  - Configurable number of desired pumps

- Alarm System: Running == Desired?
  - … with delay to handle tests, switchover
- Same applies to devices that are only needed on-demand

Create Alarms in PLC or in IOC?

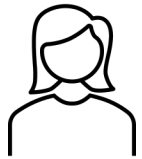
```
# Read just the value
record(ai, “plc_value”)
{
    field(DTYP, “EtherIP”)
    field(INP, “@plc tags[42]”)
}

# Get alarm indicator from PLC
# and turn into MINOR alarm
record(bi, “plc_alarm”)
{
    field(DTYP, “EtherIP”)
    field(INP, “@plc alarms[42]”)
    field(OSV,  “MINOR”)
}

# Optionally, expose the alarm threshold
# Omit this to hide that in the PLC
record(ai, “plc_threshold”)
{
    field(DTYP, “EtherIP”)
    field(INP, “@plc limits[42]”)
}
```

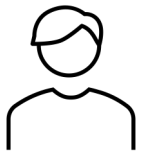
```
# All in one record
record(ai, “plc_value”)
{
    field(DTYP, “EtherIP”)
    field(INP, “@plc tags[42]”)
    field(HIGH, “95”)
    field(HSV,  “MINOR”)
    field(HYST, “5”)
}
```

Create Alarms in PLC or in IOC?



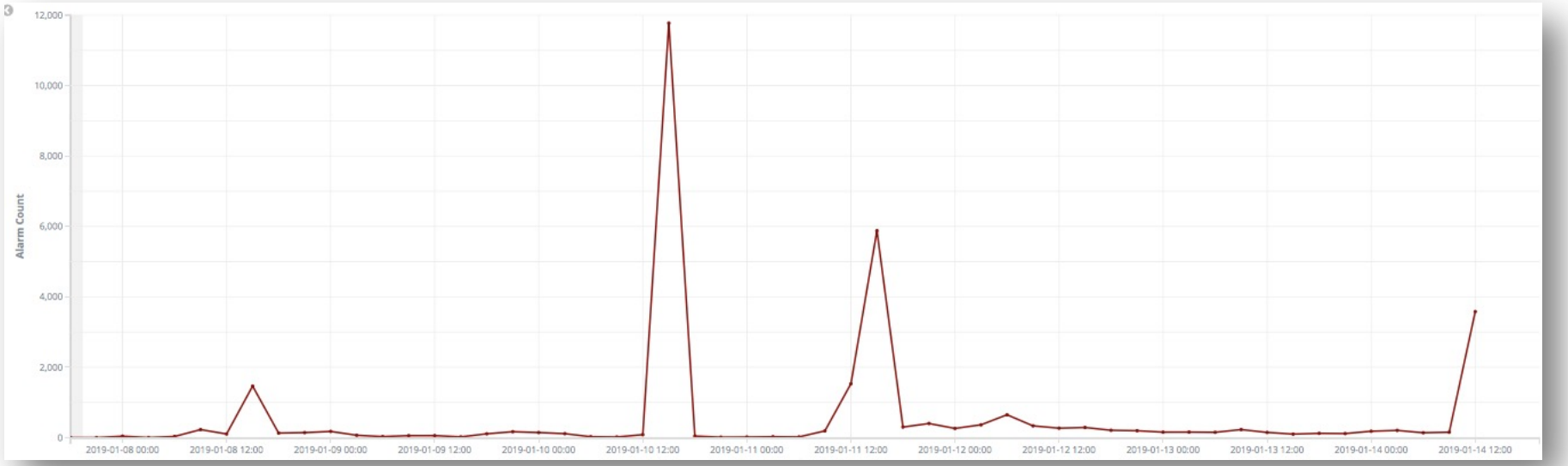
"In IOC is simpler, plus allows knowledgeable users to see configuration (HIGH, HYST, ..) and even change it"

"You're right, but interlocks are not alarms. Keep your interlocks in the PLC and show the status via records. Use the IOC for alarms that are meant to help operators, which operators might have to adjust"

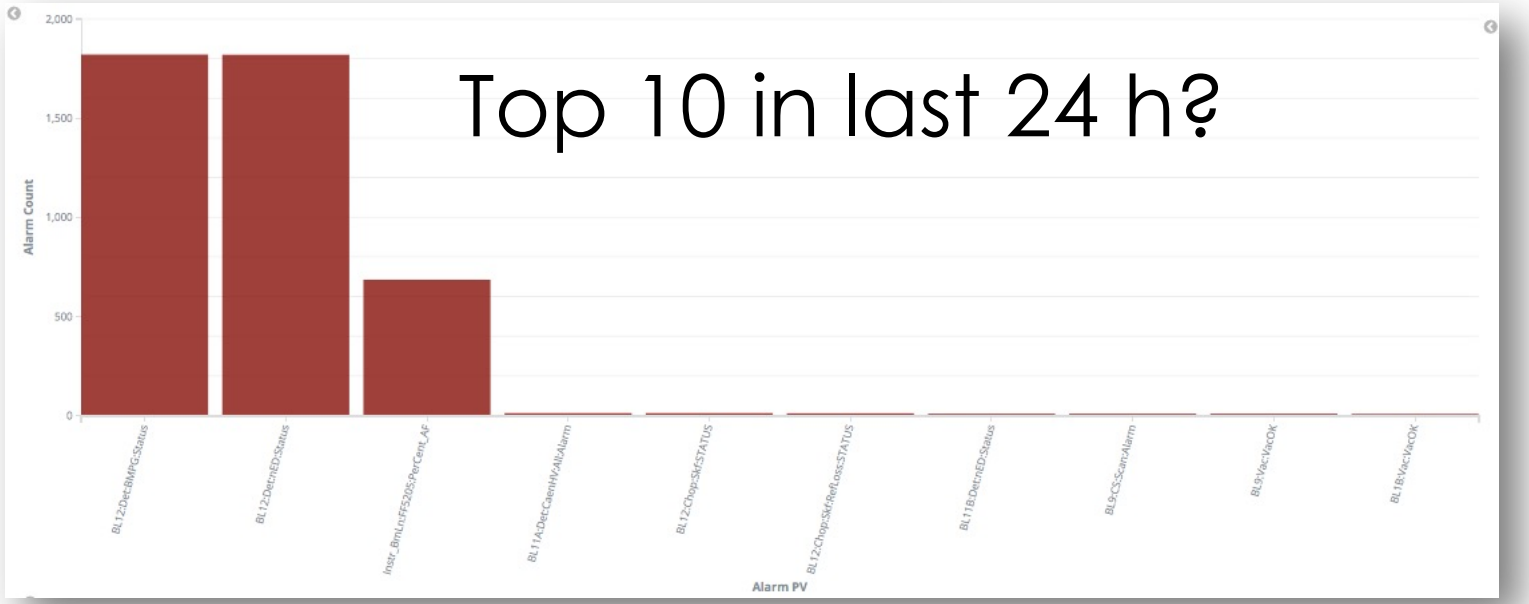


"But this is an important interlock, it's handled by the PLC, and nobody should be able to change it from the outside"

Review: How Many alarms in last week?



Top 10 in last 24 h?



Suggested Roles

- Alarms should help operators take correct actions
  - ➔ Operators can disable alarms, update guidance
  - ➔ Operations leader adds trigger PVs to alarm system, with guidance and display links
- Subsystem expert can suggest alarms, describe their purpose and guidance for handling them
- Control system engineer creates/configures PVs and displays

Summary

- Easy to use
  - Check alarms in Table, Tree, Panel
  - Fix it: Read Guidance, use Display Links
  - ✔Acknowledge
- Configuration
  - Can be changed online
  - Operators can update guidance, add better display links
- Alarm System Setup
  - Somewhat Involved, but only once
- Producing a good configuration
  - Hard, never ending