ERAMOSA

excellence. period.

Introduction to the ISA 18.2 Alarm Management Standard

York Region

Alarm Management Program

Training Outline

- Review of Alarm System
- What is ISA-18.2
- Overview of 18.2
- Alarm Life Cycle

- Review of 18.2 Features
- Master Alarm Database
- Alarm Identification, Rationalization, Design & Implementation

- Alarm Philosophy Document

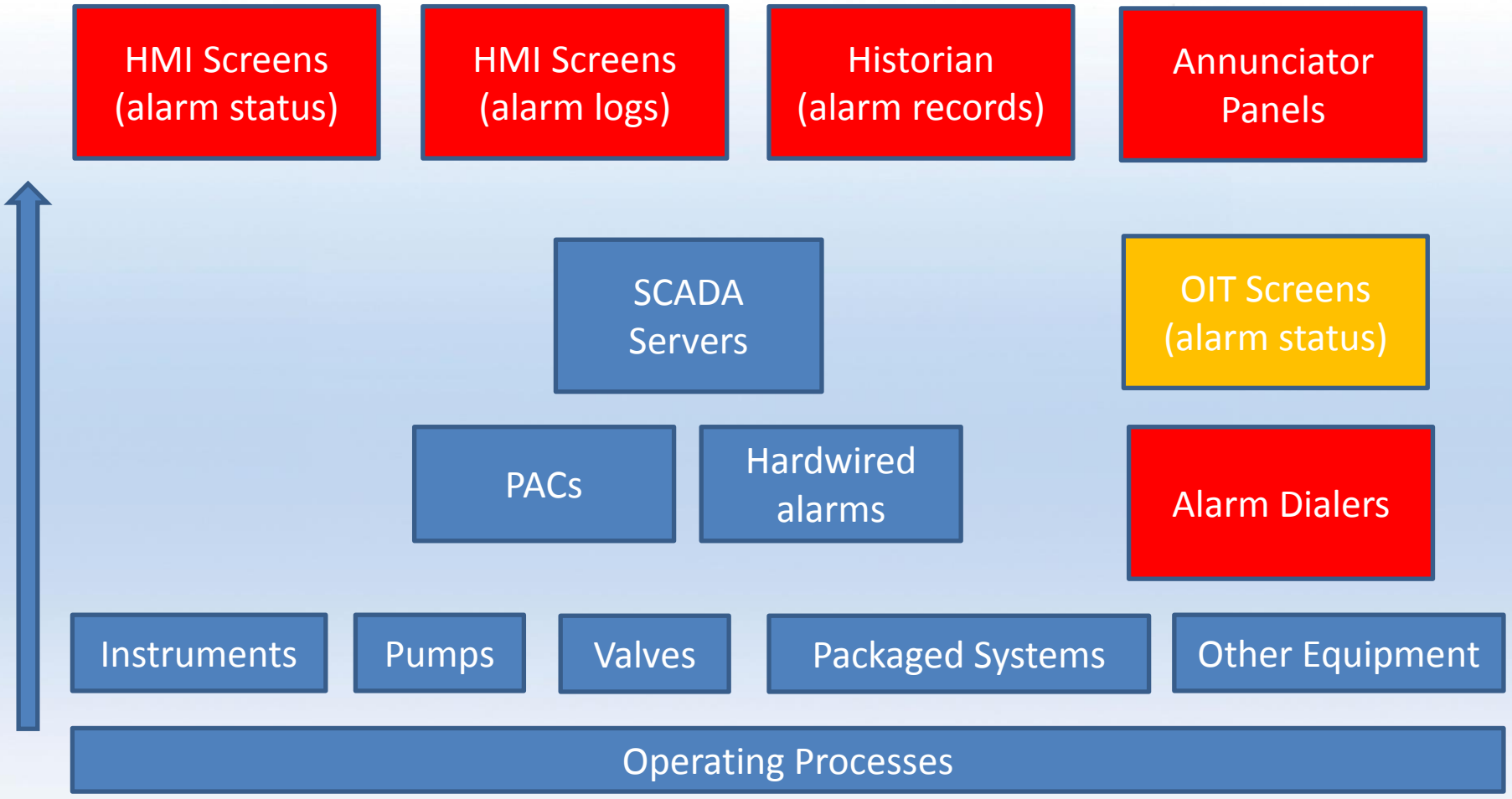
- Identification and Rationalization Workflow Details
- Monitoring Alarm Performance
- Applying 18.2 to York Region

Today's Format

- Part 1 – overview of 18.2
- break
- Part 2 – introduction to 18.2 features
- lunch
- Part 3 – alarm philosophy document
- break
- Part 4 – identification, rationalization, performance & monitoring

Alarm System Review

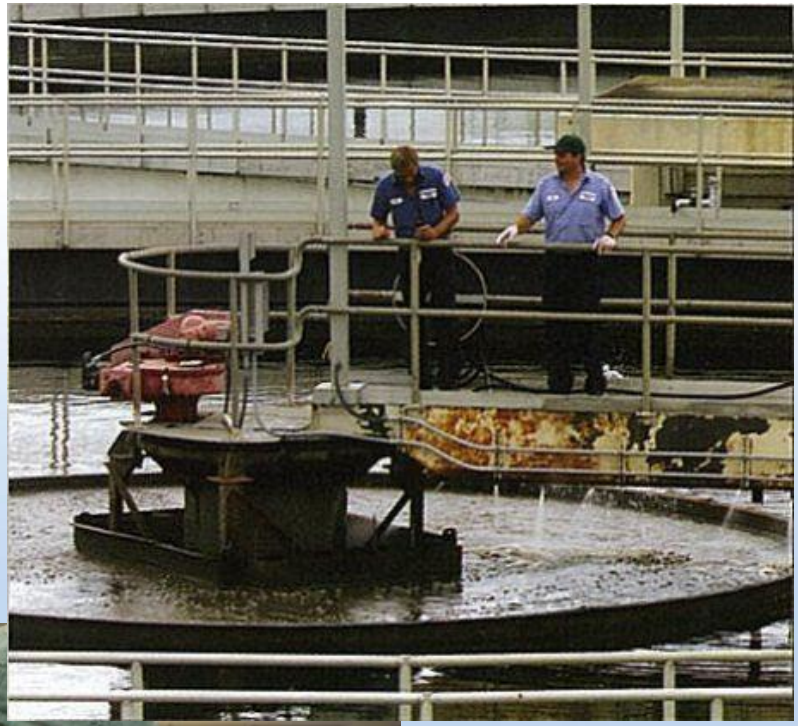
Review: The Alarm System



Common Alarm Problems

- Too many alarms
- TOO MANY ALARMS
- **TOO MANY ALARMS**
  - too much clutter in alarm system to get meaningful information
  - So many alarms, there is a tendency to ignore the alarm system
  - important alarms can be missed

- Nuisance alarms
- Alarms about conditions operator already knows about
- Alarms that do not require an operator response
- Alarms being routed to the wrong person



Common Alarm Problems – cont'd

- "Too many alarms"
  - Alarms that serve no purpose
  - Nuisance alarms
  - Chattering & fleeting alarms
  - Stale alarms
  - Alarms with no response
  - Alarms with the wrong priority
  - Redundant alarms
  - Alarm floods

ISA 18.2 guidelines recommend a max. of 1 alarm per 10 mins for an operator to effectively deal with alarms

We also don’t want to miss important alarms

Common Alarm Problems – cont'd

- Hard to track/control changes to alarm setpoints
- Hard to track/control unauthorized disabling of alarms

- Alarms that need to be disabled for maintenance but can't
- Very important high priority alarms don't stand out enough

- Excessive overtime costs from calling-in operators to investigate alarms in the field

- Operators spending too much time dealing with alarms, rather than using their time to ensure plants run efficiently

- Loss of "situational awareness" due to too many interruptions

What is the ISA 18.2 Standard?

What is ISA 18.2?

- **Alarm Management Standard by the ISA – International Society of Automation**
- **Released in June 2009**
- **Currently being adopted as IEC 62682**

- **Consists of:**
  - **Core Standard: 80 pages**
  - **Seven Technical Reports: 3 published + 4 coming**

- **Result of 6 years of work of 200+ volunteers across multiple industries.**
- **Builds on work in other standards including EEMUA 191, NA102, API1165, ASM Reports**

18.2 “Standards Family”

- **The standard**
  - **ANSI/ISA-ISA18.2-2009 – Alarm Management for the Process Industries**

- **Technical Reports**
  - **ISA-TR18.2.1 – Alarm Philosophy**
  - **ISA-TR18.2.2 – Alarm Identification and Rationalization**
  - **ISA-TR18.2.3 – Basic Alarm Design**
  - **ISA-TR18.2.4-2012 – Enhanced and Advanced Alarm Methods**
  - **ISA-TR18.2.5-2012 – Alarm System Monitoring, Assessment and Auditing**
  - **ISA-TR18.2.6-2012 – Alarm System for Batch and Discrete Processes**
  - **ISA-TR18.2.7 – Alarm Management for Packaged Systems**

TR 1, 2 and 3 are to be published in 2013/2014

TR 7 currently being developed, target is 2016

ISA 18.2 in a Nutshell

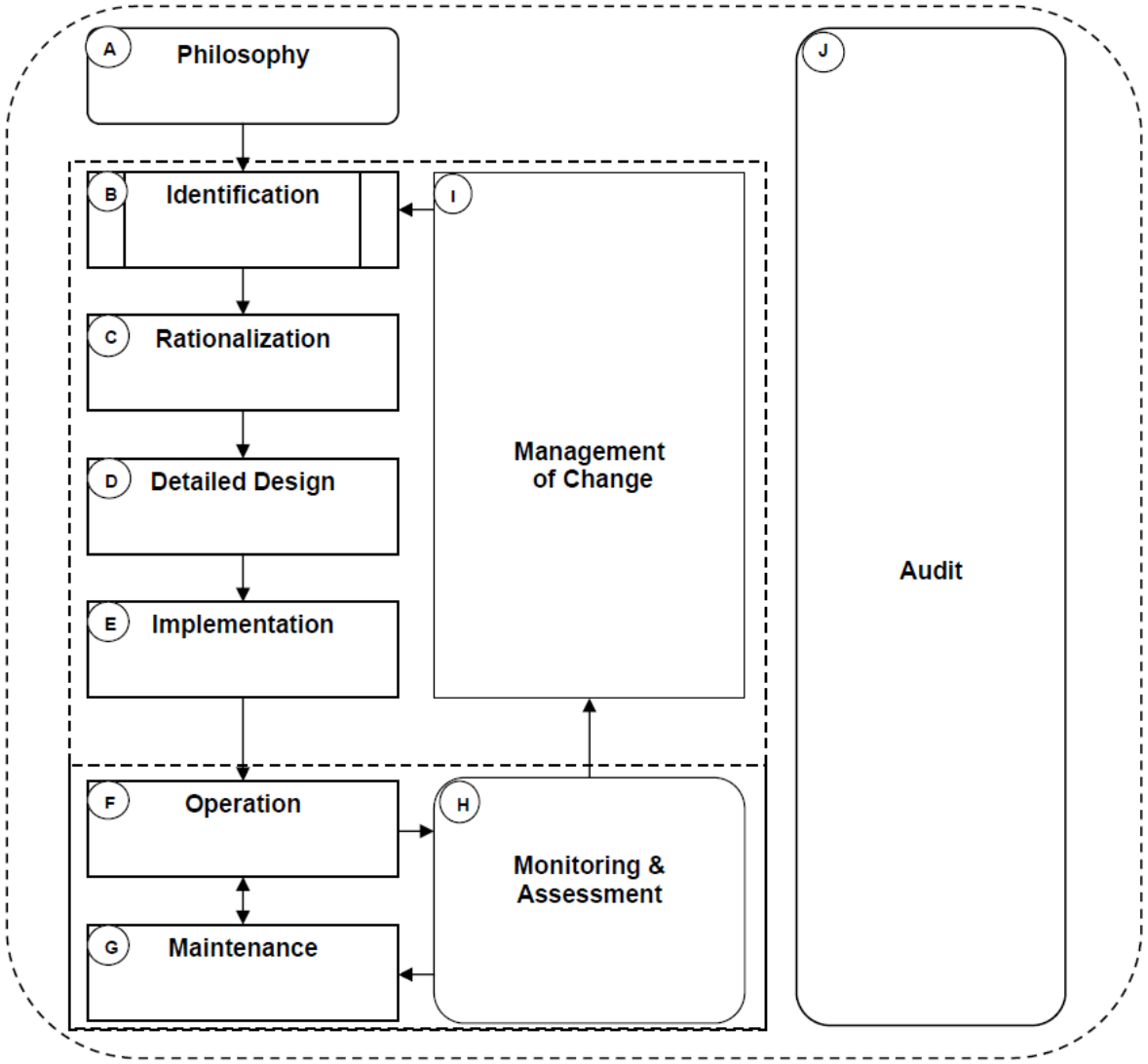
- Set of work processes for managing the alarm system
- Alarm system is meant to be used by Operators
- Central coordinating document is used: Alarm Philosophy

- Definition of an alarm – all must be true:
  - Indicates an abnormal situation to the Operator
  - Requires an immediate operator response
  - Has a defined action that he operator must do, within defined time limit
  - Has a defined consequence if the operator ignores it, within time limit

- All alarms are “rationalized”
  - If an alarm does not meet criteria for an alarm, remove it from alarm system

- Alarms details stored in a Master Alarm Database (MADB)
- Formal Management of Change (MOC) procedures used

The 18.2 Work Processes



Where is 18.2 being used

- Oil & Gas Plants
- Refineries
- Offshore Oil Platforms
- Pipelines
- Chemical Plants
- Pulp & Paper
- Mines & Mine Processing
- Pharmaceutical Plants
- Power Plants
- Water & Wastewater Facilities ←

- Anywhere Operators are responsible for running and monitoring automated processes. Alarms interrupt the operator so they can deal with something that requires their immediate attention

Ideas behind 18.2

- Alarm System should help operators in their jobs
- Investigating/responding to alarms consumes resources
  - Staff costs to investigate alarms can be significant – call-outs & overtime
  - Operators should only be investigating “real alarms”
- How do we ensure important alarms are getting to operators?
- How do we manage change?
- How do we assess alarm system performance?
- How do we audit the system?

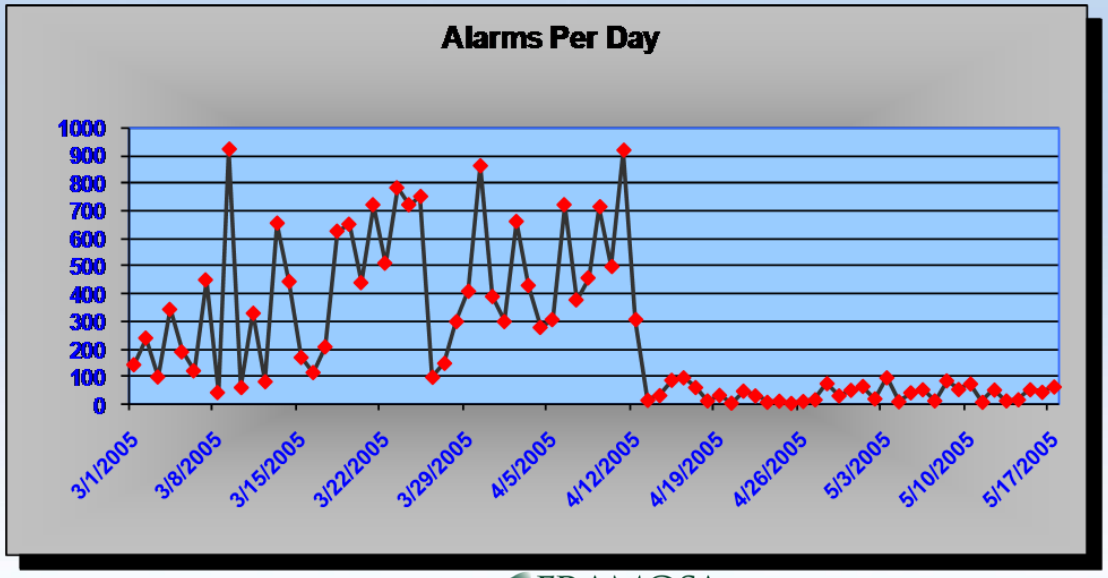
Motivations behind 18.2

ANSI/ISA-18.2-2009,

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 requiring a response.*

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)

Major Features of ISA 18.2

Major 18.2 Features

- Alarm Philosophy Document
- Operator-centric definition of an alarm
- Master Alarm Database (MADB)

- Identification and Rationalization of Alarms
- Standardized Alarm Design Techniques

- Alarm classification, prioritization, and “highly managed alarms”
- Calculated alarm setpoints, deadbands, ON/OFF-delays

- Alarm Shelving
- Ability to take alarms out of service for maintenance

Major 18.2 Features – cont'd

- Improved HMI Alarm Display techniques

- Management of Change
- Using Master Alarm Database to track changes

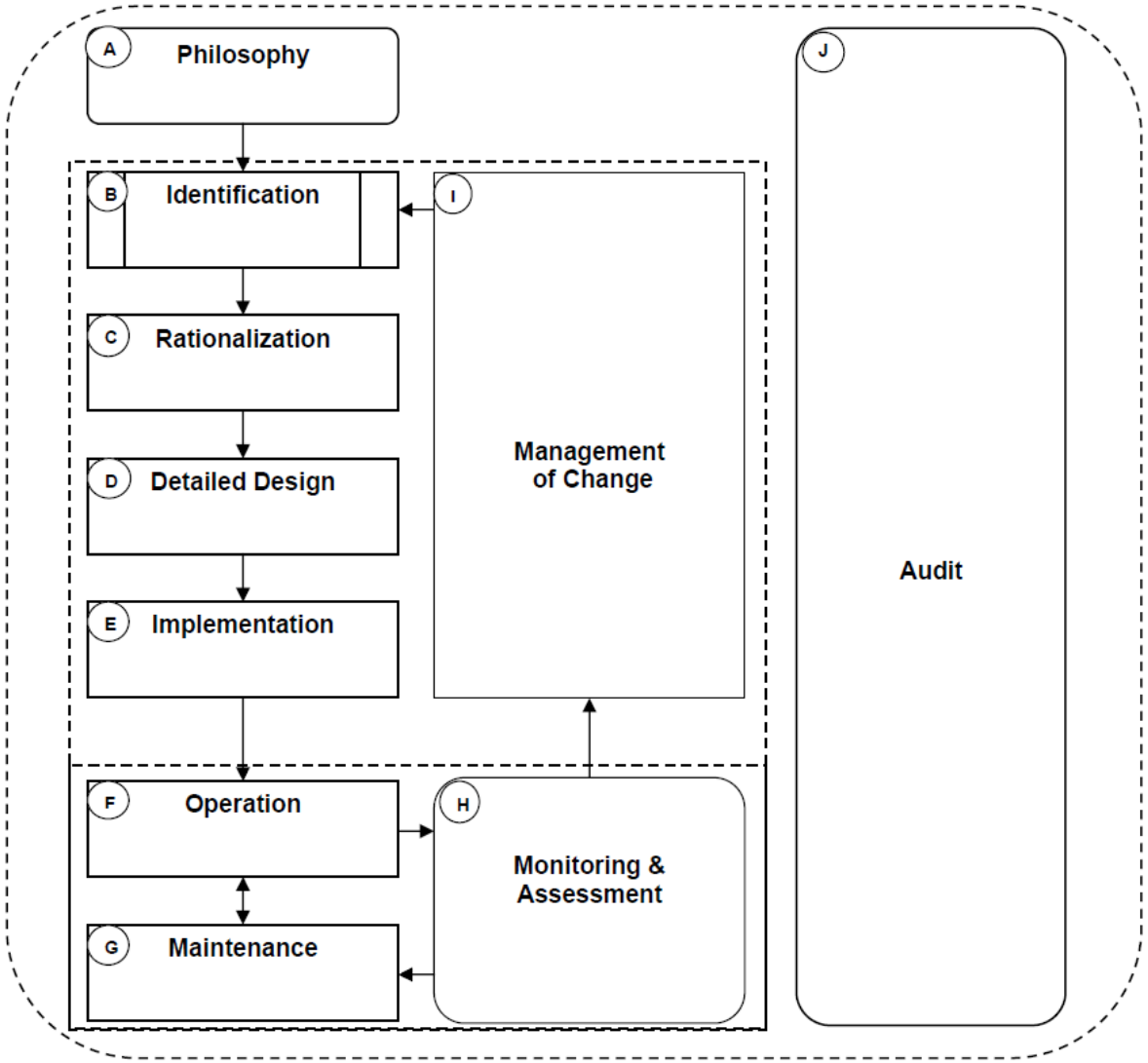
- Metrics for monitoring/assessing
- Procedures for Auditing

- Training for Operators on using alarm system effectively
- Periodic maintenance for the alarm system

- Staff member who is responsible for managing the alarm system

Alarm Lifecycle

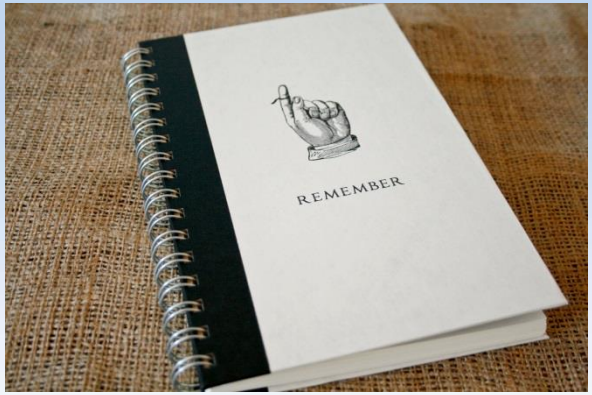
The 18.2 Work Processes



Alarm Philosophy

- Main Document which defines the Alarm Management Program
- Organization specific, written based on 18.2 & stakeholder input

- Documents how the program is to work
  - Roles and Responsibilities
  - Definition of Alarm
  - Master Alarm Database Details
  - How to Identify & Rationalize Alarms
  - Alarm Design Techniques to use
  - Alarm classes, priorities and how to determine
  - HMI Design Guidance
  - How to measure alarm history performance
  - Management of Change
  - How Alarm Records are stored
  - Training Requirements



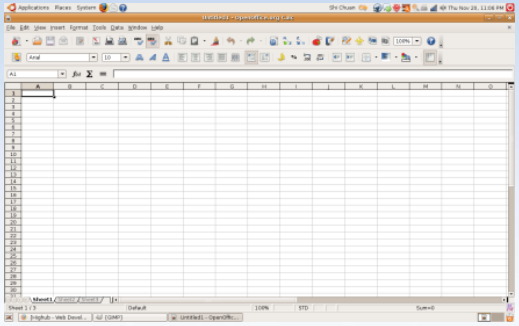
Identification

- Identifies alarms to be brought under alarm management
- Gather information from existing alarm logs

- Populates “Master Alarm Database” with records to rationalized

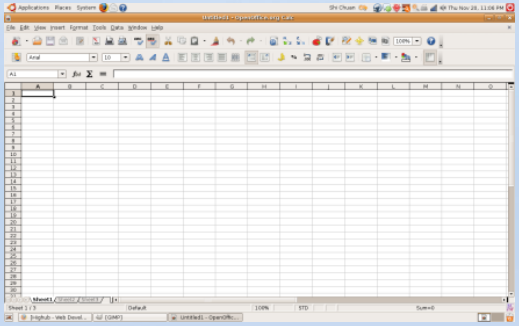
- New Sites
  - Get preliminary list of alarms from process designer
  - Get input from stakeholders (operations, maint., etc.) on possible alarms

- Existing Sites
  - Get list of all existing configured alarms & settings
  - Get copy of alarm log for X months
    - Identify low hanging fruit – Bad Actor Analysis
    - Calculate overall statistics on performance



Rationalization

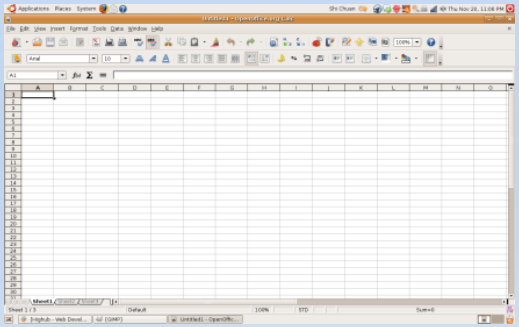
- Evaluate draft alarms in the “Master Alarm Database”
- Alarm Entries are reviewed one at a time to ensure they meet the “alarm criteria” in AP to be an alarm. If not, they are deleted.
- Valid “alarm” criteria includes:
  - Is it for an abnormal condition?
  - Requires an (immediate) operator response
  - Operator response will have real effect
  - Defined consequence if ignored
  - Severity/type of consequence is defined/quantified
  - Does not duplicate awareness Operator will already have

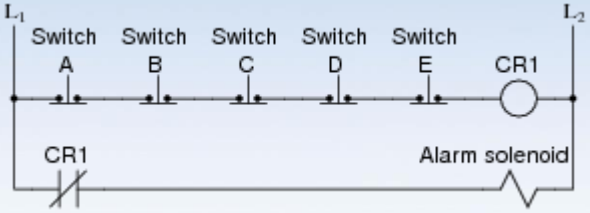


- Alarm priorities & classification are assigned
- Draft alarm attributes (setpoint, deadband, ON-Delay, OFF-Delay)

Detailed Design

- Finalizes details for alarms the “Master Alarm Database”
- Uses Design techniques outlined in Alarm Philosophy
- Finalize how the alarm will be programmed:
  - Setpoint
  - Deadband
  - ON-Delay
  - OFF-Delay
- Sort out any alarm vs. interlock issues
- Record results in the MADB





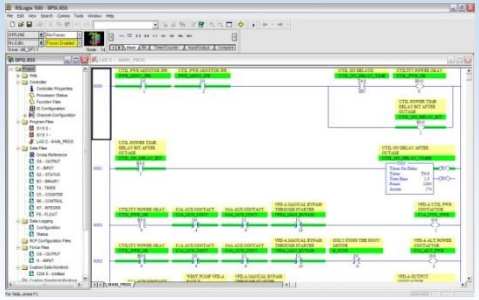
Implementation

- Program the actual alarms into the SCADA System
- Combination PAC and HMI programming – use Region standards

- Use the Master Alarm Database as the programing spec
- Test the new alarms before deploying (FAT testing)

- Start-up/commission new alarms into production

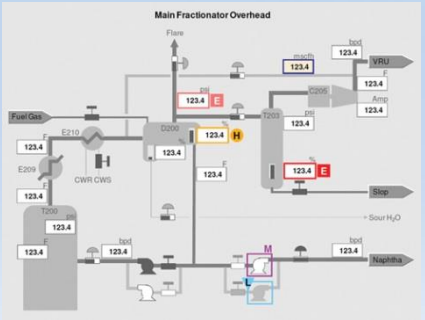
- Any commissioning “adjustments” are subject to MOC
  - Checked against what is in the MADB
  - Changes are rationalized before proceeding
  - Any changes are documented in MADB.



Operation

- **Operators are trained on how to use the alarm system**
  - Control Room Operators
  - Field Operators
  - On-Call operators that receive alarm dialer call-outs

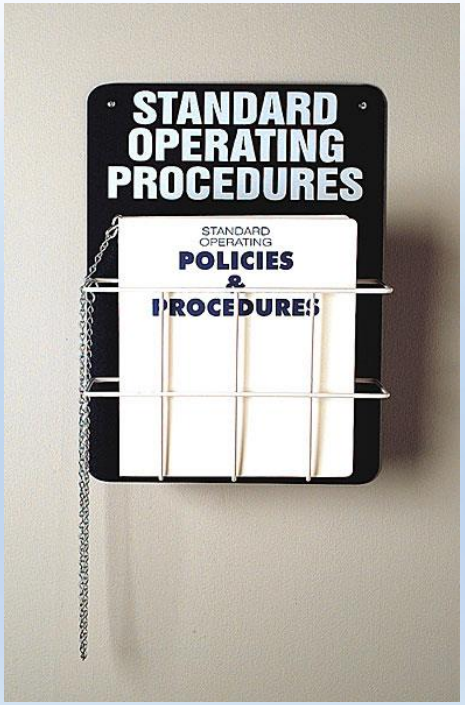
- **Training on how to use:**
  - Operating by Surveillance vs. by Alarm
  - HMI Alarm Screens
  - Alarm Priorities / Classifications



  - How Alarms are Designed
  - How to Acknowledge and Respond to Alarms
  - "Alarm Shelving" Procedures
  - Putting Alarms "Out of Service" for maintenance
  - Shift Change Procedures with respect to shelved alarms
  - Where to find documentation for Alarm Reponses, Consequences, SOPs

Maintenance

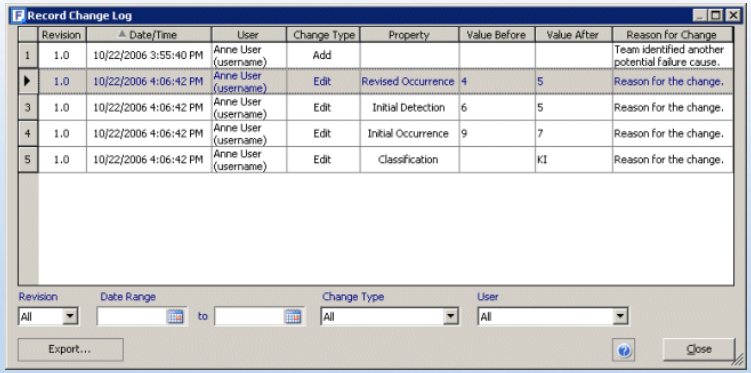
- **Formal Procedures**
  - Record Keeping
- **Alarm Shelving**
  - Equipment “not in use”
  - Calibration of Instruments
  - Equipment down for maintenance
  - Shelving alarms arising from a known problem
- **Putting Alarms Out of Service**
  - Equipment not in use (not in use)



- **Note: Permanent removals, additions or changes to alarms triggers “Management of Change” work process**

Management of Change

Any changes to alarms must be tracked, evaluated and documented



Examples of changes:

- **Addition of new alarms**
- **Removal of existing alarms**
- **Modification to alarm settings**
  - **Setpoints**
  - **Deadband**
  - **On-Delay/Off-delay**
  - **When alarm is programmatically enabled/disabled**
  - **Any automated alarm actions (interlocks, triggers, etc.)**

- **Proposed changes must be:**
  - **Logged and tracked**
  - **Subject to Identification, Rationalization, and Detailed Design before being deployed.**
  - **Master Alarm Database must be kept up to date**
  - **Last step – make the change**

Monitoring and Assessment

- **ISA 18.2 gives guidelines for a variety of metrics to use, such as:**
  - **Max alarms per 10 minutes (goal is 1 alarm per 10 minutes)**
  - **Distribution of alarm priorities**

- **The Alarm Philosophy will define what is measured and how often**

Common Metrics

- **Percent alarms rationalized (initially will just be pilot sites)**
- **Average number of alarms per 10 minutes**
- **Max number of alarms per 10 minutes each day**
- **Percent of time system is in "flood" (e.g. 10+ per 10 min)**
- **Alarm priority distribution (percentages)**
- **Number/percent of shelved alarms and average duration**
- **Number/percent of Out of Service Alarms**
- **List and count of most frequent alarms**
- **Etc.**

Audit

- Audit of reality vs. what is written in alarm philosophy
- Review of records/logs to see that work processes are being carried out

- Carried by small team of people within organization
- Goal to assess program compliance and make action items to improve

- Usual documentation audited:
  - Alarm philosophy (used as source document)
  - Master Alarm Database
  - Alarm Monitoring Reports
  - Alarm System Change Log (from Management of Change: problems & resolutions)
  - Alarm out-of-service permits
  - Management of Change documentation
  - Test records for alarms
  - Training records for operators
  - Any relevant incident investigations (alarming aspect)

BREAK

Post Break Review

- ISA 18.2 is an international standard for Alarm Management

- 18.2 is driven by a document called "Alarm Philosophy"
- Uses 10 work processes for better design, selection and application of alarms
- Master Alarm Database is used to document/track alarm configuration

- The Alarm system is for the benefit of operators
- New Alarm Definition: Abnormal condition requiring an operator response

- Alarms are identified, rationalized, designed, and implemented
- Procedures and training put in place for Operations and Maintenance
- Formal Management of Change for any changes to alarms

- Operators have ability to "shelve alarms" for maintenance and/or known issues
- Periodic Monitoring and Assessment of Alarm System

- Annual Audits of the Alarm Management Program

Part 2: “18.2 Features” - Outline

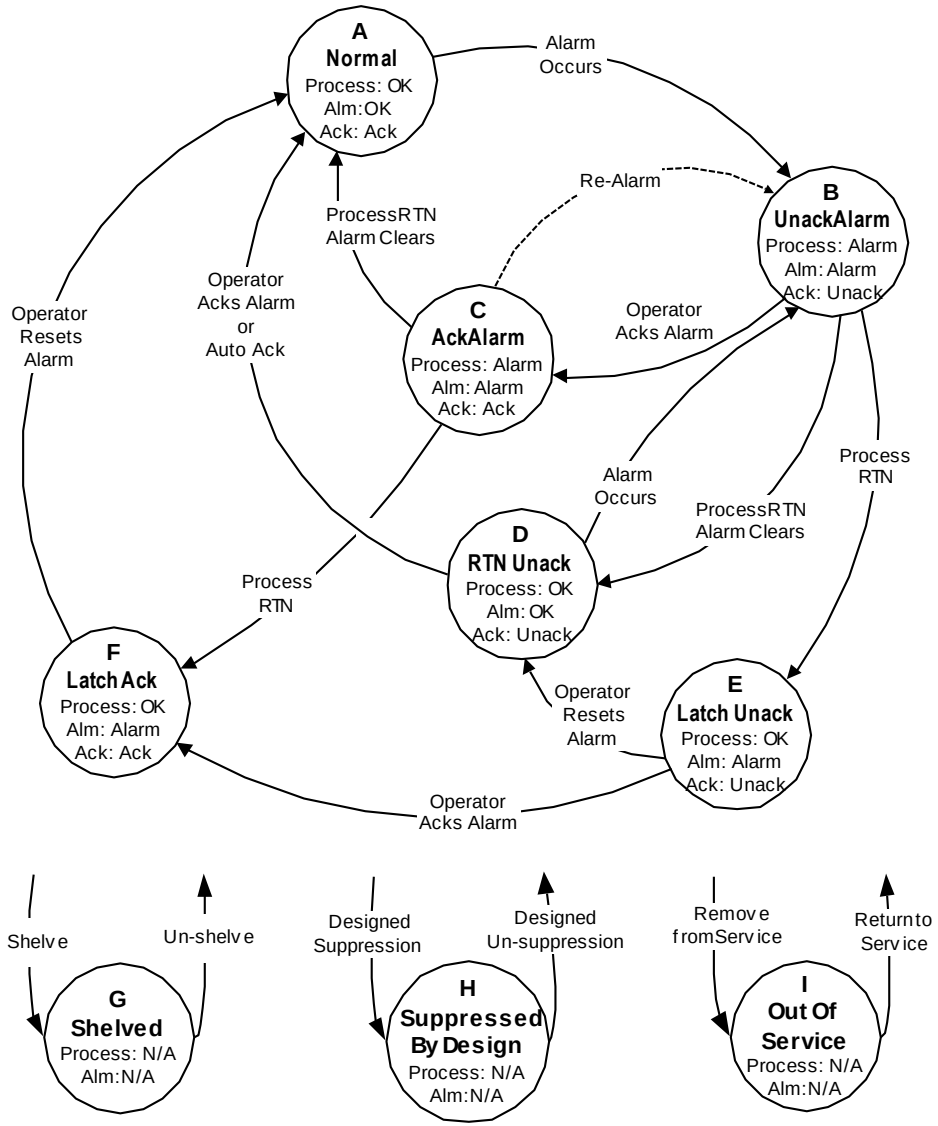
- Definition of an Alarm & Alarm Thresholds

- Master Alarm Database
- Management of Change
- Alarm Priorities
- Alarm Classification
- Highly Managed Alarms
- Alarm Routing

- Alarm Setpoints
- Additional Alarm Attributes: ON-Delay, OFF-Delay, Deadband
- Designed Alarm Suppression

- Alarm Shelving & Marking Alarms Out-of-Service
- HMI Display of Alarms
- Alarm Logging

How an Alarm works – a flow chart



18.2 Definition of an Alarm

- **Old Definition**

  "Alarm calls attention to an abnormal condition"

- **Definition from 18.2:**
  "An audible and/or visual means of indicating to the operator an equipment malfunction, process deviation or abnormal condition requiring a response"

- **Simplified:**
  "Notification of an abnormal condition to an operator requiring an immediate response"

- **But we need to define:**
  - **Who is the operator?**
  - **How are we notifying them?**
  - **What is a response?**

18.2 Definition of Alarm: Operator

- **Operator**
  - **The person responsible for the process**
  - **The person who monitors and decides to make changes to process**
- **The alarm should only go to one person**
- **That person needs to have the training to know what to do**
- **That person is who acknowledges it (as being dealt with)**

18.2 Definition of Alarm: Response

- **An alarm is an interruption to the operator**
- **We only want to interrupt the operator with an alarm, if the following are true:**
  - **There is *something* they can truly do to make the situation better**
  - **They have to do that *something* quickly**
  - **If don't do that *something* quickly, the situation will get worse (there is a defined consequence)**

18.2 Definitions: Alarm Consequence

- **Alarm notifies the operator so they do something to avoid a consequence.**

- **Examples of strong consequences:**
  - **Wet well overflows → discharge, flooded basements**
  - **Water Tower Drops below safe level for fire protection**
  - **Chlorine Residual drops below safe operating level (defined by Region)**
  - **Chlorine Residual drops below minimum required level (defined by MOE)**

- **Examples of weaker consequences**
  - **A pump turns on automatically**
  - **A pump failed to start but it is in a bank of 4 pumps**

- **As part of "Rationalization" the type consequence and severity is defined for every alarm**

18.2 Definitions: Alarm Timeline

- How long does operator have to respond?
- How soon will the defined consequence occur?

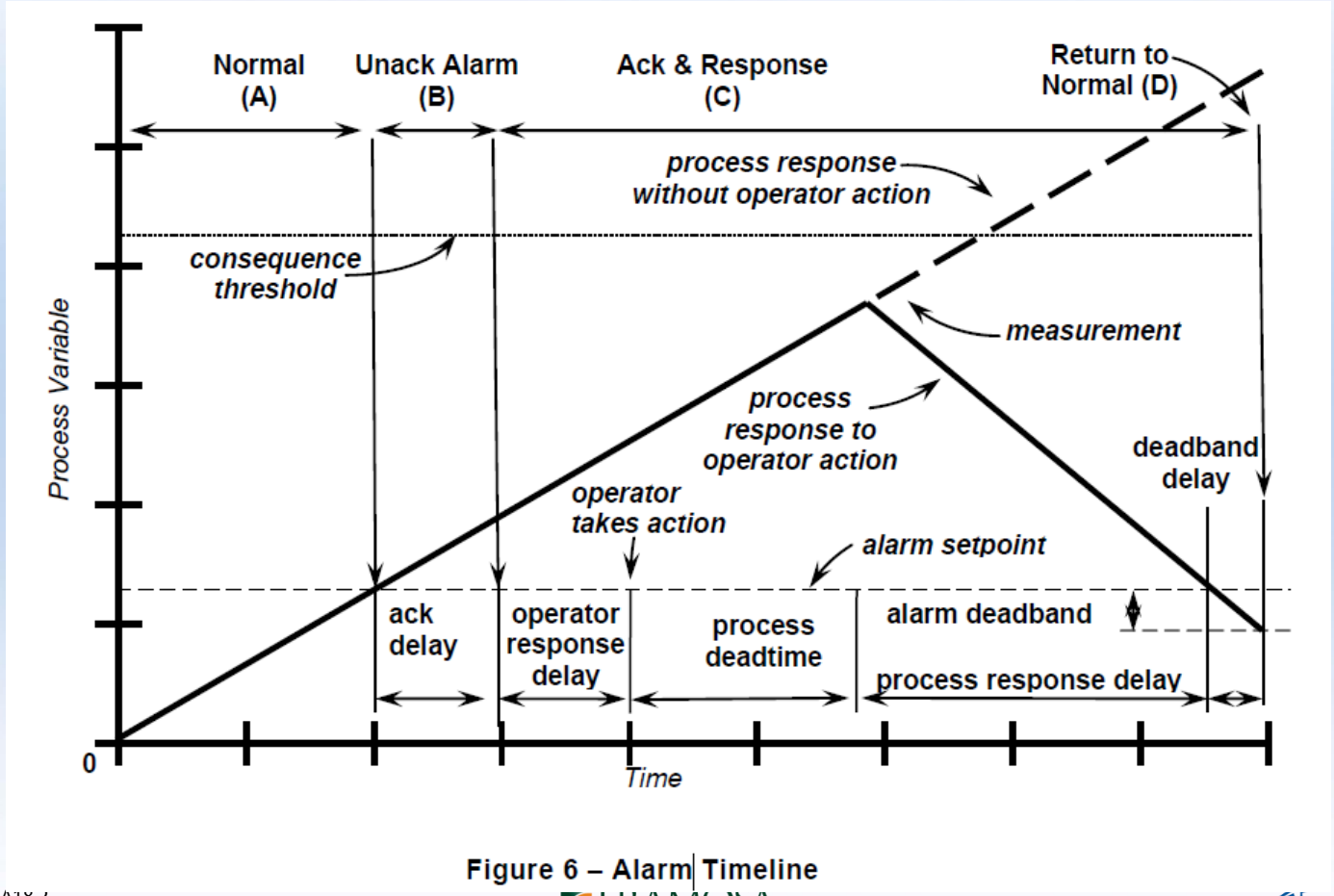


Figure 6 – Alarm Timeline

18.2 Definitions: Operator Notification

- 18.2 was originally written based on an operator being a "control board operator"
  - 24/7 staffing of a control room by an operator who is in charge
  - Operator continually monitors the process via the HMI
  - They receive alarms via the HMI and/or an annunciator panel
    - Visual & auditory notifications, which interrupt them
  - They call in additional resources when needed
  - They call a field operator/tech if field investigation required

- Adapting 18.2 to the Region
  - 24/7 staffed central control room with board operators
  - Roving field operators in the field

18.2 Definition of Alarm: Threshold

- How do we choose if an “event” is bad enough to alarm?
- When is it worth interrupting the operator?

CAUTION:

- As per 18.2, the operator is expected to keep situational awareness of processes as part of their normal duties
- Operators are expected to keep an eye on process screens regularly to “keep tabs” on what is going on
- Large “overview” screens on the HMI make this easier
- The alarm system should never be used give situational awareness

18.2 Definition of Alarm: Threshold 2

- Thresholds are defined in the Alarm Philosophy (more later)

- "Every alarm requires a demonstrable response"
  - Valid:
    - Operator needs to make adjustment via SCADA
    - Operator needs to call someone in field to make adjustment
    - Operator needs to call someone in field to investigate
    - Contacting other personnel regarding situation**
  - Probably not Valid:
    - Write something down in a log book
    - Notification that the operator needs to pay more attention to something
    - A heads up that there is something that the next shift should deal with

** for operator notifying other personnel about something that does not require immediate attention, there are often better ways of doing this than using an alarm

18.2 Definition of Alarm: Threshold 3

- **Alarm responses need to have a time limit to them:**
  - **How long does the operator have to make their response?**
  - **How long can they delay?**
  - **Is it better if they react quicker?**
  - **When alarm annunciates how long until the "consequence" happens?**
  - **Alarms with "worse consequences if ignored" often need faster responses – provided that operator's actions will have an effect**
  - **Note: No point in reacting to alarm if the operator can't do anything**

18.2 Master Alarm Database

- Central Location to document details for every alarm
  - Typically an “Excel Spreadsheet” or “Access Database”
  - Specialized software can also be used
  - Note: This is separate from the actual SCADA programming.

- MADB is used as a “spec” for programming alarms in SCADA
- When alarm system is audited MADB is compared against SCADA

- If any changes are made to an alarm, it must be documented in MADB

- Formal “Management of Change” procedures are used to keep MADB up to date, and the SCADA programming synchronized

18.2 Management of Change

- Formal procedures are used to manage changes to the alarm system
- For some changes, minimal paperwork is needed, e.g. a form filled out and sent to the person managing the MADB and change made
- For other changes, sign-offs and justifications are required before changes can be made.
- Depends on which alarm it is and how the alarm is being changed
- Applies to both alarm additions and alarm deletions
- Procedures will be defined in the Alarm Philosophy

18.2 Management of Change 2

- **Example of procedures used in one plant for permanent alarm changes:**

- **Formal MOC** – a full review by the appropriate people or departments, full documentation and formal classroom training for operations and maintenance department personnel are required.

- **Informal MOC –** documentation requirements are the same as for a formal MOC. There may be a smaller number of reviewers and the training may be face to face.

- **Change log –** the change is entered into the operations log. If the alarm is restored to its original state, that change is also entered into the log.

- **Change Log – a log book is used to log any changes to the alarm system that have been made, in addition to updating MADB**

18.2 Management of Change 3

- **Example of a formal/informal MOC determination:**

Type of change	Level of MOC
Alarm setpoint	Formal
Alarm type	Informal
Alarm priority	Formal
Alarm description or alarm message	Informal
Alarm presentation on graphics	Formal
Alarm addition or deletion	Formal
Point execution status (turned on or off)	Informal
Alarm suppression	Formal
Alarm deadband	Informal
Alarm on/off delay	Informal
State-based alarm configuration	Formal

Example MOC table

18.2 Alarm Priorities

- In the alarm system all alarms are assigned “priorities”
- When multiple alarms come in, priorities help the operator decide which alarms to address first

- Typically in an 18.2 alarm system, there are 4 or 5 priorities defined:
  - DIAGNOSTIC (normally not shown to operator)
  - LOW
  - MEDIUM
  - HIGH
  - CRITICAL
- The number/type of priorities are defined in the Alarm Philosophy

- In some systems there are additional notifications: “Alerts”, “Messages” or “Events” are also used – but these are not alarms

18.2 Example Priorities

Type of Consequence	Proximate Consequence of Inaction or Incorrect Action		
	MINOR	**MAJOR**	**SEVERE**
Public or Environ-mental	Local environmental effect, contained release, minor cleanup Internal or routine reporting requirements only	Non-permanent damage from contamination, single exceedance of statutory or prescribed limit Reporting required at the local or state agency level	Uncontained release of hazardous materials with significant environmental and/or 3rd party impact or publicity Extensive cleanup measures and financial consequences Reporting required at the state or federal agency level
Cost, Efficiency, Downtime, Lost Production, Quality, Equipment Damage	Event or lost production costing <$10,000. Minor efficiency impact or quality excursion. Reporting required only at the department level	Event or lost production costing $10,000 to $100,000 Significant efficiency loss, multiple unit impact Reporting required at the site level	Event or lost production costing >$100,000 Extensive outage, potential equipment damage Reporting required above the site level
Speed of Response	**Event has only Minor Consequence**	**Event has Major Consequence**	**Event has Severe Consequence**
Immediate (<3-5 min)	Medium Priority	High Priority	High Priority
Rapid (<15 min)	Low Priority	Medium Priority	Medium Priority
Prompt (<30 Min)	Low Priority	Low Priority	Medium Priority
Not Urgent (>30 Min)	Re-engineer the alarm for urgency		

Figure 4 - Example of an Alarm Priority Matrix

18.2 Alarm Classes

- Not to be confused with alarm priorities
- These are logical groupings of alarms based on what they are for and/or the type of alarm

- Alarm Classes help by:
  - Reduce training requirements – operators can be trained to use a standardized response for a class of alarms
  - Make rationalization faster – by grouping alarms together, and rationalizing together
  - Decrease complexity
  - Make alarm design, programming and implementation easier

18.2 Highly Managed Alarms

- This is a special class of alarms, which additional administrative requirements are used
- Reserved for alarms that have significant environmental, safety or compliance consequences associated with them

- Examples:
  - Low Chlorine Residual in a Drinking Water Distribution System (MOE limit)
  - UV Disinfection Unit Failure
  - CSO Tank High High Level that could lead to CSO Overflow

- These will be defined in the alarm philosophy document (more later)
- Should be used sparingly:
  - additional requirements can be labour-intensive to do
  - highly managed alarms often draw increased regulatory interest

18.2 Highly Managed Alarms 2

- **Typical additional requirements for HMAs:**
  - **Restrictions on Alarm Shelving**
  - **Additional data logging, security, access control and/or paperwork for Alarm Shelving**
  - **Additional procedures for taking HMA out of service for maintenance**
  - **Additional staff training requirements**
  - **Increased HMA testing requirements and test documentation – initial and periodic**
  - **Increased Auditing requirements, including type and frequency**

18.2 Alarm Routing

- Alarms are grouped into “alarm areas” so that the alarms get routed to the right operator
  - Can also be used to route “maintenance” notifications to maintenance personnel
- “Alarm areas” are also used for sorting alarms on the HMI, in the historian, and for alarm statistics
- Commonly used for large facilities with multiple sites
- The Region already makes uses of this in their iFix HMI

18.2 Alarm Setpoints

- As part of the Alarm Rationalization / Alarm Design work process, alarm setpoints are calculated for every alarm

- Calculated alarm setpoints mean:
  - Documented record of what the alarm setpoint should be
  - Setpoint is based on design/operations principals
  - Makes it possible to
    - calculate how long operator has to respond to alarm
    - Calculate how long until consequence occurs if alarm is ignored

- For every alarm the proper alarm setpoint is documented in the "Master Alarm Database", along with other alarm attributes

18.2 Other Alarm Attributes

- In 18.2 alarms can have several attributes in addition to Setpoint

- ON-DELAY in seconds
  - How long the alarm condition has to be true before the alarm is triggered
  - Make sure condition has been “bad for long enough” for it to matter
  - Helps prevent unnecessary nuisance alarms

- OFF-DELAY in seconds
  - How long the alarm condition has to be false before alarm returns to normal
  - Helps prevent nuisance alarms that keep triggering over and over again

- DEADBAND in percent
  - For an analog alarm, provides hysteresis so alarm won’t chatter on/off
  - Example: High alarm of 8m on a signal of 0-10m with 1% deadband:
    - Alarm ON: rises above 8 m
    - Alarm OFF: drops below 7.9 m

18.2 Other Alarm Attributes 2

- **Commonly used deadbands and ON-Delays**

Signal Type	Deadband (Percent of Operating Range)	Delay Time (On or Off)
Flow Rate	5%	~15 Seconds
Level	5%	~60 seconds
Pressure	2%	~15 seconds
Temperature	1%	~60 seconds

- **There are often used in addition to process-specific adjustments to these attributes to prevent nuisance alarms**

18.2 Alarm Setpoint Enforcement

- Some industries will use automated means to enforce setpoints
  - Scripts that "copy over" proper setpoints once per day
  - Hard-coded setpoints that cannot be changed
- Often requires special programming / scripting to implement
- Typically only done for "high importance/risk" alarms
  - E.g., quality alarms in pharmaceutical plant
  - E.g., critical alarms in a oil refinery
  - E.g., alarms setpoints that require significant calculations to determine
- Alarm setpoint enforcement is detailed in alarm philosophy doc
  - If it will be used
  - Which types of alarms and how the enforcement is done is pre-defined
  - Criteria are developed to determine if alarm needs setpoint enforcement

18.2 Designed Suppression

- **Designed Suppression is when logic on the PAC is used to prevent alarms from happening under specific conditions**

- **Example 1**
- **On a pump with a flow meter on its discharge**
- **The “low flow” alarm that uses the flow meter signal will be programmed so that it is not active when the pump is off**

- **Example 2**
- **On a packaged bar screen system when the “equipment online” signal from the vendor panel is not active, process alarms from the bar screen’s vendor control system are automatically disabled in SCADA**

18.2 Alarm Shelving

- This is a new feature in 18.2

- Ability of the Operator to temporarily disable any alarm in the SCADA system in a controlled manner using a function on the HMI
- SCADA system disables the alarm, provides a “Shelved Alarm List” on the HMI, this list is reviewed at each shift change

- Benefits
  - Prevents nuisance alarms from known problems
    - Equipment Out of Service
    - Instrument taking offline for Calibration
    - Known broken equipment
    - Ability to take problem alarm Out-of-Service, until alarm can be fixed
  - Operator knows which alarms have been disabled by looking at the “Shelved Alarm List” on the HMI

18.2 Alarm Out-of-Service

- This is a new feature in 18.2

- Like “Shelving,” but usually for a longer period of time
- Used to put an alarm out of service for equipment maintenance

- This is often implemented as part of alarm shelving on SCADA

- Under Management of Change, alarms that are marked out-of-service are usually not reviewed every shift, instead they are managed using a longer-term procedures for justification and tracking

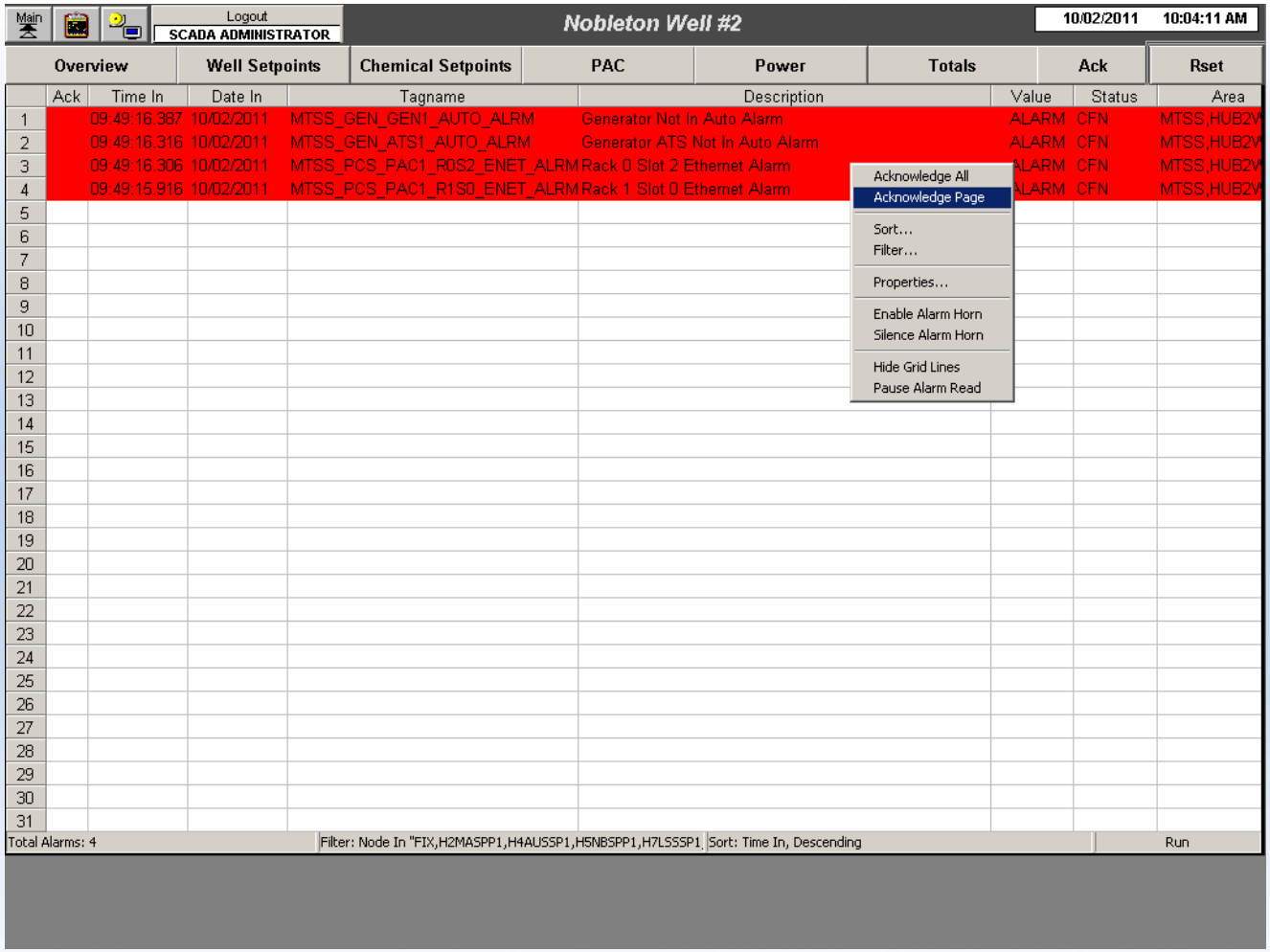
18.2 HMI Display of Alarms

- Recommends alarms be displayed on the HMI several ways

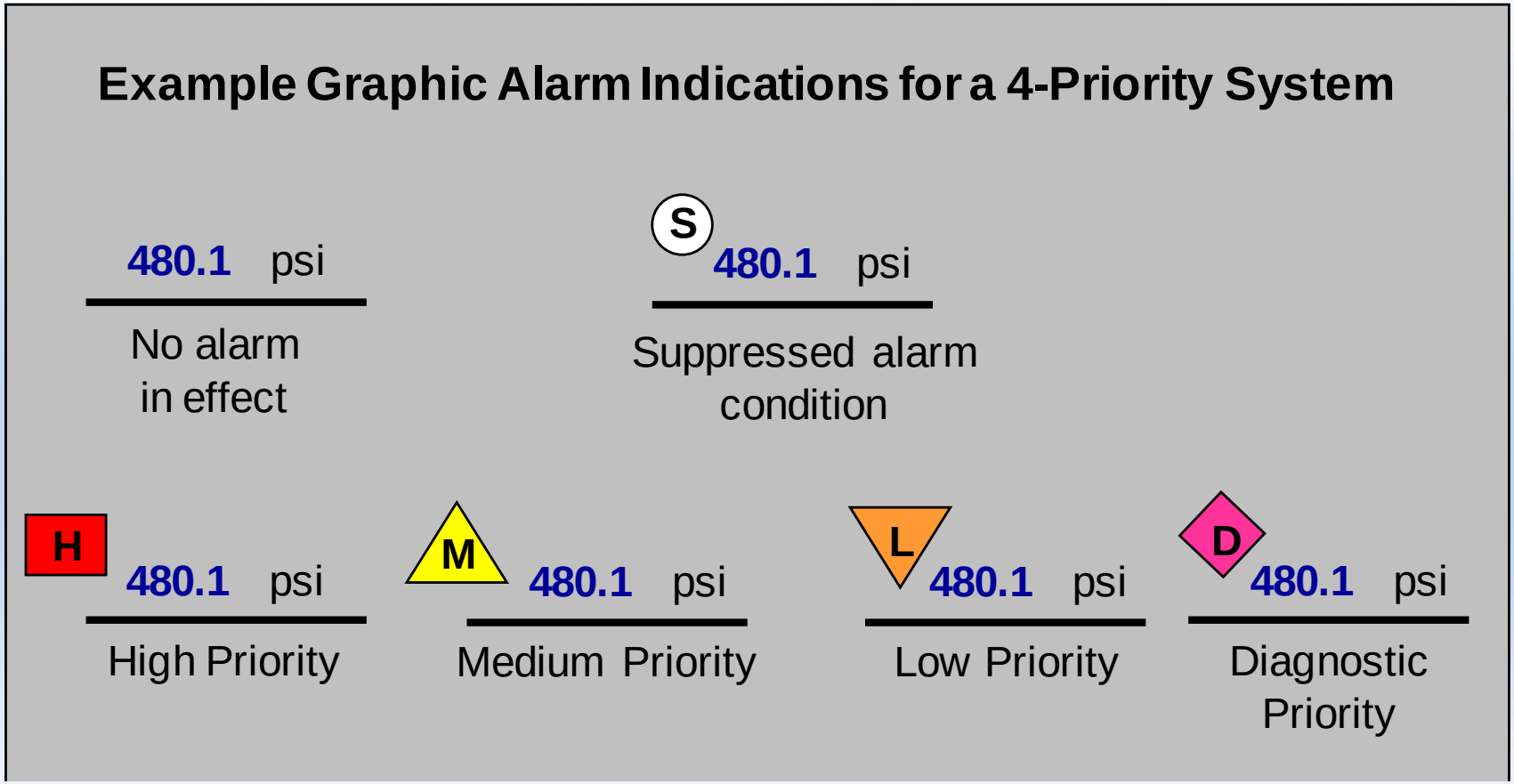
- In a dedicated “alarm log” HMI screen that is always visible
- Typical information to display:
  - Alarm Tag
  - Alarm Description
  - Priority
  - Current Status: ACTIVE UnAck, ACTIVE Ack’d, RTN UnAck, RTN Ack’d
  - Time/Date of Alarm
  - Time/Date of Acknowledgement

- Status indicators on process screens and on overview screens

18.2 HMI Alarm Log Example



18.2 HMI Alarm Status Example



18.2 Alarm Logging

- **Under 18.2 alarms must be automatically logged in the historian so that they are available for future analysis**
- **When alarm are active they are displayed on the HMI in an "alarm log" screen**
  - **Sometimes two alarm log screens are used – one for high priority alarms and the other for regular alarms**
- **Short term alarm records reside on the HMI**
- **Long term storage of alarm records is in the Historian**

18.2 Alarm System Performance

- **The alarm system is regularly monitored for how well it is performing**
- **Alarm records are periodically analyzed, and often correlated with process data records, to determine Key Performance Indicators**
- **What the KPIs are to be used are defined in Alarm Philosophy**
- **The Alarm Philosophy will also outline target values**

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

Figure 8 - Alarm Performance Metric Summary Table from ISA-18.2

BREAK FOR LUNCH

Post Break Review

- ISA 18.2 is an international standard for Alarm Management

- 18.2 is driven by a document called "Alarm Philosophy"
- Uses 10 work process for better design, selection and application of alarms
- Master Alarm Database is used to document/track alarm configuration

- The Alarm system is for the benefit of operators
- New Alarm Definition: Abnormal condition requiring an operator response

- Alarms are identified, rationalized, designed, and implemented

- Alarms are prioritized, classified and routed to help the right operator get them
- Alarms should only interrupt the operator for them to make immediate response
- Situational awareness should come from monitoring the process, not alarms

- Alarm records are kept, and alarm system performance is regularly measured

Part 3: “Alarm Philosophy” Outline

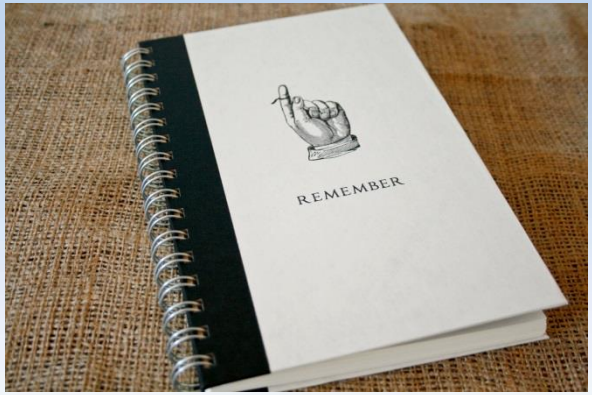
- Review of the Purpose of Alarm Philosophy
- Alarm Philosophy Contents

- Key topics the Alarm Philosophy Covers
- How Alarm Philosophy aligns with Work Processes

- Alarm Definition
- Documentation Requirements
- Identification & Rationalization
- Design
- Implementation
- Operations & Maintenance
- Performance Monitoring
- Audit

Alarm Philosophy

- Cornerstone of the Alarm Management Program
- Defines how the Alarm Management Program will work
- Customized for Region needs
- Written based on stakeholder input
  - Facilitator
  - Working Group members from various groups



Typical Contents

- Statement of Purpose
- Roles & Responsibilities
- Definition of an Alarm
- Terminology

- Alarm Identification Methods
- Alarm Documentation & Rationalization
- Alarm Design Principals
- HMI Design Techniques

- Procedures for Implementation
- Procedures for Operation/Maintenance
- Training Requirements & Intervals
- Performance Monitoring & Audits
- Management of Change
- Appendices: PAC/RTU/HMI programming details

Alarm Philosophy Purpose

- Serves to document what the alarm system is for
  - How the alarm system is implemented in SCADA
  - Where the alarms comes from
  - Who uses the alarm system
  - How they use it
- Define who receives alarms
  - Where and how operators receive alarms
  - How operators respond to alarms
  - Other personnel that get involved with alarms, and how
- Define Users: Alarm System Data, Stats, etc.

Define: Definition of Alarm

- **Document the alarm definition being used**
- **E.g., "Notification of an abnormal condition to the operator that requires an immediate response"**

- **Define criteria used to determine the threshold at which alarm is needed**
  - **Type of Operator Response**
  - **How Quickly Operator Response Required**
  - **Method of Determining Consequences**
  - **Method for determining priority/impact of consequence**
  - **Method of estimating how soon consequence will occur**
  - **Method used to determine alarm priority**

Define: Roles & Responsibilities

- **Define who does what!**

	Site Manager	Unit Manager	Shift Supervisor	Head Operator	Console Operator	Alarm System Owner	Control Systems Technician	Process Control Engineering	Maintenance Technician	IT Support	Training & Development	Safety, Health, & Environmental	Project Eng./Third Party (Vendor)
LIFECYCLE STEP - PHILOSOPHY													
Development of the Alarm Philosophy	I	A	I	I	I	R	R	R	I	I	I	I	
LIFECYCLE STEP - IDENTIFICATION													
Identification of alarms			A	R	R	A	R	R					
LIFECYCLE STEP - RATIONALIZATION													
Rationalization and prioritization of alarms		I	I	I	R	A	C	C	C				R
LIFECYCLE STEP - DETAILED DESIGN/IMPLEMENTATION													
Implementation of alarm improvements	I	I	I	I	I	A	A	I	I	I	I	I	
LIFECYCLE STEP - OPERATION													
Suggestion and review of alarm improvements			A	C	A	C	C	C	R			I	
Operator Training		A	C	C	R	C	C	C			A		
Testing of alarms			A	A	R	C	C	C	R			I	
LIFECYCLE STEP - MAINTENANCE													
Implementation of instrumentation improvements			A	I	I	I	I	C	R				
LIFECYCLE STEP - MANAGEMENT OF CHANGE													
Authorization of improvements to the alarm system		I	I	I	R	A	C	R				A	
Maintenance of alarm logs and chronology			I	I	I	A	C	C		A			
LIFECYCLE STEP - MONITORING & ASSESSMENT													
Development and implementation of alarm metrics	I	I	C	C	C	A	R	C	I			I	R
Review of performance on alarm metrics	I	I	A	R	R	R	C	C	I	I	I	I	
LIFECYCLE STEP - AUDIT													
Auditing		I	I	I	I	A	C	R					

Key: R = Responsible | A = Accountable | C = Consulted | I = Informed

Define: Terminology

- People use words differently
- The Alarm Philosophy must define any alarming related terms that the Region will be using to avoid confusion

- Some terms that can have multiple meanings:
- Alarm Disable
- Alarm Inhibit
- Alarm Priority
- Alarm Class
- Alarm Type
- Alarm Group
- Active Alarm
- Highly Managed Alarm

Define: Identification

- **Define the processes used to identify alarms to be improved using alarm management**

- **Existing Sites**
  - **Get list of all configured alarms**
  - **Get copy of alarm logs for previous X months**
  - **Method for collecting feedback from Operators, Maint., etc. who use that site**
  - **List of out what stats to gather from alarm log data**
  - **Define how to the stats should be used**
- **New Sites**
  - **What groups of people need to be consulted to generate preliminary lists of alarms**
  - **Standard lists of alarms that should be considered for typical site types**
  - **What format the alarm list should be generated in (spreadsheet template)**

Define: Documentation

- Define what documentation will be used
- Format of the Master Alarm Database

- Define what information will be tracked in Master Alarm Database
- Tag, Description, Date Added, Date Deployed, Active/Deleted
- Reason for Alarm
- Alarm Priority & Reason why
- Alarm Classification & Reason why
- Defined Operator Response & Time for Response
- Defined Consequence if Ignored & Time Delay
- Alarm Setpoint, ON-Delay, OFF-Delay, Rationale for Attributes

Define: Rationalization

- Methods use for rationalization
- Team members that need to be participate
  - Who needs to participate and/or review the results

- Detailed checklist of criteria for a “real alarm”
- Method used to determine priority
- Method used to determine consequence severity

- Other attribute determination techniques:
  - Setpoint, ON-Delay, OFF-Delay, Class, HMA Alarms
- How action items from rationalization are handled

Define: Design Techniques

- It is important to design what standard alarm designs are going to be used. E.g. for a "high level alarm" this is how it works,
- Provides a "menu" of alarm types and standard designs that can be used by the rationalization teams and alarm designers to use
- Examples of alarm types:
  - Analog Alarms (absolute alarms)
  - Deviation Alarms
  - Rate-of-change Alarms
  - Discrepancy Alarms (command-disagree)
  - Hardwired Alarms
  - Calculated Alarms
  - Re-Alarming Alarms
  - Common Alarms

Define: HMI Design Techniques

- Covers minimum requirements the HMI need to have to support the alarm management program
- In the Region's case, this is written in conjunction with the "HMI Standard". HMI Standard might be updated as part of the AMP.

- Typical things to define:
  - How alarms are shown on process screens (status, type, priority)
  - How alarms are shown on process overview screens
  - How the alarm log screen is laid out, columns used, colours and flashing/not-flashing
  - When/how the operator can Ack alarms
  - Alarm response procedures and advanced workflows for alarms
  - Guidance on how to design process screens for situation awareness
  - How alarms from legacy controllers/systems are shown on HMI

Define: Implementation

- Define procedures for what workflow is to be used when alarms are to be programmed into the SCADA system, how they are checked, tested and deployed
- Done in collaboration with existing Region SCADA Standards

- Procedures to make sure alarms are programmed as per MADB
- Ensuring commissioning changes are inserted back into MADB
- Criteria when a commissioning change needs to be reviewed first

- Outline how operators need to be trained when new alarms added
- Outline what needs go into SOPs that relate to alarms
- What specific HMI alarm features Operators need to be trained on
- Training for how to use Alarm Shelving, Alarm Out-of-Service

Define: Operations & Maint.

- Define what periodic alarm training must be done for operators
- Define how often alarms should be tested and how, and by priority

- Written procedure for how to do alarm Shelving
- Limits for shelving duration based on class & priority if applicable

- Written Alarm Out of Service Procedure

- What information about the alarm system and alarms, if any, should be recorded in the Operators Log book

- If there is an incident involving an alarm, what information from the alarm system log should be analyzed and how

Alarm Out-of-Service Procedure

- **Example: A written "permit" system**

The permit should include:

- the identification of the alarm placed out-of-service (e.g., tag and alarm type),
- the class of the alarm,
- the consequence of deviation related to the alarm,
- the reason the alarm is taken out of service,
- the date the alarm is placed out-of-service,
- the name of the person requesting the alarm be placed out-of-service,
- the name of the person authorizing the alarm be placed out-of-service,
- the name of the person placing the alarm out-of-service,
- the method used to place the alarm out-of-service,
- alternate protection for the consequence, if necessary,
- the date the alarm is returned to service (filled out later), and
- the name of the person returning the alarm to service (filled out later).

Define: Training Requirements

- Who needs training and when?
  - Operators
  - Control Room Operators
  - Maintenance
  - PCS Group

- What training is done when new site is deployed
- What changes to existing system necessitate additional training
- How often is periodic refresher training needed

Define: Measuring Performance

- What metrics (KPIs) are tracked
- How often they are measured
- Written targets for each metric

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

Figure 8 - Alarm Performance Metric Summary Table from ISA-18.2

Define: Management of Change

- Define Management of Change Procedures
- How changes are tracked
- Paperwork/forms if required
- How the Master Alarm Database is kept up to date
- Procedures for New Sites
- Procedures for upgrading Existing Sites

Define: Audit

- Reviews the managerial and work practices associated with the alarm system
- Review of Procedures vs. Actual Practice
- Typically only done once per year

- The Alarm Philosophy will define:
  - Audit Roles and Responsibilities
  - Audit content
  - Frequency of audits
  - Documentation needed for audits
  - Audit Interview recommendations
  - Action plans arising from audits

Define: Control System Details

- Appendices to Alarm Philosophy
- Alarm programming details for the current Modern System
  - Allen Bradley PACs
  - GE Proficy iFix HMI
- Connection/Programming Details for Legacy Sites
  - Fix32
  - Bristol
  - Which Alarm Management Features will be implemented, and which not
  - What is done when a Legacy Site is converted to the Modern System

BREAK

Post Break Review

- ISA 18.2 is an international standard for Alarm Management

- 18.2 is driven by a document called "Alarm Philosophy"
- Uses 10 work process for better design, selection and application of alarms
- Master Alarm Database is used to document/track alarm configuration

- The Alarm system is for the benefit of operators
- New Alarm Definition: Abnormal condition requiring an operator response

- Alarms are identified, rationalized, designed, and implemented

- Alarms are prioritized, classified and routed to help the right operator get them
- Alarms should only interrupt the operator for them to make immediate response
- Situational awareness should come from monitoring the process, not alarms

- Alarm records are kept, and alarm system performance is regularly measured

Part 4: “Using the Alarm Philosophy” Outline

- Identification Workflow
  - Get List of Existing Alarms
  - Gather Alarm Logs
  - Analyze the Logs to look for trends and stats
    - Bad Actor Analysis
  - Populating the Master Alarm Database

- Rationalization Workflow
  - Starting List of Alarms
  - Gathering Reference Materials
  - Team Composition
  - Outcomes of Rationalization

- ISA 18.2 Alarm Performance Guidelines
- Review of 18.2 Work Processes
- Open Discussion

Alarm Identification Workflow

- Once the alarm management program is setup, this is the first step taken to improve alarms at a site
- Get List of Alarms
- Get Copy of Alarm Log for previous 2 months (or longer)
- Analyze Alarm Log
  - Identify Bad Actors – pick top 10-20 most frequent alarms
  - Calculate alarm metrics to establish base line of alarm performance
  - Establish baseline that you will be improving from
- Put the list of Alarms into a Master Alarm Database Template
- Mark off list of obvious “bad actor” alarms to be rationalized first

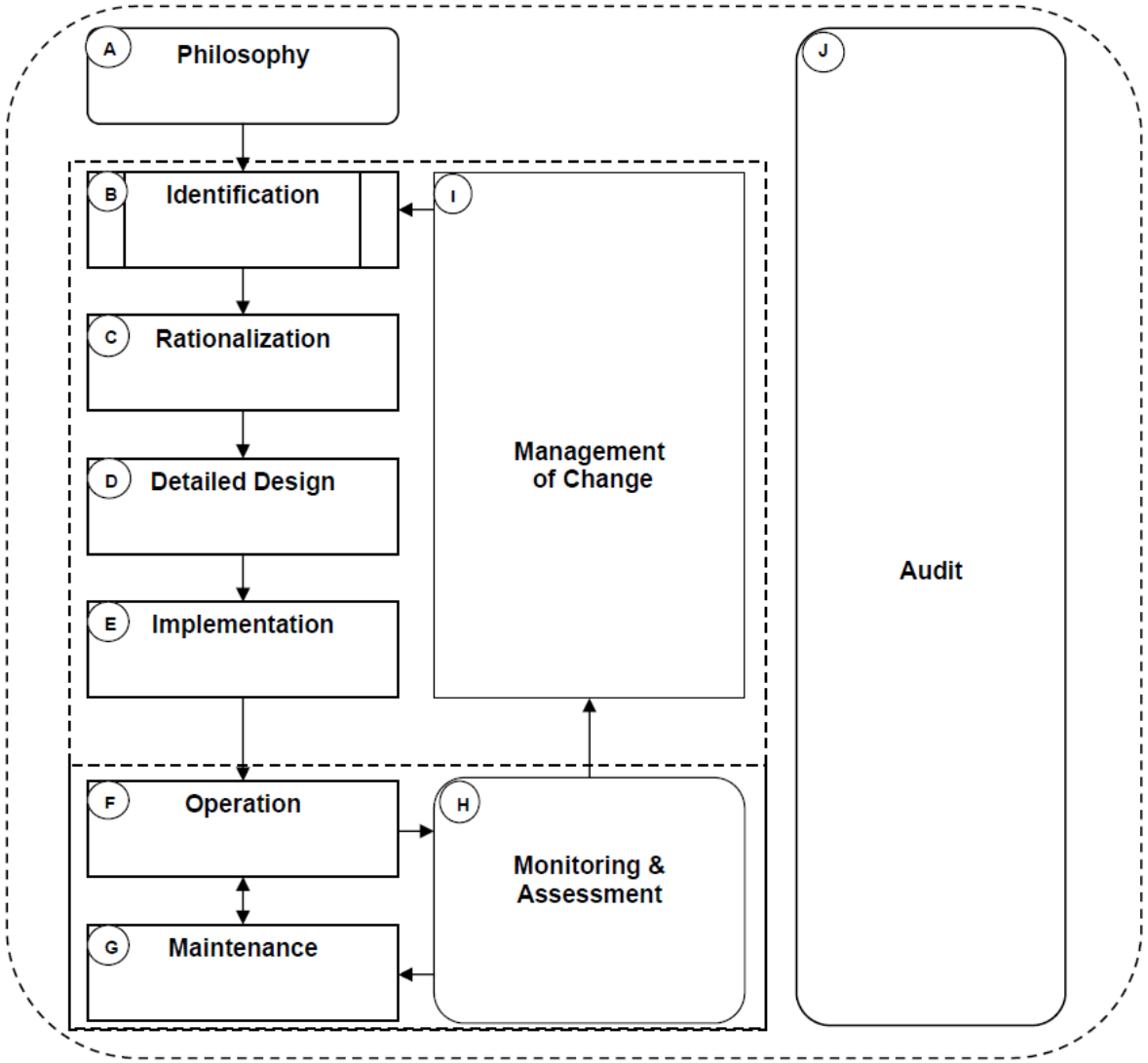
Alarm Rationalization Workflow

- Start with the completed MADB List from Identification
- Assemble reference documents:
  - Site Floor Plan, P&IDs, Process Narratives, SOPs, Design Briefs, etc.
- Assemble the team to rationalize the alarms
  - Reps from: Operations, Management, Maintenance, PCS Group, Compliance, Engineering, Process, Team Leader
  - Facilitator to help process
- Meet and review each alarm one at a time
  - Consequence if ignored? How severe/important is the consequence?
  - Expected operator response
  - Is alarm duplicating another alarm
  - What should the setpoint and other alarm attributes be
  - If alarm is valid, what should its priority and class be
  - Does it qualify as a Highly Managed Alarm
- Record results into the MADB

18.2 Performance Goals

- Gold standard is max of 1 alarm every 10 minutes per operator
- Avoid “Alarm floods” – more than 10 alarms in 10 minutes
- Minimal number of alarms that have to be shelved for long periods of time
- Regular monitoring and assessment of alarms
- Often when organizations embark on alarm management, they find that up to 70% of their existing alarms are not needed or can be assigned to the lowest non-visible priority

18.2 Work Processes Review



18.2 Benefits Summary

- **Cuts down the number of alarms to a manageable/more-useful level, so that operations can focus running sites effectively**

- **Provides a framework for managing the alarm system as a whole**
- **Ensures that alarms reflect the needs of stakeholders**

- **Focuses the alarm system on helping operators**
- **Significantly reduces the number of nuisance alarms**

- **Provides mechanism for continuous improvement of alarm system**

- **Ensures that all active alarms are documented, and their configuration and reason for existing has been reviewed and recorded**

- **Management of Change and Regular monitoring to ensure performance**

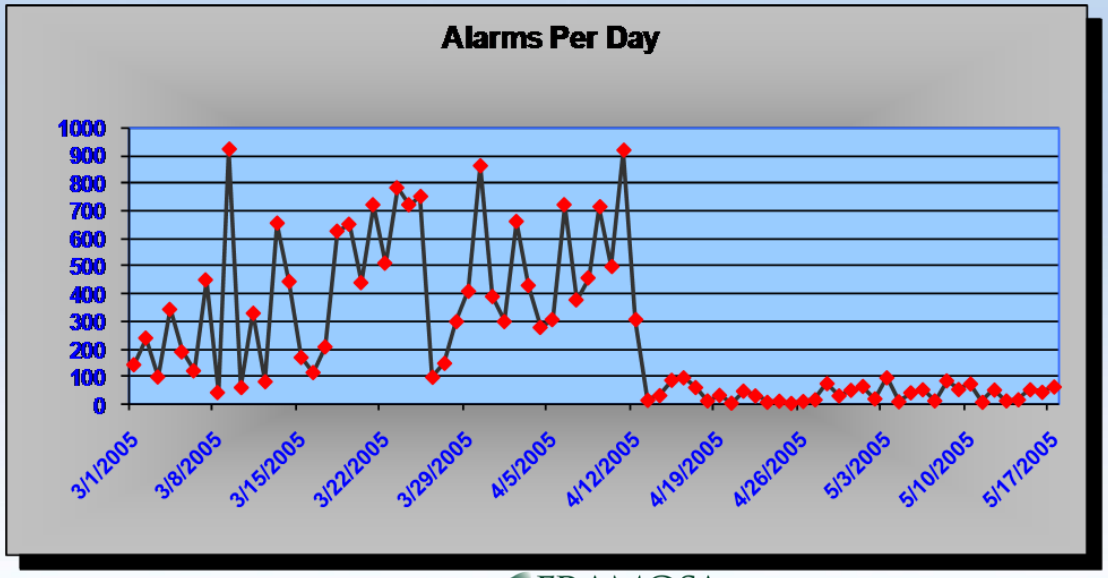
18.2 in a Nutshell

ANSI/ISA-18.2-2009,

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 requiring a response.*

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)

Exercise

Exercise 1 – Sewage Lift Station

- **Identify Possible Alarms**
- **Rationalize Each Alarm**

- Sewage Lift Station
- 12 m deep wet well, Fills at a rate of 1 m/hr in worst case scenario
- 4 equally sized pumps, 1 pump can pump at 0.25 m/hr
- Normal working levels are 1m to 5m, overflow occurs at 8m
  - Duty1Start=2m, D2 = 3 m, D3 = 4m, D4 = 4.5m, Duty Stops= 1m, 1.5m, 2m, 2.5m
- Ultrasonic level transmitter: reads 0-10m from bottom
- Hydrostatic Level Transmitter : reads 0-10m from bottom
- Float-based backup on each pump (high float start, low float stop)
- High High Alarm Float
- Generator with Automatic Transfer Switch (auto-starts on power outage)
- Fancy new PAC, with fibre connection to SCADA
- Alarm Dialer (6 channels)