Introduction to Alarm Management – An Overview of ISA 18.2 & IEC 62682

Donald G. Dunn – Principal Consultant

Donald Dunn

W.S. Nelson

Senior Consultant

ISA Fellow

ISA 18 Co-Chair, IEC 62682 Convenor

ISA Technical Assembly Chair, ISA Technology Search Committee Co-Chair

Past ISA Standards & Practices VP

If your organization needs support, Waldemar S. Nelson and Company may be able to provide assistance.

Waldemar S. Nelson and Company is a multi-discipline engineering firm with offices in New Orleans and Houston. Our firm has provided engineering services for offshore and onshore oil and gas production facilities, refineries, chemical plants, pipelines, liquids and bulk solid terminals, mining and other industries in most of the states and more than 20 countries since 1945.

NELSON's capabilities include all engineering disciplines (civil/structural, mechanical, chemical/process, electrical, instrumentation/control systems), as well as architectural, environmental and project management services. NELSON's experience includes complete design services, serving as owner's engineer, and participating on design-build teams.

- History of ISA 18.2 & IEC 62682
- Introduction to Standards
- Importance of Alarm Management
- Incidents in Industry
- Lifecycle
- Entry Points
- Alarm Management Lifecycle
    - Philosophy
    - Identification
    - Rationalization
    - Detailed Design
    - Implementation
    - Operation & Maintenance
    - Monitoring & Assessment
    - Management of Change (MOC)
    - Audit
- Getting Started, Summary, & References

- History of ISA 18.2 & IEC 62682

History of Published Alarm Documents

- Organizations developed guidance for design and maintenance of alarm systems
  - ISA formed survey committee (1955) – "Instrument Alarms and Interlocks"
  - Standard & Practices committee 18 evolved
  - ISA-RP18.1- Completed 1965
    - "Specifications and Guides for the Use of General Purpose Annunciators"
  - ISA18 and ISA67 committees released ISA-18.1-1979
    - Annunciator Sequences and Specifications
  - Honeywell forms "Alarm Task Force" that becomes the ASM Consortium™ in 1992 (funded by NIST grant and industry companies).
    - Amoco, Chevron, Exxon, Shell and Honeywell
    - Develop a vision for better response to plant incidents
  - The ASM Consortium funded EEMUA to publish "191 Alarm Systems - A Guide to Design, Management and Procurement " in 1999
    - A second edition was published in 2007 and third edition in 2013. Adopting ISA18.2 lifecycle
  - NAMUR NA 102 Alarm Management recommendation issued – 1st edition 2003, 3rd 2008
  - ISA18.2 Effort kicked off at Expo 2003
  - In 2003, the ASM privately releases the "ASM Consortium Guidelines for Effective Alarm Management Practices". Later published on Amazon in 2009

Historical Timeline

ISA 18 Begins Effort to write a Standard on Alarm Management - 2003

ANSI/ISA–18.2–2009

Management of Alarm Systems for the Process Industries

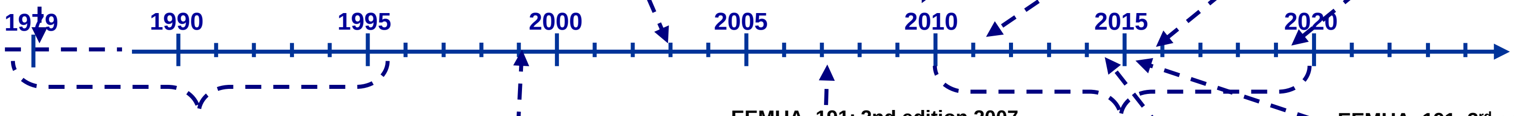
Approved 23 June 2009

API RP 1167

AMERICAN PETROLEUM INSTITUTE

18.2 - 2015

IEC 62682 Begins Update to Publish version 2 - 2019



EEMUA -191: 2nd edition 2007

EEMUA -191: 3rd edition - 2013

Impetus for Alarm Management:
1979 - Three Mile Island
1984 - Bhopal
1994 - Milford Haven
Bransby, ML and Jenkinson J., The Management of Alarm Systems, HSE Contract Research Report 166/1998 ISBN 07176 15154, First published 1998.

EEMUA -191-1999: 1st edition

IEC 62682
Edition 1.0 2014-10

IEC 62682: ISA18.2-2009 basis of this standards development. Improvements were made in clarity of language, as well as other edits for simplification.
Approved November 2014

ANSI/ISA-18 Technical Reports – 2010 - WG8 Currently in process
ISA 18.2 Technical reports:
TR1 – Alarm Philosophy
TR2 – Alarm Identification & Rationalization
TR3 – Basic Alarm Design
TR4 – Enhanced and Advanced Alarm Methods
TR5 – Alarm Monitoring, Assessment and Audit
TR6 – Alarm Systems for Batch and Discrete Manufacturing
TR7 – Alarm Systems for Packaged Systems
WG8 – Management of Alerts and Notifications for the Process Industries
JWG84.91-18 Safety Alarms and SCAI

Introduction to Standards

What is a Standard?

- Standards are voluntary documents
  - Cover specifications, procedures and guidelines
  - Goal is to ensure products, services, and systems are safe, consistent, and reliable
- Standards are often adopted by regulatory bodies
  - OSHA, EPA, FDA, HSE & etc.
  - Write regulations based on (globally agreed) standards
  - Are then enforceable
- Standards are created by SDO's (Standards Development Organizations)
  - API, IEEE, IEC, ISA, ISO, NFPA, and etc….
- Standards are everywhere and play an important role in the global economy

OSHA – Occupational Safety and Health Administration
EPA – Environmental Protection Agency
FDA – Food and Drug Administration
HSE – Health and Safety Executive

API – American Petroleum Institute
IEEE – Institute of Electrical and Electronics Engineers
IEC - International Electro-Technical Commission
ISA - International Society of Automation
ISO – International Organization for Standardization
NFPA – National Fire Protection Association

Key SDO Principals

- Produces voluntary standards
  - May become regulation
- Must follow 5 imperative principles
  - Due process, openness, consensus, balance, and right of appeal
- Types of standards
  - Based on preponderance of SHALL, SHOULD, MAY
  - Standard, Recommended Practice, Guide

ISA Standards Development

- ISA
  - Established 1945, headquartered in Research Triangle Park, North Carolina
  - Non-profit
- Creating a better world through automation
- Publishes
  - International Standards,
  - Recommended Practices,
  - Technical Reports
- Over 4,000 experts from around the world participate in more than 150 committees
- Over 2,000 companies are represented on committees
- Process is open, transparent, and balanced with no control from any industry sector or type of member (e.g., user, supplier, etc.)

International Electro-technical Commission

- IEC
  - Established 1906, headquartered in Geneva, Switzerland
  - Non-profit
- Promotes collaboration in electro technical and electronic standardization
- Publishes
  - International Standards,
  - Technical Specifications,
  - Technical Reports,
  - Publicly Available Specifications (PAS) and Guides
- Members are nominated by their countries national committee
- Process varies from IEEE, ISA and numerous other SDO's

Key Parts of a Standard

- Terms, definition and abbreviations
  - Create a common understanding between end-user, engineers, manufacturers, and service providers
- Mandatory normative requirements
  - Set of requirements which the subject of the standard MUST comply
  - Term used - shall
- Non-mandatory recommendations
  - Set of recommendations which the subject of the standard should comply
  - Term used - should
- Conditional or optional recommendations
  - Set of recommendations which the subject of the standard can optionally or conditionally comply
  - Term used - may

RaGAGEP

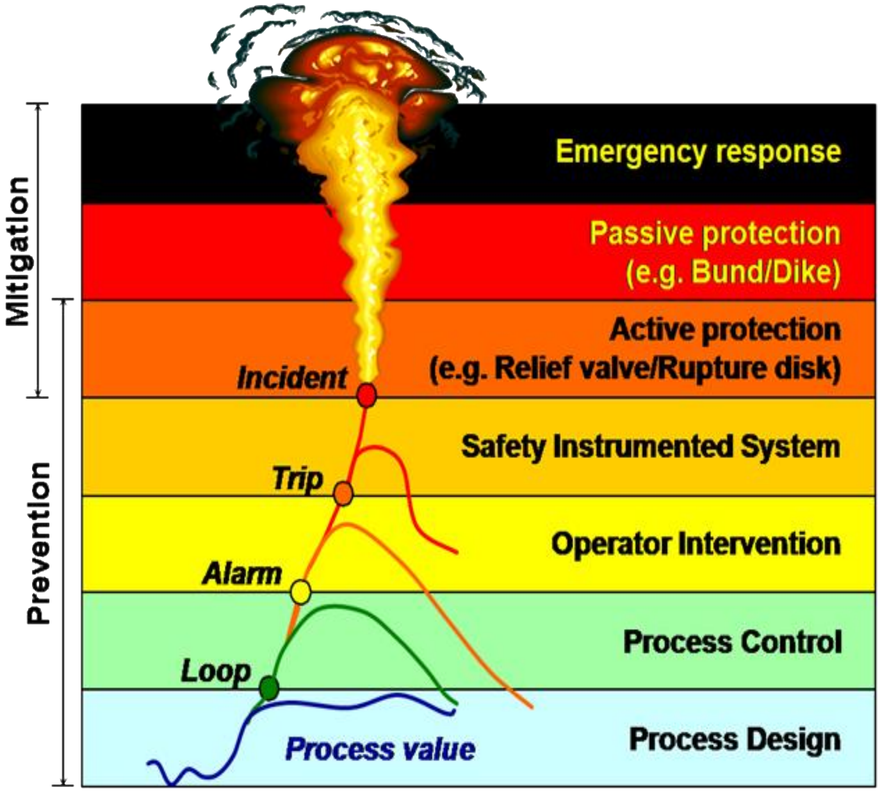
- Recognized and General Accepted Good Engineering Practice
- Regulatory bodies such as OSHA, HSE, etc. refer to “general duty” clauses
  - i.e. …..must comply with Recognized and General Accepted Good Engineering Practice
- Standards are developed based on this principle
- Standards specify “the minimum”
  - NOT “the optimal” or “most efficient” or “most effective” way

Do ISA18.2 & IEC62682 apply to you?

- Both are RaGAGEP - Recognized and General Accepted Good Engineering Practice
- OSHA and CSB have cited ISA18.2 during incident investigations
- Applies to all process types: continuous, batch, discrete or mixed
  - Alarms and alarm response is not function of the process

Importance of Alarm Management

Alarm Failures



- Alarms as IPLs and Safeguards failed to prevent incidents

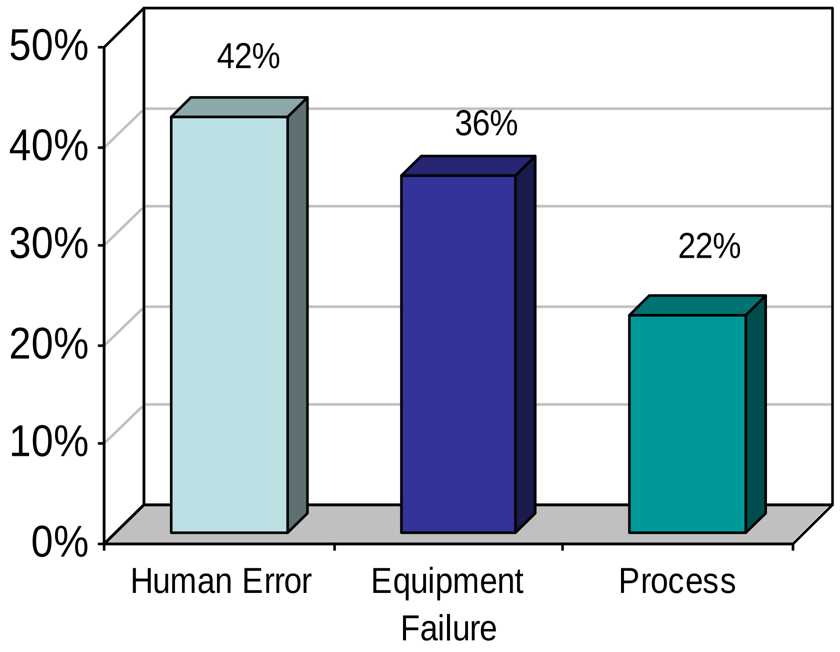
Cost of Poor Alarm Management

- Recognized as a common problem in industry.
- Estimated cost to US industry of more than 20 billion dollars/year.
- Often cited as contributing factor in industrial incidents.
- Many alarm management features built into the control system are not used.
- Many alarm systems are not monitored.

Why Human Error?

- **Weak Link**
- **Operator consolidation**
- **DCS Opportunities**

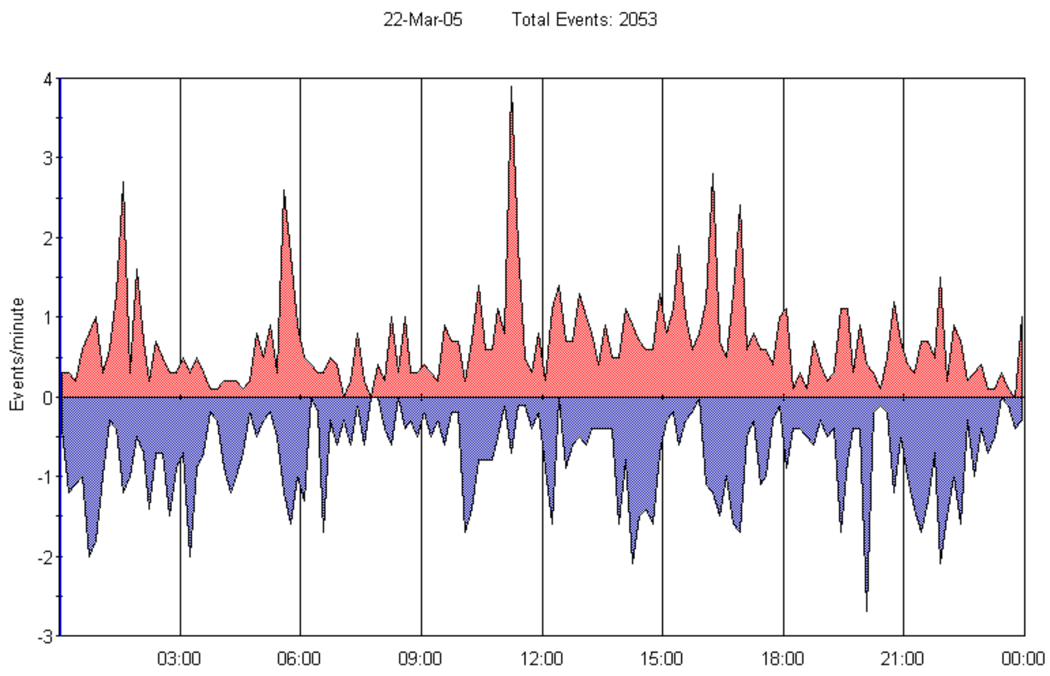
Causes of Abnormal Situations



Drivers for Improved Alarm Management

- Recognized as a common problem
  - Since the advent of Distributed Control Systems
  - Often cited as contributing factor in major industrial incidents
- Business Drivers include:
  - Safety and Environmental Performance
  - Quality
    - Often quality incidents result from missed alarms
  - Cost
    - Alarms protect equipment from damage
  - Uptime
    - Shutdowns can be prevented by responding to alarms
- Linking alarm management improvements to bottom line
  - Difficult since benefit is a reduction in upsets or incidents

Alarm Problems Today



- 983 alarms
- 1070 Operator

- Many more alarms to the operator than needed
- Many alarm management features are not used
- Many alarm systems are not monitored

Control Panel to Control Systems

- Distributed Control Systems have replaced panel control rooms
- The number of tags, or data points has increased 100X

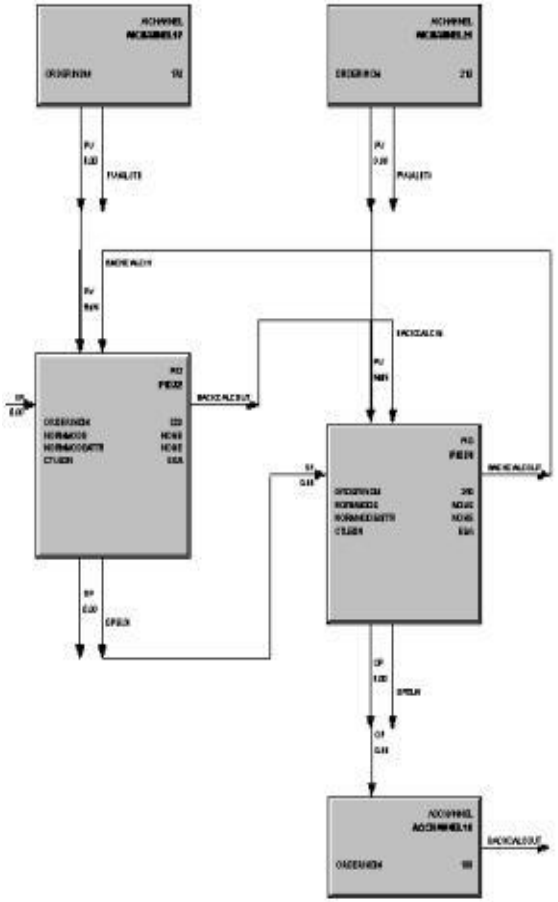
- The space to display process information has decreased
- The area of responsibility for operators has increased

Decreasing display area per operator

Increasing point count per operator

Increasing Alarm Count

- Panel alarms were space limited and it was expensive to add alarms
- DCS alarms are built into the tags, with up to 14 alarm limits
- Many alarms are set because the are “free”

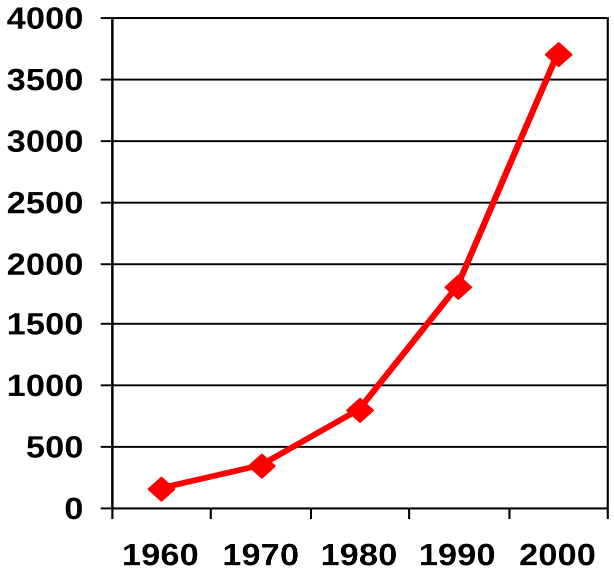


Decreasing cost per alarm

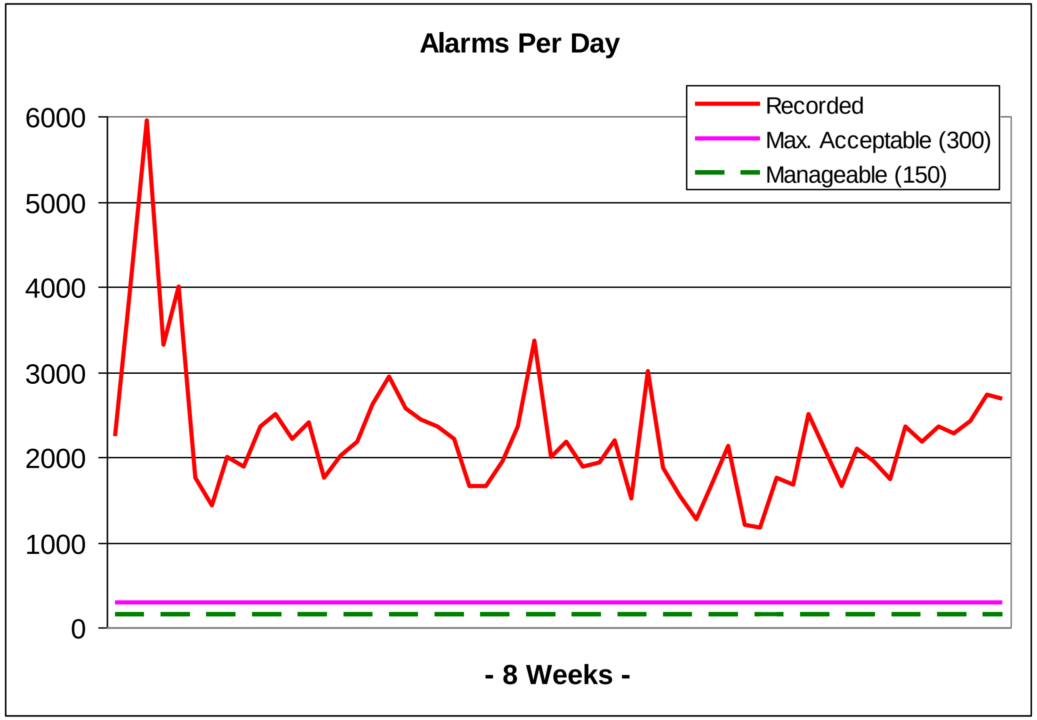
Increasing alarms per point

Alarm System Problems

The DCS Alarm Problem In A Nutshell



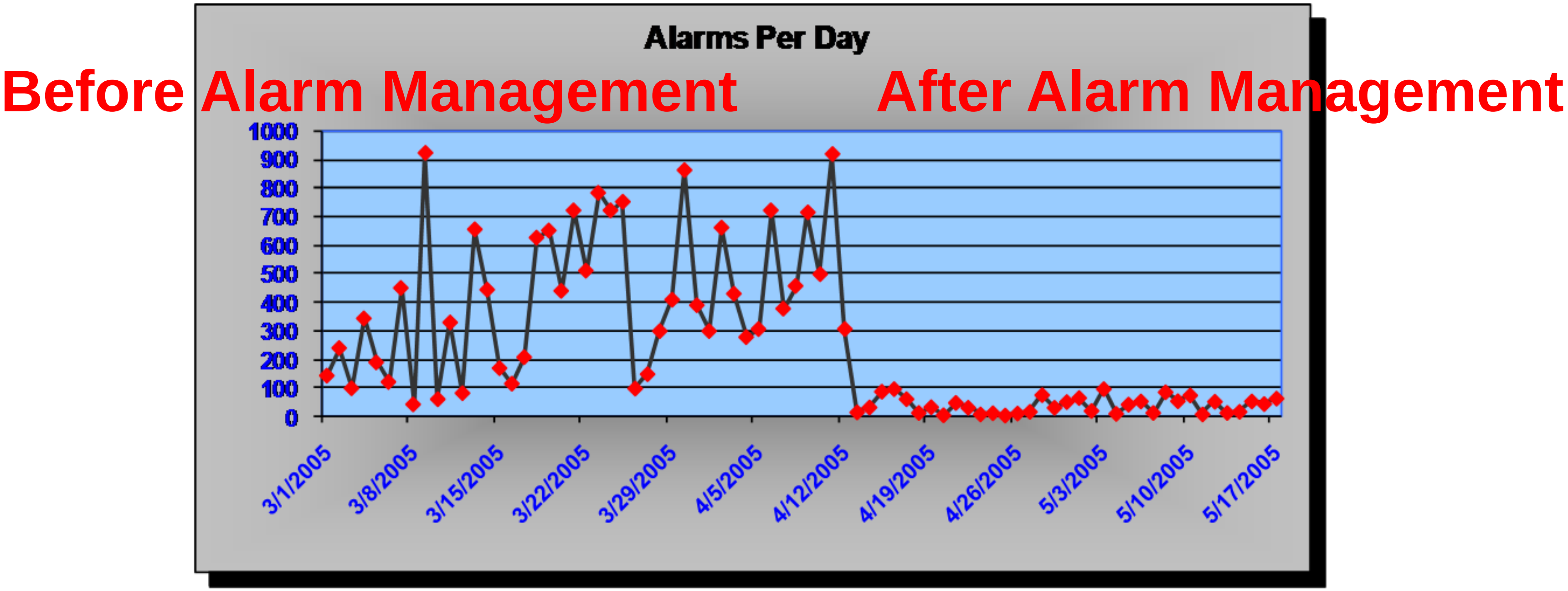
Alarms Per Operator Position Configured



Thousands of Alarm Events *Cannot* be Evaluated By The Operator!

Which alarms are safe to be ignored by the operator?

Addressing Common Problems

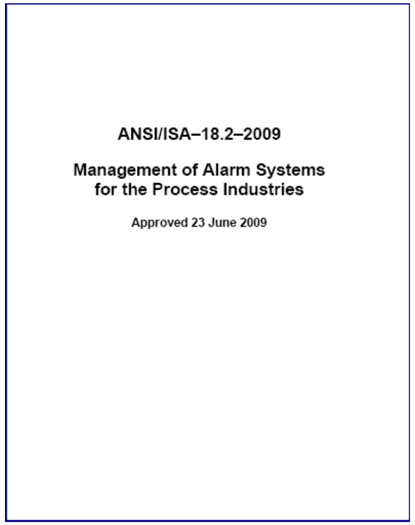


To get a different result

We need to do something <u>different!</u>

What is a Good Alarm ?

- **Alarm:** *An audible and/or visible means*
- *of indicating to the operator*
- *an equipment malfunction, process deviation or abnormal condition*
- *requiring a timely response.*
- From ISA 18.2 & IEC 62682



Key Design Principles

- Every alarm should have a defined response
- Adequate time should be allowed for the operator to carry out a defined response
- Every alarm presented to the operator should be useful, relevant and unique
- Each alarm should alert, inform and guide

If Operator Response (Action) can not be defined

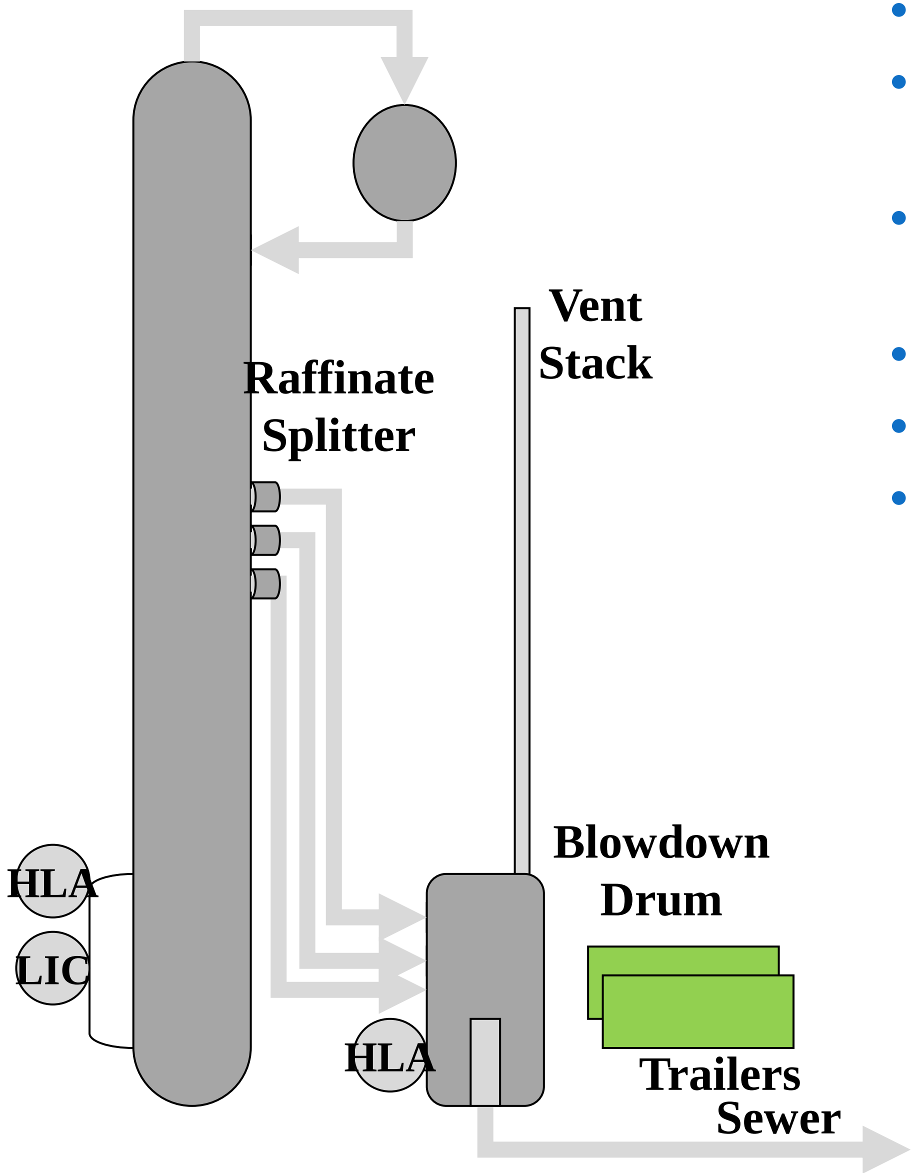
Not an alarm

Incidents in Industry

BP Texas City - Overview

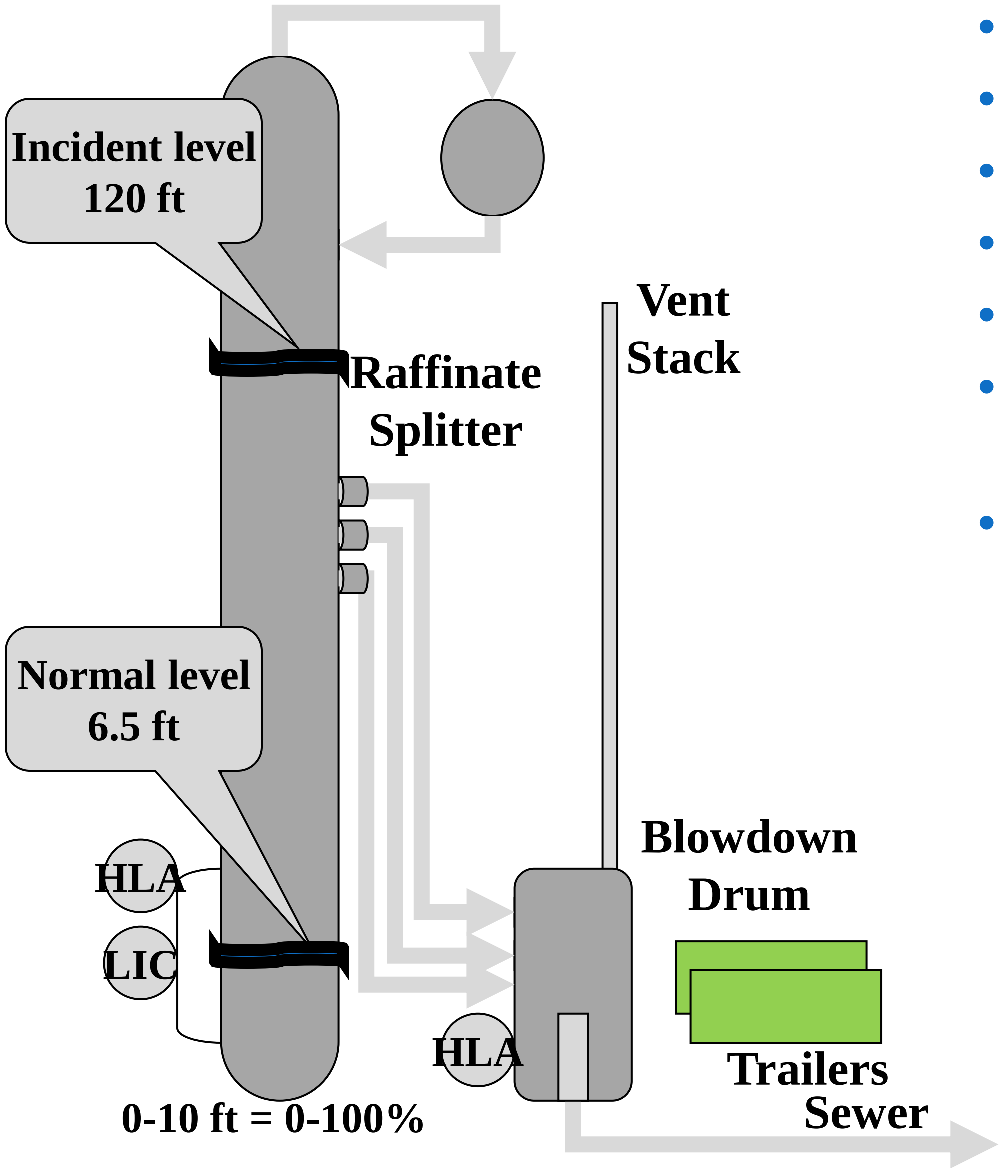
- Explosion at BP Texas City Refinery
- 1:20 PM on May 23, 2005
- 15 people were killed
- Over 100 people were injured
- Isomerization unit processing hydrocarbons

BP Texas City - Process



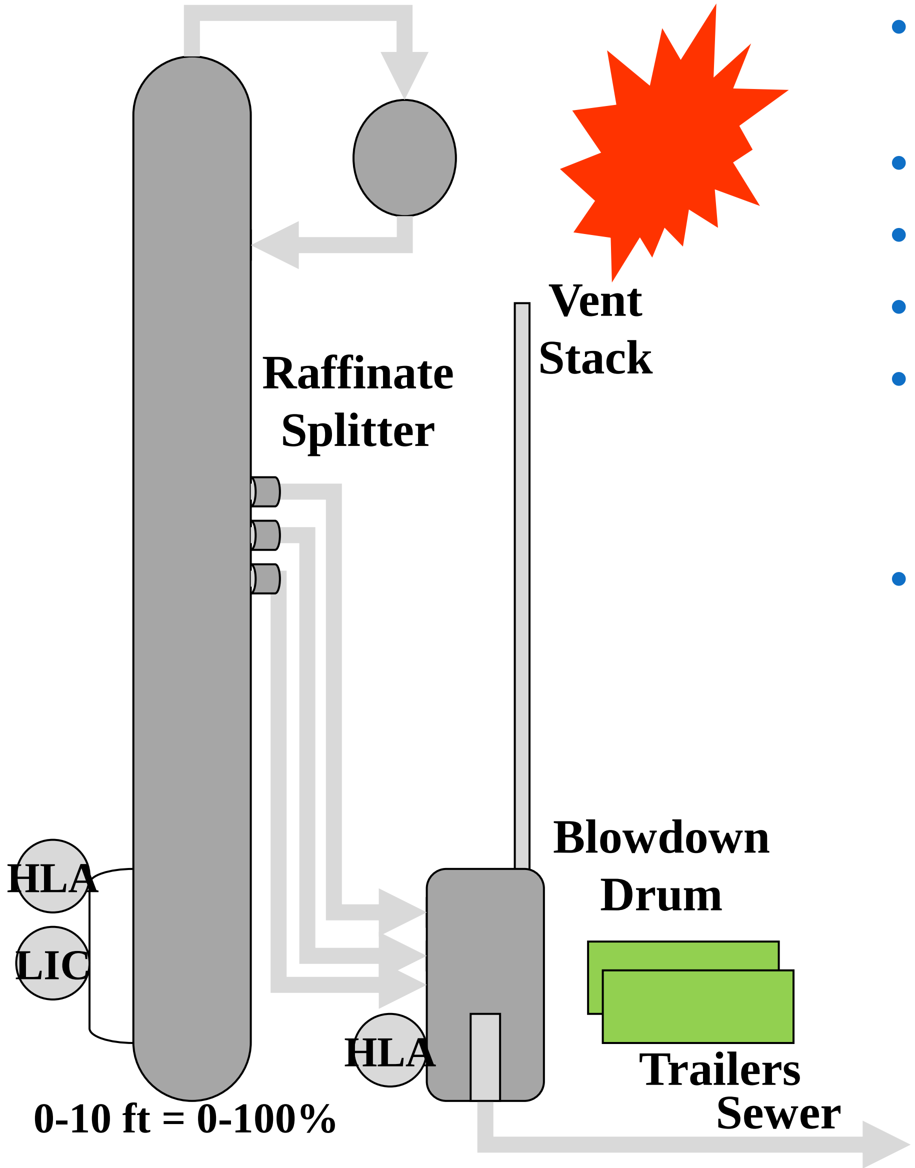
- 164 ft tall Raffinate splitter column
- Separates extremely flammable hydrocarbons like pentane and hexane
- Column has 3 relief valves at 40 PSIG that vent to a 1950s vintage blowdown drum
- Blowdown drum vents via 114 ft stack
- Blowdown drum drains to a sewer
- Trailers housing contractors are located 100-150 ft from unit

BP Texas City - Incident



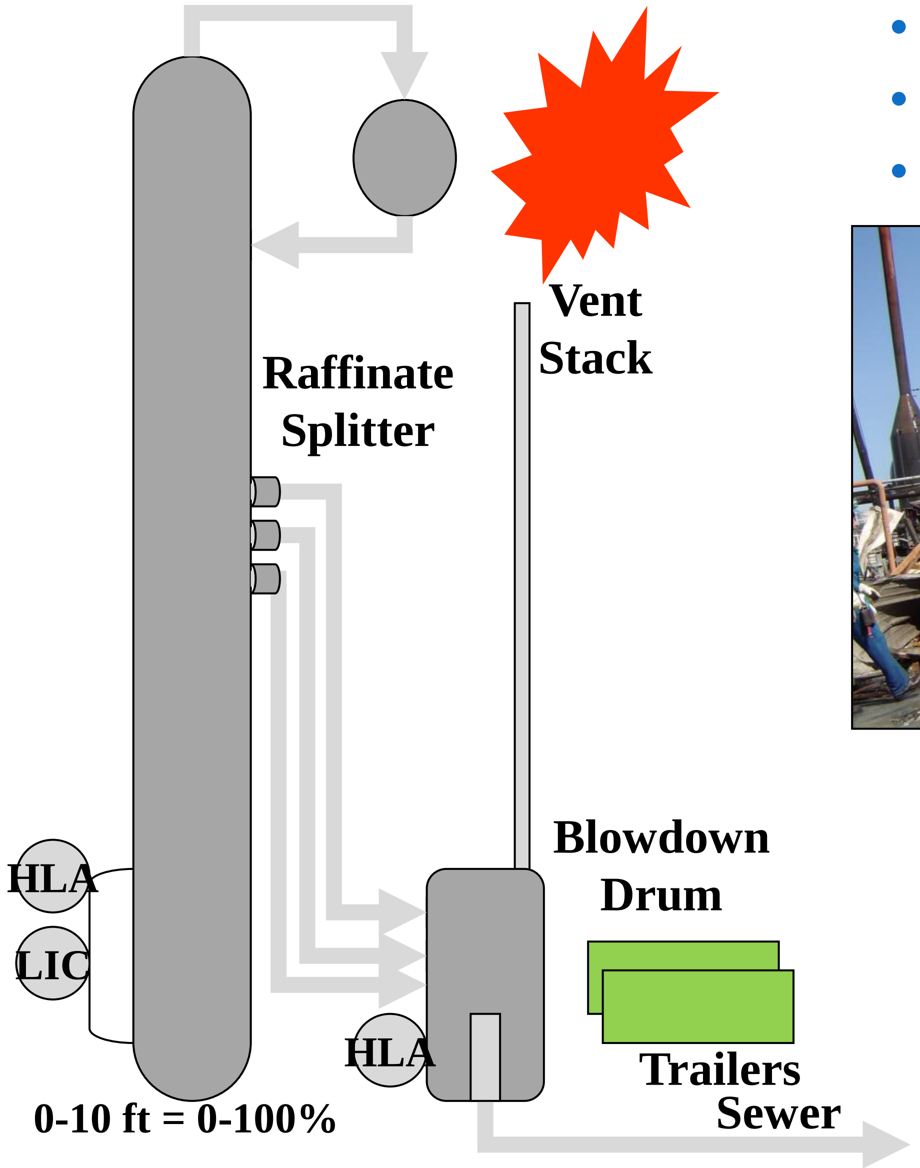
- Column startup after maintenance shutdown
- Start-up was abnormal
- At 3:05am, high column level alarm at 72%
- Level soon at 100% or 10ft
- Redundant high level alarm @10 ft did not sound
- From 7:30 am to 1:20pm level drifts down from 100% to 77%
- Actual level estimated at 120 ft at the time of the incident

BP Texas City – Incident (2)

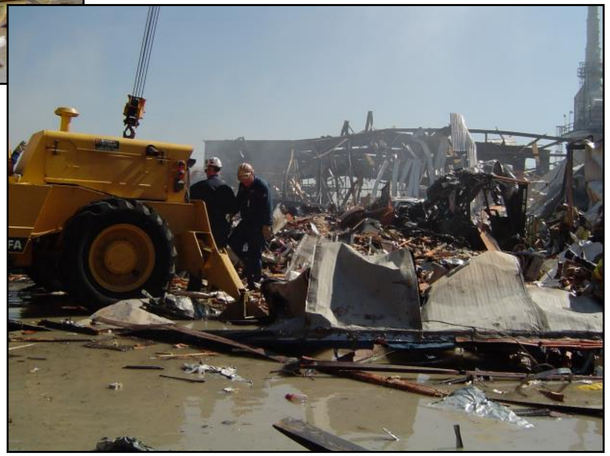


- Column pressure spiked from 20 PSIG to 60 PSIG. Reason still unknown
- The relief valves opened for 6 minutes
- The blowdown drum high level alarm did not sound
- Hydrocarbons flow into the sewer
- A large volume of hydrocarbons erupts in a geyser like fashion from the vent stack, forming a large vapor cloud
- The vapor cloud ignites from one of many possible ignition sources

BP Texas City - Summary

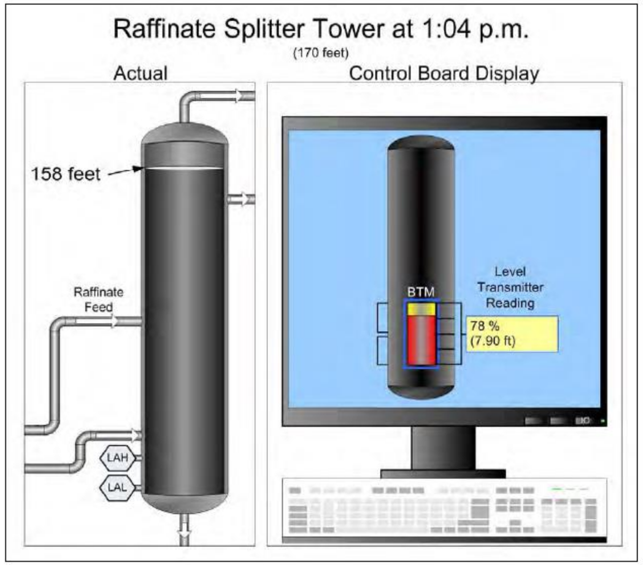


- 15 people in the trailers are killed in the explosion
- There may have been as many as 5 explosions
- The sewer also ignites



BP Texas City

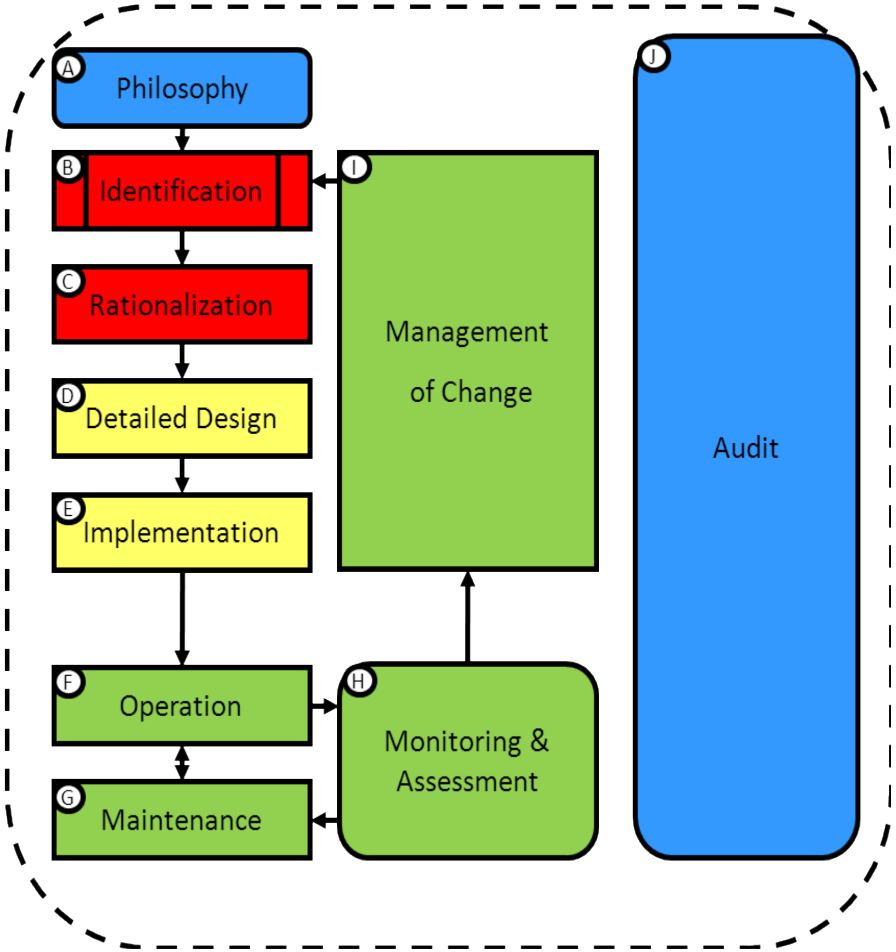
- Restart of an Isomerization Unit after turnaround
- Overfill Tower / KO Drum leads to release
- Explosion / Fire killed 15 people, injured 180 more, and cost $1.5B



	Facts from Incident	Failure Mechanisms: Measurement	Detect	Diagnose	Design	Situation Awareness
1	Tower level instrumentation indicated level was decreasing when it wasn't			*Incorrect Diagnosis*		*Errant Mental Model*
2	Tower redundant high level alarm did not activate	*Instrument Failure*	*Instrument Failure*			
3	Operator displays did not show imbalance of flows in & out of tower		*Poor HMI Design*		*Poor HMI Design*	*Errant Mental Model*
4	Operators not trained to handle abnormal situations during startup			*Insufficient Training*		*Errant Mental Model*
5	Process unit was started with malfunctions in key instrumentation					

Alarm Failure Mechanisms

- Relevant stages:
  - Rationalization
  - Design
  - Operation
  - Maintenance
- Different Failure Mechanisms associated with each Stage



Summary of Incident Analysis

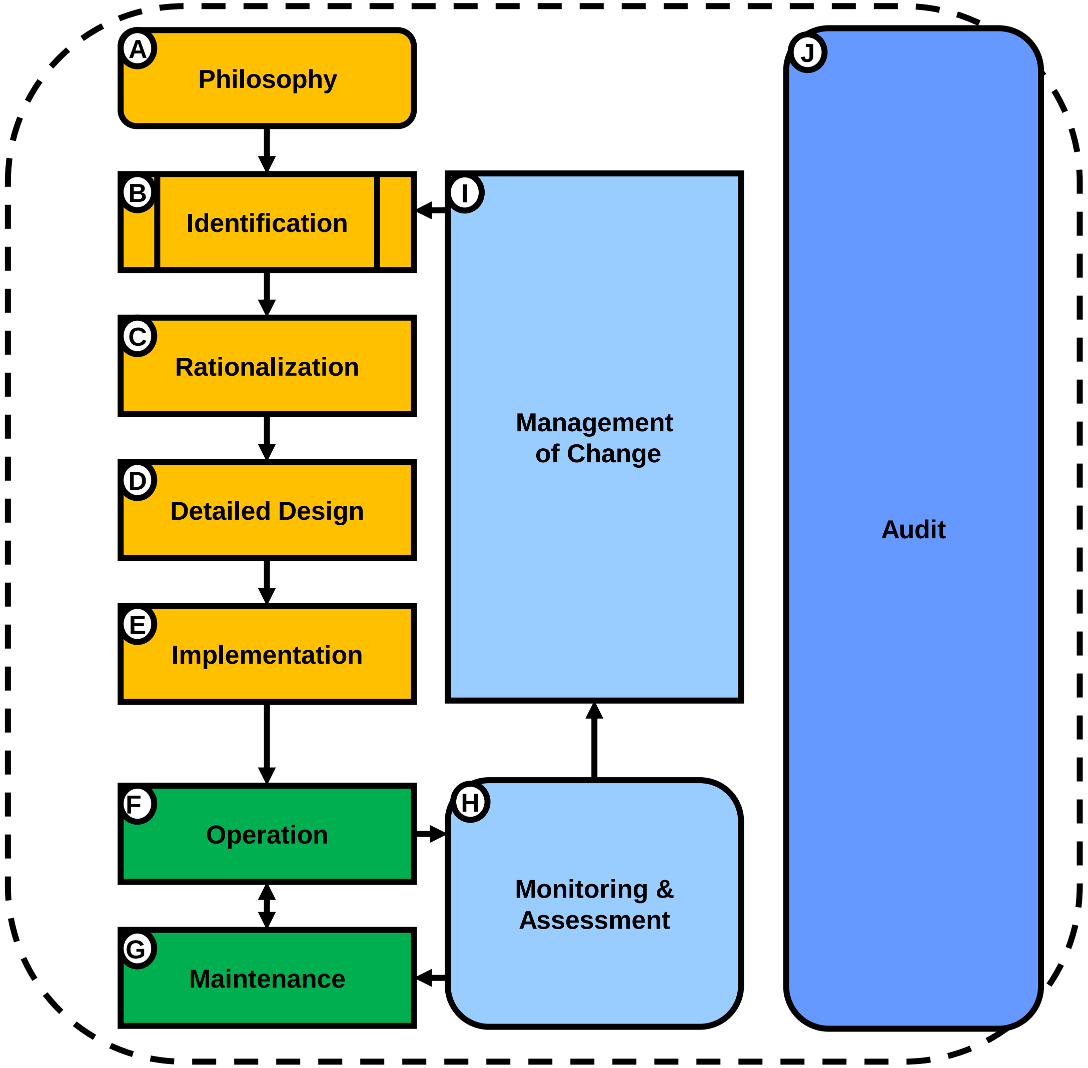
	Failure Mechanisms (FM)								Situation Awareness (SA)								
Incident	Rationalization	Design	Measurement	Detect	Diagnose	Respond	FM Totals		Attention Tunneling	Requisite Memory Trap	Workload, Anxiety, Fatigue...	Data Overload	Misplaced Salience	Complexity Creep	Errant Mental Models	Out-of-the-Loop	SA Totals
1		X		X	X		3				X	X			X		3
2		X	X	X	X		4								X		1
3		X	X	X			3								X		1
4	X				X		2		X						X		2
5	X				X		2								X		1
6					X		1								X	X	2
7					X		1		X			X					2
8					X		1								X		1
9					X		1					X		X	X		3
10		X		X	X		3								X		1
11		X	X	X			3		X			X					2
12					X		1		X			X					2
	2	5	3	5	10	0	25		4	0	1	5	0	1	9	1	21
% of FM/SA Total	8%	20%	12%	20%	40%	0%			19%	0%	5%	24%	0%	5%	43%	5%	
FM/SA % of Incidents	17%	42%	25%	42%	83%	0%			33%	0%	8%	42%	0%	8%	75%	8%	

Alarm Management Lifecycle

Alarm Management Lifecycle

ISA-18.2 & IEC 62682 Lifecycle:

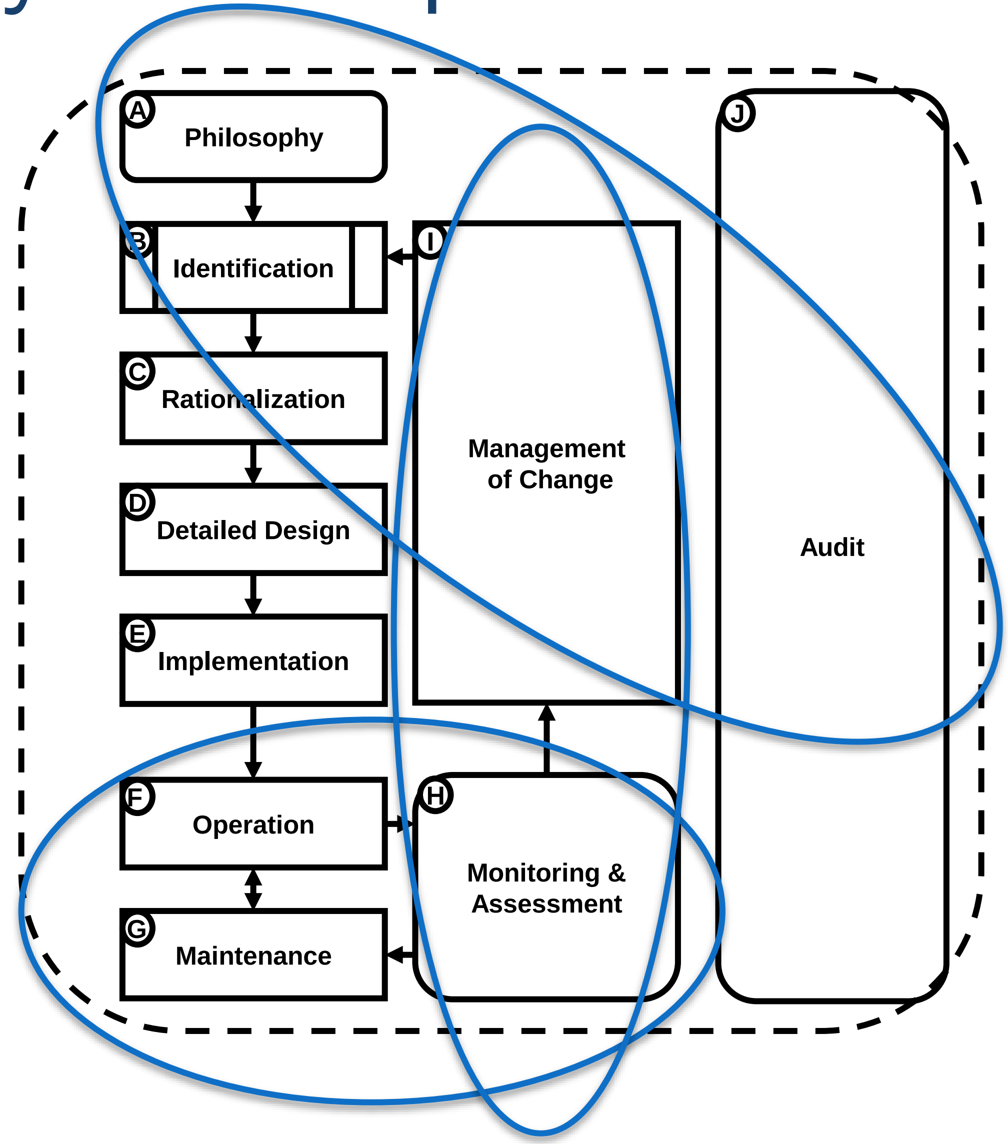
- Includes practices to solve the common alarm problems
- Includes practices for new facilities and existing plants
- RAGAGEP
- Builds on the work of ASM and EEMUA



- ASM = Abnormal Situation Management Consortium
- EEMUA = Engineered Equipment and Materials Users Association

Alarm Management Lifecycle - Loops

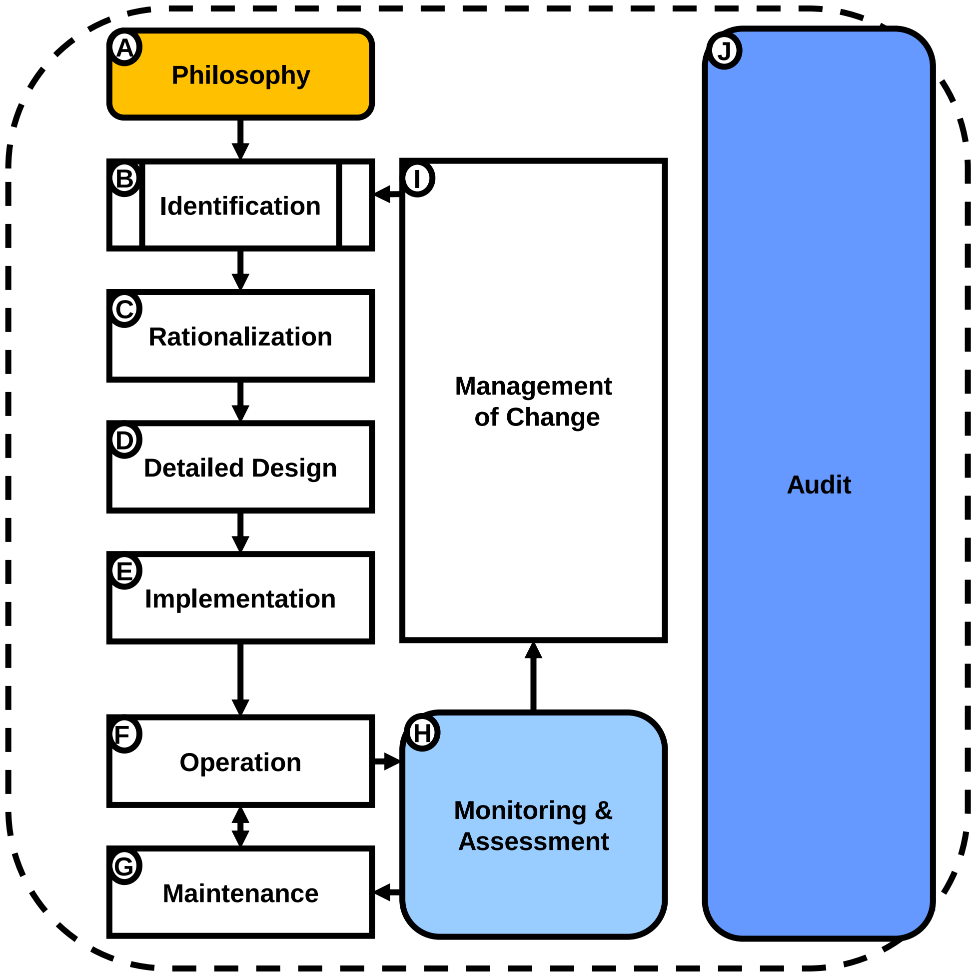
- Monitoring and maintenance loop
  - Daily or weekly process of analyzing the monitored data
    - Determine if unauthorized changes have been made
    - Instruments in need of repair
    - This process can be simple or very complex depending on implementation
- Monitoring and management of change loop
  - Less frequent, but necessary process
    - Identify changes to the alarm system based on analysis of the monitored data
    - Nuisance alarms and alarm floods identified
- Audit and philosophy loop
  - Periodic execution audit on alarm philosophy and procedures
    - Improvements in alarm clarity
    - Changes to the processes and alarm philosophy



Entry or Starting Points

Entry or Starting Points

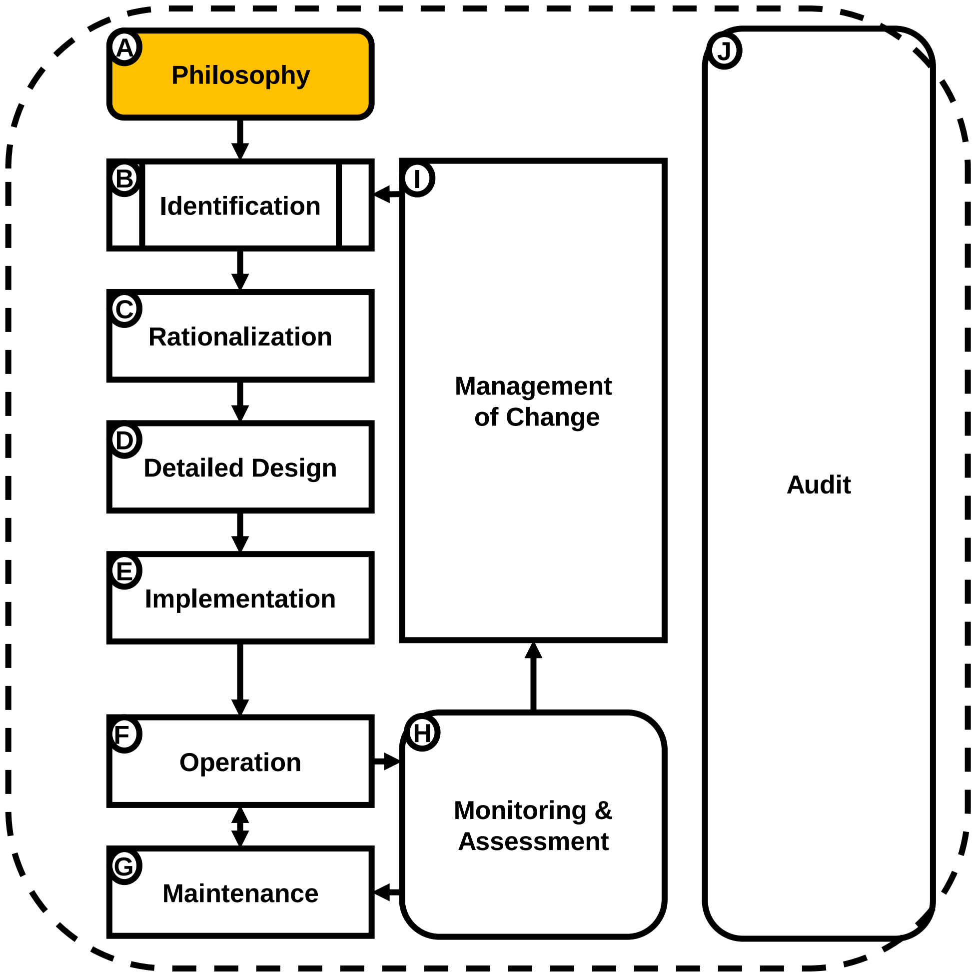
- Development of an alarm philosophy is the most common starting point
- Monitoring can be starting point to develop management support
- Some organizations conduct benchmarking by initial audit which highlights issues



Philosophy

Alarm Management Philosophy

- Guide for all alarm management activities at corporate/site
- Written philosophy is required
  - To maintain an alarm system over time
- Typically the first step for a new facility
  - Recommended starting point for new facilities
- Existing plants typically do not start at this step
- Required document per ISA-18.2 & IEC 62682
- Key Deliverables Includes:
  - Definitions
  - Performance goals
  - Roles and responsibilities
  - Methods for rationalization activities



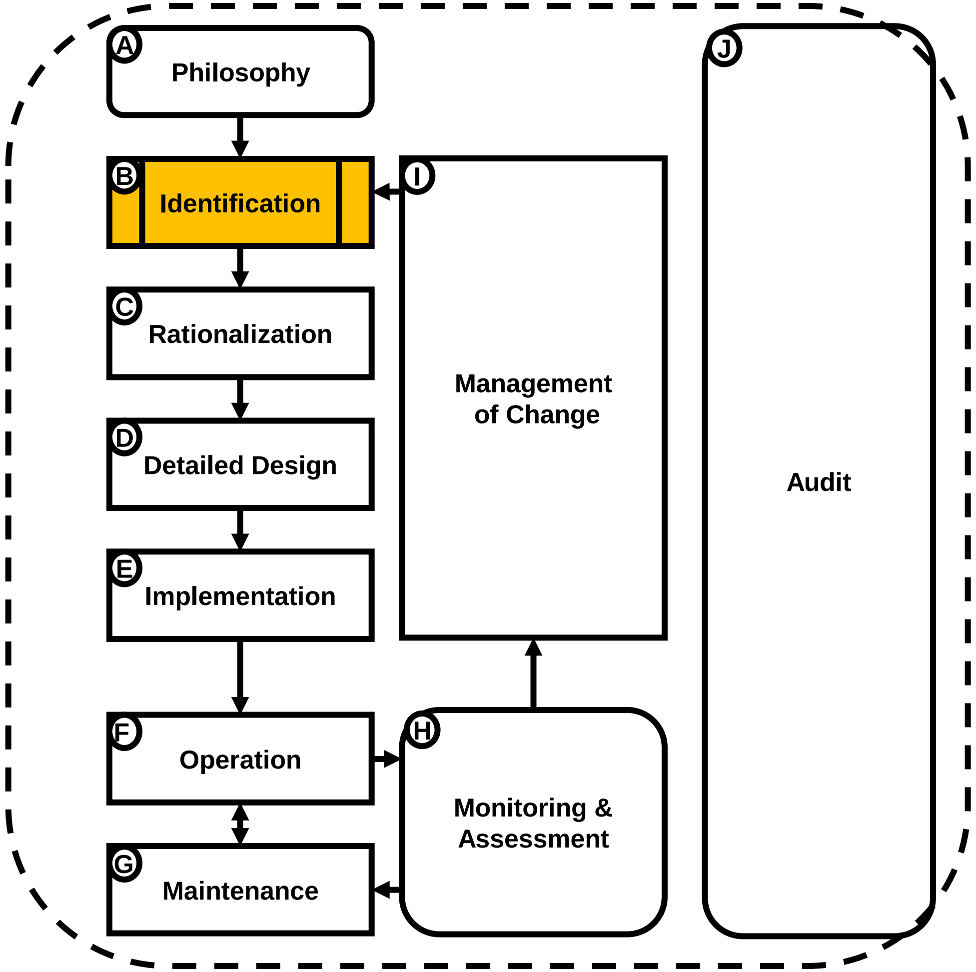
Philosophy - Purpose

- Purpose to PROVIDE guidance for:
  - Consistent and safe approach to alarm management
  - Alarm management lifecycle activities per stage
- Without an alarm philosophy document, alarm system improvements are not sustainable
- Alarm philosophies can vary per site

Identification

Alarm Management Identification

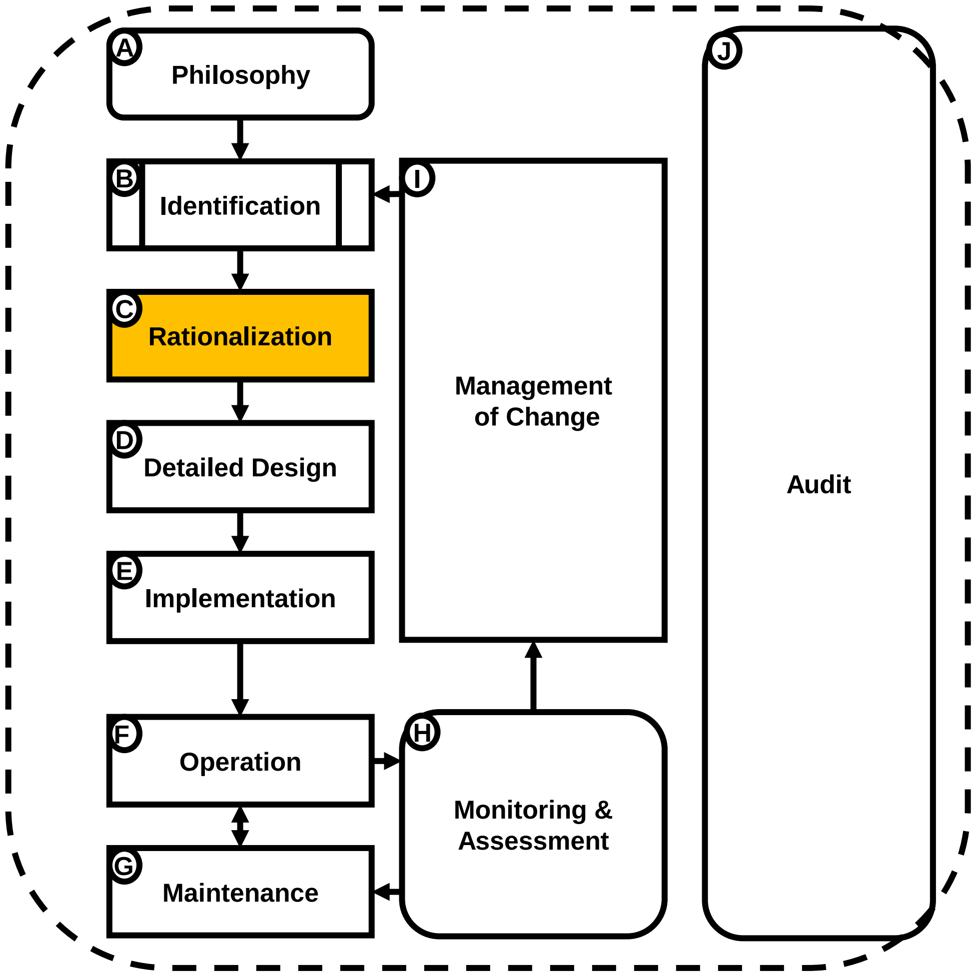
- Potential alarms are identified through many processes:
  - Functional descriptions
  - P&ID reviews
  - Process Hazard Reviews
  - Operating procedure reviews
  - Quality reviews
  - Incident investigations
- Potential alarms until they are rationalized
- Alarms are not prioritized during identification
- Highly Managed Alarms should have documented identification source



Rationalization

Alarm Management Rationalization

- Potential alarms are reviewed, rationalized, and documented
- Classification and prioritization are included in rationalization
- This STEP is the most important part of the lifecycle and requires the most resources
- Common alarm problems solved
  - Stale alarms
  - Alarms without response
  - Alarms with the wrong priority
  - Redundant alarms

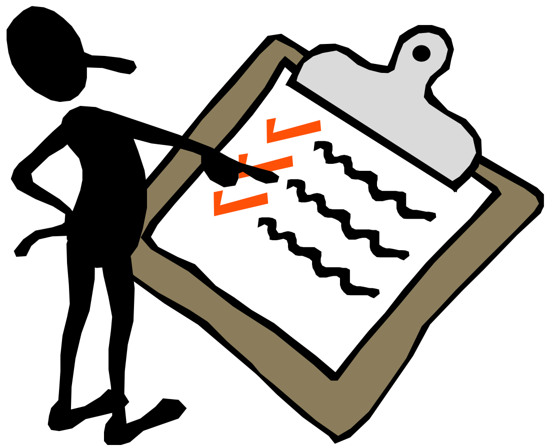


Alarm Management Rationalization – The Why

- Develop consistent alarm system
  - Each alarm must be reviewed against the principles & guidance of alarm philosophy
- Rationalization is review process
- Alarm philosophy must be in place before rationalization
- Result is master alarm database that documents each alarm

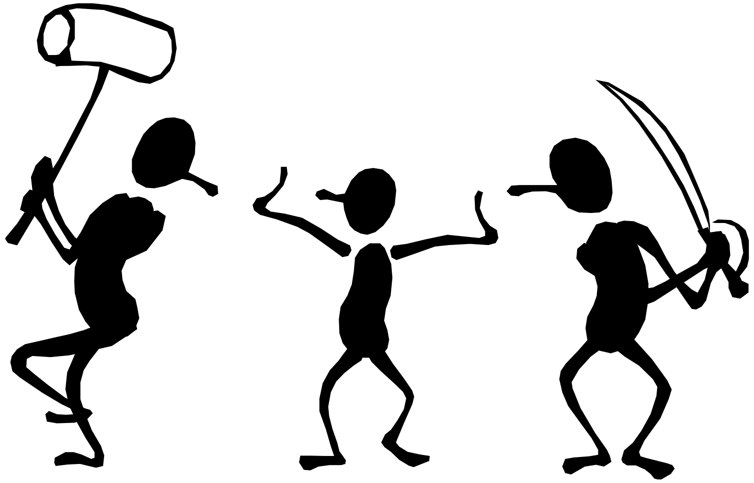
Alarm Management Rationalization – The What

- Review / analyze / justify what points should be alarms
- Goal - to create the minimum set of alarms needed to control the process and keep the plant safe
- Define / document alarm attributes (limit, priority…)
- Team activity typically facilitated by an alarm expert (similar to a HAZOP)
- Tools make the process go quicker and make it easier to document results



Alarm Management Rationalization – The Activities

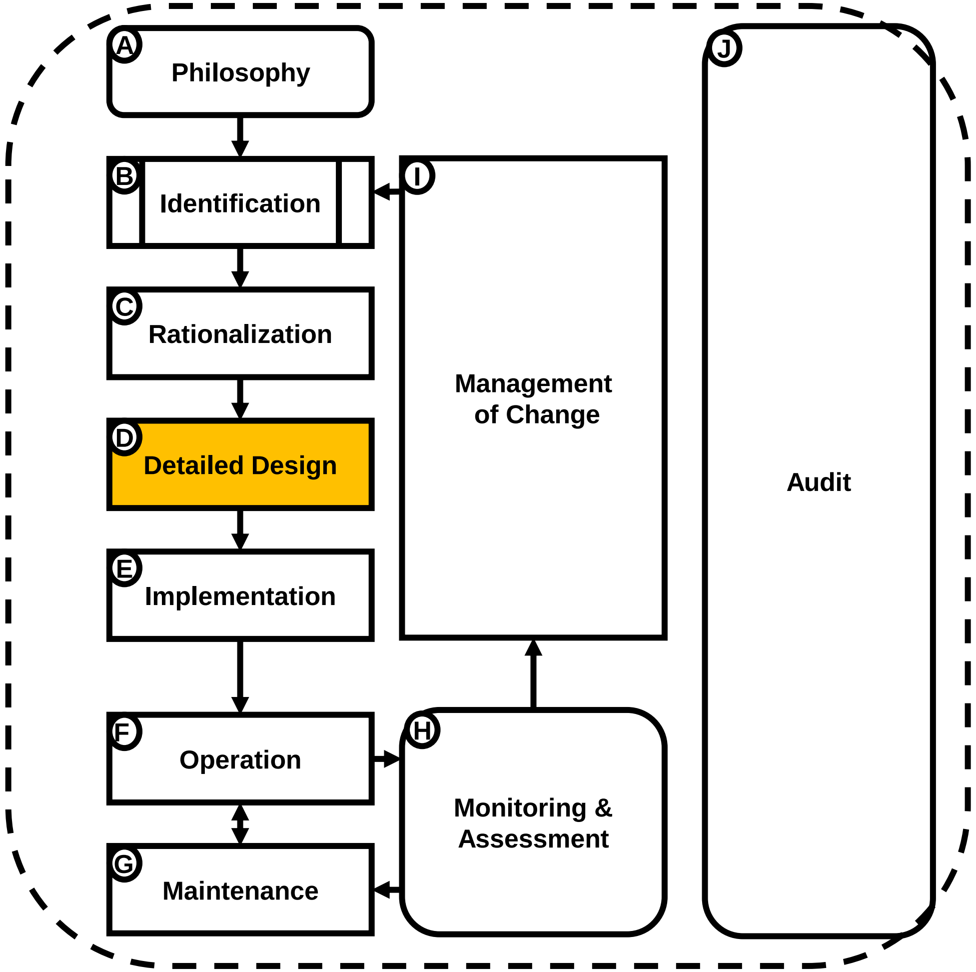
- Alarm Objective Analysis
  - The alarm basis, consequence, operator action, and response time
  - Rejected alarms
- Setpoint Determination
- Alarm Classification
- Alarm Prioritization
- Advanced Alarm Requirements
  - Designed suppression conditions
- Alarm Documentation
  - Master alarm database information



Detailed Design

Alarm Management Detailed Design

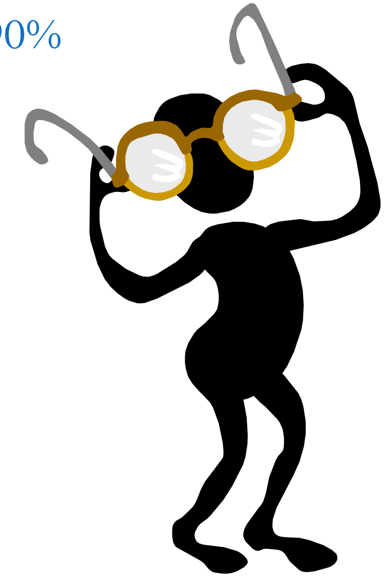
- Three parts of design:
  - Basic alarm design
    - includes alarm types, deadbands, and delays
  - HMI design, which includes indications and summaries
  - Advanced alarm design, which includes designed suppression
- Good alarm design prevents many typical alarm problems
- HMI design can have a substantial impact on alarm effectiveness
- Common alarm problems solved
  - Nuisance alarms
  - Stale alarms
  - Alarm Floods
  - Suppressed alarms
  - Redundant alarms



Alarm Management Detailed Design – Basic Alarm Design

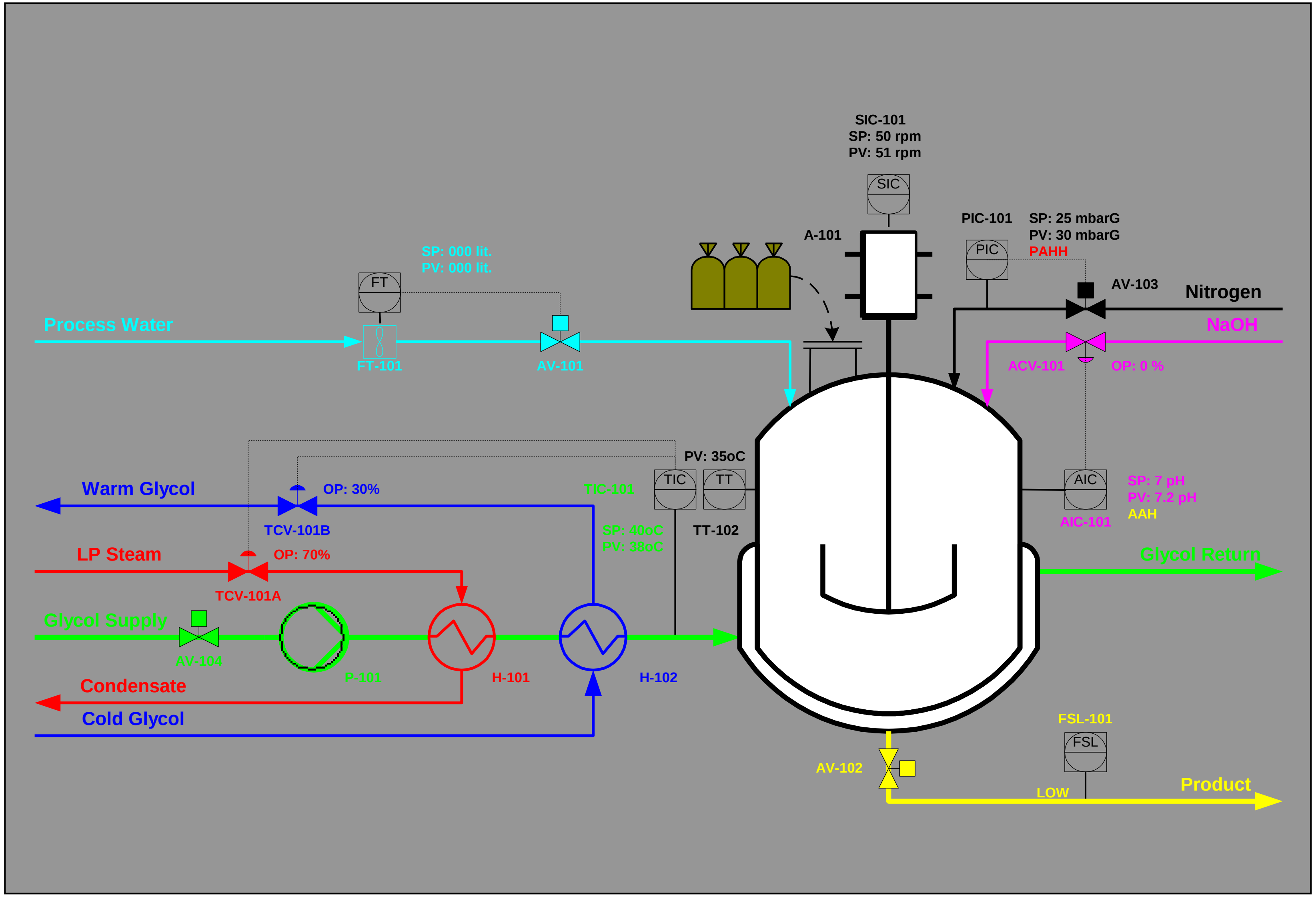
Requirements & Design considerations for configuration of alarms

- Poor Configuration practices cause a significant number of alarms
  - >50% of standing alarms are usually motors (pumps, fans, etc) not running
  - Redundant transmitters are usually allowed to generate redundant alarms
  - Deadbands and time delays are often under utilized
    - ASM Study: Configuration of deadband and time delays reduced alarm load by 45-90%



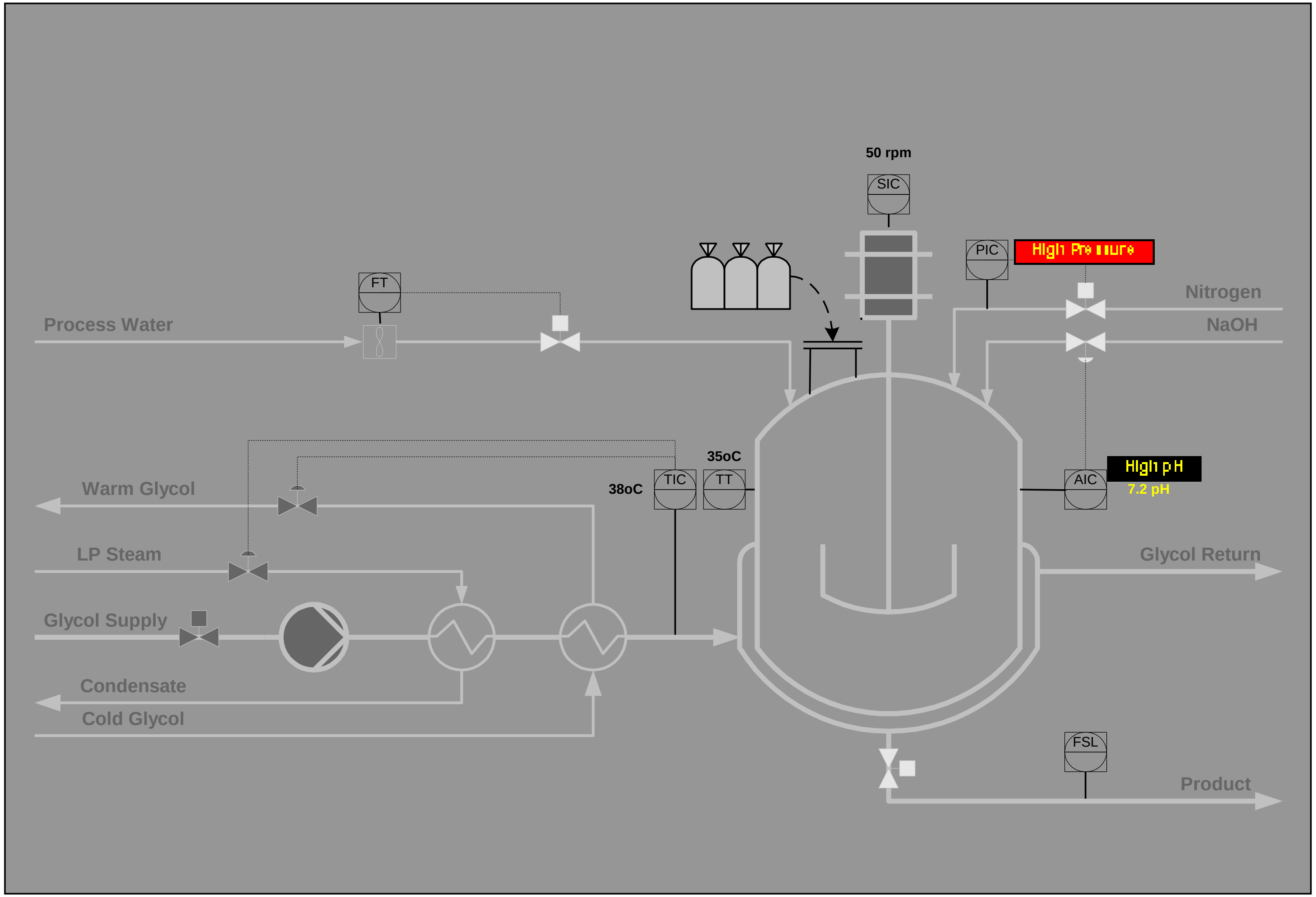
Alarm Management Detailed Design – HMI example

Do you see the alarms?
Do you see the alarms?
Do you see the alarms?
Do you see the alarms?
Do you see the alarms?
Do you see the alarms?
Do you see the alarms?



Alarm Management Detailed Design – HMI example

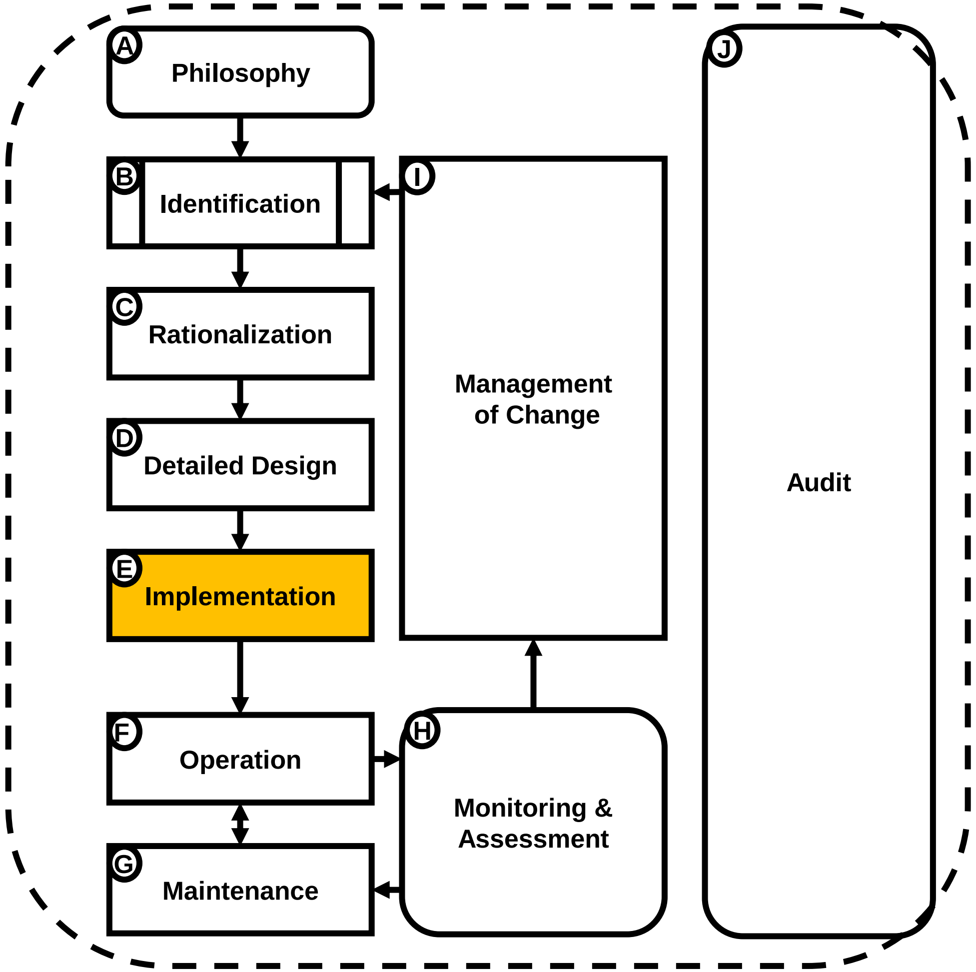
Do you see the alarms?
Do you see the alarms?
Do you see the alarms?
Do you see the alarms?
Do you see the alarms?
Do you see the alarms?
Do you see the alarms?



Implemenation

Alarm Management Implementation

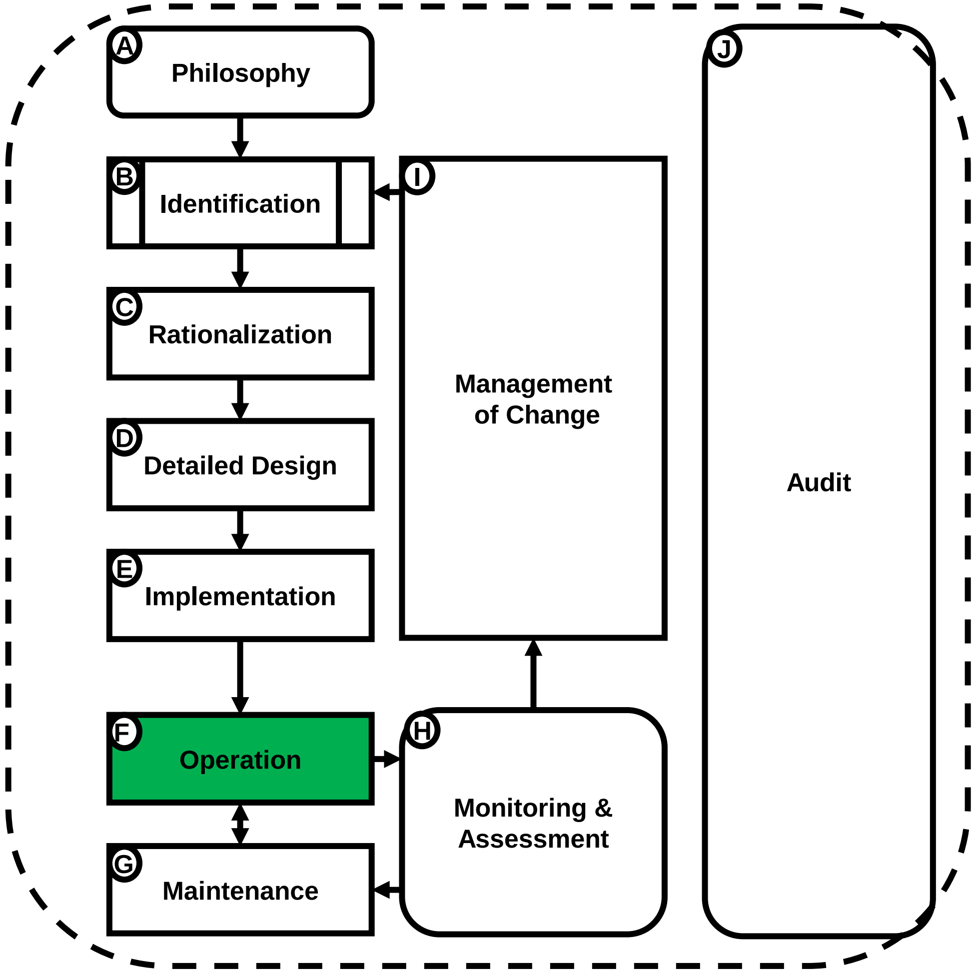
- Implementation is process of putting alarm or alarm system into operation
- Training and Testing are key activities
  - Different alarm types require different levels of testing and training
- Implementation is transition from design to operation
  - Operator actions are documented in operating procedures
  - Initial operator training on alarm system design or modifications
  - Initial testing for alarms or modifications
- Training and testing requirements vary by class



Operation

Alarm Management Operation

- Operation is stage where alarm is in service and performing its function
- Shelving and removal from service are essential processes to define for operations



Alarm Management Operation – Operating Procedures

- Operating procedure system should contain information on alarms documented in alarm rationalization (called alarm response procedures)
  - Limits (alarm setpoint)
  - Consequence
  - Operator response (corrective action)
- Procedures should cover certain activities
  - Alarm shelving
  - Placing an alarm out-of-service
- Training should take place prior to operation
- Electronic systems are preferred

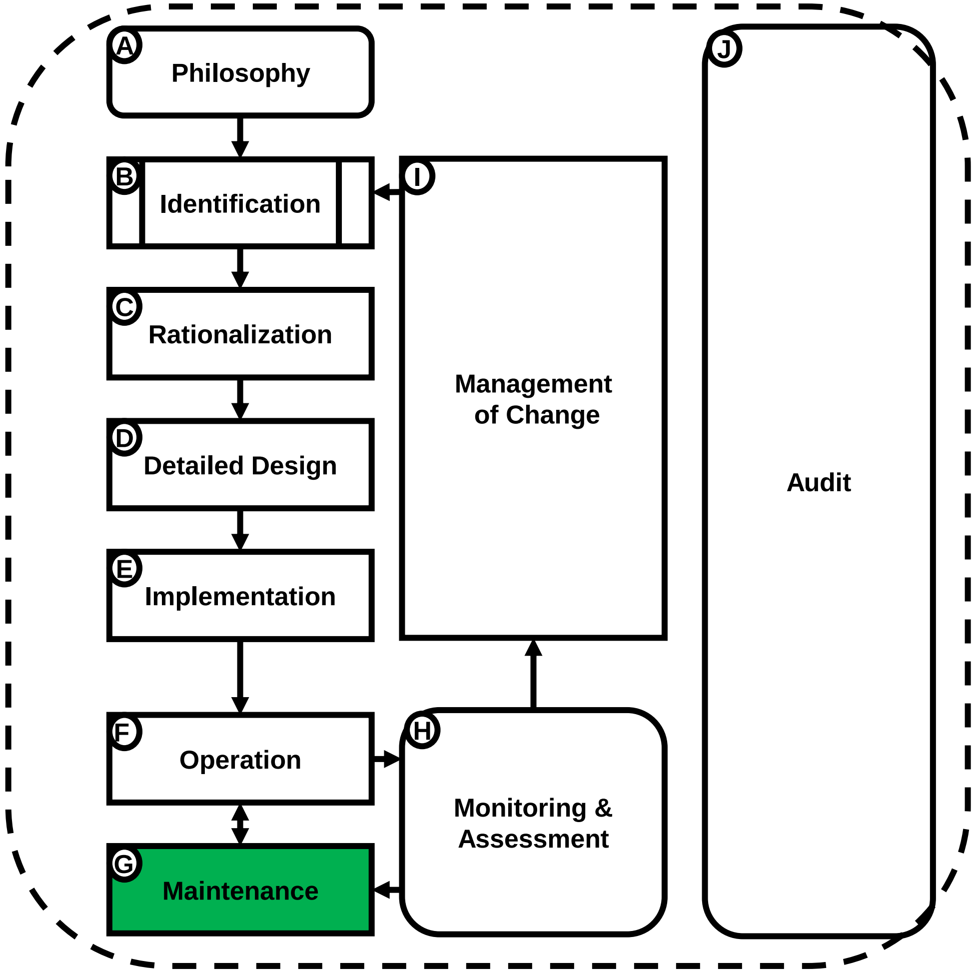
Alarm Management Operation – Operating Training

- Operators must be trained on alarm response procedures
  - Operator must know or find correct action for each alarm
  - Refresher training should be conducted on an appropriate frequency
  - Training requirements may vary by class of the alarm
  - Training should part of operator training program
- Operators must be trained on alarm system design
  - Alarm priorities
  - Alarm indications and navigation
  - Alarm summaries
  - Alarm suppression methods

Maintenance

Alarm Management Maintenance

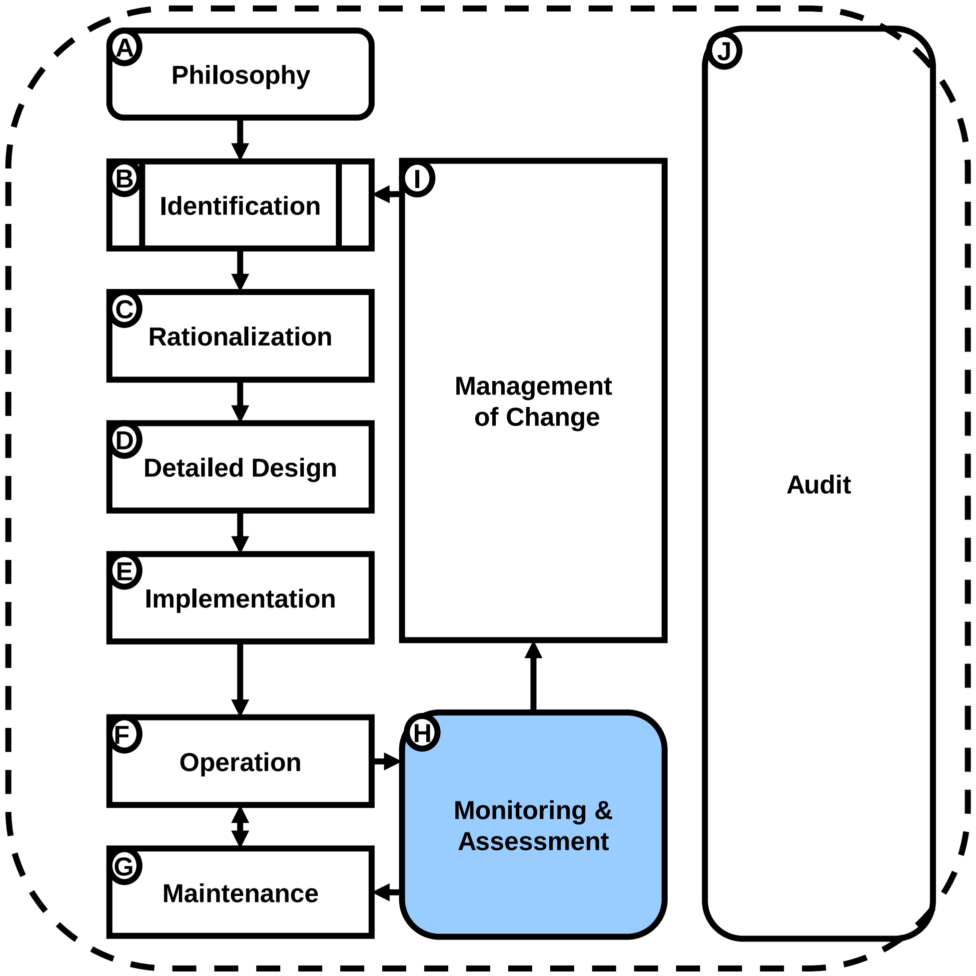
- Maintenance is the step where the alarm is out of service for repair, replacement, or testing
- Testing and return to service are key activities in maintenance



Monitoring & Assessment

Alarm Management Monitoring & Assessment

- Monitoring and Assessment consists of tracking the alarm system performance vs objectives in the philosophy
- An unmonitored alarm system is almost always broken
- Monitoring is the most important stage of the lifecycle
  - Runs concurrent with Operation & Maintenance
- Alarm state changes are tracked from both operation and maintenance
- Common alarm problems solved
  - Nuisance alarms
  - Stale alarms
  - Alarm Floods
  - Suppressed alarms
  - Redundant alarms



Alarm Management Monitoring & Assessment – Metrics

- Philosophy defines key metrics:
  - Alarm rate
  - Alarm frequency
  - High priority alarm frequency
  - Stale alarms
  - Standing alarms
  - Shelved, out-of-service alarms
  - Alarm priority distribution
- Goal levels
  - Goal value for each metric
- Action limits
  - Action limit for each metric that alerts the alarm system owner to an issue

Alarm Management Monitoring & Assessment – Industry Metrics

	EEMUA	Oil & Gas	PetroChem	Power	Other
Average Alarms per Day	144	1200	1500	2000	900
Average Standing Alarms	9	50	100	65	35
Peak Alarms per 10 Minutes	10	220	180	350	180
Average Alarms/ 10 Minute Interval	1	6	9	8	5
Distribution % (Low/Med/High)	80/15/5	25/40/35	25/40/35	25/40/35	25/40/35

Recommended *Actual*

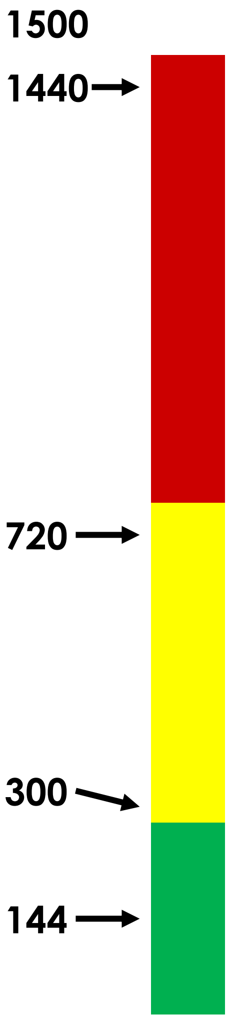
Source: Matrikon

- Metric goals and action limits should be documented in the philosophy

Alarm Management Monitoring & Assessment – Guidance on Metrics

- How many alarms is too many?
  - 1 alarm per minute = 1440 alarms per day = 60 alarms per hour
  - 1 alarm per 2 minutes = 720 alarms per day = 30 alarms per hour
  - 1 alarm per 5 minutes = 288 alarms per day = 12 alarms per hour
  - 1 alarm per 10 minutes = 144 alarms per day = 6 alarms per hour
- Guidance from EEMUA 191

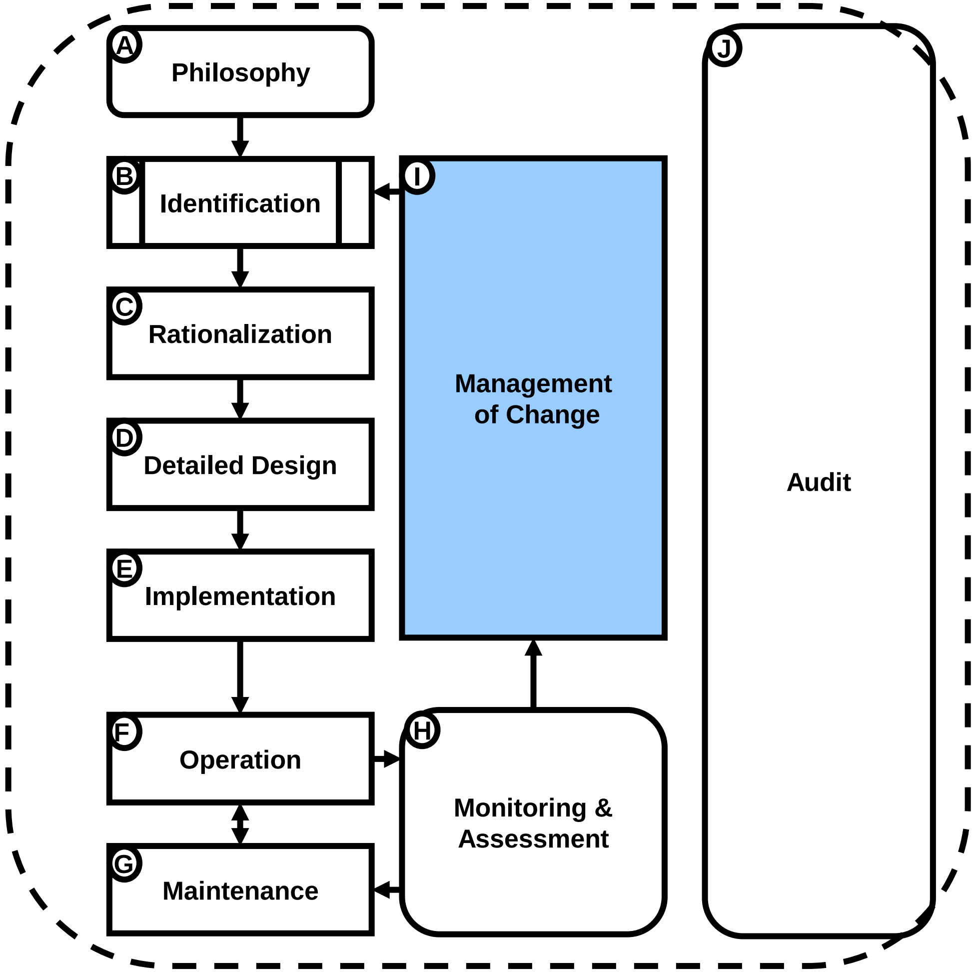
Average Alarm Rate (steady-state operation)	Acceptability
more than 1 per minute	Very likely to be unacceptable
one per 2 minutes	Likely to be over demanding*
one per 5 minutes	Manageable
less than one per 10 minutes	Very likely to be acceptable



Management of Change

Alarm Management Management of Change

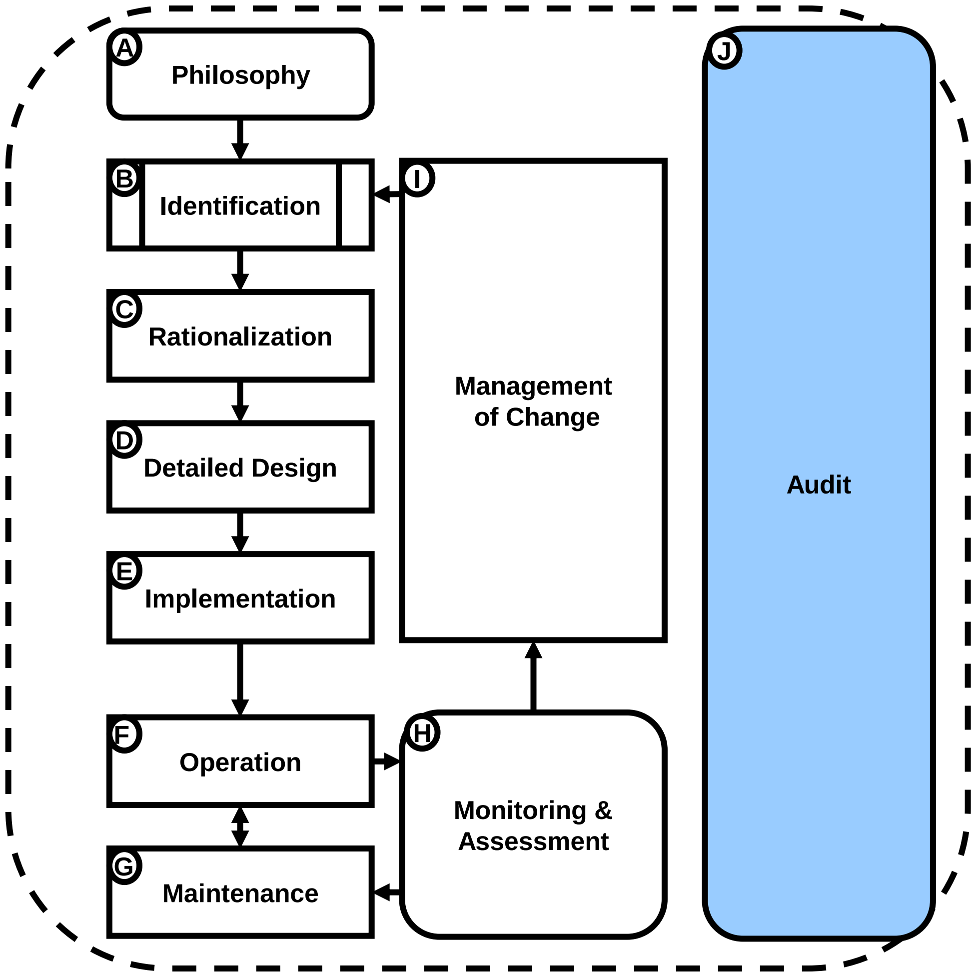
- Management of Change (MOC)
  - Authorization for modifications to the alarm system
- Each change is reviewed and approved prior to implementation
- MOC should also be used for alarm setpoints changes, alarms additions, alarm removal, and advanced alarm changes
- Changes should follow the steps of the lifecycle
- OSHA 29 CFR 1910.119 (l) – MOC
  - Employer SHALL assure the following considerations are addressed prior to any change:
    - Technical basis for change
    - Impact of change on safety and health
    - Modifications to operating procedures
    - Necessary time period for change
    - Authorization requirement for change
  - Required Except for "replacement in kind"



Audit

Alarm Management Audit

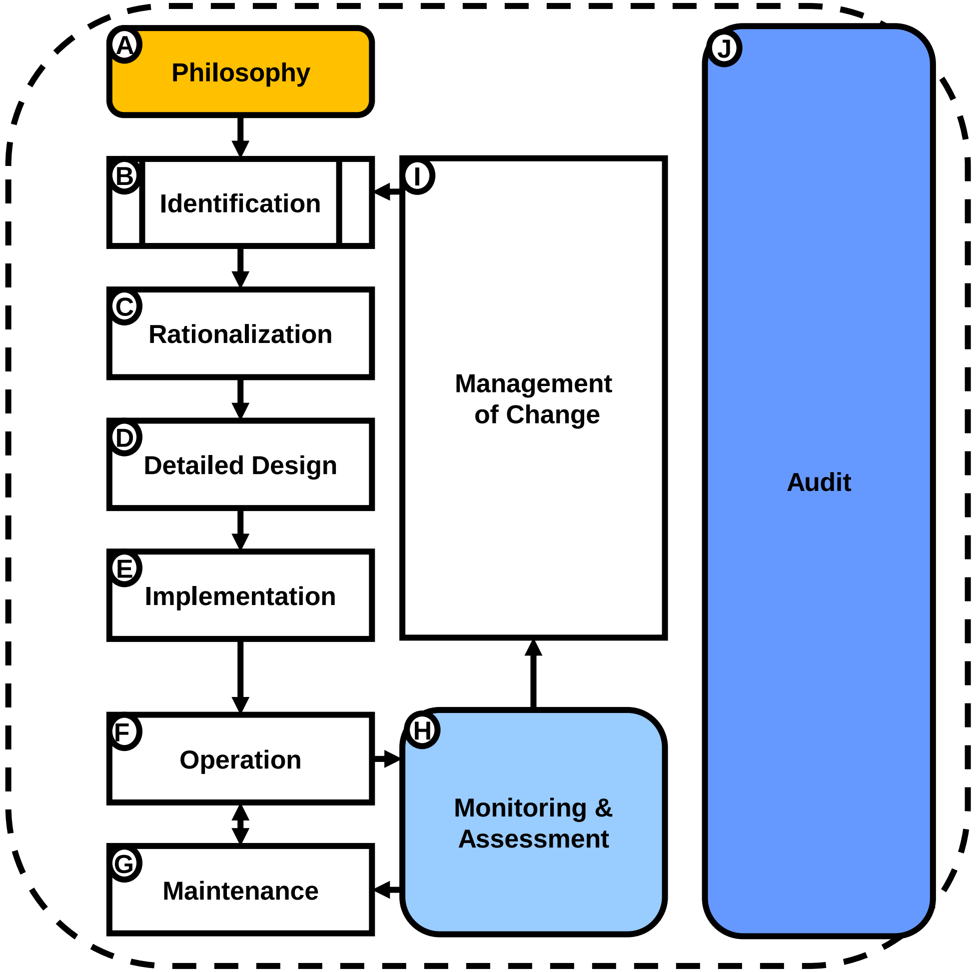
- Audit is the periodic check
  - Determine if the alarm system is meeting design objectives and procedures are followed
- Audit drives changes to the alarm philosophy
- Audit is standalone and not connected to the other lifecycle stages
  - Audits of different scope and length can be conducted
  - Benchmark is a type of audit
  - OE audit is comprehensive and would review all policies and procedures



Getting Started & Summary

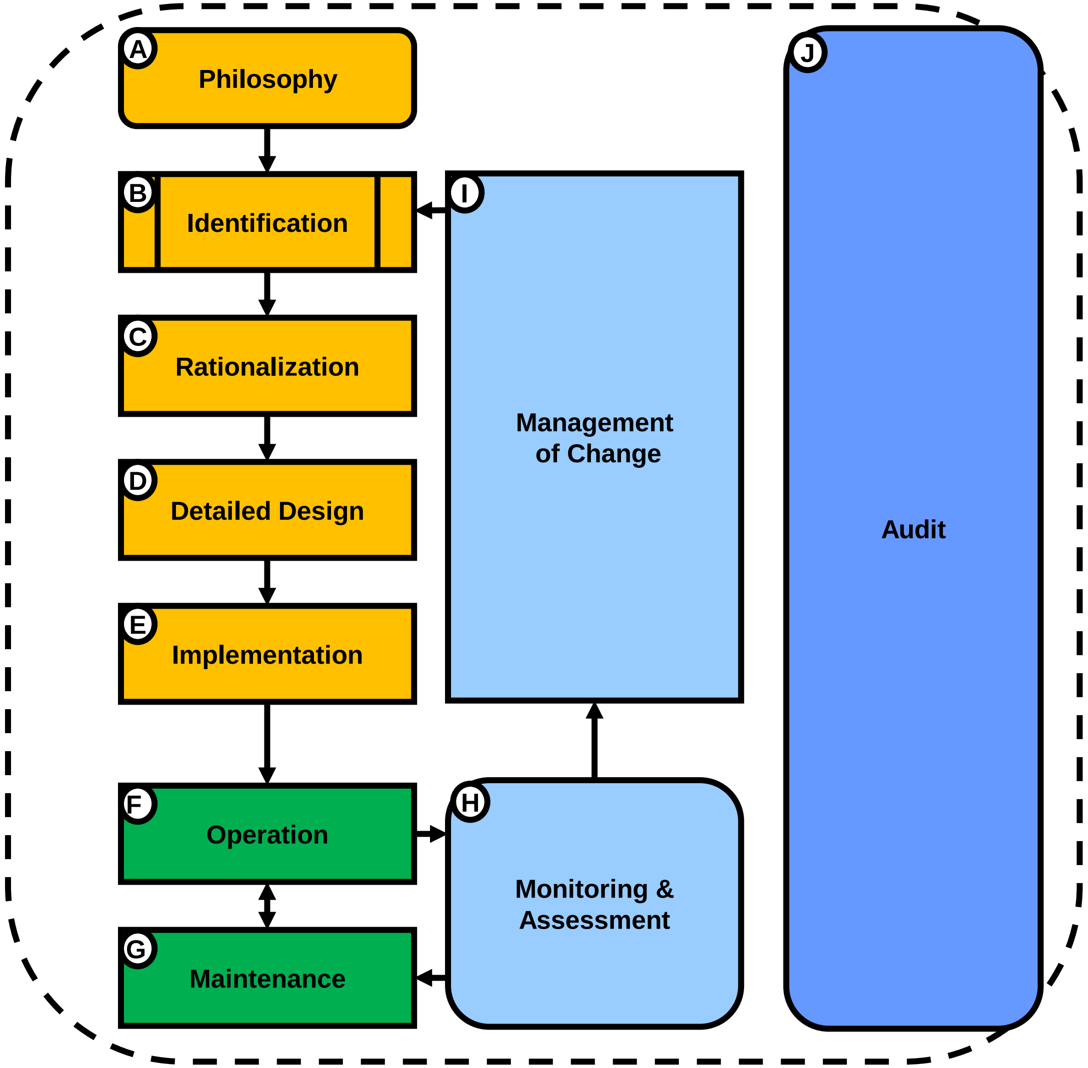
Alarm Management Getting Started

- Develop a philosophy
- Install a monitoring package
- Benchmark your system
- Don’t start improvement without a measurement



Alarm Management Summary

- Alarm system is a key indicator of operational excellence
- Improved alarm management improves
  - Safety
  - Reliability
  - Efficiency
- Don't wait for incidents, design for performance of the alarm system
- Use a lifecycle approach to alarm management




Thank You.