Alarm Rationalization Study in EPC Projects

VERONICA FOX - Design HSE Manager

AGENDA

01	WHY ALARM MANAGEMENT	A BIT OF CONTEXT THE MILFORD HAVEN REFINERY INCIDENT (WALES, 1994)
02	PRINCIPLES OF ALARMS MANAGEMENT	KEY PRINCIPLES OF ALARM MANAGEMENT SOME CONTEXT - EPC PROJECT ALARMS IDENTIFICATION
03	THE WORKSHOP	SCOPE THE TEAM THE WORKFLOW KEY STEP # 1 KEY STEP # 2 TYPICAL MATRIX RULES BASED PRIORITIZATION EXEMPLARS ALARM RATIONALIZATION WORKSHEETS
04	PERFORMANCE MONITORING	TARGETS CASE STUDY – POLYOLEFINS #1 CASE STUDY – POLYOLEFINS #2 WORKSHOP CRITICALITIES RESOLUTION

01

WHY ALARM MANAGEMENT

WHY

A BIT OF CONTEXT

The Control Room panel operator must always be provided:

- ✓ With **reliable** and **accurate information** with respect to any abnormal situation, an equipment malfunction or a process upset condition that could potentially trigger a process shutdown;
- ✓ The information needs to be presented to the panel operator **with a clear identification of its importance** and relevance, to enable an effective and diligent operator action.

What happen if alarms priority is not given?

ALARM FLOODING….

Industrial experience identifies clearly that ineffective process alarm systems can be significant contributing factors in **major process incidents**.

WHY

THE MILFORD HAVEN REFINERY INCIDENT (Wales, 1994)

THE INCIDENT

The incident was caused by flammable hydrocarbon liquid being continuously pumped into a process vessel that had its outlet closed. The flare system was not designed to cope with this excursion from normal operation and failed at an outlet pipe.

This released 20 tonnes of a mixture of hydrocarbon liquid and vapour which subsequently exploded.
Injured 26 people, caused millions of GBP damage and significant production loss.

THE CAUSES

A combination of events, including:

1) a control valve being shut when the control system indicated it was open;
2) a modification which had been carried out without assessing all the consequences;
3) control panel graphics that did not provide necessary process overviews;
4) attempts to keep the unit running when it should have been shut down.

WHY

THE MILFORD HAVEN REFINERY INCIDENT (Wales, 1994)

It was seen that in the last 10 minutes before the explosion the two operators had to recognize, acknowledge and take appropriate action on **275 alarms**.

At times during the morning operators were doing nothing but acknowledging alarms.

HSE GOV Report - Recommendation # 6 [1]

The use and configuration of alarms should be such that:

1) safety critical alarms, including those for flare systems, are distinguishable from other operational alarms;
2) alarms are limited to the number that an operator can effectively monitor;
3) ultimate plant safety should not rely on operator response to a control system alarm.

Ref. [1] The explosion and fires at the Texaco refinery Milford Haven

02

PRINCIPLES OF ALARMS MANAGEMENT

PRINCIPLES OF ALARMS MANAGEMENT

KEY PRINCIPLES OF ALARM MANAGEMENT

- ✓ Alarms should direct the operator's attention towards plant conditions requiring timely assessment or action;
- ✓ Alarms should alert, inform and guide required operator action;
- ✓ Every alarm should be **useful** and relevant to the operator, and **have a defined response**;
- ✓ **Alarm levels should be set such that the operators have sufficient time to carry out their defined response before the plant condition escalates**;
- ✓ The alarm system has to **accommodate human capabilities** and **limitations.**

PRINCIPLES OF ALARMS MANAGEMENT

KEY PRINCIPLES OF ALARM MANAGEMENT

Internationally recognized references include:

- 2014 IEC 62682 Alarm Management Standard for Process Industries
- 2009 ISA 18.2 Alarm Management Standard
- 1999 EEMUA Publication 191

Nowadays the biggest companies are developing their internal standards….

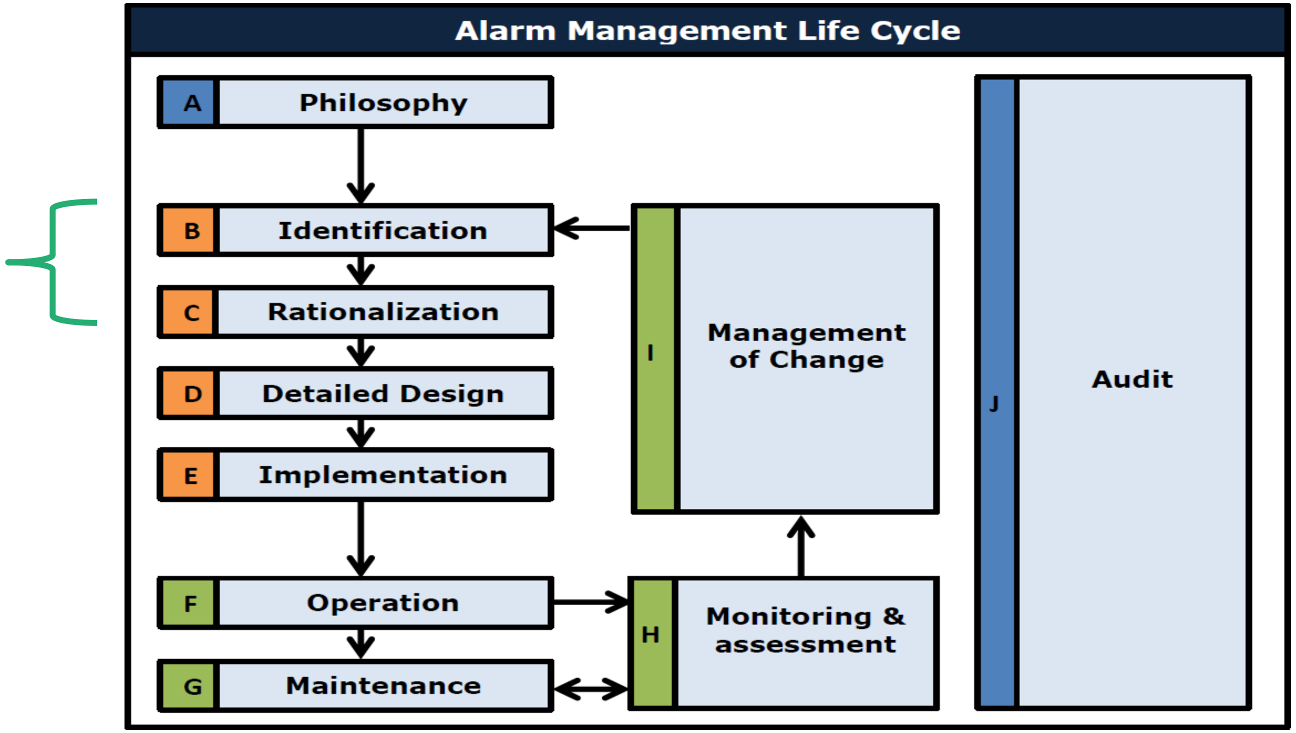
PRINCIPLES OF ALARMS MANAGEMENT

SOME CONTEXT - EPC PROJECT

The ISA18.2 flowchart presents the relationship between the stages of the alarm management lifecycle.

The lifecycle model is useful in organizing the requirements and responsibilities for implementing an alarm management system. The lifecycle approach is applicable for new alarm systems as well as for existing systems.

The inputs to our study



ALARM MANAGEMENT LIFECYCLE MODEL

ALARMS IDENTIFICATION

PRIMARY SCOPE

- ✓ Process related Alarms

Included in Project documents such as in:

- Alarm and Trip Summary
- Cause and Effects Diagrams and
- P&IDs.

EXTENDED SCOPE

- ✓ Analyzer common fault alarm;
- ✓ Deviation alarm (e.g. between 2 level gauges);
- ✓ Electrical heat tracing alarm;
- ✓ Electrical failure alarm (e.g. substation alarms);
- ✓ F&G detection alarms;
- ✓ Control room cabinet fault alarm;
- ✓ HVAC failure alarm;
- ✓ Maintenance alarm; and
- ✓ Instrument alarms (e.g. hand switch, opening/closure of MOV etc.).

For some of these predefined priority can be assigned (i.e. FGS alarms)

PRINCIPLES OF ALARMS MANAGEMENT

ALARM IDENTIFICATION

Documents required for the assessment:

- ✓ P&IDs;
- ✓ Alarm and trip set point list;
- ✓ Interlocks/cause & effect diagrams.

The above shall be duly updated with HAZOP and SIL recommendations.

Additional supporting documentation:

- ✓ HAZOP and LOPA reports;
- ✓ Safety requirements specifications;
- ✓ Access to process historical data (existing system rationalization);
- ✓ Recommendations from an incident investigation, licensor, good manufacturing practice.

03

THE WORKSHOP

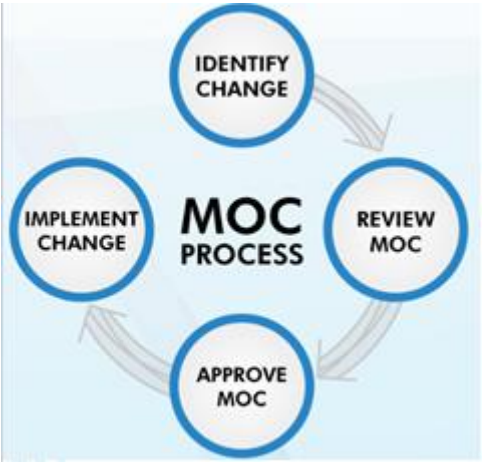
THE WORKSHOP

SCOPE

Rationalization is the process of reviewing the requirement of an alarm and generating the supporting documentation such as the **purpose**, the **consequence** and **corrective action that can be taken** by the panel or plant operator.

Rationalization includes:

- ✓ The prioritization of an alarm;
- ✓ Deletion of unnecessary/ redundant alarms.



The rationalization results are documented in the master alarm database (MADB), which is maintained for the life of the alarm system and subject to management of change.

THE WORKSHOP

THE TEAM

FULL-TIME WORKSHOP PARTICIPANT:

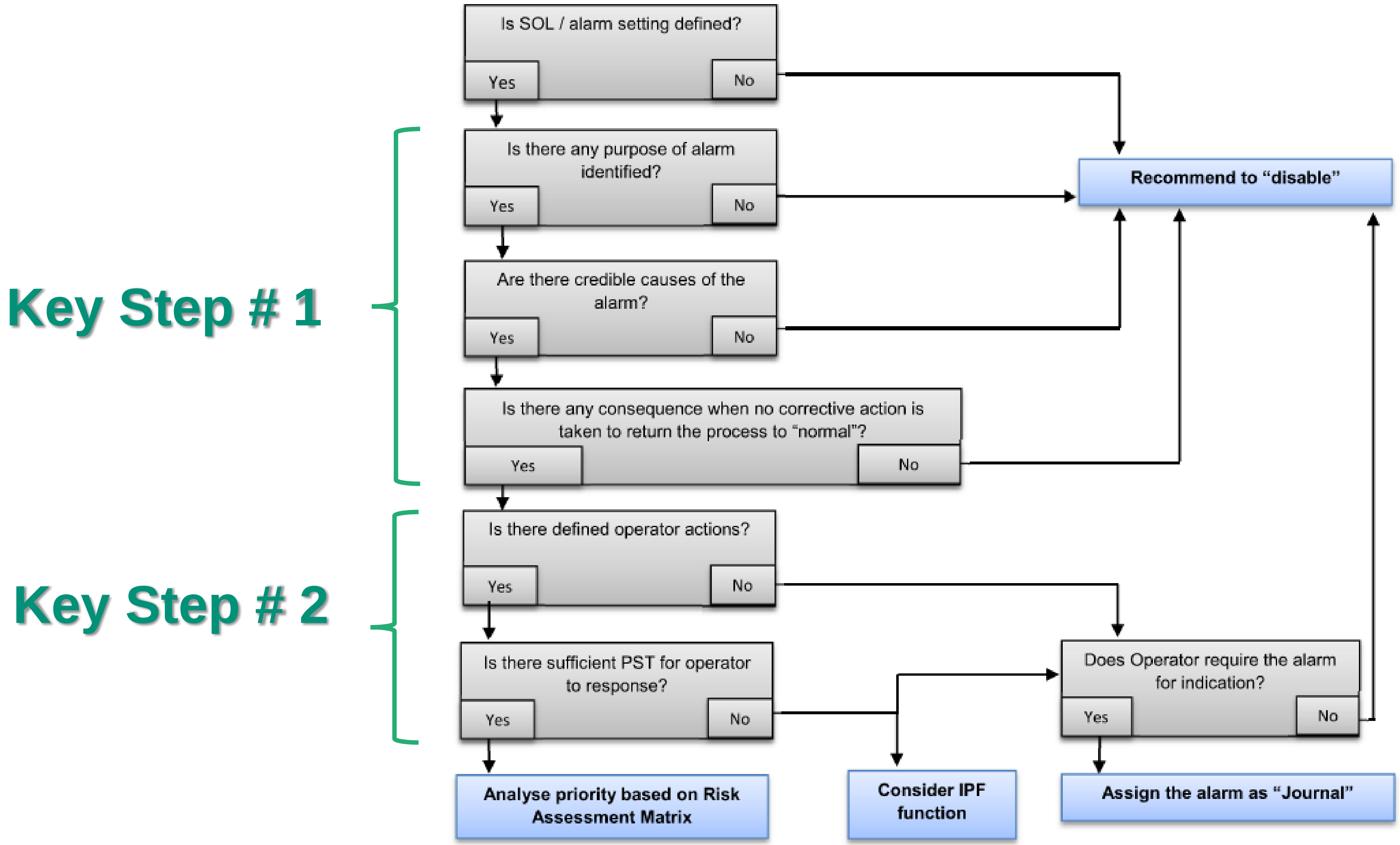
- ✓ Process engineers familiar with the process;
- ✓ Operations such as production engineers, supervisors, panel operators.

  Preferably two panel operators from different shift teams with experience in use of the control system;
- ✓ Control Engineers/System Engineers;
- ✓ Process Safety Engineers.

Special focus shall be on the selection of the **FACILITATOR**:
recommended knowledgeable in alarm management principles and practices, with a background in areas such as human factors, process engineering, operations, control systems.

THE WORKSHOP

THE WORKFLOW



THE WORKSHOP

KEY STEP # 1 – PURPOSE, CAUSE AND CONSEQUENCES

PURPOSE → Why is the alarm raising????

CAUSE → Can include:

- Control loop failure;
- Leakage from bottom of tank ;
- Mis-operation/operator error.

CONSEQUENCE if the operator does nothing → Each alarm should have an undesired consequence that results if the operator does not take action within an allowable response time.
HAZOP and SIL/ LOPA shall be checked.

THE WORKSHOP

KEY STEP # 2 – OPERATOR ACTIONS AND PST

The Available Operator Response Time shall be estimated both considering panel and field operator corrective actions.

ALARM HANDLING STRATEGY	TIME TO INTERVENE
Action by Panel Operator - Stop Pump - Close valve	**SHORT** **(Less than 5 min)**
Action by Field Operator - Isolation of manual valve (less than 6”) - Open by-pass valve (less than 6”)	**MEDIUM** **(5-15 min)**
Action by Field Operator requiring longer time - Isolation of manual valve (more than 6”) - Open by-pass valve (more than 6”) - Clean/ replace filter	**LONG** **(more that 15min)**

THE WORKSHOP

TYPICAL MATRIX

Alarms will be prioritized following an **Alarm Priority Matrix**:

Response Class		Available Response Time	PRIORITY CLASS				
	SHORT	< 5 mins	L	M	E	*E	*E
	MEDIUM	5-15 mins	L	M	M	*E	*E
	LONG	>15 mins	L	L	M	*M	*E
Consequence Category	ECONOMICS		No/Slight Effect (<10k)	Minor Effect (10-100k)	Medium Effect (100k-1M)	Major Effect (1M to 10M)	Extensive (>10M)
	HEALTH & SAFETY		No/Slight Injury	Minor Injury	Major Injury	Single Fatality	Multiple Fatalities
	ENVIRONMENT		No/Slight Effect	Minor Effect	Local Effect	Major Effect	Massive
CONSEQUENCE CLASS			NEGLIGIBLE	LOW	MEDIUM	HIGH	EXTREME

E – Emergency / Urgent / High
M - Medium
L – Low

THE WORKSHOP

RULE-BASED PRIORITIZATION EXEMPLARS

FIRE & GAS DETECTION ALARMS

H - Confirmed fire, flammable gas, H_2S gas detection

M - Un-confirmed fire, flammable gas, H_2S gas detection

L - Fire suppression aborted

L - F&G MOS time out

Alarm/ Journal - F&G MOS status

ESD ALARMS

H - Command failure ESD valve (valve moved without command, valve not moved with command)

L - Equipment trip, ESD trips

Alarm/ Journal - System cabinet alarm (PCS, ESD, F&G, PLC)

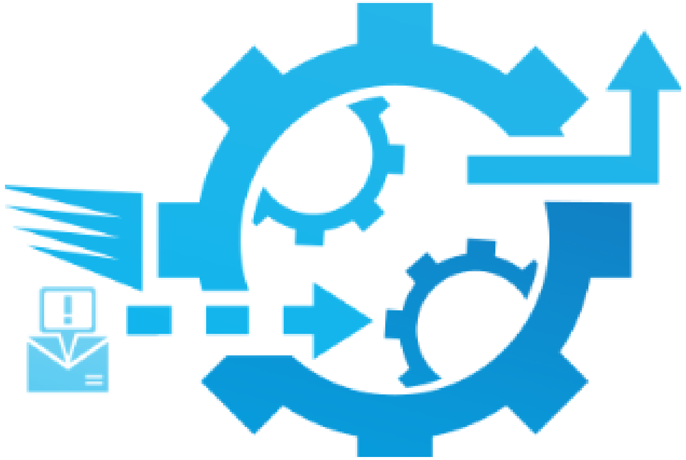
ELECTRICAL SYSTEM INTERFACE

H - UPS/Switchgear/Battery fault

L - Power system diagnostic Alarms

THE WORKSHOP

RULE-BASED PRIORITIZATION EXEMPLARS



TYPE OF ALARM	ALARM HANDLING STRATEGY
Redundant Alarms with same functions	Maintain one alarm and disable the other alarm
Alarms with no action required by operator	1- Journal or Event message 2- If alarm not require, recommended to disable
Alarms with Insufficient time for operator action and No Operator Action	Journal

Additionally grouping and suppression assessment can be carried out post rationalization workshop.

THE WORKSHOP

ALARM RATIONALIZATION WORKSHEETS

Tag Number	Current Setpoint	Alarm Parameter	Eng Unit	Purpose of Measurement	Purpose of Alarm	Causes	Corrective Actions by Panel Operator	Corrective Actions By Field Operator	Consequences	Operator Response Time	Available Process Response Class	Economics Consequence Class	Safety Consequence Class	Environment Consequence Class	Overall Priority	Remarks
XXXX-FICA-1235	-5%	DEV% L	kg/h	ML TO XXXX-R-121 Flow %DEV. L	To detect flow deviation low and prevent clogging	1. XXXX-FCV-1235 stuck closed	1. Break control ML and put in manual 2. Inform maintenance	1. Manually open XXXX-FCV-1235 valve	Possible density increase resulting in loss of production. Production loss due to cleaning activity.	5-15	>15 mins	Medium Effect (100K - 1M)	No/Slight Injury	No/Slight Effect	**MEDIUM**	
XXXX-TIZA-3182	255	H	°C	XXXX-C-312A MIDDLE Temperature H	To detect high temperature during regeneration and pre alarm for TIZA-3182 HH	1. During regeneration	-	-	TIZA-3182 HH will eventually trigger.	-	N/A	N/A	N/A	N/A	**JOURNAL**	This alarm will be journal due to insufficient response time
XXXX-LIA-3265	29	L	%	XXXX-C-321 Level L	See remark(s)	See remark(s)	See remark(s)	See remark(s)	See remark(s)	-					**REMOVE**	Recommend to remove since it is duplication of LICA-3264 L alarm

04

PERFORMANCE MONITORING

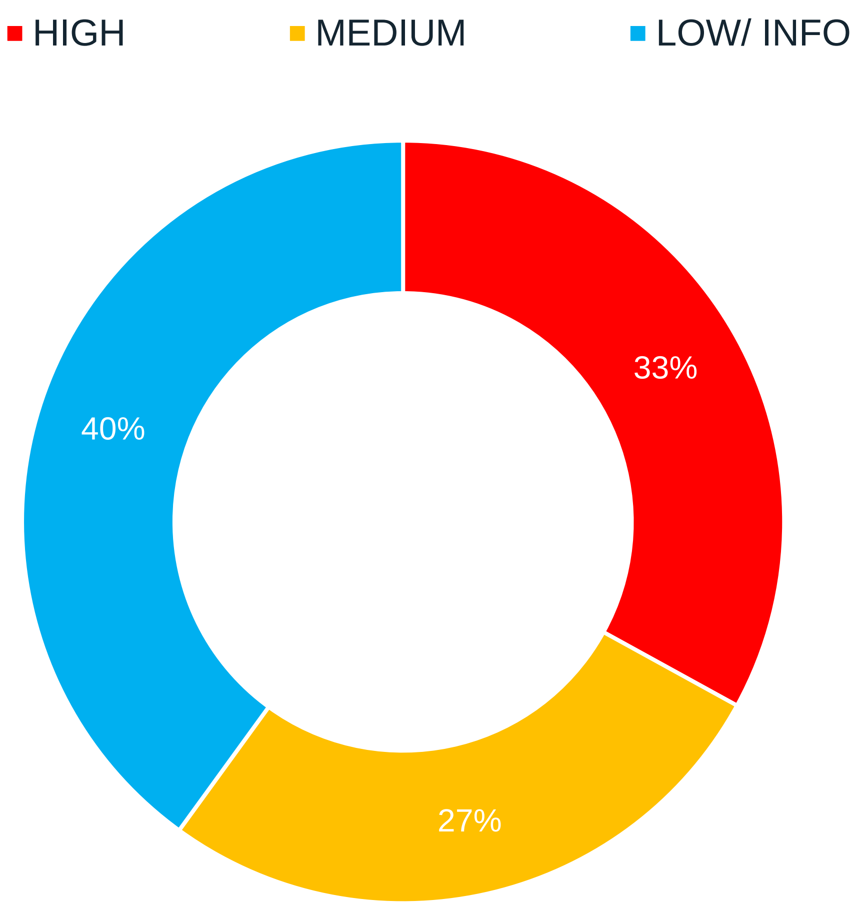
PERFORMANCE MONITORING
TARGETS

PRIORITY	ALARM HANDLING STRATEGY
URGENT	A target of 5% and no more than 10%, or 2 to 3 emergency alarms per piece of major equipment
MEDIUM	A target of 10% and no more than 20%
LOW	The rest, i.e. a target of 85% and no less than 70%

Each major COMPANY is now having a KPIs so to and continually improve performance levels of an alarms system

PERFORMANCE MONITORING

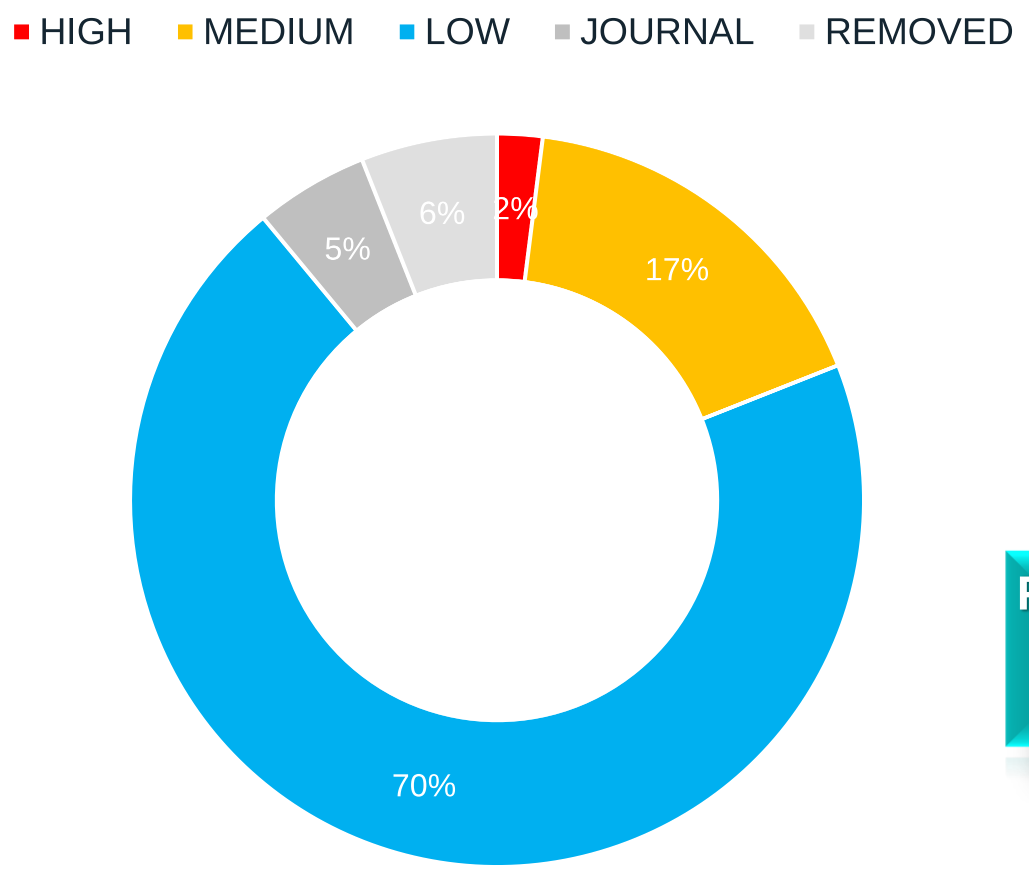
CASE STUDY - POLYOLEFIN PLANT # 1



Total Alarms – 1383
Workshop Duration – 6 weeks

FINDINGS: results not matching with EMUAA guidelines, further optimizations to be performed.

PERFORMANCE MONITORING
CASE STUDY - POLYOLEFIN PLANT # 2



Total Alarms - 806
Workshop Duration – 3weeks

FINDINGS: results matching with EMUAA guidelines. Further optimizations can be performed as part of the continuous improvement plan.

PERFORMANCE MONITORING

WORKSHOP CRITICALITIES RESOLUTION

AVAILABILITY OF INPUT VS EPC SCHEDULE

WORKSHOP DURATION

- ✓ Rules sets to be pre-defined as much as possible
- ✓ Parallel workshop trains
- ✓ Pre-filling

RESULTS NOT MATCHING WITH KPIs

- ✓ Further optimizations to be done during FAT (not advisable)
- ✓ Continuous improvement – further session to be conducted in operation phase

TECNIMONT