Eskom	Guideline	Generation Engineering

Title: **Alarm Management System Guideline**

Unique Identifier:	**240-56355466**
Alternative Reference Number:	**EED_GTD_C&I_006**
Area of Applicability:	**Generation Engineering**
Documentation Type:	**Guideline**
Revision:	**3**
Total Pages:	**35**
Next Review Date:	**March 2030**
Disclosure Classification:	**CONTROLLED DISCLOSURE**

APPROVED FOR AUTHORISATION
GENERATION ENGINEERING
DOCUMENT CENTRE ☎ X4962

Compiled by	Approved by	Authorised by
……..	……..	……..
Zubair Moola	**Thokozani Msibi**	**Christoph Kohlmeyer**
Chief Engineer: Generation Engineering, C&I Engineering	**Chief Engineer: Generation Engineering, C&I, Control Systems Care Group**	**Senior Manager: Generation Engineering: C&I Engineering (Acting)**
Date: 06/03/2025	Date: 2025-03-06	Date: 2025-03-11

Supported by SCOT SC

……..

Craig Boesack

PP C&I SC Chairperson

Date: 2025-03-11

PCM Reference : **240-56355828**

SCOT Study Committee Number/Name : **PP C&I SC08-03**

CONTENTS

Page

FIGURES

TABLES

1. INTRODUCTION

The introduction of modern digital control systems has brought about that plant operators in various industries are regularly presented with unmanageable process alarm rates. The result is an ineffective alarm system that impedes the tasks of the plant operators. This is especially true for Eskom, as highlighted by recent control system refurbishment and upgrade projects. The main reasons for this are poor alarm system design, poor control system configuration and the lack of alarm system performance indicators.

There are simply too many annunciated alarms for the operator to effectively identify, diagnose and take corrective action in a timeous manner. This has led to an undesirable situation in which the operator acknowledges alarms without considering the consequences of doing so.

This guideline (and alarm philosophy document contained within) is based on the Alarm Management Handbook by PAS [1]. In addition, reference is made to EEMUA 191 [2], ISA 18.2 [3], ISA SP18 [4], and NAMUR 102 [5]. These are international best practice guidelines and standards for an effective alarm management system.

As alarm systems are critical for the safe and reliable operation of plant and equipment, it is recognized that best practices and principles, proper design and maintenance strategies must be implemented to support the plant operators in performing their task.

2. SUPPORTING CLAUSES

2.1 SCOPE

This document specifies the principles, rationale, process and resources required to ensure that effective alarm management systems are implemented and maintained at all Eskom Power Stations.

2.1.1 Exclusions

2.1.1.1 Human Machine Interface

The Human Machine Interface (HMI) design, which shall follow the relevant Eskom HMI related standards and guidelines, is excluded from the scope of this document.

2.1.1.2 Events

The indication and analysis of event data and events (that are not alarms) are excluded from the scope of this document.

2.1.2 Purpose

The purpose of this document is to ensure that effective alarm management systems are implemented using a consistent technical basis at all Eskom Power Stations.
The objective of this document is to set clear high level criteria required for an alarm system’s functional performance in order to have Manageable Alarm Rates annunciated to plant operators.

The document thus aims to have effective and auditable Alarm Management Systems implemented on all plant. This will ensure that all Process Alarms are applicable, timely and effective thus assisting operating personnel in operating plant effectively, reliably and safely.

2.2 APPLICABILITY

This document shall apply throughout Eskom Generation Engineering (Gx Engineering) and Nuclear Engineering excluding Peaking.

2.3 QUALITY AND SAFETY

An ineffective alarm management system implies that the operator will not be able to take action in a timeous and effective manner in response to an abnormal situation. This could result in process downtime and hence will impact quality of supply and safety.

The solution to this problem will involve the efforts and cooperation of a multi-disciplinary team.

2.4 NORMATIVE/INFORMATIVE REFERENCES

Parties using this document shall apply the most recent edition of the documents listed below.

2.4.1 Normative

[1] Bill Hollifield and Eddie Habibi, *The Alarm Management Handbook, A Comprehensive Guide*. PAS, Houston, TX, 2006. ISBN: 0-9778969-0-0.

[2] *Alarm systems: A Guide to Design, Management and Procurement*, The Engineering Equipment and Material User's Association (EEMUA) Publication No. 191.

[3] *Management of Alarm Systems for the Process Industries*. ANSI/ISA 18.2 Standard,.

[4] D.G. Dunn and N.P. Sands, "ISA-SP18 - Alarm Systems Management and Design Guide", presented at ISA Expo, Chicago, Illinois, 2005.

[5] *Alarm Management,* NAMUR Recommendation and Worksheets NA 102.

2.4.2 Informative

[6] *Ergonomic Design of Power Station Control Suites Guideline,* Eskom Generation Engineering 240-56355808.

[7] *Human Machine Interface Design Requirements Standard*, Eskom Generation Engineering 240-56355728

[8] *Management of alarms systems for the process industries,* SABS, SANS 62682:2016

2.5 DEFINITIONS

Definition	Description
Alarm	A "(process) alarm is a mechanism for informing an operator of an abnormal (process) condition for which an operator action is required. The operator is alerted in order to prevent or mitigate process *upsets and disturbances."* This definition is significant in that no event other than one that represents an abnormal situation and requires an operator action should be an alarm. The system that performs the alarming function can therefore be seen as an operator-centric system.
Alarm Floods	A burst rate of alarms which begins when the alarm rate exceeds 10 or more alarms occurring in 10 minutes and ends when the rate drops to below 5 alarms in 10 minutes.
Alarm Management	The process of applying ergonomic principles and engineering to manage the design of alarms and optimize its usability to ensure safe and reliable plant operation.

Definition	Description
Alarm Priority Distribution	A means to convey the sense of urgency of a specific process condition to the operator and is used to drive the order of operator responses.
Chattering Alarm	An alarm that appears and clears at least three times in one minute
Controlled Disclosure	Controlled Disclosure to External Parties (either enforced by law, or discretionary)
HMI	The Human Machine Interface (HMI) is used by the operator for the operation and monitoring of plant systems including mechanical, electrical and C&I systems.
HMI Graphic	The graphical representation or plant mimic of any plant component.
Manageable Alarm Rate	Less than one alarm per 10 minutes, per plant operator, on average.
Operator Workstation	The primary interface of the operating plant personnel via which the HMI is accessed with the specified number of operating display units and pointing devices.
Process Alarm	A process alarm is a mechanism for informing a plant operator of an abnormal process condition for which operator action is required. The plant operator is alerted in order to prevent or mitigate process upsets and disturbances.
Standing Alarm	An alarm that is active but intentionally overridden in the alarm system such that it is not visible or audible to the plant operator.
Suppressed Alarm	A suppressed alarm is an alarm that is intentionally temporarily disabled (suppressed) due to a known condition.
Target Average Process Alarm Rate	The number of Process Alarms per day as an indicator of the overall health of the alarm system.

2.5.1 Disclosure Classification

Controlled Disclosure: Controlled Disclosure to external parties (either enforced by law, or discretionary).

2.6 ABBREVIATIONS

Abbreviation	Description
C&I	Control and Instrumentation
D&R	Documentation and Rationalization
DCS	Distributed Control System
EPB	Emergency Push Button
ESD	Emergency Shutdown System
HAZOP	Hazards and Operability Process
HMI	Human Machine Interface
KPI	Key Performance Indicator
SCADA	Supervisory Control and Data Acquisition
SIL	Safety Integrity Level
TDAC	Technical Document Authorisation Committee

2.7 ROLES AND RESPONSIBILITIES

2.7.1 Alarm System Champion

The Alarm System Champion's role is to ensure that the provision for the Alarm System at the specific site meets the requirements as set out in this document. This role is site-specific.

The Documentation & Rationalization (D&R) process and on-going maintenance of the Alarm System shall be facilitated/co-ordinated by the Alarm System Champion. Checklists and sign-off sheets will be signed-off by the appointed Alarm System Champion.

This definition is re-iterated in the Alarm Philosophy Document (Appendix A: 8).

2.7.2 Engineering Manager

The site-specific Engineering manager, or person to whom this responsibility has been delegated, will sign-off the rationalized Master Alarm Database after the D&R process.

The Engineering Manager shall appoint the Alarm System Champion. In addition, an engineering resource from the site-specific C&I Engineering department must be identified to shadow the Alarm System Champion.

2.8 PROCESS FOR MONITORING

This document shall be reviewed as and when necessary.

2.9 RELATED/SUPPORTING DOCUMENTS

- None

2.10 BOUNDARY ANALYSIS

2.10.1 Human interface

As described in Section 2.5, the alarm system should be operator-centric. The process to achieve this requires that an Alarm System Champion be selected by the site-specific Engineering Manager. The duties of the Alarm System Champion role are specified in Sections 2.7.1 and 8.7.1. The Alarm System Champion must put together a team with the members as specified in Section 8.9 Alarm Documentation and Rationalization (D&R). The responsibility of this team will then be to identify, rationalise and document the alarms using the principles and process defined in the Alarm Philosophy.

2.10.2 Technical interface

The alarm management system for an Eskom Power Station resides within the main DCS. The use of third party alarm management systems is not allowed.

2.10.3 System interface

In terms of alarms from third party systems to be passed to the DCS, these alarms have to adhere to the principles outlined in this document.

2.10.4 Process interface

The alarm management system must adhere to the principles defined in Sections 2.5 and 8.5, Alarm Definition and Alarm Criteria, when identifying process alarms.

3. PRINCIPLES OF ALARM MANAGEMENT

3.1 GENERAL APPROACH

This document prescribes the lifecycle of alarm management [1], [3], as shown in Figure 1 below.

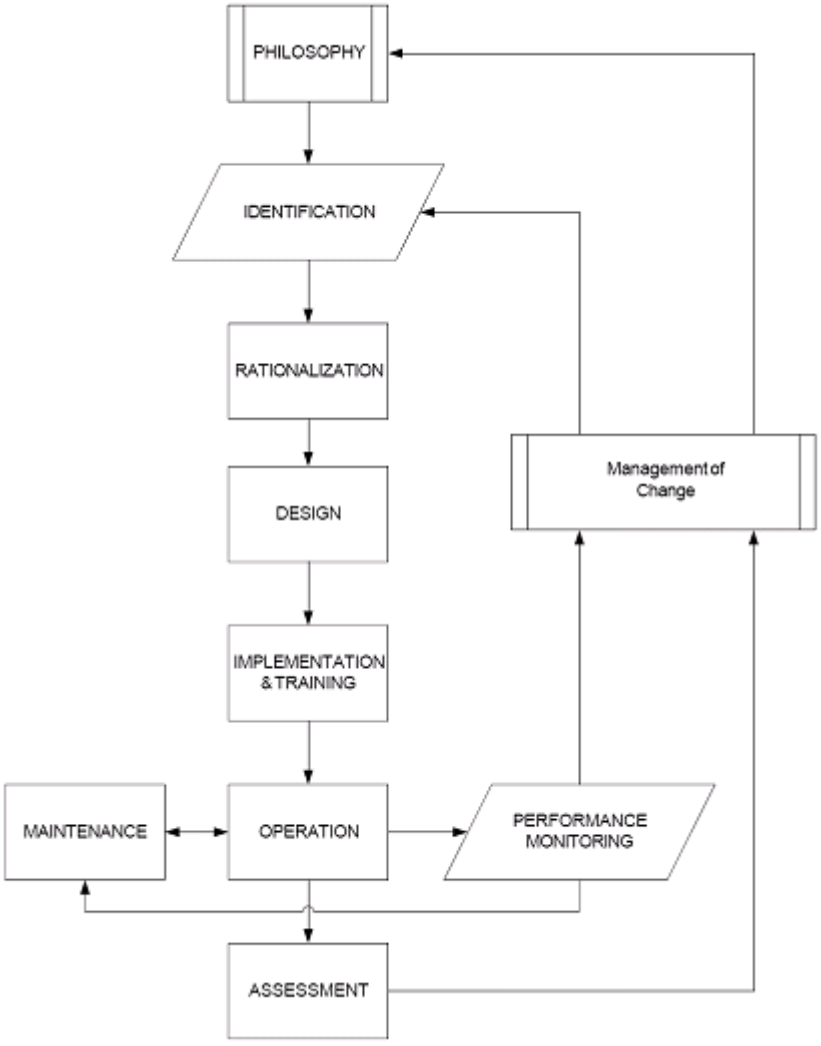

Figure 1: Alarm Management Lifecycle

This management process can be summarised in five phases, namely;

Phase 1: Define – Establish your desired alarm philosophy

Phase 2: Measure – Assess the performance of the designed/existing alarm system

Phase 3: Analyse – Alarm performance benchmarks

Phase 4: Improve – Document and rationalise the existing alarms.

Phase 5: Control – Maintain the improved alarm system

3.1.1 Philosophy

The alarm philosophy documents Eskom's approach to alarm management, and is included herein. It specifies the criteria, definitions and principles for the alarm system. Refer to Appendix A: 8. Alarm Philosophy Document.

3.1.2 Identification

Identification of possible alarms must be done using the principles and processes as per Section 8.9 Alarm Documentation and Rationalization (D&R).

3.1.3 Documentation & Rationalization

D&R is the process of reconciling and documenting each of the identified individual alarms against the principles and requirements of the alarm philosophy.

The identified possible alarms are reviewed to document the rationale for the alarm, as well as the basic information such as the operator action, response time and consequence of deviation. Once the consequences and the response time have been documented, each alarm is assigned a priority based on a matrix of consequences and priorities. This matrix is defined in Section 8.9 Alarm Documentation and Rationalization (D&R), as part of the Alarm Philosophy Document.

The D&R process ensures that the operator receives only those alarms that are meaningful and actionable [1]; it is described further in Section 8.9 Alarm Documentation and Rationalization (D&R).

Pro-forma signoff sheets to be used for the D&R exercise are provided in Appendix A: 9. PRO-FORMA D&R SIGN-OFF SHEET PER ALARM.

Similar alarms can be grouped and signed-off using a single sign-off sheet provided they are identical in characteristics (Impact, time to respond, priority, set points and operator response).

3.1.4 Design

The design stage includes the basic configuration of alarms, the design of the HMI for alarms, and the advanced methods of alarm management.

The design is supported by a design guide prepared by the contractor and documents control system specific implementations of the alarm philosophy principles.

3.1.5 Implementation & Training

In this phase, the activities necessary to bring the alarm system into service are completed. This phase will include training for the operator and initial testing of the functionality of the alarm system.

3.1.6 Operation

In this phase, the alarm system is in service and reporting abnormal conditions to the operator, as designed.

3.1.7 Performance Monitoring

Performance monitoring is the periodic collection and analysis of data from the alarm system (in the operation stage) to detect problems such as nuisance alarms, stale alarms, and alarm floods. Performance criteria for the alarm system are defined in Section 8.7.2, Alarm System Key Performance Indicators (KPIs). Monitoring during operation is a routine activity that may trigger maintenance work to be done or identify changes to be made to the alarm system, alarm philosophy, or operating procedures.

All necessary changes shall be done via appropriate Management of Change procedures. Monitoring and analysis of data from the Maintenance stage provides an indication of the maintenance efficiency.

3.1.8 Maintenance

Periodic maintenance is necessary to ensure the alarm system functions as designed. It covers system testing, replacements and repairs and is the stage during which issues such as chattering/fleeting alarms are rectified.

3.1.9 Assessment

Assessment is a periodic audit of the alarm system and the processes, which are detailed in the alarm philosophy, against performance criteria contained in Section 8.7.2, Alarm System Key Performance Indicators (KPIs). The assessment could lead to a modification of the alarm system process, the philosophy, the design guidance, or the need to improve the organization's discipline to follow the processes.

3.1.10 Management of Change

Management of Change is the structured process of proposing, approving and authorizing modifications to alarms and/or alarm system. This change process should feed back to the identification stage to ensure that each change is consistent with the alarm philosophy. Refer to 8.10.13, Management of Change.

3.2 PERFORMANCE CRITERIA

Please refer to the Alarm Philosophy Document, Section 8.7.2, Alarm System Key Performance Indicators (KPIs).

4. AUTHORISATION

This document has been seen and accepted by:

Name & Surname	Designation
Pharuma Madike (Acting)	C&I Engineering Manager – Matimba Power Station
Sonto Mkhithi	C&I Engineering Manager – Camden Power Station
Geoff Ledwaba	C&I Engineering Manager – Tutuka Power Station
Thapelo Theledi	C&I Engineering Manager – Arnot Power Station
Louis Nel	C&I Engineering Manager – Lethabo Power Station
Harry Mokabane	C&I Engineering Manager – Kriel Power Station
Thabo Magagula (Acting)	C&I Engineering Manager – Kendal Power Station
Mantombi Mkemezulu	C&I Engineering Manager – Grootvlei Power Station
Katlego Mangope	C&I Engineering Manager – Matla Power Station
Yolanda Makhuhleni	C&I Engineering Manager – Hendrina Power Station
Thabani Nxumalo	C&I Engineering Manager – Majuba Power Station
Vero Masuku	C&I Engineering Manager – Duvha Power Station
Nthabi Mashigo	C&I Engineering Manager – Medupi Power Station
Puseletso Ndlovu	C&I Engineering Manager – Kusile Power Station
Zieyaad Isaacs	C&I Engineering Manager -- Koeberg Power Station
Felix Bosch	Generation Engineering Documentation Manager

5. REVISIONS

Date	Rev.	Compiler	Remarks
March 2007	0	B. Moodley	Compilation of Alarm Management System guideline document
November 2010	0.1	N. Moodley N. Soodhoo	Minor update in line with ISA 18.2.
July 2012	0.2	N. Moodley	Formatted as per the updated Eskom 32-4 Document Template.
February 2013	1	N. Moodley	Review and update (template only) of existing document as per B2B TDAC process Final Document for Authorisation
October 2015	1.1	Nimesh Soodhoo	Review and consolidation of 240-57859210: Alarm System Performance of Control Systems Applied in Fossil Plant Standard into one document represented in this guideline.
October 2015	1.2	Nimesh Soodhoo	Draft Document for Comments Review
July 2016	1.3	Nimesh Soodhoo	Update as per comments review cycle
October 2016	2	Nimesh Soodhoo	Final Document for Authorisation and Publication
February 2025	2.1	Zubair Moola	First Draft Document for Review and update
March 2025	2.2	Zubair Moola	Final Draft Document after Comments Review Process
March 2025	3	Zubair Moola	Final Document for Authorisation and Publication

6. DEVELOPMENT TEAM

- Navern Moodley
- Devan Govender
- Nimesh Soodhoo

7. ACKNOWLEDGEMENTS

- None

APPENDIX A: 8. ALARM PHILOSOPHY DOCUMENT

8.1 INTRODUCTION

The alarm philosophy documents Eskom's approach to alarm management. It specifies the criteria, definitions and principles for an alarm system, in line with international best practices and related to the lifecycle of alarm management ([1], [3]).

8.2 PURPOSE OF THIS ALARM PHILOSOPHY

The purpose of this alarm philosophy is to ensure that effective alarm management systems (based on best practices for alarm management) are implemented and maintained at all Eskom Power Stations. An effective alarm management system is one that acts as a tool to help the operator take the correct action at the correct time, **always**.

The following are the key assumptions made in this alarm philosophy:

1. No amount of alarm management is able to replace the constant surveillance of a qualified operator.
2. Operators are trained on the alarm management strategy.
3. Operators will respond to all alarms, regardless of priority.

The acknowledgement of an alarm without assessing the situation is NOT acceptable.

4. The alarm priorities will determine the order of an operator's response to the annunciated alarms.
5. The alarm system is routinely maintained and kept up to date.

8.3 DEFINITIONS

Definition	Description
Alarm	A "(process) alarm is a mechanism for informing an operator of an abnormal (process) condition for which an operator action is required. The operator is alerted in order to prevent or mitigate process upsets and disturbances." This definition is significant in that no event other than one that represents an abnormal situation and requires an operator action should be an alarm. The system that performs the alarming function can therefore be seen as an operator-centric system.
Diagnostic Alarm	An alarm which is primarily used to warn the operator of instrument and system malfunctions.
Nuisance Alarm	An alarm that annunciates excessively, unnecessarily, or does not return to normal after the correct response is taken (e.g., chattering, fleeting, stale, instrument malfunction alarms).
Shelving	Shelving is the mechanism of temporarily suppressing an alarm, typically initiated by an operator.

8.4 ROLES AND RESPONSIBILITIES

8.4.1 Alarm System Champion

The Alarm System Champion's role is to ensure that the provision for the Alarm System at the specific site meets the requirements as set out in this document and associated Alarm Philosophy. This role is site-specific.

The Documentation & Rationalization (D&R) process and on-going maintenance of the Alarm System shall be facilitated/coordinated by the Alarm System Champion. Checklists and sign-off sheets will be signed-off by the appointed Alarm System Champion.

8.5 ALARM CRITERIA

The definition of an alarm translates into the following core principles when choosing / deciding on an alarm during a D&R process:

1. **Alarms must require an operator action**
2. **Multiple alarms should not be produced during a single process event.**
3. **Alarms must activate only on abnormal conditions, not expected cases of operation.**

If the above definition of an alarm and the associated principles are adhered to when performing the alarm identification exercise, it will go a long way in achieving the objectives of this document.

NOTE: Although the output from a Hazard and Operability (HAZOP) Study and associated Safety Integrity Level (SIL) review process may assist in identifying alarms, they are not the basis for the design of alarms, and further it is not a pre-requisite that they precede the D&R process.

8.6 ALARM ANNUNCIATION AND RESPONSE

8.6.1 Annunciated Alarm Priority

Based on best practice guidelines, 3 levels of alarm priority are recommended to be used when annunciating to an operator. The 3 levels of alarm priority for Eskom Power Stations are:

Table 1: Alarm Priority Levels

Priority Level	Percentage Alarm Distribution	HMI Colour
Emergency	5	RED, RGB = 255,0,0
High	15	YELLOW, RGB = 255,255,0
Low	80	CYAN, RGB = 0, 255, 255

The alarm priority matrix provided in Section 8.9.7, Table 6 allows the priority of a specific alarm to be determined during the D&R process. In addition, the distribution of the full complement of alarms shall adhere to the Percentage Alarm Distribution identified in Table 1.

There is one sub-category of the Low priority that is essentially used for instrument malfunctions (Section 8.10.4, Instrument Malfunctions) or Diagnostic alarms that are not feeding the above mentioned priority alarms. This sub-category is the lowest priority and applies to (instrument malfunction or Diagnostic) alarms with very limited and prescribed operator action. There is no recommended percentage distribution for such Diagnostic alarms, since there is no recommended frequency for instrument failure.

The Diagnostic alarm only requires the operator to log a maintenance work order. The rationale for having this sub-category is that during high alarm rate situations, the Diagnostic alarm sub-category can be safely ignored.

No other levels of alarm priority are allowed.

All alarms regardless of the associated priority require an operator response.

The colours shown in Table 1 are reserved for the Alarm Management System i.e. they are used only for the annunciation of the alarms on the alarm system and on associated HMI graphics which are depicting plant items in the abnormal state. No other symbols in their normal state will use these colours.

8.6.2 Navigation and Alarm Response

The operator shall respond to all alarms regardless of the priority, by taking the following steps:

1. **Detect**: The operator's attention is drawn to the symptoms of an abnormal situation that requires operator response.
2. **Identify**: The operator then identifies the abnormal situation and the part of plant that is affected.
3. **Verify**: The operator then verifies whether the situation is an abnormal situation.
4. **Acknowledge**: The operator acknowledges the alarm having gone through the above 3 steps.
5. **Assess**: The operator then assesses the abnormal situation and determines what corrective action must be taken.
6. **Corrective Action**: The operator carries out the required corrective action to ensure that the plant returns to normal operation or that the risk posed by the abnormal situation has been mitigated.
7. **Monitor**: The operator monitors the process to ensure that the corrective action taken was appropriate i.e. plant returns to normal operation or no further alarms of the same abnormal situation are detected.

The Alarm System shall be designed to support the above 7-step process that the operator needs to follow to respond to an alarm. The System shall exhibit the characteristics as shown in Table 2 below.

Table 2: Alarm System Characteristics to support the operator in the alarm response process

#	Problem Process Phase	Alarm System Characteristic
1	Detect	• Text Size • Segregation of Alarms • Colour • Flashing Text • Sound
2	Identify	Provision of a quick link to the associated process HMI graphic.
3	Verify	Trending and Alarm Page Layout
4	Acknowledge	The previously unacknowledged alarm must then become steady i.e. does not flash.
5	Assess	Trending and Alarm Page Layout
6	Corrective Action	Plant-specific abnormal situation operating procedures (as defined in the D&R process) available on-line via the DCS system with additional hard-copies also available in the control room.
7	Monitor	Trending and Alarm Page Layout

8.6.3 Use of External Annunciators

Wherever possible, no annunciators external to the DCS shall be used.

8.6.4 HMI Design

The HMI design is not part of the scope of this document. However, it shall follow the appropriate Eskom standard and guidelines.

8.7 ALARM SYSTEM PERFORMANCE

Alarm Management is an integral part of the Generation Division risk mitigation systems and as such due diligence and good practice must be applied in all alarm or alarm system design and implementation-phases as well as during the life cycle of the alarm system.

Alarm systems shall be designed, implemented and maintained in such a manner that:

a. Under all reasonably foreseeable conditions, steady state and abnormal conditions, the alarm rate annunciated to the plant operator is manageable.

b. Each individual process alarm meets the following criteria:

- The condition must require plant operator action.
- The alarm must be the best indicator of the condition's root cause.
- The alarm must be resulting from an abnormal condition.
- The plant operator must have adequate time to respond.

c. Each individual alarm must have an associated alarm response procedure as per 240-56355530 Alarm Response Work Instruction; Power Station's Owner Manual, Operating function, Alarm Response Procedures, or equivalent document.

d. Each alarm must be prioritised according to the respective Business Units priority matrix. It is recommended that three priority levels be used (Low, high and Emergency).

8.7.1 Alarm System Champion

As per Section 8.4.1, the site-specific Alarm System Champion shall ensure that the specific performance criteria as laid out in Table 3 below, is met. In addition, the Alarm System Champion shall produce a report .. Following the implementation of a new system or for the maintenance of an existing system, each Power Station must monitor the performance of these alarm systems installed on its plant and take corrective action when the alarm system's performance doesn't meet the key performance indicator (KPI) targets as set out in Table 3.

Alarm Performance Report

8.7.2 Alarm System Key Performance Indicators (KPIs)

Table 3: Alarm System KPIs

Key Performance Indicator	Interim target for systems undergoing an alarm improvement effort	Long-term target / New alarm systems, including refurbished systems
Target Average Process Alarm Rate	< 300 per day	< 150 per day
Percentage of time alarm rate exceeds Target Average Process Alarm Rate	5%	0%
Alarm Priority Distribution based on at least one week of data	~80% Low, ~15% High, ≤ 5% Critical	~80% Low, ~15% High, ≤ 5% Critical
Suppressed Alarms	Zero (Unless as part of defined Shelving, Flood Suppression, or State-based Strategy)	Zero (Unless as part of defined Shelving, Flood Suppression, or State-based Strategy)
Chattering Alarms	10 occurrences or less in a one-week period	0 per day
Standing Alarms (more than 24 hours old)	20 or less in a one-week period	0 per day
Alarm Floods (10 to 20 alarms in a 10 minute period)	≤ 5 per day	≤ 3 per day
Alarm Floods (>20 alarms in a 10 minute period)	≤ 3 per day	0 per day
Changes in Alarm Priority, Alarm Trip Point, Alarm Suppression Status, Point Execution Status	None that is unauthorized. None that are not part of a defined Shelving, Flood Suppression, or State-based Strategy.	None that is unauthorized. None that are not part of a defined Shelving, Flood Suppression, or State-based Strategy.

Following the implementation of a new system or for the maintenance of an existing system, each Power Station must monitor the performance of these alarm systems installed on its plant and take corrective action when the alarm system's performance doesn't meet the key performance indicator (KPI) targets as set out in Table 3.

8.7.3 Alarm Performance Report

The performance report will be produced by the Alarm System Champion. It will include the KPIs as defined in Table 3. The Alarm System Champion may use the template in Appendix A: 10. PRO-FORMA ALARM PERFORMANCE REPORT or an equivalent site-specific defined template. Once the DCS has been commissioned and handed over to site , the Alarm Performance Report must be drawn up quarterly.

8.8 ALARM HANDLING METHODS

8.8.1 Manual Alarm Shelving (Nuisance Alarms)

A nuisance alarm which occurs "too frequently" can obscure those alarms signifying "real" abnormal situations from the operator's attention. These nuisance alarms may be temporarily suppressed (shelved) only if all the following conditions are met:

1. The station shift supervisor is made aware of this problem and authorises the temporary suppression using the template contained in Appendix A: 11. PRO-FORMA TEMPORARY SUPPRESSION REQUEST.
2. The method to suppress the alarm does not suppress other alarms on the same point e.g. the operator must not suppress the high alarm when only the rate of change alarm requires suppression.
3. The DCS holds a record (electronic version) of the suppressed alarms.
4. The DCS can issue a print out of the suppressed alarms which is maintained in a paper file titled “Suppressed Alarms for [Power Station Name]”.
5. The DCS provides a pop-up list of suppressed alarms when the operator for the next shift logs in. The operator must be able to choose to maintain or remove the suppressions.
6. The problem is reported to a site-specific technical person (C&I Engineering/Maintenance) and changes to Alarm System must be made using the Alarm System Management of Change Process. Refer to Section 8.10.13.

8.8.2 Semi-automatic Alarm Suppression (State-Dependent Alarms)

State-dependent alarming implies a dynamic configuration of alarms such that only abnormal situations are alarmed. For example the OFF-state of a system in most cases means that some process variables will be below the alarm values, however, these do not constitute alarms since it is not an abnormal situation.

Therefore, methods must be employed to ensure that no alarms (including stale alarms) are produced in these normal situations. Care should be taken to ensure that the state is in fact the OFF-state and must include operator confirmation of the state.

8.8.3 Automatic Alarm Suppression (Alarm Flood Suppression)

There shall be no automatic suppression of alarms on Eskom Power Stations.

8.8.4 Out of Service Alarms

The suppression of alarms by placing them in an out of service state allows for maintenance to be performed on the alarm [3]. Methods to individually remove and return alarms from/to service should be provided and controlled via access control methods. Alarms that will be out-of-service for extended periods of time should be examined to determine if a temporary alarm is necessary. Should the temporary alarm be needed, Management of Change procedures should be followed. Displays of out of service alarms should be available to indicate all alarms that are currently out of service.

Alarms can be placed in an out-of-service state only if the following conditions are met:

1. The station shift supervisor is made aware of the problem and authorizes placing the alarm in an out-of –service state using the template contained in Appendix A: 12. MAINTENANCE – OUT OF SERVICE REQUEST.
2. The method to place the alarm in an out-of-service state does not affect other alarms on the same point.
3. The DCS holds a record (electronic version) of all out-of-service alarms including any replacements.
4. The DCS can issue a print out of the out-of-service alarms which is maintained in a paper file titled “Suppressed Alarms for [Power Station Name]”.
5. The DCS provides a pop-up list of out-of-service alarms when the next operator logs in.

8.8.5 Consequential, Duplicate and Common Alarms

In cases where alarms indicate the same abnormal condition, these alarms can be fed to a common alarm. The single common alarm will take on the highest priority of the individual alarms. Only the

common alarm will be annunciated with the contributing alarms available to the operator upon further investigation.

8.8.6 Operator Alert Systems

A separate operator alert system is not to be specifically requested with the DCS. It shall be an integrated component of the DCS.

8.9 ALARM DOCUMENTATION AND RATIONALIZATION (D&R)

The D&R process is the accountability of the Alarm System Champion. He will select the D&R team with the following members:

1. Operators – at least 2 from different shifts (Operating Knowledge)
2. Process Engineers/Production Engineers (Process Knowledge)
3. C&I Engineers including C&I Suppliers (DCS Knowledge)
4. Maintenance Engineers (Maintenance Knowledge/Strategies)
5. Safety Health and Environment Personnel

It is important to keep the team small (maximum 8 members) but ensuring that the team is sufficiently represented as per above roles. The Alarm D&R methodology seeks to achieve the performance criteria specified in Section 8.7.2 Alarm System Key Performance Indicators (KPIs) by applying the core principles defined in Sections 0 and 8.5 (Alarm Definition and Alarm Criteria), using a logical, consistent and rigorous method.

For each point on the DCS, the D&R process has the following tasks:

1. Determine which events are alarms.
2. Prioritise these alarms.
3. Document the alarm (including justification, but not limited to this).

8.9.1 Determining which Event is an Alarm

The definition of the alarm translates into the following core principles when identifying an alarm during a rationalization process:

1. **Alarms must require an operator action.**
2. **Multiple alarms should not be produced during a single process event.**
3. **Alarms must activate only on abnormal conditions, not expected cases of operation.**

In essence, <u>if the event does not satisfy all the above 3 principles, then it must NOT be configured as an alarm.</u>

8.9.2 Alarm Classification

Alarms shall be assigned to one or more classes based on the properties of the alarm. Not all the alarms in the same class need to have the same priority. The classes may include Maintenance, Testing, Training, Process etc. These classes will allow for alarms with a certain property to be easily accessed.

8.9.3 Prioritise the Selected Alarms

Once all the points in the DCS have been considered and alarms selected, priority of the alarms (as identified in Section 8.6.1, Annunciated Alarm Priority) need to be set individually, to guide the operator to the alarms that will require his/her attention first.

This priority must take into consideration the severity of consequences of the operator not responding to the alarm and the maximum time that the operator has in which to respond to the alarm.

8.9.4 Document the Alarm

The alarm must be documented in this task as specified in Section 8.9.8, Alarm Documentation.

8.9.5 Area of Impact and Severity of Consequences

The severity of consequences is classified into 4 groups namely **None, Minor, Major, Severe.** These 4 groups of severity of consequence are defined for 3 Areas of Impact namely **Personnel Safety, Environment** and **Economic** (Production Losses etc.). Refer to Table 4 below.

For each point on the DCS, the discussion will be “If this was an alarm and the alarm was annunciated, how severe would the consequences be if the operator did not take action?” for each of the 3 Areas of Impact.
After the severity of consequence for each area of impact has been assigned **separately**, the **worst-case** severity of consequence amongst the 3 areas of impact is taken to be the overall severity of consequence for the alarm.

Table 4: Severity of Consequences for Areas of Impact

		Severity of Consequences			
		None	**Minor**	**Major**	**Severe**
Areas of Impact	**Personnel Safety**	No Injury or Health Effect	• Slight injury (first aid) or health effect • No disability • No lost time recordable	• Injury affects work performance, maximum one week. • Reversible health effects (such as skin irritation).	• Lost time injury >1 week, or worker disabling, or severe injuries, or Life Threatening
	Environment	No Effect	• Local Environmental Effect. • Does not cross fence line. • Contained release. • Little, if any, clean up. • Internal or Routine reporting requirements only.	• Contamination causes some non-permanent damage. • Single complaint. • Single exceedance of statutory or prescribed limit. • Reporting at provincial governmental level.	• Limited or extensive toxic release. • Crosses fence line. • Impact involving surrounding communities. • Repeated exceedances. • Extensive clean-up measures. • Reporting at national governmental level.

	Economic (Costs / Production Loss / Downtime / Quality)	No loss	• Event cost < ZAR 100k. • Reporting required only at the department level.	• Event cost is between ZAR 100k and ZAR 1 Million. • Reporting required at Eskom power station .	• Event cost is > ZAR 1 Million • Reporting at Eskom Holdings level

8.9.5.1 Examples of Assigning Severity of Consequences

If an event had a severity of consequence of MINOR for the personnel safety area of impact, NONE for environmental area of impact and MAJOR for the economic area of impact, then the overall severity of consequence would be MAJOR.

If the overall severity of consequence turns out to be **None**, then this should not be an alarm. However, if the overall severity of consequence is classified as **Minor**, **Major** or **Severe**, then this overall severity of consequence rating will be consolidated with the maximum time to respond to the alarm (as per Section 8.9.6) to arrive at a priority for the alarm.

NOTE: It is inappropriate to consider probability in this D&R exercise. This is based on the premise that the event (however improbable) can occur during the life cycle of the plant.

8.9.6 Maximum Time for Response and Corrective Action

The “maximum time to respond” is defined as the time within which the operator must take action to prevent or mitigate the undesired consequence(s) caused by an abnormal situation. Table 5 specifies the classes for maximum time to respond (t). These classes are based on the principle that if there is a shorter time to respond to Alarm X than another Alarm Y, then Alarm X assumes a higher priority (assuming equal severity of consequences).

Table 5: Maximum Time Available to an Operator to Respond and Correct

Time Response Category	Categorisation Criteria
No Alarm	t > 30 minutes
Promptly	10 < t ≤ 30 minutes
Rapidly	3 < t ≤ 10 minutes
Immediately	t ≤ 3 minutes

NOTE: Exceptions to the “No Alarm” decision can be made in cases where the consequences are severe but require some action that can be taken within a period greater than 30 minutes. However, this has to be justified and documented as stated in Section 8.9.8, Alarm Documentation.

8.9.7 Severity of Consequences and Time to Respond Matrix (Consolidated)

The tables presented in the preceding sections are consolidated to provide a Priority Determination Grid as presented in Table 6 below.

Table 6: Alarm Priority Determination

		Consequence of Severity		
		Minor	**Major**	**Severe**
Maximum Time to Respond	t > 30 minutes	No Alarm	No Alarm	No Alarm
	10 < t ≤ 30 minutes	Low	Low	High
	3 < t ≤ 10 minutes	Low	High	High
	t ≤ 3 minutes	High	Emergency	Emergency

It is recommended that every Emergency alarm have a pre-alarm configured. This recommendation must be considered if it is practical and if there is adequate time for the operator to take effective action to address the pre-alarm.

8.9.8 Alarm Documentation

The documentation used and produced in the D&R process should broadly contain the following as per Appendix A: 9. PRO-FORMA D&R SIGN-OFF SHEET PER ALARM.

- Defines the alarm.
- Defines the alarm purpose.
- Individual matrices used for the determination of the alarm priority.
- Possible causes of the alarm.
- P&ID number.
- Operation Procedure (normal situation)
- Operator action (abnormal situation).
- If applicable:
  - Reason for overriding priority determination as per matrices.
  - Any modifications to the alarm.

If time permits, the following could also be provided as part of the D&R alarm documentation set:

- Method of alarm verification that the operator could use.
- HAZOP study output documents

8.9.9 Alarm Trip Point Selection

- Alarm/Trip points must not be set on normal operation values. This leads to chattering alarms.
- It is poor engineering practice to use a rule of thumb that assigns default values to Low, Low-
- Low, High and High-High alarms (10%, 20%, 80% and 90% are commonly used in poorly designed alarm systems).

8.9.10 Important Guidelines for the Facilitation of a D&R Process

The D&R process is rigorous and time-consuming. Therefore, to achieve success with the D&R process, the following is to be avoided by the Alarm System Champion:

- The D&R is not an equipment design process. Therefore, issues that focus on this must be minuted separately and addressed in equipment design meetings, not in this D&R process.
- Similar grids developed from HAZOP studies should not be used in the D&R process without modification
- Work within the tables provided in Appendix A: 9. PRO-FORMA D&R SIGN-OFF SHEET PER ALARM.
- Begin each event discussion by starting with the matrices provided in Appendix A: 9. PRO-FORMA D&R SIGN-OFF SHEET PER ALARM.
- D&R Sign-off Sheet per Alarm rather than discussion around the alarm causes or other items **(Avoid time consumers that add minimal value to the alarm D&R exercise)**.

8.10 SPECIFIC ALARM DESIGN

When deciding to configure an alarm, always adhere to the principles defined in Section 8.9.1.

8.10.1 Pre-Alarms

In some texts this is referred to as combination alarms [1]. It is poor engineering practice to use a rule of thumb that assigns default values to Low, Low-Low, High and High-High alarms. **Best practice dictates that a point must NOT be alarmed twice for the operator to take the very same action**.

It is recommended that every Emergency priority alarm have a pre-alarm configured. This recommendation must be considered if it is practical and if there is adequate time for the operator to take effective action to the pre-alarm.

8.10.2 Alarm Dead-band

The alarm dead-band attribute ensures that a process value crosses into the normal range by some percentage before its associated alarm returns to the normal state. Good engineering judgement should be employed when choosing dead-bands to minimise nuisance alarms while avoiding excessive deadbands which create stale alarms. Table 7 [2] provides typical starting dead-bands for common signal types.

Table 7: Recommended Dead-Band Starting Points based on common Signal Types

Signal Type	**Dead-band** (Percentage of Operating Range)
Flow Rate	~5%
Level	~5%
Pressure	~2%
Temperature	~1%

8.10.3 Alarm On-Delay and Off-Delay

The On-Delay alarm attribute is used to avoid unnecessary alarms, by allowing alarms to be triggered once the signal has remained in the alarm state for a specified length of time. The Off-Delay alarm attribute is used to reduce chattering alarms by locking in the alarm indication for a specified period after

it has cleared. On-Delay and Off-Delay times should be used after careful evaluation of potential control system operational effects. Table 8 [2] below provides recommended time delays based on signal types.

Table 8: Recommended Delay Times based on common Signal Types

Signal type	Delay Time (On and Off)
Flow Rate	~15 Seconds
Level	~60 Seconds
Pressure	~15 Seconds
Temperature	~60 Seconds

8.10.4 Instrument Malfunctions

Best practice dictates that all sensor points will have Bad Value alarms. These Bad Value alarms shall be configured as Diagnostic priority alarms.

The exception to this rule is when the Bad Value alarm is configured on a sensor that feeds an Emergency priority alarm. In this case, the Bad Value alarm will take on a High priority.

8.10.5 Isolated Process Systems

Alarms from process systems that are isolated (i.e. not in use) shall be suppressed. See Section 8.8.2.

8.10.6 Redundant Sensors, Voting and Emergency Shutdown Systems

It is poor practice to provide alarms for situations that are not abnormal situations and do not require operator action. This is equally applicable to redundant sensors, voting and emergency shutdown systems. It is paramount that the principles defined in Section 8.9.1 is applied consistently across all systems.

8.10.7 ESD Bypasses (For Testing Purposes)

During ESD testing, the operator shall be made aware of the bypass in place, by means of a low priority alarm.

8.10.8 External Device Health and Status Alarms

The principles defined in Section 8.9.1, shall be applied. If individual alarms can be fed to a common alarm, the directions provided in Section 8.8.5, Consequential, Duplicate and Common Alarms must be adhered to.

8.10.9 Flammable and Toxic Gas Detectors

All flammable and toxic gas detector alarms shall be Emergency priority.

8.10.10 Safety Shower and Eyebath Actuation

All safety shower and eyebath actuation alarms shall be Emergency priority. The rationale here is that someone has been exposed (to a hazardous chemical) and needs help immediately.

8.10.11 Building-related Alarms

Smoke, fire, carbon monoxide, explosive gases, low percentage oxygen shall all take Emergency priorities.

8.10.12 DCS System Status Alarms

The principles defined in Section8.6.1 shall be applied.

8.10.13 Management of Change

The site-specific Management of Change document shall be adhered to.

8.11 TRAINING

8.11.1 Initial Training

The initial training will be coordinated and provided by the DCS supplier and contain the following as a minimum:

- General overview of the Alarm Philosophy.
- Core principles that the operator has to adhere to (e.g. every alarm requires a response as identified in the D&R exercise).
- Section-by-section description of the requirements of the alarm philosophy.
- The audible and visual indications for alarms provided by the DCS including the use of HMI features and distinction between priorities as well as corrective actions for each alarm.
- Proper methods for suppression, removing alarms from service etc.
- Alarm System Management of Change process (Provided by Eskom).

8.11.2 Initial Maintenance training

The initial training will be coordinated and provided by the DCS supplier and contain the following as a minimum:

- General overview of the Alarm Philosophy
- Alarm System Management of Change process (Provided by Eskom)
- Periodic testing requirements
- Equipment repairs/replacement
- Suppression/Out-of-service requests

8.11.3 Refresher Training

Refresher training will be conducted to keep operators up-to-date with modifications to the alarm system. Training shall be provided by Eskom.

8.11.4 Training Documentation

Training will be documented and contain the following information at minimum:

- The person trained
- Dates of training
- Last date of training
- Methods of training

8.12 MAINTENANCE

Maintenance of the alarm system is essential to keep it functioning optimally. This will include periodic reporting, testing, replacements and repairs. The design of the Alarm System shall take into consideration the maintenance aspects identified below.

8.12.1 Periodic testing

Periodic testing [3] shall be determined by the classification and criticality of the alarm. When tests are performed, records shall be kept and shall contain at minimum the following:

- Date(s) of testing.
- Names(s) of person(s) who performed the test.
- Equipment identification (Loop Number, Tag Number, Equipment Number etc.).
- Results from test.

Test procedures should be provided for all alarm testing and contain at minimum the following:

- Steps for placing the alarm in an out-of-service state as well as steps to place the alarm back into service.
- Information regarding affected control loops and equipment.

8.12.2 Equipment Repair

Malfunctioning alarms resulting from equipment failures should be placed in an out-of-service state if the equipment cannot be repaired in a reasonable time. The rationale for this action is that the operator is not overwhelmed with instrument-malfunction alarms.

8.12.3 Equipment Replacement

If identical replacement equipment is not used, resulting in a change of operating conditions or alarm attributes, Management of Change procedures need to be adhered to. The replacement will require the alarm to be validated to ensure the functionality of the alarm is preserved.

8.12.4 Out-Of-Service State

Alarms must be placed in an out-of-service state during maintenance. A list of out-of-service alarms should be available to the operator including their replacements if applicable.

APPENDIX A: 9. PRO-FORMA D&R SIGN-OFF SHEET PER ALARM

Date: YYYY-MM-DD

Attendees: _____

_____

_____

_____

_____

_____

_____

_____

1. Alarm KKS / AKZ (including 3rd level breakdown): _____ _____ _____ _____
2. Alarm Description (Displayed on DCS):

_____

3. Alarm Purpose:

_____

_____

_____

4. Alarm Value

_____

5. P&ID Number: _____ / _____

6. Severity of Consequences: "If this was an alarm and the alarm was annunciated, how severe would the consequences be if the operator did not take action ?" for each of the 3 Areas of Impact (Personnel Safety, Environment, Economic):

		Severity of Consequences			
		None	**Minor**	**Major**	**Severe**
Areas of Impact	**Personnel Safety**	No Injury or Health Effect	• Slight injury (first aid) or health effect • No disability • No lost time recordable	• Injury affects work performance, maximum one week. • Reversible health effects (such as skin irritation).	• Lost time injury >1 week, or worker disabling, or severe injuries, or Life Threatening
	Environment	No Effect	• Local Environmental Effect. • Does not cross fence line. • Contained release. • Little, if any, clean up. • Internal or Routine reporting requirements only.	• Contamination causes some non-permanent damage. • Single complaint. • Single exceedance of statutory or prescribed limit. • Reporting at provincial governmental level.	• Limited or extensive toxic release. • Crosses fence line. • Impact involving surrounding communities. • Repeated exceedances. • Extensive clean-up measures. • Reporting at national governmental level.
	Economic (Costs / Production Loss / Downtime / Quality)	No loss	• Event cost < ZAR 100k. • Reporting required only at the department level.	• Event cost is between ZAR 100k and ZAR 1 Million. • Reporting required at Eskom power station or Generation Cluster Level.	• Event cost is > ZAR 1 Million • Reporting at Eskom Holdings level

Place an "X" for each of the 3 Areas of Impact (Personnel Safety, Environment, Economic).

7. Overall Severity of Consequences (worst-case for the 3 Areas of Impact – place an “X”):

None	Minor	Major	Severe

8. The “maximum time to respond” is defined as the time within which the operator must take action to prevent or mitigate the undesired consequence(s) caused by an abnormal situation.

Time Response Category	Categorisation Criteria
No Alarm	t > 30 minutes
Promptly	10 < t ≤ 30 minutes
Rapidly	3 < t ≤ 10 minutes
Immediately	t ≤ 3 minutes

Place an “X” for the time response category.

9. Determine the Priority of the alarm using the information gained in points 7 and 8.

		Consequence of Severity		
		Minor	**Major**	**Severe**
Maximum Time to Respond	t > 30 minutes	No Alarm	No Alarm	No Alarm
	10 < t ≤ 30 minutes	Low	Low	High
	3 < t ≤ 10 minutes	Low	High	High
	t ≤ 3 minutes	High	Emergency	Emergency

Place an “X” for the alarm priority.

NOTE: Exceptions to the “No Alarm” decision can be made in cases where the consequences are Severe but require some action that can be taken within a period greater than 30 minutes.

10. If applicable:
a. Reason for overriding priority determination as per matrices:

_____

b. Any modifications to the alarm:

11. Specify the Operator Action when the alarm is annunciated (Abnormal Situation).
Please use a point-form format:

12. Specify the Possible Causes when the alarm is annunciated:
Please use a point-form format:

13. Additional Information
If time permits, please attach the following information:

- Operation Procedure (normal situation)
- Method of alarm verification.

- Output documents from the associated HAZOP study.

14. Alarm System Champion Signature

Name: _____

Signature: _____

Date: _____

APPENDIX A: 10. PRO-FORMA ALARM PERFORMANCE REPORT

Date: YYYY-MM-DD

#	Key Performance Indicator	Target	Measurement
1	Average Process Alarm Rate	< 150 per day	
2	Percentage of time that the alarm rate exceeds the target Average Process Alarm Rate	0 %	
	Alarm Event Priority Distribution based on at least 168 hours (1 week) of data.	• Emergency <= 5% • High ~ 15% • Low ~ 80%	
4	Suppressed Alarms	0 per day (unless part of defined shelving)	
5	Chattering Alarms (Alarms that come and clear at a rate of > 3 times per minute)	0 per day	
6	Stale Alarms (more than 24 hours old)	0 per day	
7	Alarm Floods Type 1 (more than 10 alarms in a 10-minute period)	<= 3 per day	
8	Alarm Floods Type 2 (more than 20 alarms in a 10-minute period)	0 per day	
9	Changes to Alarm Priority, Trip Point, Suppression	No unauthorised changes.	

Alarm System Champion Signature

Name: _____

Signature: _____

Date: _____

Production/Operations Manager Signature

Name: _____

Signature: _____

Date: _____

APPENDIX A: 11. PRO-FORMA TEMPORARY SUPPRESSION REQUEST

Date: YYYY-MM-DD

1. Alarm KKS / AKZ (including 3rd level breakdown): _ _____ _____ ____
2. Alarm Description (Displayed on DCS):

_____

3. P&ID Number: _____ / _____
4. Reason for Alarm Suppression:

_____

_____

_____

5. Date and time of suppression enforcement

   YYYY-MM-DD at HHhmm

6. Date and time of intended suppression removal

   YYYY-MM-DD at HHhmm

Operator's Signature

Name: _____ Signature: _____

Date: _____

Shift-Supervisor's Signature

Name: _____ Signature: _____

Date: _____

Suppression Removed:

Operator's Signature

Name: _____ Signature: _____

Date: _____

APPENDIX A: 12. MAINTENANCE – OUT OF SERVICE REQUEST

Date: YYYY-MM-DD

1. Alarm KKS / AKZ (including 3rd level breakdown): _____ _____ _____ _____
2. Alarm Description (Displayed on DCS):

_____

3. P&ID Number: _____ / _____
4. Reason for taking alarm out-of-service:

_____

_____

_____

5. Date and time of placing alarm out-of-service

YYYY-MM-DD at HHhmm

6. Date and time of placing alarm back in service

YYYY-MM-DD at HHhmm

Operator's Signature

Name: _____ Signature: _____

Date: _____

Shift-Supervisor's Signature

Name: _____ Signature: _____

Date: _____

Suppression Removed:

Operator's Signature

Name: _____ Signature: _____

Date: _____