TATA STEEL

TATA

Tata Steel Technical Directive

R2301001 Alarm philosophy Tata Steel IJmuiden BV

ISA 18.2 Step 1 in the Alarm Management Lifecycle process

Author: V. Toorenburg

Edition: 1-3-2017
Version 1.0

The latest version can be retrieved from https://www.tatasteeleurope.com/ts/nl/gezondheid-en-veiligheid/toegang-en-veiligheid-ijmuiden/voorschriften

Information on

Contents of document:	V. Toorenburg, PTC EIC	+31 (0)251-494428
Standardisation:	ptc-adm@tatasteel.com	+31 (0)251-494443

Table of contents

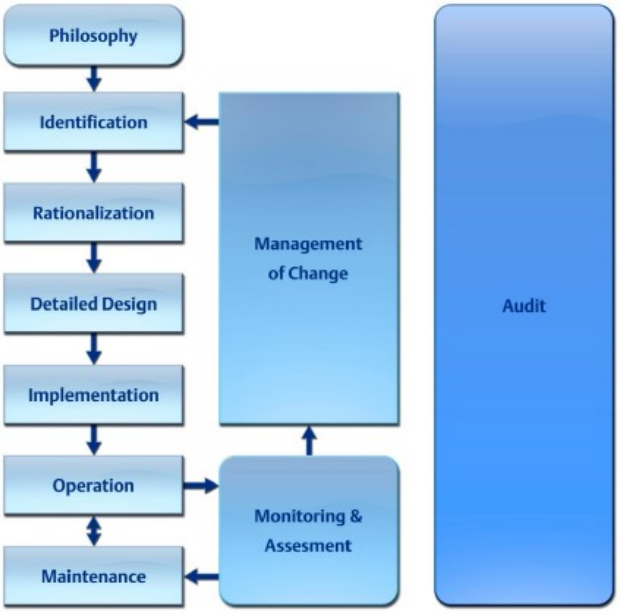
1 Alarm philosophy Tata Steel IJmuiden

1.1 Introduction

The purpose of this document is to establish the objectives, guidelines, principles and work processes for the alarm system. A properly functioning alarm system can help the process to operate closer to the ideal operating point. This results in higher yields, reduced production costs, increased throughput and higher quality. In the past ineffective alarm systems have often been designated as factors that contributed to serious process accidents. In fact the operator is pre-occupied with many alarms, many of which should not even be considered as alarms. As a result, the possibility exists that the operator does not assess the real alarms correctly or even misses them, with potentially serious accidents or process disruptions as a result.

The philosophy in this document is based on the following standard:
BS EN IEC 62682: 2015: Management of Alarm Systems for the process industry. This standard is derived from the ISA 18.2 standard: Alarm Management Lifecycle.

In this latter standard, this "Alarm Management Lifecycle" scheme is included:



The alarm philosophy constitutes the first step in the "Alarm Management Lifecycle" process.
It is important to determine first what an alarm is.

1.2 What is an alarm?

According to ISA-18.2 an alarm is:

1. an audible and / or visual form of an indication
2. for the operator
3. of the failure of a production component, process deviation or an abnormal condition,
4. for which an action of the operator is required.

1) There must be an indication of the alarm.
2) The indication should be sent to the operator to be an alarm.
3) The alarm must indicate a problem and not a normal process condition.
4) There must be an operator-defined action in order to restore the condition and bring back the process to the desired situation (safe and / or productive).

We can only speak of an alarm when the four conditions are met. Otherwise the situation is regarded as an event (log) or status message. See appendix 2.1 for examples of alarms.

1.3 Alarm priority

As already indicated, alarms require actions from operators, however, most of the systems generate so many alarms that it is impossible for the operator to handle all of them at the same time. It is therefore important to give each alarm a priority so that the operator is assisted in the handling of alarms. ISA 18.2 recommends to use four alarm levels: critical, high, medium and low.

From the operators perspective the alarm priority is determined by:

- The available time
- The required activities
- The possibilities to intervene
- The potential consequences of the disturbance (severity of consequence).

Tata Steel selected to relate the priority to the severity of consequence (the matrix is based on the risk matrix according to QHSE 5.01 of Tata Steel):

Alarm priority matrix						
Potential consequence when alarm is ignored						**Priority**
Category	**Health and Safety**	**Environment**	**Reputation**	**Financial**	**Product- and service quality**	
Catastrophic	≥ 5 fatalities on-site and/or one or more fatalities off-site	Very large excess of allowable emissions. Very serious contamination of ground or water course; long-term loss of aquatic life	Continuing international unrest. Prolonged damage TATA name	> € 100 million	Loss of considerable market share	Critical
Major	One or more (<5) fatalities and/ or major injuries on-site. People off-site hospitalised.	Excess of allowable emissions and serious damage to the environment.	National unrest. External investigation, nationwide media attention	€ 10 -100 million	Loss of clients	Critical
Severe	Severe injuries with lost time (LTI) on-site and/ or minor health and safety effects off-site	Repeated limited excess of allowable emissions; disturbing visual evidence.	Regional unrest, negative attention nationwide media	€ 0,5 - 10 million	Complaints from several clients	High
Moderate	Moderate injuries, modified work (recordable). No health and safety effects off-site	Excess of allowable emissions; notifiable release, possible warning from authorities.	Local unrest, possible local media attention	€ 100.000 - 500.000	Formal client complaint	High
Minor	Minor injuries or health effects, first aid treatment, no impact on employability	Small amount released to water course; release may be notifiable to authorities.	No public unrest, no media attention	€ 10.000 - 100.000	Off-spec/ failure to comply appointment	Medium
Not significant	No effects	No effects	No effects	< € 10.000	No complaints	Low

Besides the priority, the sub-priority for operator handling for each alarm has to be assigned. There are two levels defined: 1) direct action, 2) postponed action.

Important:
Assignment of the alarm priority shall be based on the situation that, when an alarm becomes active, the existing control- and safeguarding systems will not intervene. This is equal to ignoring the alarm with related potential consequences as result.

The setup of the matrix results in higher priority alarms chosen less frequently than lower priorities. This contributes to the effectiveness of the alarm priorities (see table paragraph 1.8: “annunciated priority distribution”).

The alarm priority “critical” shall only be applied in exceptional conditions. When an alarm is considered “critical”, the design of the (process) section needs to be reviewed to determine if the design can be modified (safety by design). When this is not feasible these critical alarms shall, besides on the HMI alarm list, be signalled on a separate annunciator panel. This to increase the availability of the alarm.

1.4 Alarm Classification

According to the standard each alarm is to be given a rating. This classification is intended for administrative purposes such as to indicate that an alarm should periodically be tested or that it is an alarm which is intended for reporting. The alarm classification that Tata Steel applies is to give each alarm a classification that indicates for which department the alarm is intended. By filtering (for example, on the basis of the log-in name), the alarms are shown on the alarm screens of the relevant departments (see remark 1 §1.15).

Please note however, that an alarm that is not intended for the operator is not an alarm (as defined in paragraph 1.2). By using the alarm functionality of software packages, priorities could be allocated to error messages by allocating colour profiles similar to that of the alarms.

The following alarm classes are defined:
PRO = production, operator
STD = maintenance shift
TBE = technical management
KTO = quality management and technical development

These classes can be followed by a number in order to create a partition within the alarm class, for example:

PRO-01 = Alarm for production entry section
PRO-02 = Alarm for manufacturing, process section.
STD-01 = Alert for maintenance shift, Y-department
STD-02 = Alert for maintenance shift, W-department
STD-10 = alert for external service organisation A where for example an automatic text message or E-mail is sent or the message is reported via an app.

1.5 Limitation of nuisance alarms

To limit nuisance alarms use can be made of alarm suppression. Alarm suppression is any mechanism that is used to prevent the indication of an alarm to the operator when the alarm condition is present. “Shelved”, “Designed Suppression” and “Out of service” are methods to suppress alarms:

- A “Shelved alarm” is an alarm that has been temporarily disabled because the component, for example, is in maintenance or because it is temporarily not working correctly and can be

restored within a short time. It is important that the alarm system periodically reports these alarms, so it will not be forgotten to put these alarms back to the normal alarm mode.
- A “Suppressed by design alarm” is an alarm that is suppressed by the logic in the control system (PLC). This could be alarms for units that are switched off and do not affect the production process. These alarms are suppressed as they would otherwise cause nuisance alarms on the operator screens and alarm lists.
- An “Out of service alarm” is an alarm that is disabled because, for example, a part is broken but cannot be repaired or replaced immediately. Here it is important to re-activate the alarm active as soon as the component is operational again.

Remark: the use of “shelving” and “out-of-service” is advised only when these are standard features of the visualisation software. When this is not the case these methods shall not be created.

To reduce nuisance alarms further, it is advised to provide a certain dead band, possibly in combination with on/ off time delays (see remark 2 §1.15):
- The “dead band” (hysteresis) is the change of the alarmed signal with respect to the alarm set point necessary to activate or deactivate the alarm.
- The “on/ off delay time” is the time in which the process measurement of the alarm/ normal status must remain before an alarm is activated / deactivated.

The following table is used as starting values (bulk of the alarms) for dead band and on/ off time delay settings (source ISA 18-2):

Signal Type	Dead band (percent of range)	Delay Time (On or Off)
Flow Rate	5%	15 seconds
Level	5%	60 seconds
Pressure	2%	15 seconds
Temperature	1%	60 seconds

For each alarm the parameters will be recorded in the Master Alarm Database (see §1.7).

1.6 Configuring alarm functionality

It is advised to make use of the standard functionality in both PLC as SCADA/HMI software for as much as this is possible. So the logic for when a signal becomes an alarm (alarm thresholds, hysteresis, time delays, suppressing logic) shall be in the PLC software and the visualisation options of the alarm (priority, flashing, colour changes, shelving, out of service conditions, acknowledgement and alarm classes) are configured in the SCADA/ HMI software.

1.7 Master Alarm Database (MADB)

Alarm parameters (among others settings) are documented in a master alarm database. This database also contains important details that were discussed during alarm rationalisation: the cause, consequence and recommended operator action. This information in the MADB shall be used during different phases in the alarm life cycle (see remark 3 §1.15). Modifications to the alarms in the MADB shall be done via the management of change procedure (see §1.9). Only after this procedure modifications may be implemented in the alarm system. See appendix 2.2 for data fields of the MADB.

1.8 Monitoring and evaluation

It is important to check the operation of the alarm system and assess it, related to key performance indicators (KPI). Particularly envisaged here are the number of alarms that an operator will process per period of time, but also the number of critical alarms in relation to the total number of alarms. Standard

18-2 contains a table of possible "alarm performance metrics" that can be used. For Tata Steel it is advised to use the values as stated in the table below:

Alarm Performance Metrics Based Upon at Least 30 Days of Data		
Metric	*Target Value*	
Annunciated alarms per time	Target value: very likely to be acceptable	Target value: maximum manageable
Annunciated alarms per day per operating position	150 alarms per day	300 alarms per day
Annunciated alarms per hour per operating position	6 (average)	12 (average)
Annunciated alarms per 10 minutes per operating position	1 (average)	2 (average)
Metric	*Target Value*	
Percentage of hours containing more than 30 alarms	<1%	
Percentage of 10-minute periods containing more than 10 alarms	<1%	
Maximum number of alarms in a 10-minute period	<10	
Percentage of time the alarm system is in a flood condition	<1%	
Percentage contribution of the top 10 most frequent alarms to the overall alarm load	<1% to 5% maximum, with action plans to address deficiencies	
Quantity of chattering and fleeting alarms	Zero, develop action plans to correct any that occur	
Stale alarms	<5/day, with action plans to address	
Annunciated priority distribution	If using four priorities: 80% low, 15% medium, 5% high, <1% critical	
Unauthorised alarm suppression	Zero alarms suppressed outside of approved methodologies	
Unauthorised alarm attribute changes	Zero alarm attribute changes outside Management Of Change	

The analysis of the alarm system also includes determining which alarms occur often (top 5), what the standing time is of alarms, which alarms remain standing for long periods, which alarms are ineffective or which alarms frequently switch on and off in a short time. Through this analysis, the number and frequency of alarms can be optimised to reduce the load on the operator and to enhance the efficiency of the operator.

1.9 Management of Change (MOC)

Management of change requires the use of tools and procedures to ensure that changes in the alarm system are assessed and approved, before these changes are implemented (see §1.7). The alarm system should have the ability to assign access rights to specific user groups and individuals. This determines who should make adjustments in the alarm system and what may be changed. Any changes should be recorded with a time and date stamp, the "from" and "to" values and which person made the change.

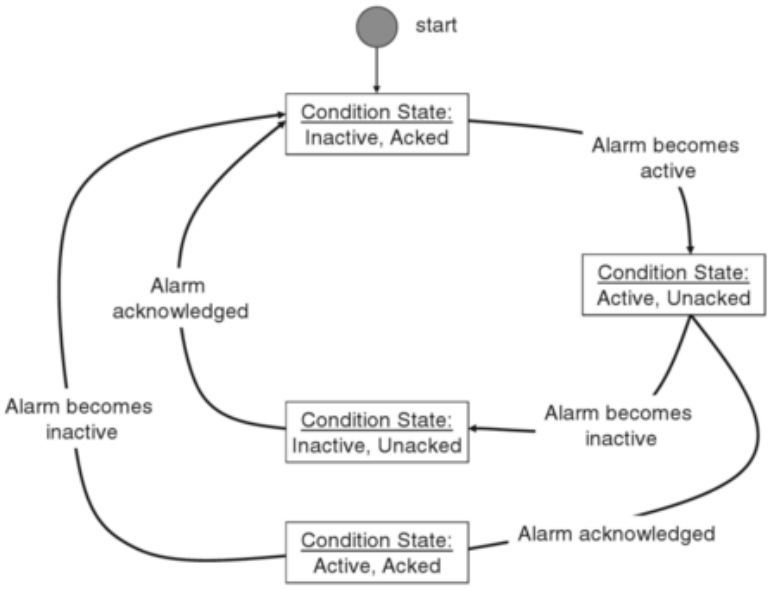
1.10 Audit

During this phase (see scheme §1.1) the operational alarm system must be verified for the things included in this document. Should the alarm philosophy require changes during the audit process, then these changes must be reflected in this document.

1.11 Alarm stages and status indications

1.11.1 Alarm stages

An alarm goes through several stages:



By using buttons on the HMI screen or alarm list, alarms can be acknowledged (acked). Often there is a separate button to turn off the sound after a new alarm has occurred. The acknowledge button has the same function. Per alarm class (§1.4) can be set if an alarm must be reset manually or if this is done automatically. For alarms with class PRO the operator shall always acknowledge manually (see §1.2 point 1).

1.11.2 Alarm status indications

The following table shows the alarm status indications:

Alarm state	Audible Indication	Visual Indication (HMI graphic & alarm list)		
		Colour	Symbol	Blinking
Normal	No	No	No	No
Unacknowledged (new) alarm	Yes	Yes	Yes	Yes
Acknowledged alarm	No	Yes	Yes	No
Return to normal state indication	No	No	No	No
Unacknowledged latched alarm*	Yes	Yes	Yes	Yes
Acknowledged latched alarm*	No	Yes	Yes	No
Shelved alarm	No	No	Yes**	No
Designed Suppression alarm	No	No	Yes**	No
Out of service alarm	No	No	Yes**	No

* Requires reset by operator. See Alarm State Transition Diagram in ISA18.2

** On HMI graphic only. Use symbol “S” see §1.12.1.

1.12 Alarm display

1.12.1 Visual

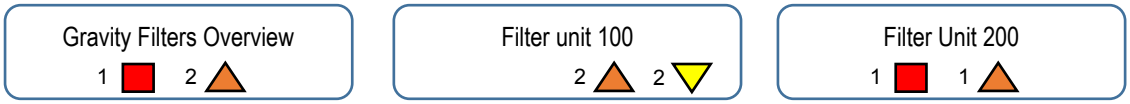
To help the operator to quickly identify which alarms (first) need action, use is made of unique mechanisms for visual display (see remark 4 §1.15):

Priority:
0 = critical
1 = high
2 = medium
3 = low
S = suppressed; for suppressed alarm functionalities.

There is a redundant visualisation of the priority of the alarm by the shape of the alarm indicator, the colour and the priority number. This threefold coding guarantees that the alarms are clearly visible on the Human Machine Interface (HMI) screens. It is important that the black lines around the symbols are used. The lines are an integral part of the symbols.
The alarm indications appear and disappear with the (de-)activation of the alarm condition. There is no indication of the specific type of the alarm (i.e. H, L, LL, bad PV etc.); this will be indicated on the faceplate of the item and/or on the alarm list.

The symbol table in paragraph 1.11.12 shows the symbols of the various alarms statuses.

By clustering the alarms by priority and by displaying them graphically on the navigation buttons on the screen, a clear overview of the (alarm) status by section is obtained:



The navigation buttons are used to navigate directly to the relevant screen image, so that the alarm can be handled.

1.12.2 Alarm list

The alarm list shows the alarms (or messages, see §1.4) in tabular form on a screen. In this list the priority is indicated with colour as explained in the previous paragraph. If technically possible any alarm row/ signal should have an accompanying text, indicating what should be the recommended action. Also the sub-priority should be displayed. This information comes from the Master Alarm Database.
For efficient alarm management a separate monitor for alarms for each operator is strongly recommended. The use of an alarm banner (alarm rows) on the HMI screens is discouraged.

1.12.3 Alarm sound

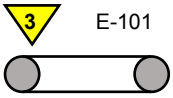
Each alarm should have its own alarm sound for each type of priority. In a control room with different operating positions this may create a problem because, on the basis of sound, it will be difficult to determine on which operating position the new alarm occurs. One could choose for a "family" of sounds per operating position. One can also choose to use a light cylinder consisting of 4 lights with colours per operating position, corresponding with the priority colours. These lights are then activated instead of, or together with the alarm sound.
The use of a single type of sound for the different alarm priorities is strongly discouraged.

1.13 Status display

For these signals, specific HMI screens can be made, so that the status of certain components (e.g. all pumps of a section, fuses in a distributor, system status, etc.) can be displayed clearly. These will be screens without alarms and specifically meant for technical and maintenance personnel. The operator can call up these screens too.

Example:
In the alarm list for the operator the following alarm is visible:
“Conveyor belt E-101 not available”.

On the HMI screen for the operator appears:



On the HMI screen for the maintenance personnel the result will be:

Equipment	Inspection switch off	Thermally tripped	Start time exceeded	Phase fault detected
E-100				
E-101		3		
E-102				

(in this case the priority of the status message for E-101 is based on the corresponding E-101 alarm).

In the “alarm” list for the maintenance personnel is shown:
“Conveyor belt E-101 thermally tripped”.

Remark:
Status signals and messages to inform operators are shown on the HMI screens for the operators. Examples: valve positions, positions machine parts, pump active, truck unloading started, etc.

1.14 Event (log) list

This list contains all the events in tabular form on a screen. This list could be a tab of the alarm list, but the events shall not be part of the alarm list. An event is a detectable significant status change. Events cannot be acknowledged by the operator. An event is a unique point in time, while an alarm has a start and an end time. An event includes: alarm acknowledgments by the operator, set point changes, status changes etc.

1.15 Remarks

Remark 1 (paragraph 1.4):
Currently the operator is often the one responsible for the handling of all alarms and alerts on alarm screens. If this is the case, there needs to be a temporary arrangement, where the operator is shown all alarm classes. When the organisation is capable of handling alarms by the relevant departments, the operator will only get to see the PRO alarm classes. So it is important that during the rationalisation of alarms (step 3 schedule paragraph 1.1) the alarm classes are allocated to alarms and notifications so that the desired structure can be realised (later).

Remark 2 (paragraph 1.5):
A study by the Abnormal Situation Management (ASM) Consortium has shown that by the use of on/ off time delay to alarms in combination with configuration changes (such as dead band adjustments) alarm loads on the operator may be reduced with 45- 90%.

Remark 3 (paragraph 1.7):
In practice, it often happens that it is forgotten why an alarm is configured, but it is assumed that there was a reason for it and therefore it cannot be deleted. One can refer to the MADB to find out why a specific alarm was created and based on this, the alarm may be deleted.

Remark 4 (paragraph 1.12.1):
The approach is based on the book: “The High Performance HMI handbook” from B. Hollifield and others. It is expected that this approach will be incorporated in the ISA101 standard “Human Machine Interfaces” that is to be released. In the “High Performance HMI handbook”, the symbol for the critical alarm (pink diamond shape) is used for alarms with diagnostic priority. This handbook has no symbol for alarms with critical priority, even though this is recommended according to ISA 18.2. As diagnostic priorities are not part of ISA 18.2, there is a deviation on this point from the handbook. Also the colours for priority 2 and 3 are switched.

2 Appendix

2.1 Some examples of alarms

Situation	Alarm?	Explanation
High level Tank 1001 activated	Yes	The automatic controller should keep the process between the operational limits of the tank. This was not successful and the operator has to take action to prevent the tank from overfilling.
High high level Tank 1001 activated (HH-trip)	Yes	The process will stop via the safeguarding system because of the HH value. This is an abnormal situation. The operator will have to take action to recover the process.
Level measurement LT-001 Tank 1001 fault ('bad PV, transmitter fail')	Yes	The level measurement is not reliable anymore and because of this the process cannot be controlled.
The system automatically switches a pump on/ off between low and high tank level	No	In this case limits have been configured to initiate control actions. These are normal operating conditions.
Conveyor belt E-101 not available	Yes	This indicates a production equipment problem. This can have different causes. See next 2 points.
Inspection switch conveyor belt E-101 switched off	No	This is a status message. On the HMI this status can be displayed. It is not an alarm (see previous point).
Conveyor belt E-101 thermally tripped	No	See previous point.
Pressure measurement PI-1001 diagnostic message (not being 'bad PV').	No	Information for technical and maintenance personnel
Emergency stop 1001 activated	Yes	This is an abnormal condition which requires operator action.
Zinc layer thickness on strip too thick	Yes	This is a process deviation which leads to quality problems
Communication fault on profibus / ethernet / etc.	No	Is a message for the maintenance department
PLC I/O card failure	No	Is a message for the maintenance department. Signals on the faulty I/O card will generate individual alarms to the operator when applicable.

2.2 Data fields Master Alarm Database

It is advised to also include (fault) messages (“alarms” for technical and maintenance personnel) in the MADB. In this way these messages are managed centrally.

Field	Description
Id	Alarm id number
Tag number	Alarm tag number
Type	Absolute, Deviation, Rate of change, calculated, bad measurement, System diagnostic (see 1.15 remark 3), etc.
Source	Field device, Control System, Safety system, HMI, gas detection etc.
Description	Alarm description.
Consequence of alarm/ no operator action	Description of consequence when alarm becomes active or when operator does not take action after activation of an alarm.
Corrective action	Description of action to be taken by operator
Class	PRO, STD, TBE, KTO (see 1.4)
Set point or logical condition	Set point value, off-normal, on-normal.
Potential Consequence	Catastrophic, Major, Severe, Moderate, Minor, Not significant (see 1.3 matrix)
Consequence category	Health/ Safety, Environment, Reputation, Financial, Product and service quality (see 1.3 matrix)
Priority	Critical, High, Medium, Low (see 1.3 matrix)
Sub priority	Direct action, postponed action (see 1.3).
Dead band	% (see 1.5)
On/ off delay timer	Time (see 1.5)
Change	Description of changed field
Reason for change	Description
Change date	Date
Responsible for change	Name
Change implemented	Is change implemented in the alarm system (Yes/ No).
Remark 1	Description
Remark 2	Description