Appendix 1: Process for Managing Instrumented Alarm Functions credited with risk reduction against MAH’s

![Diagram](image)

**Figure 1:** Process for the management of Instrumented Alarm Functions credited with risk reduction against MAH’s
Operator Response within Instrumented Safety Functions in the Chemical, Oil & Gas, and Specialist Industries

Notes to Figure 1:

Note 1: Identification of instrumented alarm functions providing risk reduction could be from hazard identification, risk assessment (e.g. HAZOP) or from review of existing plant documentation for legacy plant or installed SIS Review and Assessment.

Note 2: Any new or existing instrumented alarm function, identified to provide risk reduction, has to be assessed to determine its risk reduction requirements. Note that the dutyholder should consider at this early stage if it is reasonably practicable to automate the response, especially if this relates to a new design / modification, prior to SIL assessment. See also note 5 below and section below on 'Preference for Automation'.

Note 3: A risk reduction factor of greater than 100 (i.e. SIL 2) should not be claimed for a SIAF as this would require human reliability better than normally achievable. Typically redesign would involve considering automating the alarm response, reducing the likelihood of the hazard causes, or providing additional risk reduction measures (considering the normal hierarchy of control measures). If this cannot be achieved then the SIAF falls outside the scope of this guidance and additional demonstration that all measures necessary have been taken will be required.

Note 4: In this case the assessment has indicated that the risk reduction required is a factor of 10 or less and therefore the alarm function is not a SIAF or a SIS. The function can be implemented in the normal control system or other systems as required. However, this alarm function does provide some risk reduction and therefore, should be implemented to good practice requirements for a LISIAF – further guidance below.

Note 5: For a SIL1 SIAF, the dutyholder should consider if it is reasonably practicable to redesign in order to remove the requirements for operator response, noting the section below on 'Preference for Automation'.

Note 6: The function should be implemented to good practice requirements for a SIAF – further guidance below.

Note 7: If it is reasonably practicable to redesign the plant to remove the necessity for a SIAF, this should be completed. If the function defined is to be automated, it should be implemented to good practice (e.g. BS EN 61511).

Preference for Automation

1. This preference for automatic systems is often referred to as 'hierarchy of control measures' and good practice typically maximises the use of inherent safety and the elimination of hazards; the avoidance of risk; the control of risk at source by the use of physical engineering controls; whilst it minimises the need for: procedural controls, e.g. to manage manual operation of safety functions, and personal protective equipment. (see www.hse.gov.uk/risk/theory/alarp2.htm)

2. Note that an automatic response does not necessarily require immediate plant 'shutdowns'. The response need only be sufficient to effectively prevent the hazardous scenario. For example: an automatic response may be to divert
Operator Response within Instrumented Safety Functions in the Chemical, Oil & Gas, and Specialist Industries

- product to another tank in the event of a high level or to initiate a timed shutdown to allow appropriate operator action to be taken to recover the process before the hazardous event and shutdown occurs. However, it is always preferable to have an automatic ‘back stop’ following failure of the operator to recover.

3. For new and modified plant, it will be more likely that it will be reasonably practicable to automate the response or redesign the plant to remove the necessity for a SIAF. However, it is acknowledged that for legacy plants, it may not be reasonably practicable to automate or redesign, or that an automatic response will generate an overall risk.

4. In any case, the dutyholder should record the decision-making process to demonstrate where it is not reasonably practicable to automate or redesign.

**Good Practice Requirements for LISIAF (PFD > 0.1)**

5. The LISIAF shall meet the relevant requirements of good practice for low integrity instrumented safety functions, e.g. HSE Operational Guidance OG-46, as well as the relevant requirements of good practice for alarm systems, e.g. BS EN 62682. This includes:

   a. Assignment to a highly managed alarm classification group (LISIAF), which has appropriate management arrangements in place (to be defined in the alarm philosophy) to ensure the reliability of the alarm function, including requirements for shelving, out of service process and management of change;

   b. The wider alarm system within which a LISIAF is implemented should meet general alarm system performance requirements to ensure that issues such as alarm flooding, excessive alarm rates etc. to not mask the LISIAF.

   c. Clear, precise and unambiguous specification of and written response to the LISIAF to include specification of the sensor, annunciator, operator response and final elements;

   d. Independence between the LISIAF and other protection layers also credited with risk reduction – including the sensor, annunciator, operator response and final elements;

   e. Accurate, accessible, controlled and easily understood engineering documentation showing the component parts of the LISIAF and how they are configured;

   f. Periodic inspection of the LISIAF, e.g. visual or more detailed inspection to reveal evidence of deterioration, damage or unexpected modifications;

   g. Periodic maintenance of the LISIAF in line with manufacturers recommendations and general good practice;

   h. Periodic testing, at intervals determined by the alarm class requirements, to ensure that the alarm continues to perform as designed. The testing procedure should be documented and results recorded to facilitate monitoring and periodic review.
Operator Response within Instrumented Safety Functions in the Chemical, Oil & Gas, and Specialist Industries

i. Sufficient training of operators on the required response to alarms, determined by the alarm class requirements.

**Good Practice Requirements for SIAF (< 0.1 PFD)**

6. The SIAF shall meet the relevant requirements of good practice for SIS (e.g. BS EN 61511) as well as the relevant requirements of good practice for alarm systems, e.g. BS EN 62682. This includes:

   a. Assignment to a highly managed alarm classification group (SIAF), which has appropriate management arrangements in place (to be defined in the alarm philosophy) to ensure the reliability of the alarm function, including no inhibiting or shelving permitted unless managed as a SIS defeat, management of change consistent with other SIS etc.;

   b. The wider alarm system within which a SIAF is implemented should meet general alarm system performance requirements to ensure that issues such as alarm flooding, excessive alarm rates etc. to not mask the SIAF.

   c. The usual SIS lifecycle approach and documentation including demonstration that the SIS meets the risk reduction requirements expected of it. Table 1 below provides additional guidance on how to apply good practice BS EN 61511 to SIAFs.

   d. Additional human reliability requirements – these are also included in table 1 below and are based upon the requirements specified for safety related alarms within EEMUA191 clauses 2.3.3 to 2.3.6 and table 5. Further interpretation of these requirements is shown in table 2.
## Table 1: Application of Good Practice for a SIAF

<table>
<thead>
<tr>
<th>Lifecycle Phase</th>
<th>Sensor, annunciator and final elements</th>
<th>Operator Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management of Functional Safety Clauses 5-7</td>
<td>All normal requirements of BS EN 61511 apply, for example lifecycle, planning, competence, audit and monitoring. This would include monitoring the performance of the SIAF with respect to actual demands and failures associated with the SIAF.</td>
<td></td>
</tr>
<tr>
<td>Setting SIS Requirements Clauses 8-9</td>
<td>All normal requirements of BS EN 61511 apply, however it should be noted that when a PFD is assumed within a SIL assessment for a SIAF, the PFD applies to the full safety function, i.e. sensor, annunciator, operator response and final elements. During SIL assessment, a SIAF or LISIAF should only be considered as an independent layer of protection if all its components (sensor, annunciator, operator response and final elements) are independent.</td>
<td></td>
</tr>
<tr>
<td>Safety Requirements Specification (SRS) Clause 10</td>
<td>In addition to the normal requirements of BS EN 61511, the SRS should specify the alarm sensor, alarm annunciator and final element(s) required to achieve functional safety. The SRS should include requirements to identify and take account of common cause failures associated with the SIAF sensors, alarm annunciator and final elements.</td>
<td>The operator response should be specified in accordance with EEMUA 191 special criteria for human reliability (Table 5): 5 – Alarm Response defined 6 – Alarm Response simplicity The SRS should specify the operator response (or link to the specific alarm response procedure) to achieve functional safety (i.e. alarm should be effective).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The SIAF including the alarm setting should be specified to ensure that there is sufficient time for operator response in both normal and abnormal operating conditions (see also figure 2). The SRS should include requirements to identify and take account of common cause failures associated with the SIAF operator response.</td>
</tr>
</tbody>
</table>

#### Notes:
- **Management of Functional Safety Clauses 5-7**
  - All normal requirements of BS EN 61511 apply, for example lifecycle, planning, competence, audit and monitoring. This would include monitoring the performance of the SIAF with respect to actual demands and failures associated with the SIAF.

- **Setting SIS Requirements Clauses 8-9**
  - All normal requirements of BS EN 61511 apply, however it should be noted that when a PFD is assumed within a SIL assessment for a SIAF, the PFD applies to the full safety function, i.e. sensor, annunciator, operator response and final elements. During SIL assessment, a SIAF or LISIAF should only be considered as an independent layer of protection if all its components (sensor, annunciator, operator response and final elements) are independent.

- **Safety Requirements Specification (SRS) Clause 10**
  - In addition to the normal requirements of BS EN 61511, the SRS should specify the alarm sensor, alarm annunciator and final element(s) required to achieve functional safety. The SRS should include requirements to identify and take account of common cause failures associated with the SIAF sensors, alarm annunciator and final elements.
## Operator Response within Instrumented Safety Functions in the Chemical, Oil & Gas, and Specialist Industries

<table>
<thead>
<tr>
<th>Lifecycle Phase</th>
<th>Sensor, annunciator and final elements</th>
<th>Operator Response</th>
</tr>
</thead>
</table>
| Design & Implementation Clauses 11-15 | In addition to the normal requirements of BS EN 61511, the sensor, annunciator and final elements should be designed in accordance with BS EN 61511 and EEMUA 191 special criteria:  
- 2 – Alarm Annunciator  
- 3 – Alarm Priority  
- 4 – Alarm Visibility  
- 7 – Information  

A PFD calculation should be completed (BS EN 61511 clause 11.9) for the sensor, annunciator and final elements. This should be combined with the PFD of the operator response (see right) to give the overall achieved PFD.  

All of the SIAF components (sensor, annunciator and final elements) should have sufficient independence, and fault tolerance as described in BS EN 61511. | A PFD for the operator response part of the SIAF should be determined (BS EN 61511 clause 11.9.2) based upon the level of compliance with the EEMUA191 special criteria. The basis for the PFD selected should be recorded, for example by making an assessment of the EEMUA 191 special criteria against the level of compliance achieved. If all criteria are only just achieved, then the PFD for the operator response should tend towards 0.1, however if the criteria are fully achieved to a high standard, then a low PFD towards 0.01 can be selected.  

The level of demonstration should be proportionate to the level of risk reduction claimed against the criteria.  

Note – There may be other human factors considerations required. Where PFDs tending towards 0.01 are used it is recommended to seek further input from HF colleagues to ensure that the HF aspects are adequately robust for that claim to be valid. |
<table>
<thead>
<tr>
<th>Lifecycle Phase</th>
<th>Sensor, annunciator and final elements</th>
<th>Operator Response</th>
</tr>
</thead>
</table>
| Operation, Maintenance and Proof   | All normal requirements apply but noting that they should be applied to the SIAF sensor, annunciator and final elements. | The operator response should be operated in accordance with EEMUA 191 special criteria:  
  • 1 – Operator training  
  The operator response should be ‘maintained’ in accordance with EEMUA 191 special criteria:  
  • 8 – Operator Performance  
  This will necessitate periodic validation of the operator training (completed for criteria 1) and performance (criteria 8). Measures should be taken to demonstrate that this is scheduled and completed at an appropriate interval. |
| Test Clause 16                     |                                        |                                                                                                                                                                                                                  |
| Modification Clause 17             | All normal requirements apply, however during modification, consideration should be given to automation if reasonably practicable.                          |                                                                                                                                                                                                                  |
### Operator Response within Instrumented Safety Functions in the Chemical, Oil & Gas, and Specialist Industries

#### Table 2: Special Requirements for SIAF

<table>
<thead>
<tr>
<th>No.</th>
<th>Criteria from EEMUA 191 (Table 5)</th>
<th>HSE Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>The operator should be trained in the management of the specific plant failure that the alarm indicates.</td>
<td>Duty holders should be able to demonstrate implementation of relevant elements of their competence management system (CMS) for each specific SIL rated operator response. Note that the EEMUA 191 criteria requires training in the ‘specific plant failure’ and therefore the competence demonstration should be developed for each scenario that the SIAF is protecting against. Therefore, the role of the operator should be clearly defined in the SRS functional safety requirements description. The CMS should include structured training and assessment as necessary and formal demonstration of competence (i.e. recorded).</td>
</tr>
<tr>
<td>2</td>
<td>The alarm presentation arrangement should make the claimed alarm very obvious to the operator and distinguishable from other alarms.</td>
<td>This requirement (along with criteria 3 &amp; 4 and the more general requirements of overall SIS integrity and independence) will generally require that the alarm is annunciated on an annunciator which is suitably independent from other protection layers and has the top priority reserved for SIAF’s. A typical approach would be to use an independent hardwired annunciator, i.e. outside of the basic process control system (BPCS), although other solutions may be possible.</td>
</tr>
<tr>
<td>3</td>
<td>The alarm should be classified at the highest priority in the system.</td>
<td>The operator should be able to very quickly distinguish between safety critical (i.e. ≥SIL1) alarms and other alarms. Note that the operator should be able to distinguish SIS alarms that rely upon specific operator action from those that alert that an automatic action has occurred and just require checking that it has been successful.</td>
</tr>
<tr>
<td>No.</td>
<td>Criteria from EEMUA 191 (Table 5)</td>
<td>HSE Comments</td>
</tr>
<tr>
<td>-----</td>
<td>----------------------------------</td>
<td>--------------</td>
</tr>
</tbody>
</table>
| 4   | The alarm should remain on view to the operator for the whole of the time it is active. | It should not be possible for the alarm to be masked or hidden. This will generally require that such alarms are separated from other (non-SIL rated) alarms.  

In this context, claims of continuous manning of a particular control panel should also be substantiated, including arrangements to ensure the availability of competent cover for rest breaks, illness, other duties etc. Alarm status should be included in shift handover to ensure operator situational awareness of oncoming shift.  

However, the use of several operators to achieve the operator sub-system does not imply that the reliability claimed can be factored-up accordingly (i.e. ‘1-out-of-2 operators’) due to issues of systematic dependencies.  

Note, if remote alarming facilities are employed (e.g. pagers), then these will have to be considered as part of the SIS and therefore meet the more general requirements for SIS described in good practice such as BS EN 61511. |
<table>
<thead>
<tr>
<th>No.</th>
<th>Criteria from EEMUA 191 (Table 5)</th>
<th>HSE Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>The operator should have a clear written alarm response procedure for the alarm.</td>
<td>Note the use of the word ‘clear’ – this will therefore require it to be quickly identifiable and separate from (or easily distinguishable within) other alarm response manuals. A typical approach is to develop unique job aides (e.g. step by step ‘grab cards’) for each SIAF which are readily available at points of use. The alarm response instruction (ARI) can be on screen rather than being a hardcopy document, though onscreen ARI’s should not hide/block the view of other critical information to the CRO. The limitations of on-screen ARIs needs to be considered as part of the operator response (e.g. does the operator need to use the ARI in one or more locations remote from the screen where it is displayed). Also, the onscreen function will need to be considered as part of the SIS and meet the associated requirements (e.g. independence, integrity, etc.) The information may require initial actions as well as follow up checks (e.g. immediately close valve XV123, and confirm flow to tank T456 is ceased). Measures should be taken to ensure that alarm responses are completed by ensuring that responders are not distracted. Note, that a full description of the function requirements (sensor to final actuator) is required because it will define the full extent of the SIS equipment with the SRS.</td>
</tr>
<tr>
<td>6</td>
<td>The required operator response should be simple, obvious and invariant.</td>
<td>The operator response includes any judgements / decision-making to be completed as well as the actions subsequently required. Decision-making should be kept to a minimum and, where necessary, informed by clearly-defined criteria. If a dutyholder identifies the need for complex operator response then Human Factors Specialist support will be required and demonstrating that the function and integrity of the SIS will fall outside the approach within this guidance.</td>
</tr>
</tbody>
</table>
### Operator Response within Instrumented Safety Functions in the Chemical, Oil & Gas, and Specialist Industries

<table>
<thead>
<tr>
<th>No.</th>
<th>Criteria from EEMUA 191 (Table 5)</th>
<th>HSE Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>The operator interface should be designed to make all information relevant to management of the specific plant failure easily accessible.</td>
<td>This would include appropriate labelling, functionality of the annunciator and any equipment associated with carrying out the response. Reliance should not be placed on other electronic systems (e.g. computers) that are not of sufficient integrity (e.g. for electronic documents). Note – EEMUA201 also provides guidance on operator interfaces and control room layout and design.</td>
</tr>
<tr>
<td>8</td>
<td>The claimed operator performance should have been audited.</td>
<td>In this context, audit goes well beyond a typical safety management system audit (although formal auditing of management systems will also be required). This criterion aims to demonstrate that actual operator performance, in terms of reliability and response time, matches the claims for risk reduction ON AN ONGOING BASIS. The following techniques should be considered to validate assumptions about operator performance under a range of abnormal, upset and emergency conditions: a. Revalidation that criteria 1-7 above remain in place, including operator training and competence. b. Simulation of scenarios using a process simulator; c. Exercises of scenarios by manipulating process inputs (e.g. this could be achieved during the proof test); d. Walk/talk-through procedures; e. Desk-top exercises (what-if etc.); f. Loss of power tests, communications checks etc. g. Other measures as deemed necessary to achieve the purpose defined above. Note that a range of measures are likely to be necessary and should be proportionate to the level of risk reduction claimed. For example, exercises often have only limited validity because they test only one of many shift operators in an artificial situation.</td>
</tr>
</tbody>
</table>
Operator Response within Instrumented Safety Functions in the Chemical, Oil & Gas, and Specialist Industries
Operator Response within Instrumented Safety Functions in the Chemical, Oil & Gas, and Specialist Industries

**Figure 2: Response Time Considerations**

Time pressure is a crucial factor that can influence operator performance when responding to safety-critical alarms. COMAH establishments should be asked to demonstrate, on a case-by-case basis, that all sub-tasks associated with responding to an alarm (see below) can be completed effectively within the actual time available for response i.e. from when the alarm is activated to when the process goes beyond the point of no return. This is especially important when risk reduction is claimed for operator response as part of a SIL1 system (SIAF).

**Alarm Activated**

**Time available for response, assuming worst-case scenario**

**Alarm Observed**

The operator must be available to respond. Claims of continuous manning, or that operators can be alerted by other means (e.g. alarm pagers), should be challenged.

Alarms should be:
- obvious and distinguishable from other alarms (2)*
- classified at the highest priority (3)
- remain on view whilst active (4)

The operator interface should be designed to support management of the plant failure (7)

**Diagnosis and Planning**

Operators should know how to respond and understand the consequences of failing to respond. They should be trained and assessed in managing the specific failure that the alarm indicates (1) and be regularly re-assessed and re-trained (using simulators if possible).

Decision-making associated with a SIL1 operator response should be kept to a minimum. The response should be simple, obvious and invariant (6). The operator should have access to a clear, written response for each SIL1 alarm (5) e.g. a hard-copy grab card, readily available at point-of-use. These cards may also include confirmatory and follow-up actions in the event that initial response has been unsuccessful.

**Action**

The extent and nature of the action required, and any associated ‘what-ifs’ should be fully explored.

For example, carrying out the required action might involve communication with a field operator, who is then required to travel to a remote part of the plant to identify and operate a manual valve.

**Time required for response (all sub-tasks)**

*Numbers in brackets denote the relevant ‘human reliability’ criteria from EEMUA 191, as summarised in Table 2 above.

All criteria relating to operator performance should be actively monitored and audited (8)