

Shell U.K. Limited
1 Altens Farm Rd,
Nigg
Aberdeen
AB12 3FY

COMAH Competent Authority

Health & Safety Executive
Belford House
59 Belford Road
Edinburgh
EH4 3UE

Tel: 131 247 2042
@hse.gov.uk

<http://www.hse.gov.uk/comah/index.htm>

HM Principal Inspector of Health & Safety

Reference: SVC4302109

13th May 2016

For the attention of: [REDACTED], Operations and Maintenance Manager, Northern Systems and Plants

Dear Mr Baird

HUMAN FACTORS INSPECTION AT MOSSMORRAN 2ND & 3RD FEBRUARY 2016

HEALTH & SAFETY AT WORK ETC ACT 1974

CONTROL OF MAJOR ACCIDENT HAZARDS REGULATIONS 2015 (COMAH)

The identification, correct prioritisation and management of alarms at Mossmorran remains a significant concern for the Competent Authority.

The two legal actions outlined below have been identified by [REDACTED] Human Factors Specialist Inspector, following inspections at St Fergus on 7th & 8th October 2015; Mossmorran on 2nd & 3rd February 2016; and after review of relevant documents and updates, provided subsequent to the inspections. Full details are included in the accompanying specialist inspector report.

Please note that our expectation is that your plans for improved alarm management at St Fergus should take into account the contents of this report, including the recommendations.

[REDACTED] will be assisting at the process safety inspection on 31st May 2016. There will be an opportunity to discuss aspects of this report at the inspection.

Legal Actions

Action 1: Conduct a preliminary review of all the MAH critical limit alarms at FNGL and identify the alarms that rely on operator response.

(Ref: SHELL/MM/HF/020216/01)

Shell should provide a list of all the MAH critical limit alarms that rely on operator response. For MAH critical limit alarms that have no layers of protection and rely solely on operator response, Shell should provide details of the MAH consequence associated with each alarm.

[COMAH 5(2); end-date 30 June 2016]

Action 2: Conduct a preliminary review of MAH critical limit alarms that rely on operator response and demonstrate that the Control Room Operator has sufficient time to respond to the alarm.

(Ref: SHELL/MM/HF/020216/02)

Detail: The following sections detail the requirements by which Shell could demonstrate compliance with Action 2. Shell should select a sample of MAH critical limit alarms that rely on operator response, and for each alarm:

- (1) Explain how the alarm has been prioritised with reference to time and consequence;
- (2) Explain how Shell arrived at the time available (where did it come from, who decided it, how was it derived for inclusion in the Variable Table);
- (3) For the sample of high criticality alarms, demonstrate that there is sufficient time to respond to the alarm, on a case-by-case basis (this should be considered in the context of the four sub-tasks associated with operator response, namely observe; diagnose; plan; action);
- (4) CA expectation is that you will draw upon competent technical support in alarm design and management to address this action.

[COMAH 5(2); end date 30 August 2016]

Information to employees

As required by Section 28 of the Health and Safety at Work etc Act 1974, I am required to provide information to the employees concerning the visit. I am therefore enclosing a copy of the letter which should be passed to the employees' representatives.

Yours sincerely,

[Redacted signature]

HM Inspector of Health & Safety
COMAH Intervention Manager

For and on behalf of the COMAH Competent Authority

CC by email: [Redacted] Onshore Asset Manager; [Redacted] Plant Installation Manager; [Redacted] Acting Plant Manager; [Redacted] HSE Manager; [Redacted] St Fergus Plant Manager; [Redacted] NSP HSE Adviser; [Redacted] SEPA; [Redacted] Energy Division



Environment
Agency



Cyfoeth Naturiol Cymru
Natural Resources Wales
















Office for
Nuclear Regulation

COMAH Competent Authority Inspection Report

ESTABLISHMENT DETAILS			
Name of Operator:	Shell UK Ltd FNGL		
Establishment Address:	FNGL, Mossmorran, Cowdenbeath, Fife, KY4 8EL	COIN Site Ref:	1008131
		Case No:	4063731
		Service order No:	SVC4302109

INSPECTION DETAILS			
Inspection Title:	Human Reliability Assessment Design and Alarm Management		
Report Discipline(s):	Human Factors		
Intervention Plan ref:	Case no. 4063731, issue no 14	Inspection Date:*	2 & 3 February 2016
<p>*NOTE TO OPERATOR: Please ensure that you have updated the "date of the last site visit" field on the public information system following this planned inspection. The date above is the date of the last planned COMAH regulatory visit in line with the intervention plan for your establishment. You can select the relevant date from the system.</p>			

Visiting CA Staff:	Discipline:	CA Organisation, Unit & Team:
	Regulatory Inspector	CEMHD1A
	Human Factors	CEMHD3I

Persons seen:	Position:
	Plant Manager
	Technical Authority
	NSP Operations Support
	Production Coordinator
	Human Factors Specialist
	HSE Team Lead
	Human Factors & Health Assurance Manager
	H & S Officer
	Shift Supervisor
	CRO
	CRO

Relevant documentation seen

[List all documentation seen - include revisions and dates where possible. If appropriate, clarify the level of review within this section e.g. only parts of the document were reviewed]

- NSP ISU Flowchart;
- Honeywell Alarm Assessment Report, Shell Mossmorran, Doc. No.: S001083-0051-001 R0, Version: 0, September 22, 2014;
- DCS Alarm Philosophy Document; SUKEP-PRODOP.OM.7149-050 marked "Original 10/12";
- Northern System Plants Alarm Management Philosophy; Document no: EP201408218135; Revision 2; 22 October 2014;
- Alarm Management; DEP 32.80.14 – GEN, February 2014;
- Furnace Trip Alarm Response Guide, MMUPSET Rev. 2;
- Hot Oil Pump Stoppage (Furnace Main Burners Trip);
- U5500 Hot Oil System – CRO Actions On A Furnace Trip; Procedure No: 7/003; SUKEP-PRODOP.OM.7503-055 Part 2;
- Human Error Analysis – Respond to impact on U1000 of hot oil furnace trip; June 2015;
- List of Critical Upset Conditions (that require Human Factors Assessment);
- Alarm Management; Procedure No: 1/007; SUKEP-PRODOP.OM.7149-050;
- Shell Training Presentation: Operating Integrity, U5500 VT Upload to DCS;
- Shell Regulators Human Factors Inspection, 2 & 3 February 2016;
- MoC Request Form – Hot Oil U5500 Alarm Variable Table Update, March 2015;
- List of Alarms associated with all Hot Oil Batches;
- Shell Report Dated 7 December ; Ref: St Fergus Human Factors Inspection 7-8 October 2015;
- Shell performance metric from October 2015 to January 2016 (various);
- *NSP ISU Flowchart R03*;
- Shell Email dated 31 March 2016 – including attachments; Request form, SR Alarms PDFs and Deviation -568737;
- Shell Email dated 10 February 2016 from David Burgess in relation to HSE concerns from Alarm Handling Inspection.

Inspection Summary:

Shell presented a detailed overview of their progress against the identification and management of safety critical tasks. The work completed by Shell represents a positive start to human factors integration into the safety management system at their Mossmorran establishment.

Shell was invited to present how the potential for human failure is acknowledged and systematically treated in the design and management of alarms. Shell explained that all the alarm tags for the Mossmorran establishment have been reviewed, from which approximately 2000 alarms have been identified as critical limit. Shell reported that alarms which have potential for MAH are embedded within the 2000 critical alarms and will be identified via a further screening process. Review of the ISU screening process identifies a possible outcome of safety related limit alarms with MAH potential that have no additional layers of protection and rely solely on operator response. Shell explained that some alarms may fit this criterion due to the existence of old equipment and processes. **(A1)**

Shell were asked to describe how the alarm design process acknowledges and accommodates

human capabilities and limitations in particular provide detail on whether prioritisation of an alarm took into consideration time available compared with the time required by the operative for the corrective action to be performed. Shell could not provide any additional information on this matter. **(A2)**.

Shell HF specialist was asked whether the time required by the CRO to perform the corrective action in response to an alarm had been considered as part of the HRAs completed for abnormal / process upsets in the control room. Shell HF personnel advised that they have completed one HRA for a control room activity 'Response to impact of U100 of Hot Oil Furnace Trip', and this aspect of time available versus time required was not explored as part of the work completed. **(A2)**

Control room operators interviewed during the visit raised a number of concerns since the upload of the VT, mainly increased alarm flooding emerging from the re-categorisation of alarms. A walk/ talk through of a COMAH safety critical task identified a range of performance influencing factors which can have a potential impact on the actions of the CRO in responding to the alarms including; workload pressures due to not having enough manpower, distraction and training. It is strongly recommended that Shell review the PIFs identified in this report and be in a position to demonstrate to the CA at future interventions how these PIFs are being, or will be optimised. **(R15)**

Overall, Shell personnel at all levels within the organisation have shown a willingness to engage with human factors and the efforts of all involved are acknowledged.

Report author: [REDACTED]

CA Organisation, Unit & Team: CEMHD 3I

Date of report: 18 April 2016

Location: HSE, Glasgow

Purpose of visit:

The key objective of the visit was to conduct an inspection to:

- verify Shell's progress with their human reliability analysis plan;
- verify the key aspects of human factors in design have been applied to alarm management.

Method

The site agenda and question-sets were framed around relevant standards and published HSE guidance. Further information is available on the human factors pages of the HSE website at www.hse.gov.uk/humanfactors/index.htm

Evidence for the observations and actions detailed below were drawn from the various elements that made up the site intervention, including:

- discussions with site management and front line personnel;
- desk-top review of sample documentation;
- partial walk / talk-through of the 'Response to impact of U1000 of Hot Oil Furnace Trip'.

Verbal feedback on preliminary findings was provided at the end of the visit.

Background

HF inspection August 2012

The CA conducted a follow-up inspection in August 2012; to verify Shell's progress in developing a programme of qualitative human failure analysis of safety critical-tasks at the Mossmorran establishment. Following the CA interventions (2009 / 10) Shell contracted Atkins (HF consultants) to complete safety critical tasks identification and human failure analysis work for both the FNGL plant and Braefoot Bay. This work was reviewed during the visit. Site personnel and management were unable to explain how this work was being taken forward, subsequently the CA raised the following action:

- Action 1: Conduct a comprehensive Intelligent Customer review of the work undertaken by Atkins to comply with Actions 2 & 3 of the HSE Human Factors report dated 12 March 2009 and provides the Competent Authority with a summary of findings and a clear action plan to address any shortfalls identified.

HF inspection March 2013

A follow-up meeting in March 2013 to verify Shell's progress with the action of the human factors report dated August 2012. During this meeting Shell personnel advised that consultant [REDACTED] (AB Risk Ltd) had been appointed to complete the review.

HF inspection November 2013

A follow-up inspection in November 2013 was completed to verify Shell's progress with the action of HSE Human Factors report dated August 2012. During this visit Shell Mossmorran provided a copy of the safety critical task list generated for the site and examples of HFAs that had been completed to date.

At the time of the inspection the Mossmorran site had completed four human failure assessments.

HF inspection March 2014

The CA conducted an inspection in March 2014; to verify Shell's progress in alarm management, during this visit Shell Mossmorran provided a further update on the progress of human failure analysis of safety critical tasks.

At the time of the inspection the Mossmorran site had completed five human failure assessments. We were told that an additional HFA for '*Displace a treater vessel*' was completed as part of an incident investigation. This work was reviewed as part of the intervention and the CA raised the following action:

- Action 1: Identify the relevant safety critical tasks associated with the Major Accident Hazard Scenarios with compliance date 09 January 2015.

HF inspection November 2014

The CA conducted an inspection in November 2014; to verify Shell's progress with action 1 of HF report dated March 2014. Shell had made little progress in integrating human factors into the safety management system at the Mossmorran site. The company explained that lack of progress in completing HFAs and addressing the subsequent actions of the HFAs was due to a shortage of human factors resource.

The company were invited to present progress against the legal action (identify the relevant safety critical tasks associated with the MAH scenarios for Shell Mossmorran) and explain how the newly completed HAZOPs would account for the potential of human error. The company advised that they had made no progress with addressing these issues due to a shortage of human factors resource.

The shortage of human factors resource had resulted in Shell taking a reactive approach in managing human performance in context of major accident hazards. Shell had been unable to demonstrate how they were proactively managing their human factors work to ensure compliance with their duty under regulation 4 of the COMAH regulations. This resulted in an improvement notice being issued (Notice No: IN/JR/021214/01). The CA raised the following actions:

Action 2: Shell Mossmorran to provide a description of how human error will be identified in the HAZOP process (compliance date 30 January 2015).

Action 3: Shell Mossmorran to provide a clear statement of how they propose to review the outcomes of the completed HAZOPs to inform the program of safety critical task analysis work and demonstrate the link between the management of human performance and the control of major accident hazards (compliance date 30 January 2015).

HF Inspection March 2015

The purpose of the visit was to verify Shell's progress against the legal actions at Braefoot Bay and Mossmorran.

Shell Mossmorran

Action 1 was extended to 28 August 2015;

Action 2 was closed;

Action 3 was extended to 29 May 2015

Factual observations and findings:

This section details key inspection findings. Actions and recommendations appear in the sections that follow and are cross-referenced here as **(A1)**, **(R1)**.... etc.

1.0 Managing Human Failure

1.1 Identification of safety critical tasks

Shell provided an update on their progress of Safety Critical Task (SCT) identification and programme of Human Reliability Analysis (HRA);

	Operations	Maintenance	Upset Conditions
SCT identified	21	10	8
HF assessments completed	20	6 (+2)	1
HFA outstanding	~	2	7
Action plans	Developed	Developed	tbc

Shell provided the following definitions for critical upset condition:

- Provide a summary of key Major Accident Hazard scenarios (MAH) at the Mossmorran establishment where reliance is placed on people responding to alarms as part of the 'necessary measure';
- This is where an upset condition / process deviation has been identified in the HAZOP where operator response is deemed to be critical to prevent the possible escalation to an MAH.

Shell explained that the process upset SCTs were identified by the screening of HAZOPs for MAH and human error. This work was completed by an external consultant Risktec. 312 events were further screened by the Shell Human Factors (HF) specialist to identify the MAH events with reliance on human response. The upset conditions which had a HAZOP action in place to control risk were removed from the list. The remaining 7 upset conditions have been identified as SCTs that require to be subjected to a HRA.

Shell HF specialist described the methodology that was followed to complete the HRA for a process upset SCT:

- Define upset condition scenario;
- Establish the starting point of the task – respond to upset condition;
- Investigate through task analysis
 - What would CRO and outside technician do;
 - Breakdown response steps;
 - Identify potential errors;
 - Identify consequences (escalations);
 - Identify Performance Influencing Factors (PIFs) (i.e. alarm, DCS);
 - Identify control measures;
- Establish how the operator would know what was happening?
- Identify the control room PIFs which have the potential to impact upon the Control Room Operator (CRO) such as staffing, communications and procedures;
- Establish the finishing point – when the CRO has the situation under control.

Shell presented the findings of the process upset HRA completed for 'Impact on U1000 from furnace trip'. A range of PIFs were identified by the HRA including:

- Experience / competence of CRO;
- Workload of CRO and time pressure;

- Supervision – i.e. supervisor who was a CRO can assist in times of high workload;
- Reliability of instruments;
- Pre-warning provided by alarms;
- Communication between CRO and outside operator;
- Labelling of valves.

In relation to the management of PIFs the Shell HF specialist was of the opinion that specific changes to the task would be most practicable to implement, whereas changes to systems would be more difficult to achieve and take longer to implement. Where PIFs point to system factors, the HF team will ensure that they are integrated into current work programmes such as PACO, FOIP, improvements to procedures and competence requirements.

2.0 Alarm design and management

EEMUA 191 states:

- *'Every alarm should have a defined purpose;*
- *Every alarm should have a defined response;*
- *Adequate time should be allowed for the operator to carry out this response.'* (1.0, pg.1).

A review of Shell's Alarm Design and Management was completed against best practice guidance EEMUA 191. The review is based on the HSE Human Factors Intervention in February 2016 and a number of documents including:

- *Shell Alarm Philosophy revision 2;*
- *Shell Alarm Management DEP;*
- *Honeywell Mossmorran Alarm Assessment Report;*
- *NSP ISU Flowchart RO3;*
- *Shell letter dated 7 December 2015 detailing response to HSE actions;*
- *Post visit email received from Shell dated 9 February 2016.*

2.1 Alarm Philosophy

EEMUA 191 states; *'that the purpose of the alarm philosophy document is to provide a set of core principles by which the alarm system is designed and to provide a consistent approach to the configuration of the alarm management philosophy is to be applied to the alarm system and how individual alarms are to be configured.*

The scope of which should cover any alarm that when activated will need to be responded to by a user of the alarm system. The document should be used by any personnel who may be involved with the design and configuration of alarms. The document is to be a 'live' document and updated in line which changes to the design of the system or operational requirements.' (EMMUA 191, Section 3.7 pg. 63)

Shell Alarm Philosophy

States that 'The following principles are core to the Alarm Management Philosophy:

- *The alarm system supports Situational Awareness;*
- *Only important (and useful) relevant conditions or situations are alarms. If no operator action is required or insufficient time to respond, then there is no alarm;*
- *Every alarm required operator corrective action from the Control Room Operator;*
- *Every alarm shall have predefined guidance to the CRO on the required corrective action.'*

2.1.1 Allocation of roles and responsibilities for design of the alarm system

Shell Alarm Philosophy

Section 1.5 of the alarm philosophy document details the key roles and responsibilities required to effectively manage the alarm system at each site.

Alarm Management DEP

'The alarm philosophy should cover the relationship of the alarm system to the users. The alarm system has many users, including operators, supervision, maintenance personnel, configuration personnel and so forth. This should align with the Operations and Maintenance Philosophy for the site / project.' (3.2 DEP 32.80)

Letter dated 7th December 2015

States that *'the NSP Alarm Philosophy Revision 2 (appendix 1) defines the roles of staff, the system ownership and responsibilities of all users and clearly identifies the system limits of the alarm system.*

The letter further states that the *"NSP asset is currently developing Revision 3 of the NSP Alarm Philosophy. This revision will also include the roles & responsibilities of contractors / project teams making modifications to the existing or adding new systems i.e. by contacting the Asset ISU focal point to carry out alarm classification based on DEP guidance (variable table & ISU process) and feedback into Project team'.*

Recommendation

Shell should ensure that the alarm philosophy defines the requirements of any alarm inhibit or shelving procedures that may be used to manage nuisance or faulty equipment and describe the levels of authorisation that may be required. (EEMUA 191, Section 3.7.1 pg. 64). **(R1)**

2.1.2 Identification of the alarm system users and their needs

The purpose of this section is to identify the alarm systems users and their needs. It should set out the philosophy on which the alarm systems should be designed and engineered.

Shell Alarm Philosophy

Alarm philosophy is a separate phase of the alarm lifecycle. The alarm philosophy serves as the framework to establish the criteria, definitions and principles for the alarm lifecycle phases by specifying items including the methods for alarm identification, rationalization, classification, prioritization, monitoring, management of change, and audit to be followed. The alarm philosophy document ensures that facilities can achieve:

- *Consistency across process equipment;*
- *Consistency with risk management goals/objectives;*
- *Agreement with good engineering practices e.g. DEPs, ISA-18.2, EEMUA 191, etc.;*
- *Design of the alarm system that supports an effective operator response;*
- *Management of the alarm system to ensure sustainability.*

Target users of the philosophy are CRO's, Shift Supervisors, Production Co-Ordinators, Process Engineers, PACO Engineers, maintenance staff, project engineers, engineering contractors and in anyone who is involved in the lifecycle of Alarm management in the NSP. (Section 3, pg. 14).

Recommendation

Shell should ensure that the following aspects are addressed in the alarm philosophy document;

- Describe how periods of high alarm load are to be managed and whether any special facilities are provided such as additional displays during these periods;
- What facilities are provided for shift handover e.g. list of inhibits reports, override reports, nuisance alarm information etc. (EEMUA 191, Section 3.7.2 pgs. 64-65). **(R2)**

2.1.3 Definition of what an alarm should be

Shell Alarm Philosophy

Defines an alarm as an audible and visible notification that annunciates in the CCR to indicate exceedance of a STANDARD or MAH /CRITICAL limit.

Alarm Management DEP

'The role of the alarm system is to notify operators of the exceedance of any defined critical, standard or target limit or the condition when the process is not behaving as expected or when other threats have impacted operations'. (Section 2.0)

2.1.4 Definition of the safety role of the alarm system

Shell Alarm Philosophy

Operating outside the operating envelope should be handled as an abnormal situation and, where appropriate the CRO shall take action Audits on the alarm system to stabilise, slow down or shut down equipment or facilities as necessary. Response to alarms should be seen as management of an abnormal situation, with the following actions:

- *Where the safety of personnel or integrity of the facility are at immediate risk, immediate action is taken to stabilise, slow down or shut down equipment or facilities as necessary and obtain assistance immediately;*
- *Abnormal situations not responding as expected, following operator control actions, shall be managed through a control hierarchy of; stabilise, slow down, shut down, as necessary, and acquiring additional assistance, as applicable, in order to return to a normal operating state or known safe state;*
- *If an IPF has been activated, all protective actions initiated by the IPF shall be physically verified and the affected equipment put in a safe condition prior to re-establishing operations;*
- *Descriptions of the alarms occurring on the shift, the reasons why the alarms occurred and the responses taken shall be recorded in the shift report. In cases where multiple alarms occur, e.g. unscheduled shutdown, only the first up alarm (root cause) needs to be described;*
- *Operators are empowered to stabilise, slow down and ultimately shut down the facilities in abnormal situations. (Section 1.4.2, pgs. 10-11)*

Recommendation

Shell should ensure that the alarm philosophy describes the safety role of the alarm system, describes how the system is to be managed to meet this role, and document the SIL rating of the alarm. (EEMUA 191, Section 3.7.4, pg. 65). **(R3)**

2.1.5 Define how many alarms are to be registered

EEMUA 191 states that the alarm philosophy document should define how many alarms claim to contribute to safety cases:

- List all safety related alarms and document any SIL rated alarms;
- Describe any key safety or environmental alarms;
- Declare any contribution to the operating safety case;
- Does the alarm system form a layer of plant protection
- Are there any alarms that require any special attention (EMMUA 191, Section 3.7.5 pg. 65)

Shell Alarm Philosophy

The philosophy document states that: *Major accident hazard alarms - these are safety related alarms and are specific set of process alarms. These are defined as part of a process safety review that falls into RAM 5 and 4 categories. These alarms will be defined as MAH (CRITICAL) limits (highest level) and will be distinguishable from others by the inclusion of the Prefix MAH in the alarm description. MAH alarms will be displayed on a dedicated matrix style graphic on the DCS which will be on permanent display in the control room. The alarm will have an audible notification and will appear in the alarm summary display.*

Process alarms refer to the audible and visual notification of abnormal operation to the operator. A rationalization process will deliver the proper identification and configuration of required alarms. These may be defined as CRITICAL or STANDARD limits will have both audible and visual notification and both will appear in the alarm summary display. (Section 6.3.1 & 6.3.2 pg. 23)

Letter dated 7th December 2015

The alarm priorities as described in section 2.1.7 of this report are those which are from the letter "anticipated to be used in the NSP Alarm Philosophy Revision 3".

"Once the Mossmorran Variable Tables are complete and the final alarm count / distribution is available, they may be modified to help manage the effectiveness of the priority distribution.

At FNGL MAH scenarios have been determined from the HAZOP & incorporated into the COMAH case."

The letter also included the list of MAH associated alarms for the Mossmorran establishment.

HSE HF Inspection 2 & 3 February 2016

Shell stated that by November 2015 9600 alarm tags had been reviewed, from which approximately 2000 alarms had been identified as critical limit and 1250 alarm tags had been identified as a standard limit. Alarms which have potential for MAH are embedded within the 2000 critical alarms. The screening process as detailed in the NSP ISU Flowchart R03 will identify how many alarms have major accident potential.

During the inspection Shell described the NSP Initial Set Up (ISU) Flowchart which is being used to screen all the alarms that have been extracted from the DCS. Every alarm able point (i.e. journal or tag) has been extracted from the DCS. The ISU team are assessing each potential alarm using the NSP ISU Flowchart. The first stage of the process requires the alarm to be assessed against the Excursion rules stated in the DEP.

The ISU Flowchart follows a 7 step process described in appendix 1 of this report.

Shell were asked to clarify the following outcome from the ISU flowchart; '*safety related limit required - no automated protection layer for the consequence*'. Shell explained that this outcome was for COMAH alarms that have no layers of protection and rely solely on operator response. Shell explained that some alarms may fit this criterion due to the existence of old equipment and processes. (A1)

Shell was invited to explain how the alarm review work would be integrated with the HRA work being conducted by the Human Factors (HF) team. Shell reported that they were considering a programme of work by which the 2000 critical alarms will be reviewed against the HAZOP / MAH / Human Error screening work being conducted by the HF specialist and Risktec. It is strongly recommended that Shell combine these two work streams together. (R4)

Post Inspection

Regulatory Inspector [REDACTED] sent an email on 5 February 2016 to Shell Mossmorran to arrange a brief session on 9 February 2016 to provide the CA with an update on the following:

Provide details of Shell's proposals to fast track the screening of critical alarms to identify:

- Which alarms require the operator to take action to prevent a major accident;
- Whether there is sufficient time for the operator to carry out this action;
- How many such alarms will be made visible to the operator.

Post visit – email received from Shell 10 February 2016

"Our proposal for Screening of Critical Alarms as per the 3 bullet points in your email is as follows:-

MAH Screening – We have allocated full-time, two of the FOIP team to work on this activity with a remit of following the 'MAH' 'Safety Related' decision Flow Chart being utilised at St Fergus ISU, that was presented to you during the inspection on the 2nd/3rd Feb . The team working this have also been asked to provide the technical limit reaction time required of an Operator under the conditions prevalent.

To ascertain if an Operator has sufficient time to carry out the action within the technical limit timing, this will be reviewed by our Human Factors expertise.

Timing of the above is anticipated to be a minimum of 1 month and maximum 2 months.

Visibility of Such Alarm 'MAH' 'Safety Related' to Operator – we will be required to reconfigure the DCS to enable any 'MAH' 'Safety Related' alarms into the system. This reconfiguration will be carried out through MOC process. The anticipated Timeline for this will be :-

W/C 8TH Feb PACO TA2 to Draft MOC to reconfigure DCS

W/C 15TH Feb MOC Screening Meeting and reviewers to approve

W/C 22ND Feb MOC Implementation actions

W/C 29TH Feb DCS Reconfigured, ready for acceptance of 'MAH' 'safety Related' alarms".

2.1.6 Definitions of alarm system performance targets (e.g. maximum rates)

The main aim of performance monitoring is to assess how usable an operating alarm system is and to identify ways of improving the system if necessary or detecting any deterioration if not.

There are two types of performance metrics objective (quantitative) and subjective (qualitative). Quantitative metrics capture all alarm activity information onto a database and using software filters to provide the metrics required. Qualitative metrics are more difficult to assess and may vary due to a number of factors associated with type of process, operator workload and operator experience.

Shell Alarm Philosophy

Table 1 of the alarm philosophy document lists the Key Performance Indicators (KPIs) which are used as an indicator of the health of the system.

Table 1 OI KPI requirements

Measure	Current KPI	Best Practice KPI	Frequency
Total alarm rate per hour	< 12	< 3	Monthly
Standing Alarm Rate	CRITICAL < 10 STANDARD < 50 ALERT < 200	CRITICAL < 0 STANDARD < 0 ALERT < 20	Monthly

Table 9 of the alarm philosophy documents the metrics required to monitor the performance of the alarm management system. The metrics include alarm rate; standing alarms; shelved alarms; Top 10 bad actors; Top 20 bad actors; Top 10 journal bad actors; Top 20 standing alarms; Maximum alarm rates; % time in exceedance – steady state; % time in exceedance – plant upset.

Alarm Management DEP

'Alarm notification responses constitute a small fraction of the normal operator workload. The alarm system is designed to limit the rate of notifications such that the operator has time to understand the operating exceedance, initiate action and complete all of the other assigned tasks before new notifications arrive.' (Section 2.5)

Bench marking the alarm system allows attention to be focussed on possible improvement measures in those areas where the system is weakest and on those measures that achieve the highest effect.

The following benchmark measurements should be used to assess the alarm systems performance:

- *The number of configured alarms per panel operator;*
- *The average alarm rate per operator;*
- *Indication of frequent alarms;*
- *Number of alarms following a trip;*
- *Number of standing alarms.*

If alarm suppression techniques cannot or will not be implemented the number of alarms should be limited to some 1000 per operator."

Table 6 in the DEP provides the average alarm rate per operator;

Long term average alarm rate in steady operation	Acceptability
> 6 per hour	Unacceptable
3 to 6 per hour	Improvement required
< / - 2 per hour	Target

Table 7 in the DEP provides the performance indication for the number of alarms following a trip (section 5.17).

Long term average alarm rate in steady operation	Acceptability
More than 100	Definitely excessive and very likely to be lead to the operator abandoning the system

10 to 100	Hard to cope with
Less than 10	Should be manageable

Section 6 of the DEP details the range of notification (alarm) suppression techniques that should be applied including: static alarm suppression, dynamic alarm suppression and dynamic state-alarm settings.

Letter dated 7th December 2015

The alarm system at the Mossmorran site is actively managed by a weekly meeting with a multidiscipline review to identify alarm system performance / bad actors using defined alarm metrics with an aim to reduce the number of nuisance alarms present to the operator. The metrics follow Shell Operating Integrity guidelines with an overall evolving aim to meet or exceed the EEMUA 191 targets.

The process has produced many improvements and actively manages bad actors / nuisance alarms and works towards reducing standing alarms. This process along with the VT improvements will see many standing alarms removed as they are reclassified through the ISU process.

Honeywell Report Recommendations

- *Background alarms are defined as the situation in which there are too many alarms occurring during normal or steady state operation. This situation often hides 'old' alarms which can be missed and promotes the need for re-alarmed that increases alarm traffic even more. In a flood situation critical alarms can get missed, the operator is distracted and tied up when he / she is needed most, and the alarms just the distract the operator from their primary task of controlling the upset;*
- *The site has around 216 standing alarms – some of the alarms have been around for 2 years because e.g. some cannot be fixed because they are not due for maintenance for a few years; remnants from old devices which have been migrated to Experion, or plant that has been decommissioned with the software still in place;*
- *Bad actors account for an average of 49% of the total alarms generated over the 7 month period. Some bad actors are repeat offenders with their alarms not being fixed for up to 12 weeks. This may be due to a number of factors, where different alarms for that individual point should be assessed at the same time by the engineering and maintenance team;*
- *Chattering alarms offer an area for further improvement. Often these alarms are caused by the alarm set point being set too close to normal operation conditions. (Section 3.2 pgs. 20 - 22)*

Post Inspection

Shell management were asked during the inspection to provide details of the performance monitoring completed for the Mossmorran establishment. Shell provided metrics collated for a period of 4 months (October 2015 – January 2016).

A review of these metrics has not been included in this report. Due to the changing situation they will be reviewed at future interventions.

Recommendation

Shell should ensure that the alarm philosophy documents key performance targets including specific targets for additions to the system giving priority to new projects. Ensure reduction at source and appropriate intelligent handling are considered. (EMMUA 191, Section 3.7.6 pg. 65).
(R5)

2.1.7 Rules for prioritisation of alarms

Prioritisation of alarms assists the operator to deal with alarms in order of importance at time of high workload. It is important to prioritise alarms at any given time such that the most important are more obvious to the operator. As this helps the operator to decide which alarms to deal with when several occur at the same time. This can be particularly useful during periods of high alarm activity when the operator needs to structure a response so that essential important operator actions are carried out first.

Alarm priorities must be allocated using a logical rationale otherwise the effectiveness of the process maybe considerably devalued. EEMUA 191 states that '*alarm priorities can be established according to two factors:*

- *The severity of consequences (in safety, environmental and economic terms) that the operator could prevent by taking the corrective action associated with the alarm;*
- *The time available compared with the time desired for the corrective action to be performed and to have the desired effect.* (EEMUA section 2.5.1 p.gs. 30 -31)

Shell Alarm Philosophy

Operating limits are identified which are then used to configure the notification priority in the DCS. The notification priorities assist the operators in differentiating the criticality and response to concurrent alarms. These are:

- *MAH (CRITICAL) limit: Highest Priority - operator action is required to correct exceedance of a limit. This is the opportunity to prevent a significant Safety consequence, prior to the next layer of protection;*
- *CRITICAL limits: Second Highest Priority - operator action is required to correct exceedance of a CRITICAL limit. Typically, this is the final opportunity to prevent significant consequence, prior to the next layer of protection;*
- *STANDARD limits: Operator action is required to validate the indicated exceedance of a STANDARD limit. Corrective action must be initiated subsequently to prevent a significant negative business impact or deterioration over time, leading to an eventual economic consequence;*
- *TARGET limits (ALERTs): Second Lowest Priority - They do appear in the alarm summary page, but do not annunciate. They are typically used to alert the operator that the process has exceeded a process optimisation limit or that a shutdown has occurred which requires no further action to prevent escalation;*
- *JOURNAL: The journal records events that do not require operator action. However, journal events may require action from other disciplines (e.g. maintenance), or may be noteworthy for future post event investigation and root cause analysis (confirmation of controls / override application). Journal events are not annunciated to the operator or appear in the alarm summary but they do appear in the separate Journal summary. (Section 5.2 pgs. 17 - 18)*

The alarm philosophy states that the ISU process will result in an alarm priority which should be in line with the date presented in table 3 of the document:

Table 3: Notification Priority Distribution

Notification Priority	Percentage Distribution
MAH (Critical)	~ <1%
Critical	~ 5%
Standard	~ 15%
Alert	~ 80%

Letter dated 7 December 2015

"Revision 3 of the NSP Alarm Philosophy is currently being worked on by the NSP PACO team to incorporate more detail on Major Accident Hazard definition in particular:

Safety related alarm: an alarm indicates an operator action is required to prevent a safety hazard from occurring or an alarm which is claimed as part of the facilities for reducing the risk from a safety hazard by a factor's or more than 10.

MAH Critical Limit alarm: an alarm whose ultimate consequences will result in a COMAH Major Accident RAM severity 4 or 5 event occurring.

Critical Limit alarm: An alarm requiring immediate operator action to prevent a safety, environmental or process safety RAM severity 2 or greater consequence from occurring.

Standard Limit alarm: An alarm that through sustained or recurring short term operation will cause cumulative degradation of equipment, integrity or reliability leading to the occurrence of a safety, environmental or process safety RAM severity 2 or greater consequence."

HSE HF inspection 2 & 3 February 2016

It became evident from discussions with control room operators (CRO) that since the VT table upload they are increasing a number of issues including:

- Exacerbated difficulty in diagnosis during alarm flooding;
- The re-classification of process alarms has increased the number of red (urgent) alarms;
- Some yellow (high) and white (low priority) alarms are now appearing as red (urgent) thus requiring the CROs to scrutinise all red alarms coming in.

Honeywell report recommendations

- *The priority distribution for alarms within the whole plant has too many alarms set at standard (high) priority according to the EEMUA guidelines;*
- *Alarm floods are probably the most difficult to deal with, the most critical, and arguably one of the most common problems. (Section 3.2 pgs. 20 - 22)*

Post visit – email from HSE to Shell 5 February 2016

Regulatory inspector [REDACTED] sent an email on 5 February 2016 to Shell Mossmorran to arrange a brief session on 9 February 2016 to provide the Competent Authority (CA) with an update on the following:

"Provide the CA with an assurance regarding the postponement of any further upload of variable table sections until a risk assessment has been carried of the current situation in which a high number of "critical" alarms are listed on the alarm page. As discussed, my concern is that a control room operator may incorrectly diagnose an upset condition, possibly leading to a major accident, due to the current high number of critical alarms showing on the alarm page. You should take steps to address this issue before any further uploads are carried out."

Post visit – email response from Shell 9 February 2016

"I can confirm that I sent an email to the relevant people on the Thursday morning (4th Feb), post your visit last week, instructing that no further VT Enforcements are to take place.

I can confirm that a Risk Assessment (Deviation) will be Carried out within FSR against the Shell DEP 32.80.10.15- Gen Alarm Management with the following timeline:-

W/C 8TH Feb 2016 – Risk Assessment(Deviation) to be Drafted and Submitted for Review
W/C 15TH Feb 2016 – Risk Assessment(Deviation) to be Reviewed by TA's
W/C 22nd Feb 2016 – Risk Assessment (Deviation) Approval by Plant Manager”.

2.1.7.1 Time to consequence

EEMUA 191 states: *'The prioritisation of an alarm should be based, in some degree, upon the possible consequences that the operator can help prevent by responding appropriately to it.'* (A.3.1 pg. 129)

The prioritisation of alarms should take into account the time available compared with the time required for the corrective action to be performed and also have the desired effect. For example if there are two alarms of similar consequence but one needs fast action to prevent the consequence and the other does not, then there will be a benefit in prioritising the first alarm higher than the second so that it gets dealt with first.

Shell Alarm Philosophy

The alarm philosophy document does not contain any information on time to consequence.

Alarm Management DEP

The alarm management document does not contain any information on time to consequence.

Honeywell Report Recommendations

- *There is still room for improvement as plant upsets create large variations in the maximum hourly alarm rates in which the plant operator is less responsive with the results heading towards stable or reactive conditions there are eight upsets that fall into this category and happen biweekly on average;*
- *The current system shows that the alarm system and more importantly the Operator's response to it, is reasonable under normal conditions, however there needs to be improvement during a plant upset where the operators response is reactive;*
- *The priority distribution for alarms within the whole plant has too many alarms set at standard (high) priority according to the EEMUA guidelines. (Section 3.2 pgs. 20 - 22)*

Shell HF Inspection 2 & 3 February 2016

During the inspection Shell management were asked to provide detail on whether prioritisation of an alarm took into consideration time available compared with the time required by the operative for the corrective action to be performed. Shell could not provide any additional information on this matter. **(A2)**

Shell HF specialist was asked whether the time required by the CRO to perform the corrective action in response to an alarm had been considered as part of the HRAs completed for abnormal / process upsets in the control room. Shell HF personnel advised that they have completed one HRA for a control room activity 'Response to impact of U100 of Hot Oil Furnace Trip', and this aspect of time available versus time required was not explored as part of the work completed. **(A2)**

2.1.8 Alarm system configuration

Letter dated 7 December 2015

Initial set up (ISU) is the process by which constraints, limits, settings, consequences of deviation in the event a limit is exceeded, recommended steps to take to correct the deviation, and other information are collected for entry into the Master Alarm Database (variable table).

Creation of the Variance table (VT) using the ISU process is the approved Shell process to determine the classification of alarm priorities and the implementation of alarm configuration reviews. The ISU process is the application of a consistent set of guidelines to eliminate unnecessary alarms and rationalise the priorities of those that remain. The VT contains the alarm settings / priorities and required operator responses for the likely causes of the alarms to allow the Operations to Stabilise, Slowdown or Shutdown the plant depending on the alarm. The ISU process uses a multidiscipline team to create the VT and collate all required data. The ISU team reviews all tags / notifications in the control system and ensures they are valid, described properly and consistently, have the appropriate priority level and the correct operator responses defined.

The ISU & VT process has been reviewed and managed in batches / process units to help manage the volume of work. At FNGL 15 batches have been identified.

Shell Alarm Philosophy

The alarm philosophy document describes the Initial Set Up (ISU), this process includes the Identification and Rationalization phases of the Alarm Lifecycle and is carried out by a multidiscipline team. The

Potential alarms in NSP sites may be identified in various ways from a number of different sources. This includes, but is not limited to: project process design, HAZOP reviews, Process Hazard Analysis, incident reviews, operating procedure reviews, SIL (IPF) assessments and PEF reviews. When a potential alarm is identified, the alarm limit or state, the risks, the rationale, time to respond, consequences and requirements are documented for review by the individuals proposing the alarm.

Any Alarm and operator action used as a layer of protection in a LOPA for an HSE IPF is a safety related alarm and shall claim a risk reduction of up to ten. These alarms will be tested at the same frequency as initiator of the protective function it is used in. (Section 4 pg. 14)

Alarm Management DEP

Section 4 of the alarm management document describes:

- Notification initial set up work process for new projects and existing projects;
- The ISU team;
- Identification phase work process;
- Rationalisation phase of the ISU work process;
- Describes the parameters that are used to configure alarms within the alarm system;
- Describes the sources of alarms and describes the notification suppression techniques and lists benchmarks for alarm system performance to deal with alarm flooding, standing alarms.

Recommendation

Shell should ensure that the alarm philosophy describes:

- What facilities are provided and how these facilities should be configured for the viewing of alarm information, e.g. active alarm lists, historical alarms, alarm hiding and in inhibit,

supressed alarms etc.;

- Alarm and event history, define the logging period and how data is to be retrieved by the different used of the data;
- Identify the source of alarms and whether alarm techniques have been used for the prevention of nuisance alarms or alarm floods such as application hysteresis or timers / delays or hiding alarms in the event of a communications failure. (EEMUA 191, Section 3.7.8 pg. 66). **(R5)**

2.1.9 Checklists for designers on the information to be recorded for each alarm

Shell Alarm Philosophy

The philosophy document does not contain any detail on the information that is required for each alarm.

Alarm Management DEP

The alarm management DEP does not contain any detail on the information that is required for each alarm.

Recommendation

Shell should ensure that the alarm philosophy specifies information that is required for each alarm giving reasons why the alarm is there and what is to be done when the alarm is activated. (EEMUA 191, Section 3.7.9 pg. 66). **(R6)**

2.1.10 Dictionary of terms of abbreviations to be used in alarm messages

Shell Alarm Philosophy

The alarm philosophy document does not contain any dictionary of terms and abbreviations to be used in alarm messages.

Alarm Management DEP

The alarm philosophy document does not contain any dictionary of terms and abbreviations to be used in alarm messages.

Recommendation

Shell should ensure that the alarm philosophy contains a dictionary of terms and abbreviations that are to be use in;

- Alarm messages;
- Control system;
- Tag naming conventions;
- Equipment (including process items). (EMMUA 191 Section, 3.7.10, pg. 66). **(R7)**

2.1.11 Guidance to sub-contractors on the design of alarms (where appropriate)

EEMUA 191 states that this section should give guidance to sub-contractors on the design of alarms in the form of checklists.

Recommendation

*Please refer to EEMUA 191 section 3.7.11 pgs. 66-67. **(R8)***

2.1.12 Guidance on the content and structure of alarm response definitions (e.g. procedures, task aids etc.)

Letter dated 7th December 2015

The alarm system at Mossmorran site currently does not allow the operators to view the VT details against each alarm with the summary page on the DCS. A system upgrade is planned at each the site over the next 2 years to give the system the required functionality it improve operator interface. The Shell human factors approved interim measure is a version of the VT spreadsheet which will be permanently displayed on a computer next to the control panel where the CRO can get the required information once the tag descriptor is typed into the filter box.

Shell Alarm Philosophy

The operator response to an alarm includes the suggested action to be used to correct the indicated event and the identification and verification of the situation prior to taking action.

The stages involved in the overall operator response to an alarm include:

- 1. **Observation** – Alarms will assist the operator in detecting, perceiving and discriminating the presence of an abnormal condition and identifying what area of the plant or equipment is involved. This is may be achieved visually through screen-based displays (process graphics, navigation tabs or the alarm summary) and/or audibly via alarm annunciator horns.*
- 2. **Analysis** -The operator analyses, interprets and makes projections of where the plant is headed based on the alarm condition. The alarm is typically silenced during this stage. The operator will use the trends and other process indications to verify the validity of the alarm.*
- 3. **Decision** – The operator decides what actions(s) are required at that time*
- 4. **Action** - The operator takes corrective action to the alarm by changing control set points, outputs or making a request to the field operator in response to the alarm. At this stage the alarm will likely be acknowledged.*
- 5. **Assessment of effectiveness of action** - The operator continues to monitor the variable to determine if the corrective action was appropriate to correct the abnormal condition. If the action was not effective, then further evaluations and actions will be required until the process returns to normal operation.(Section 8 pgs. 29 -30)*

HSE HF Inspection 2 & 3 February 2016

During the walk / talk through exercise the CRO explained that they are required to input the tag number associated with alarm into the VT which is located on another computer in order to access the operator response for the alarm. The CRO reported this action is time consuming and there is an increased risk of introducing error working between two screens. The VT window has to be enlarged to make the text readable and enlarging the screen size results in a number of clicks and re-alignments which all takes time which may not be available during a process upset which all results in increasing operator stress.

Recommendation

Shell should ensure that the alarm philosophy defines how the responses are to be recorded and presented to the operator. Basic alarm messages tend to be made up of a simple set of components such as tag description, alarm status message and time. Shell should describe what is provided for the operator to see the alarm in in context. (EEMUA 191, Section 3.7.12 pg. 67). **(R9)**

The VT table should include a clear description of the operator action or set of sequential actions to be taken in response to alarms. Actions should be structured to enable an operator to:

- Understand the current process conditions;

- Correctly identify the initiating cause;
- Ascertain potential consequences.

Actions should enable the operator to:

- Prevent escalation of consequence;
- Return the process to normal operation conditions or, if required, move the process to a safe operating position or shut down all or part of the process. **(R10)**

2.1.13 Guidance on interpreting patterns of alarms

Recommendation

EEMUA 191 states that *the alarm philosophy should include a section detailing guidance on interpreting patterns of alarms, grouping, suppression and their acceptance (where appropriate).*

Typical inclusions would be:

- *Guidance to address repeating and fleeting alarms;*
- *Prevention techniques for nuisance alarms;*
- *Suppression of our of service equipment alarms;*
- *Implementing of suppression logic. (Section 3.7.13 pgs. 67-68). (R11)*

2.1.14 Guidance on establishing alarm equipment test frequencies

Recommendation

EMMUA 191 states that the alarm philosophy should:

- *Identify those alarms that require testing on a regular basis;*
- *Give guidance on how to determine if testing is required and how to calculate test frequencies;*
- *Consider automatic checks by identifying those alarms that have not been activated during the test period. (Section 3.7.14, pg. 68) (R12)*

3.0 Operator Response to Alarms

EMMUA 191 defines the four stages of operator response as;

- Observation: *the timely receipt of information;*
- Analysis: *using the available information (both the alarm and supporting information from the control panel indications) to determine what state the plant and process is in;*
- Decision: *using the results of the analysis to decide what action(s) to take;*
- Action: *delivering the actions decided upon. (Section 2.3.4 pg. 21)*

During the visit a walk / talk through of the 'Response to impact of U1000 of Hot Oil Furnace Trip', was conducted with an experienced CRO. The objective of the walk-through was to assess the four stages of operator response.

3.1 Stage 1 Observation

The purpose of this stage is to assess the likelihood of the operator failing to observe the alarm on the Human Machine Interface (HMI).

If an operator is to be effective, it is essential that they cope with all the tasks demanded to them under normal and emergency conditions. Given the variety of other activities required from the operator it is very desirable that the operator is not overloaded with alarms as this will severely limit the operator's capacity for analysing them.

The correction of an abnormal situation often requires number of separate tasks to be carried out, some of them in parallel.

Task step 1: Respond to impact on U1000 of hot oil furnace

The CRO explained that a number of different process alarms are used to monitor the status of the hot oil furnace from tripping including:

- Low / high pressure alarm / alerts for fuel gas;
- High temperature alarms;
- Low flow on hot oil;
- Potential trip on high vibration pump.

The CRO explained that from his competence and experience, monitoring of these process alarms / alerts would provide enough warning in advance to prevent a trip.

Success at the observation stage is primarily dependent upon a well-managed working environment, HMI design and alarm rationalisation regime. Such that the operator is always present in the control room and is aware that the alarm is part of their area of responsibility and will not ignore the alarm at times of high stress.

The CRO reported that since the VT alarm upload majority of the process alarms have been reclassified, many of the yellow (high priority) and white (low priority) alarms now appear as red (urgent). There are now an increased number of red (urgent) alarms appearing and in many instances they disappear off the first alarm page and therefore are not immediately visible to the CRO. The CRO raised concern that due to the reclassification, some yellow (high) alarms may actually be more important than the red (urgent) alarms thus they are requiring to scrutinise all alarms coming in.

The CRO was asked how the current status of the alarms would affect his efficiency in a process upset. The CRO explained that he would be in an alarm flood situation, where he would have to acknowledge and interrogate a large number of alarms. The CRO reported that in a flood situation there is a high chance that critical alarms can get missed, as he could get distracted and tied up where he is needed most.

With alarm flooding in an abnormal situation the operator will have only a limited amount of time available to analyse incoming alarms and there may be more important things that the operator should be doing with their limited time which would have a greater impact on reducing or preventing consequence or loss. Having too many alarms with a high priority, means that alarms which actually require a quicker response than others may be missed by the operator. The alarm summary display page displays chronologically, therefore the operator just looks at the new alarms that are created, but will tend to prioritise the higher priority ones.

CRO explained that management are currently proposing to display the COMAH safety critical alarms on a separate screen. There are a number of issues with this as the CRO feel that their ability to maintain situational awareness will be reduced as the information trending alarms will be divided between two screens.

CRO reported that the purpose of the video wall is to provide an overview which will assist in maintaining situational awareness and making decisions during process upsets. However, the design of the software for the video wall has a number issues including:

- The equipment displayed in grey and the equipment tags are in a lighter shade of grey. This can often make it difficult to distinguish between the information presented;
- 'Trip' alarms are audible on the DCS. There is slight delay in the alarm appearing on the

video wall, the associated module tag flashes in red and the word 'trip' appears alongside the kit. But if you acknowledge / accept the alarm on the DCS before identifying it on the video wall it stops flashing which makes it difficult to identify which kit has tripped.

It is recommended that Shell should consider the elimination of alarm overload. This may however be a difficult and long drawn-out exercise and event; even so it will be very hard to be certain that all potential for alarm overload has been eliminated. Therefore Shell should ensure measures are put in place to ensure that the CRO performs as effectively as possible during incidents of alarm overload. (R13)

To assist with this the CRO information displays should be designed such that the CRO can easily access all key plant information even if the alarm system does become overloaded. In addition the CRO should be explicitly instructed and trained in how to respond when the alarm load is too high. (R14)

3.2 Stage 2 Analysis

If the level of analysis is simple and no additional data is required the immediate problem should be easily identified. Therefore to aid with analysis and decision making there should be a predetermined written response which will reduce the overall response time and minimise any errors associated with diagnosing and reacting to the potential problem.

Many alarms may have a very similar response and may be covered by a general definition. However, for critical alarms an individual response definition per alarm is generally justified.

The CRO provided a copy of the alarm response card for the furnace trip located in the Mossmorran plant upset event recovery guide (tarifold). The CRO reported that it was a good guide to make quick reference to the key points. The information within the response guide was considered to provide adequate detail on the main elements which would be required to be addressed. The CRO advised that there is a full operating instruction available in hard copy, but it would be time consuming to locate it in the event of an emergency situation.

The CRO provided a copy of the procedure titled 'CRO actions on a furnace trip', located in the Plant Operating Procedure Manual (POPM). The CRO reported a number of issues with the procedure mainly:

- The procedure had not been updated;
- And the procedure does not list the tag numbers associated with the kit;

In practice the role of the CRO during abnormal situations can be very complex. The CRO reported that there were as number of different causal factors which could result in a furnace trip. Thus the operator response may involve several quite different types of tasks. The CRO's required response to one furnace trip may be quite different from that required to an apparently similar furnace trip at another time. Therefore, it would be difficult to have one generic alarm response for the furnace trip, however a guide which lists the key principles would be useful to prompt the CRO to investigate different sources which may have caused the furnace to trip.

3.3 Stage 3 Decision

At this stage once the problem has been identified, the decision on what actions to be taken should be uncomplicated and well defined.

The furnace trip procedure states '*rapidly reduce Reflux in all 3 columns to match reduced Feed and so that Reflux is Zero within 10 minutes*'.

The CRO was asked to explain the time element associated with this task step. The CRO was of the opinion that this action could be achieved within 10 minutes. The CRO was probed further to explain the implications if the reflux zero could not be achieved, the CRO could not provide any additional information in this regard. The CRO stated that he had never been provided with an explanation as why this action had to be achieved within 10 minutes.

3.4 Stage 4 Action

It should be ensured that, following the alarm, all actions required are easily and safely achievable within the time to consequence and under all reasonably expected operating conditions.

To efficiently correct an abnormal situation the operator will have to work under time pressure and stress to string together a series of unrelated sub-tasks. It is clear that whilst alarms are a useful tool to help the operator, the need for more general task management during an abnormal situation should be addressed.

For this reason a partial walk / talk-through of the 'response to impact on U100 of hot oil furnace', was completed with the CRO to identify any potential errors and associated PIFs. The findings are as follows:

PIFs:

(a) Supervisor not having the right background: The CRO explained that some shift supervisors have been replaced by personnel who don't have experience of working in the Mossmorran control room i.e. supervisors from an offshore background. The CRO reported that in a process upset condition these supervisors would be unable to provide the technical support that may be required.

(b) Workload pressures due to not having enough manpower: There are a number of reasons why there may not be enough manpower including:

- outside operators tied up in another responsibility thus unable to provide CRO with live feedback of the trip function;
- 2nd CRO (supervisor) being away from control room e.g. due to attending training, toilet break, meal break etc.;
- Supervisor in a meeting and radio turned off;
- Reduced manpower due to sickness absence.

(c) The CRO expressed concern that they may experience lack of confidence in the event of being alone during a process upset condition due to the absence of a 'second pair of eyes';

(d) Distraction

- The CRO explained that distraction can occur due to the 2nd CRO having a different way of working;
- Distraction can also occur during instances where the CRO has to bring the 2nd CRO up to speed with the current situation.

(e) Training

- The CRO reported that they have not been provided with any bespoke process upset training;
- The format of the training provided entails the shift supervisor selecting a COMAH scenario and getting the shift to talk through the actions required to bring the plant back to a safe operating state;
- The CRO reported that the external training course 'Handling Emergency', is very high level and does not go into the same amount of depth as the walk / talk through exercise that was completed by the Competent Authority;
- Training on the panel tends to be provided by the trainee CRO shadowing a more

experienced CRO; this is the reason why there are different ways of working among the CROs;

- Training and experience in addressing process upsets is based on the self-learning acquired from reading the POPM or dependent on what the CRO has been exposed to while shadowing. The CRO explained that you don't get to see all the trips that can occur when shadowing; for example the CRO may never see a compressor trip, in such a situation the CRO would be required to address the trip based on their level of experience;
- Training provided by Shell does not allow the CRO to apply problem solving skills.

(f) Due to the increased number of urgent alarms, the CRO reported an increase in alarm flooding since the VT upload.

(g) The CRO is required to input the tag number associated with alarm into the VT which is located on another computer in order to access the operator response for the alarm. The CRO reported this action is time consuming and there is an increased risk of introducing error working between two screens. The VT window has to be enlarged to make the text readable and enlarging the screen size results in a number of clicks and re-alignments which all takes time which may not be available during a process upset which all results in increasing operator stress.

It is strongly recommended that Shell review the PIFs identified in this report and be in a position to demonstrate to the CA in future interventions how these PIFs are being, or will be optimised. **(R15)**

Discussion and Conclusions :

Shell presented a detailed overview of their progress against the identification and management of safety critical tasks. The work completed by Shell represents a positive start to human factors integration into the safety management system at their Mossmorran establishment.

Shell was invited to present how the potential for human failure is acknowledged and systematically treated in the design and management of alarms. Shell explained that all the alarm tags for the Mossmorran establishment have been reviewed, from which approximately 2000 alarms have been identified as critical limit. Shell reported that alarms which have potential for MAH are embedded within the 2000 critical alarms and will be identified via a further screening process. Review of the ISU screening process identifies a possible outcome of safety related limit alarms with MAH potential that have no additional layers of protection and rely solely on operator response. Shell explained that some alarms may fit this criterion due to the existence of old equipment and processes. **(A1)**

Shell were asked to describe how the alarm design process acknowledges and accommodates human capabilities and limitations in particular provide detail on whether prioritisation of an alarm took into consideration time available compared with the time required by the operative for the corrective action to be performed. Shell could not provide any additional information on this matter. **(A2)**.

Shell HF specialist was asked whether the time required by the CRO to perform the corrective action in response to an alarm had been considered as part of the HRAs completed for abnormal / process upsets in the control room. Shell HF personnel advised that they have completed one HRA for a control room activity 'Response to impact of U100 of Hot Oil Furnace Trip', and this aspect of time available versus time required was not explored as part of the work completed. **(A2)**

Control room operators interviewed during the visit raised a number of concerns since the upload of

the VT, mainly increased alarm flooding emerging from the re-categorisation of alarms. A walk/ talk through of a COMAH safety critical task identified a range of performance influencing factors which can have a potential impact on the actions of the CRO in responding to the alarms including; workload pressures due to not having enough manpower, distraction and training. It is strongly recommended that Shell review the PIFs identified in this report and be in a position to demonstrate to the CA in future interventions how these PIFs are being, or will be optimised. **(R15)**

Overall, Shell personnel at all levels within the organisation have shown a willingness to engage with human factors and the efforts of all involved are acknowledged.

Actions Legal

Action 1: Conduct a preliminary review of all the MAH critical limit alarms at FNGL and identify the alarms that rely on operator response.

Reference: SHELL/MM/HF/020216/01

End date: 30 June 2016

Detail: Shell should provide a list of all the MAH critical limit alarms that rely on operator response. For MAH critical limit alarms that have no layers of protection and rely solely on operator response, Shell should provide details of the MAH consequence associated with each alarm.

Action 2: Conduct a preliminary review of MAH critical limit alarms that rely on operator response and demonstrate that the Control Room Operator has sufficient time to respond to the alarm.

Reference: SHELL/MM/HF/020216/01

End date: 30 August 2016

Detail: The following sections detail the requirements by which Shell could demonstrate compliance with Action 2. Shell should select a sample of MAH critical limit alarms that rely on operator response, and for each alarm:

- (1) Explain how the alarm has been prioritised with reference to time and consequence;
- (2) Explain how Shell arrived at the time available (where did it come from, who decided it, how was it derived for inclusion in the Variable Table);
- (3) For the sample of high criticality alarms, demonstrate that there is sufficient time to respond to the alarm, on a case-by-case basis (this should be considered in the context of the four sub-tasks associated with operator response, namely observe; diagnose; plan; action);
- (4) CA expectation is that you will draw upon competent technical support in alarm design and management to address this action.

The actions detailed above are made under Regulation 5(2) of the Control of Major Accident Hazards Regulations 2015.

Glossary

CA – Competent Authority
CRO – Control Room Operator
ISU – Initial Set Up
HF – Human Factors
HMI – Human Machine Interface
HRA – Human Reliability Assessment
MAH – Major Accident Hazards
PIFs – Performance Influencing Factors

SCT – Safety Critical Tasks
VT – Variable Table

References

Alarm Systems: A guide to design, management and procurement, EMMUA publication 191: Edition 3

APPENDIX 1 – NSP ISU Flowchart

Step 1: Are any of the following imminent? (will they happen in a relatively short time, on the order of 15 minutes or less)?

Outcome of step 1:

- Critical limit required – no automated protection layer for the consequence;
- Critical limit required – automated protection layer in place for the consequence;
- MAH Critical limit required – automated protection layer in place for consequence and the critical limit is the last instrumented layer of protection before the hazard could be released;
- Safety related limit required - no automated protection layer for the consequence.

Step 2: Will sustained or recurring short-term operations begin to cause cumulative degradation of equipment integrity or reliability, or other cumulative effects that could lead to any of the following consequences?

Outcome of step 2:

- Standard limit required – no automated protection layer for the consequence;
- Standard limit required - automated protection layer in place for the consequence;
- MAH Critical limit required – automated protection layer in place for consequence and the critical limit is the last instrumented layer of protection before the hazard could be released;
- Safety related limit required - no automated protection layer for the consequence.

Step 3: Will any of the following consequences occur (significant negative impact to business / inability to meet turnaround run length expectations / economic RAM severity 2 or greater)

Outcome of step 3: Standard limit required.

Step 4: If a standard limit has been set for this variable but no critical limit has been defined, is it possible that this variable may further exceed the standard limit, within the allowable time in exceedance, potentially causing any of the consequences listed in step 1?

Outcome of step 4:

- Critical limit required – no automated protection layer for the consequence;
- Critical limit required – automated protection layer in place for the consequence;
- MAH Critical limit required – automated protection layer in place for consequence and the critical limit is the last instrumented layer of protection before the hazard could be released;
- Safety related limit required - no automated protection layer for the consequence;

Step 5: Does the variable have a value above or below which the reliability, stability or operability of the equipment or process is impacted and, if not responded to, could cause a negative impact on one or more of the following (equipment performance / process performance / product quality);

Outcome of step 5: Target limit required

Step 6: Does the operator need to know about this event to control or optimise the process?

Outcome of step 6: Target limit required

Step 7: Can the alert be delayed by up to three days and still be useful?

Outcome of step 7: Complete

Memo

CEMHD3i

To: [REDACTED]
CC:
From: [REDACTED]
Date: 26/06/2018
Re: Human Factors Feedback of Shell St Mossmorran Action 1 (HF1/AH/FEB2016) from Human Factors Report dated April 2016 SVC 4302109.

[REDACTED]

I have conducted a prima face review of the documentation submitted by Shell Mossmorran in response to Action 1 from the Human Factors (HF) report '*Human Reliability Assessment and Design and Alarm Management*, April 2016.

Action 1

30 June 2016

Conduct a preliminary review of all the MAH Critical Limit alarms installed on Mossmorran assets and identify the alarms that rely on operator response.

Detail: *Shell should provide a list of the MAH critical limit alarms that have no layers of protection and rely solely on operator response. The response should detail of the MAH consequence associated with each alarm.*

Shell have devised two additional alarm priority categories; MAH Critical and Safety Related Alarms (SRA); for the process alarms on the establishment. Both MAH Critical and SR alarms have major accident consequences.

A MAH alarm has been classified as the final alarm which would alert the Control Room Operative (CRO) to the development of a scenario with MAH potential. MAH alarms are where if the operator failed to take action, an additional layer of protection would be provided by an Instrumented Protective Function (IPF) and / or a Pressure Relief Valve.

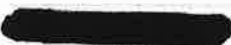
A SR alarm has been classified as the final alarm which would alert the CRO to the development of a scenario with MAH potential. These alarms do not have any further automated / mechanical layers of protection in place to prevent the MAH event. The operator is the final prevention measure against the escalation to the MAH event. Shell acknowledges that the CRO should have sufficient time to react and take corrective actions

to prevent escalation into a MAH event. Shell state that the CRO available response time has been derived from reviews based on operations experience and not process calculations.

Shell conducted a review of the alarms on the establishment associated with MAH scenarios. The review examined the 106 scenarios identified by the FNGL site HAZOP and technical safety team which have an associated alarm to alert the CRO. All scenarios were reviewed against the ISU flow sheet to determine the final alarm associated with scenario.

The alarm review has identified 88 MAH Critical Alarms and 84 Safety related alarms. The figures of 84 and 88 represent a significant reduction on the 2,000 alarms previously identified as 'critical'. For all MAH and SR alarms the associated MAH consequences and the current safeguards / mitigations have been identified.

In the context of the documentation provided, and the feedback above, I recommend that Action 1 in the human factors report dated April 2016 should be closed.


Human Factors Specialist
HID CEMHD3I
09 August 2016

Glossary:

CRO – Control Room Operative
HF – Human Factors
IPF - Instrumented Protective Function
MAH – Major Accident Hazard
SRA - Safety Related Alarm

References

HSE Human Factors report – Human Reliability Assessment and Design and Alarm Management, Yasmeen Ahmad, SVC4302109, April 2016;

HSE Process Safety report – Alarm Management and other issues, Euan Ross, SVC4320196, 09 August 2016;

FNGL SR and MAH Critical Alarm Review, 25 March 2016.