Audit of LPP operations with respect to Verification, Incident Investigation, and compliance with IEC 61508

Offshore Audit carried out 22nd to 24th June 2020
© Copyright RPS Group Plc. All rights reserved.
The report has been prepared for the exclusive use of our client and unless otherwise agreed in writing by RPS Group Plc, any of its subsidiaries, or a related entity (collectively ‘RPS’), no other party may use, make use of, or rely on the contents of this report. The report has been compiled using the resources agreed with the client and in accordance with the scope of work agreed with the client. No liability is accepted by RPS for any use of this report, other than the purpose for which it was prepared. The report does not account for any changes relating to the subject matter of the report, or any legislative or regulatory changes that have occurred since the report was produced and that may affect the report. RPS does not accept any responsibility or liability for loss whatsoever to any third party caused by, related to or arising out of any use or reliance on the report.
RPS accepts no responsibility for any documents or information supplied to RPS by others and no legal liability arising from the use by others of opinions or data contained in this report. It is expressly stated that no independent verification of any documents or information supplied by others has been made. RPS has used reasonable skill, care and diligence in compiling this report and no warranty is provided as to the report’s accuracy. No part of this report may be copied or reproduced, by any means, without the prior written consent of RPS.

Prepared by:  
RPS  
John Davies  
Principal Adviser  
35 New Bridge Street  
London, EC4V 6BW  
T +44 207 280 3300  
E DaviesJ@rpsgroup.com

Prepared for:  
Ministry of Energy  
Victor Bariudin  
Head of Engineering Inspection Division  
7 Bank Israel St. POB 36148,  
Jerusalem 9136002, Israel.  
T +972-74-7681563  
E victorb@energy.gov.il
Contents
Abbreviations .................................................................................................................. 0
Executive Summary ............................................................................................................. 1
  LPP Audit Findings ........................................................................................................ 1
  Way Forward .................................................................................................................... 1
  Verification ....................................................................................................................... 1
  Incident investigation ...................................................................................................... 2
  Functional Safety ........................................................................................................... 3
1 INTRODUCTION ........................................................................................................... 6
  1.1 Audit Process ............................................................................................................ 6
     1.1.1 Preparation ........................................................................................................ 6
     1.1.2 Team .................................................................................................................. 6
     1.1.3 Approach .......................................................................................................... 6
2 VERIFICATION ............................................................................................................. 8
  2.1 Purpose .................................................................................................................... 8
  2.2 Verification – Requirements ..................................................................................... 8
  2.3 What Was Done During The Audit ......................................................................... 9
  2.4 What Was Found ..................................................................................................... 9
  2.5 Summary ................................................................................................................ 10
     2.5.1 Requirements .................................................................................................. 10
     2.5.2 Current Status .................................................................................................. 10
     2.5.3 Verification Key Finding .................................................................................. 10
     2.5.4 Verification Key Recommendations ............................................................... 10
3 INCIDENT INVESTIGATION ....................................................................................... 12
  3.1 Purpose ................................................................................................................... 12
  3.2 Incident Investigation – Requirements ................................................................... 12
  3.3 What Was Done During The Audit ......................................................................... 12
  3.4 What Was Found ..................................................................................................... 13
     3.4.1 2nd May Gas Release ....................................................................................... 13
  3.5 Summary ................................................................................................................ 16
     3.5.1 Requirements .................................................................................................. 16
     3.5.2 Current Status .................................................................................................. 16
     3.5.3 Incident Investigation Key Finding ................................................................. 16
     3.5.4 Incident Investigation Key Recommendations ................................................ 16
4 COMPLIANCE WITH IEC 61508/11 ....................................................................... 18
  4.1 Purpose ................................................................................................................... 18
  4.2 Functional Safety – A Brief Overview .................................................................... 18
  4.3 What Was Done During The Audit ......................................................................... 18
  4.4 What Was Found ..................................................................................................... 19
     4.4.1 System Implementation ..................................................................................... 19
     4.4.2 Process Incidents .............................................................................................. 20
  4.5 Future Actions ......................................................................................................... 23
  4.6 Summary ................................................................................................................ 23
     4.6.1 Requirements .................................................................................................. 23
     4.6.2 Current Status .................................................................................................. 23
     4.6.3 Functional Safety Key Findings ......................................................................... 24
     4.6.4 Functional Safety Key Recommendations ....................................................... 24
5 OTHER MATTERS DURING THE AUDIT ................................................................. 25
Appendices

Appendix A Outline Scope Of Audit .......................................................... 26
Appendix B Audit Scope And Potential Interviewees ................................. 28
Appendix C Initial Question Set For Interviewees ...................................... 30
### ABBREVIATIONS

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BPCS</td>
<td>Basic Process Control System</td>
</tr>
<tr>
<td>BSEE</td>
<td>Bureau of Safety and Environmental Enforcement</td>
</tr>
<tr>
<td>BV</td>
<td>Bureau Veritas</td>
</tr>
<tr>
<td>Cat.</td>
<td>Category</td>
</tr>
<tr>
<td>CBT</td>
<td>Computer Based Training</td>
</tr>
<tr>
<td>CFR</td>
<td>Code of Federal Regulations</td>
</tr>
<tr>
<td>CMMS</td>
<td>Computerised Maintenance Management System</td>
</tr>
<tr>
<td>ESD</td>
<td>Emergency Shutdown System</td>
</tr>
<tr>
<td>EU</td>
<td>European Union</td>
</tr>
<tr>
<td>FSA3</td>
<td>Stage 3 functional safety assessment</td>
</tr>
<tr>
<td>HART</td>
<td>Highway Addressable Remote Transducer</td>
</tr>
<tr>
<td>HAZOP</td>
<td>Hazard and Operability Study</td>
</tr>
<tr>
<td>IEC</td>
<td>International Electrotechnical Commission</td>
</tr>
<tr>
<td>IGV</td>
<td>Inlet Guide Vane</td>
</tr>
<tr>
<td>I/O</td>
<td>Input/Output</td>
</tr>
<tr>
<td>IVB</td>
<td>Independent Verification Body</td>
</tr>
<tr>
<td>LOPA</td>
<td>Layer of Protection Analysis</td>
</tr>
<tr>
<td>LOTO</td>
<td>Lock Out-Tag Out</td>
</tr>
<tr>
<td>LPP</td>
<td>Leviathan Production Platform</td>
</tr>
<tr>
<td>mA</td>
<td>milliamperes</td>
</tr>
<tr>
<td>MoC</td>
<td>Management of Change</td>
</tr>
<tr>
<td>MoE</td>
<td>Israeli Ministry of Energy</td>
</tr>
<tr>
<td>MoEP</td>
<td>Israeli Ministry of Environmental Protection</td>
</tr>
<tr>
<td>NAMUR</td>
<td>User Association of Automation Technology in Process Industries</td>
</tr>
<tr>
<td>NEML</td>
<td>Noble Energy (Mediterranean) Limited</td>
</tr>
<tr>
<td>OIM</td>
<td>Offshore Installation Manager</td>
</tr>
<tr>
<td>OMS</td>
<td>Operations Management System</td>
</tr>
<tr>
<td>PIC</td>
<td>Person(s) In Charge</td>
</tr>
<tr>
<td>PSD</td>
<td>Process Shutdown</td>
</tr>
<tr>
<td>PSSR</td>
<td>Pre Start-Up Safety Review</td>
</tr>
<tr>
<td>RIO</td>
<td>Remote Input/Output</td>
</tr>
<tr>
<td>SCE</td>
<td>Safety Critical Element</td>
</tr>
<tr>
<td>SEMS</td>
<td>Safety &amp; Environmental Management System</td>
</tr>
<tr>
<td>SIL</td>
<td>Safety Integrity Level</td>
</tr>
<tr>
<td>SIS</td>
<td>Safety Instrumented System(s)</td>
</tr>
<tr>
<td>SMART</td>
<td>A web based system for compliance checks (in accordance with 30.CFR.250 requirements)</td>
</tr>
<tr>
<td>SRS</td>
<td>Safety Requirements Specification</td>
</tr>
</tbody>
</table>
EXECUTIVE SUMMARY

LPP Audit Findings

This report describes the findings, recommendations and suggested solutions from an audit carried out on the Leviathan Production Platform (LPP), offshore Israel, between the 22nd and 24th June 2020 by the Ministry of Energy (MoE) and RPS.

It has been compiled from a significant number of interviews, document reviews and conversations with management, supervisory and technical staff from Noble Energy Mediterranean Limited (NEML). It presents a significant number of future steps for improvement, these are all linked to the overall findings presented in this executive summary.

The audit team would like to thank the interviewees, platform team and the team monitoring and supporting the audit for their help, openness and efforts to respond to the auditors’ requests and comments. Whilst we hoped to minimise disruption and inconvenience during the audit, these activities will always require a significant effort from platform and shore management, this was unstintingly given, making the audit significantly easier to perform and almost certainly more effective.

Way Forward

Following discussions within the Ministry of Energy (MoE), the following steps have been given agreed deadlines for completion. The intention is that NEML will issue regular progress reports on the identified actions and the MoE will revisit LPP to assess the progress and conduct audits on further matters of interest / concern to them.

Verification Requirements

LPP production lease requires verification throughout the installation lifecycle.

Current Status

During design and construction, Bureau Veritas (BV) were contracted as the Independent Verification Body (IVB). At the moment, there is no incumbent operational phase IVB although a contract is about to be let. There is currently no ongoing verification activity, nor have there been any preparations with respect to CMMS/Smart or the relevant OMS standards to enable verification to be carried out.

Design performance standards were produced and BV state that the installation has been verified in accordance with them.

Verification Key Finding

Operational verification is not being carried out. This is a major non-compliance with good oilfield practice

Verification Key Recommendation

Implement a verification scheme and all its associated processes that clearly define and maintain the expected performance of safety critical elements.

Suggested solution

Step 1: Configure the maintenance and inspection processes, including CMMS and other related systems to link tagged and non-tagged equipment to the relevant safety critical elements and their performance requirements.
Step 2: Prepare operational performance standards which draw from the design hazard studies and good international practice to establish the necessary functionality, availability, reliability, survivability (of a major accident event) and interdependency to maintain a safe operating environment.

Step 3: Draft the supporting OMS documents and job plan procedures to carry out the assurance and verification tasks.

Step 4: NEML must ensure they select a competent IVB and can demonstrate that the system is working effectively with, *inter alia*, all necessary reporting and standards by February 28th 2021.

**Incident investigation**

**Requirements**

The LPP Lease requires compliance with 30.CFR 250-1900 to 1933 (Clause 1919 requires the investigation of incidents) and Guidelines of the Petroleum Commissioner: Reporting Exceptional Events (latest 02 June 2020).

**Current Status**

NEML is carrying out incident investigations in accordance with OMS Element 11 and 30 CFR 250 requirements.

**Incident Investigation Key Findings**

There are concerns regarding the event reporting, as well as the content and quality of the incident reporting. This is a minor non-conformance with 30.CFR.250.1919.

**Incident Investigation Key Recommendations**

Undertake the actions necessary to improve the quality of the investigations and ensure that lessons are learnt from the investigated incidents.

**Suggested Solutions**

Step 1: NEML should consider establishing a core team with the necessary competence to generate effective and professional investigations. The team should operate with clear procedures and guidelines to ensure a consistent and thorough approach. Investigation reports should be based around a timeline which extends as far as is necessary to include all initiating or root causes, and the recovery.

Step 2: MoE should consider revising the instructions given in Guidelines of the Petroleum Commissioner: Reporting Exceptional Events (latest 02 June 2020) to separate the reporting and investigation requirements such that initial reporting occurs as soon as is practicable, with appropriate weekly updates and sufficient time is given for NEML to conduct an effective and professional investigation.

Step 3: NEML should implement a mechanism to promote consideration of the ramifications of incident investigation findings to help prevent future occurrences from similar causes.

Step 4: NEML should ensure that all studies which aim to satisfy compliance with the installation hazard analysis and the job safety assessments, as per 30.CFR.250-1911 are readily available to all operational personnel, and particularly those conducting investigations who need to consult them, and that studies are updated/amended as a result of the investigation.

Step 5: NEML should conduct process safety training to ensure that all management and investigation personnel can assess the necessary level of investigation that is required to be carried out should an incident occur. Process safety knowledge should be incorporated within NEML’s training and competency processes for all personnel but with emphasis on the competency of management personnel.

Step 6: NEML should review the current incident investigation training to ensure that all personnel are aware of their potential roles and responsibilities in an incident investigation.
Functional Safety

Requirements

The LPP design performance standards stated that the ESD system would be designed in accordance with IEC 61508. The associated process industry standard is IEC 61511 and it would be expected that LPP would comply with this element.

Current Status

The LPP design process incorporated Hazard and Operability (HAZOP) studies, Layer of Protection Analysis (LOPA) studies, Safety Integrity Level (SIL) Assignment and SIL Verification; as well as the creation of a Safety Requirements Specification (SRS).

It is not clear if BV verified compliance with IEC 61508 from the information currently available. Wood have stated that they did not undertake Functional Safety Assessments stages 1, 2 or 3, as required by the standard prior to operations commencing. A level of testing has been carried out during the commissioning process by an NEML contractor, but the level of compliance with IEC 61508 is not known.

NEML is understood to have contracted DNV GL to undertake a Stage 3 Functional Safety Assessment.

Functional Safety Key Findings

There is no evidence of direct compliance with IEC 61508, nor the associated process industry standard IEC 61511. This is a major non-conformance with NEML’s design performance standards; overall it is classed as a minor non-conformance with good oilfield practice.

Functional Safety Key Recommendations

NEML should carry out a stage 3 functional safety assessment, which incorporates the necessary elements of stage 1 and stage 2 functional safety assessments, to ensure alignment with the design performance standards.

Suggested Solutions

Step 1: NEML should ensure that the Functional Safety Management Plan incorporates all the requirements of the relevant functional safety standard.

Step 2: NEML should consider using suitable guidance (e.g. NAMUR 43) for settings on analog smart sensors such that fault conditions can be identified and conveyed to the control room operator.

Step 3: NEML should consider preparing a suitable Safety Instrumented Function (SIF) Validation Test Procedure for each individual SIF which is under the control of the installation. The procedure should include all relevant requirements of the functional safety standard, including management of change and fault identification.

Step 4: Following successful completion of the Stage 3 Functional Safety Assessment (FSA3), the future compliance methodology should be agreed between MoE and NEML.
<table>
<thead>
<tr>
<th>Topic</th>
<th>Step Description</th>
<th>Agreed completion deadline</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Verification</strong></td>
<td>Configure the maintenance and inspection processes, including CMMS and other related systems to link tagged and non-tagged equipment to the relevant safety critical elements and their performance requirements.</td>
<td>1st February 2021</td>
</tr>
<tr>
<td></td>
<td>Prepare operational performance standards which draw from the design hazard studies and good international practice to establish the necessary functionality, availability, reliability, survivability (of a major accident event) and interdependency to maintain a safe operating environment.</td>
<td>31st October 2020</td>
</tr>
<tr>
<td></td>
<td>Draft the supporting OMS documents and job plan procedures to carry out the assurance and verification tasks.</td>
<td>30th November 2020</td>
</tr>
<tr>
<td></td>
<td>NEML must ensure that the selected IVB is performing competently and can demonstrate that the system is working effectively with, <em>inter alia</em>, all necessary reporting and standards.</td>
<td>28th February 2021</td>
</tr>
<tr>
<td><strong>Incident Investigation</strong></td>
<td>NEML should consider establishing a core team with the necessary competence to generate effective and professional investigations. The team should operate with clear procedures and guidelines to ensure a consistent and thorough approach. Investigation reports should be based around a timeline which extends as far as is necessary to include all initiating or root causes, and the recovery.</td>
<td>30th September 2020</td>
</tr>
<tr>
<td></td>
<td>MoE should consider revising the instructions given in Guidelines of the Petroleum Commissioner: Reporting Exceptional Events (latest 02 June 2020) to separate the reporting and investigation requirements such that initial reporting occurs as soon as is practicable, with appropriate weekly updates and sufficient time is given for NEML to conduct an effective and professional investigation.</td>
<td>30th September 2020</td>
</tr>
<tr>
<td></td>
<td>NEML should implement a mechanism to promote consideration of the ramifications of incident investigation findings to help prevent future occurrences from similar causes.</td>
<td>15th October 2020</td>
</tr>
<tr>
<td></td>
<td>NEML should ensure that all studies which aim to satisfy compliance with the installation hazard analysis and the job safety assessments, as per 30.CFR.250-1911 are readily available to all operational personnel, and particularly those conducting investigations who need to consult them, and that studies are updated/amended as a result of the investigation.</td>
<td>31st October 2020</td>
</tr>
<tr>
<td></td>
<td>NEML should conduct sufficient process safety training to ensure that all personnel can assess the necessary level of investigation that is required to be carried out. Process safety knowledge should be incorporated within NEML’s training and competency processes for all personnel but with particular emphasis on the competency of management personnel.</td>
<td>31st December 2020</td>
</tr>
<tr>
<td></td>
<td>NEML should review the current incident investigation training to ensure that all personnel are aware of their potential roles and responsibilities in an incident investigation.</td>
<td>31st October 2020</td>
</tr>
<tr>
<td><strong>IEC 61508/11</strong></td>
<td>Ensure that the Functional Safety Management Plan incorporates all the requirements of the relevant functional safety standard.</td>
<td>30th September 2020</td>
</tr>
<tr>
<td></td>
<td>NEML should consider using suitable guidance (e.g. NAMUR 43) for settings on analog smart sensors such that fault conditions can be identified and conveyed to the control room operator.</td>
<td>30th September 2020</td>
</tr>
<tr>
<td></td>
<td>NEML should consider preparing a suitable Safety Instrumented Function (SIF) Validation Proof Test Procedure for each individual SIF which is under the control of the installation. The procedure should include all relevant requirements of the functional safety standard, including management of change and fault identification.</td>
<td>30th September 2020</td>
</tr>
<tr>
<td></td>
<td>Following successful completion of the stage 3 functional safety assessment, the future compliance methodology should be agreed between MoE and NEML.</td>
<td>30th November 2020</td>
</tr>
</tbody>
</table>

**Table 1:** Action Items with Deadlines from the LPP June 2020 Audit
When MoE revisit these steps, the criteria for judging completion will be given at the beginning of any audit. As a minimum it is expected that the evidence of completion will be systems appropriately modified (this will include OMS standards and procedures as well as CMMS / SMART, etc.), plus the personnel who will be interviewed should be able to demonstrate an appropriate level of training, awareness and expertise.
1 INTRODUCTION

1.1 Audit Process

As part of the preparation for the audit NEML, were asked to supply a considerable number of documents to allow the audit team to become familiar with the NEML processes and allow suitable preparation for the audit.

The chosen main topics for the audit were based upon ongoing concerns regarding incident investigations and their quality, and uncertainty regarding the situation post start-up of production in terms of verification. An additional topic was added concerning NEML’s operational compliance with IEC61508/11 as a result of answers which were received during a previous visit to LPP by MOE/RPS personnel.

1.1.1 Preparation

In preparation for the audit a significant number of documents were requested from NEML. These documents were supplied by NEML Team

The audit took place over the period 22nd to 24th June 2020 inclusive. The initial team comprised XXXX, XXXX and XXXX until the 23rd with the three MOE personnel being exchanged for XXXX and XXXX for the 23rd and 24th. The RPS Energy team members were XXXX (audit team leader) and XXXX for the duration of the visit.

1.1.2 Approach

The outline scope of work was supplied to NEML and is presented in Appendix A; further clarification was requested by NEML, which was supplied by MoE, and is presented in Appendix B.

The majority of personnel positions identified in the listing were either interviewed utilising the pre-prepared questionnaires or in the discussions with the NEML team who were monitoring the audit. Amongst that monitoring team were:

YYYY –
RRRR –
VVVV –
TTTT –
WWWW –
CCCC – .

Prior to the audit a set of high level questions were prepared and these were utilised with all interviewees; these are presented in Appendix C. A further set of more detailed questions had been prepared for the interviewees but given the responses that were being obtained the audit team leader decided to not utilise them.

1.1.2.1 Compliance

Within the findings, where issues were noted these were referred back to the OMS documents, other NEML documents or in a small number of cases ‘good oilfield practice’.

Where the audit team felt that the intent of the governing document was not being achieved, these were noted as major non-compliances.

Where the team felt the overall intent was largely in place but details were not compliant, this was described as a minor non-compliance.

Lesser issues were classed as opportunities for improvement.
There were several items noted during the visit which have been classed as **Observations**. This approach was on the basis they were comparatively minor matters in terms of compliance or they were outside the strict remit of the three themes of this audit.
2 VERIFICATION

2.1 Purpose

The purpose of the verification audit was fivefold:

1. To establish personnel’s knowledge of the verification process and requirements – primarily for platform management positions.
2. To investigate the ability of the CMMS to identify, schedule and report on performance standards and verification activities.
3. Assess how NEML have structured their maintenance and inspection activities to align with the verification process.
4. Assess how NEML will schedule assurance and verification tasks.
5. Assess how NEML will monitor the status of their SCEs.

2.2 Verification – Requirements

The requirements for verification are included within the Leviathan production leases (North and South) and are reproduced below:

11. Independent Verification Body

11.1. Without derogating from the supervision authority of the Commissioner and of any other competent authority and any other provisions of this Lease and any Applicable Law, and without derogating from liability of the Lease Holder, the planning of the Production System, the production of the components of such system, its construction and operation will be executed under the verification of qualified Independent verification Body experienced in supervising marine production systems, with which the Lease Holder will engage for the purpose of supervision and issuance of independent professional certifications and verifications.

11.2. The Lease Holder will inform the Commissioner, at least 30 days prior to any engagement of such Independent verification Body, the identity of the intended Independent verification Body and ask for the Commissioner’s approval. The Lease Holder will inform the Commissioner of the identity of the Independent verification Body for the first time within three months after the grant of the Lease, and will also do so whenever the Lease Holder is interested in engaging an additional Independent verification Body during the Lease Term. The Commissioner may refuse the approval of Independent verification Body, if the Commissioner was not satisfied that such company lacks independence or that such company has the professional capabilities and experiences required for the performance of supervision at a high standard.

11.3. All the reports, verifications and certifications of the Independent verification Body will be directly provided to the Commissioner; For the avoidance of doubt, the Lease Holder will fully bear the costs involved in the engagement and the services of such Independent verification Body.

11.4. Once every year or if an exceptional event occurs, the Commissioner may require the supervision, testing, control, certification or verifications by the Supervision Company, to the extent required, as the Commissioner may deem proper, for assuring the reliability and security of the Gas supply.

From these lease clauses it can be seen that the verification requirement largely echoes the process of verification under the EU Offshore Safety Directive, with the additional requirements that reporting is to the MoE as well as NEML.
2.3 What Was Done During The Audit

The team interviewed several personnel on the installation using a proforma of initial questions which had been shared with the installation management team in advance. The audit team intended to ask the questions on the proforma to each person and type a brief summary of the answers given. This question set is in Appendix C. All of the initial interviewees were asked the initial question set. Occasionally, the team asked additional questions related to the answers provided by each interviewee to further clarify some of the answers given.

A more detailed question set had been prepared in advance of arrival at the platform, which was intended to guide much more in-depth questioning, but on consideration within the audit team, it was decided to address most of these questions to the NEML team who were monitoring the audit and who were considered to be appreciably better informed than the majority of the interviewees.

2.4 What Was Found

Overall, the platform personnel were almost completely unaware of the requirements for verification. Some made ‘educated guesses’ as to what the interviewers were asking, but overall, it was apparent that there had been no effort to inform the personnel.

G. When these questions were asked of the audit monitoring team, they candidly admitted that there were no verification activities ongoing. NEML has issued a contract to Xodus to review the Operational Performance Standards and the wording of the Leviathan Operating Permit was used as justification that verification was not required. An extract of the clause in the Operating Permit used in that justification is reproduced below: *Unless determined otherwise in law and subject to the provisions of this Authorization, the Lease Holders will operate and maintain the production system in accordance with the US Regulations; the Lease Holders will act with regard to control, inspections, guidelines, and registration in accordance with the relevant sections in the US Regulations 30 CFR 250, without derogating from the provisions of the Lease Deeds.*

Whilst there is no doubt there is little compatibility between the full set of 30.CFR.250 regulations and verification, reading this clause in isolation does not appear to negate the lease conditions whilst the ‘relevant sections of 30.CFR.250’ would normally require reference to the sections of CFR regulations specifically identified in the lease.

It was not the intent of the audit to establish the reasons for verification during the operating phase not being undertaken. However, within the preparatory documentation received from NEML, it is apparent that the preparatory works which would normally be undertaken by a combined project and operations team were not undertaken. NEML has two procedures for the allocation of criticality to equipment, neither of these documents define safety critical in a way that aligns with the verification processes.

Equally within the CMMS there is no linkage to whether or not equipment is part of a safety critical element (SCE). Compliance checks (in accordance with 30.CFR 250 requirements) are included within a web-based system called SMART. This system was shown to the audit team and generally seemed to be an effective tool to carry out what would in verification terms, be called assurance tasks. It would however require significant re-configuration to properly support the assurance tasks required from verification activities.

There is no provision currently in place, for tasks being scheduled against equipment that is not part of the tagging system. This would typically be passive fire protection, structural elements, ranging down to items as small as temporary refuge doors.

The correspondence between inspection and maintenance tasks required within the draft operation performance standards and tasks scheduled within CMMS is largely non-compliant – although this will require to be done once NEML has an acceptable set of operational performance standards.

To summarise the situation, the NEML team did not undertake the tasks which would be expected to prepare for verification during the operational phase. Thus, the platform went into production without a complete
demonstration that the design performance standard requirements had been met. The operational team are thus left with a situation where an extensive body of work is required to get verification to function.

Within this body of work, possibly the least effort is the writing of effective operational performance standards and the necessary assurance actions. The greater effort is to configure the maintenance and inspection systems so that equipment can be determined to be safety critical and therefore assurance tasks can be effectively carried out, assessed and reported. This will require additional LPP specific documentation within OMS and a large training effort to ensure the requirements of the verification process and the methods to align with it.

2.5 Summary

2.5.1 Requirements

LPP production lease requires verification throughout the installation lifecycle.

2.5.2 Current Status

During design, construction, installation and commissioning, Bureau Veritas (BV) was contracted as the Independent Verification Body (IVB). Design performance standards were produced and developed by Wood and NEML. On December 12, 2019, BV issued a Final Report (Report No. 18316-102020.00 – C Rev. 0) on the Commissioning Phase of the LPP that stated the LPP had been verified in accordance with the design performance standards. MoE accepted BV's verification with the Permit to Operate on December 19, 2019.

At the time of the audit, NEML had issued the contract for the operational phase IVB to BV. Although operational verification activities had started they were incomplete and not ready for use. Nor has there been any preparations with respect to CMMS/Smart or the relevant OMS standards to enable verification to be carried out.

Design performance standards were produced and BV state that the installation has been verified in accordance with them.

2.5.3 Verification Key Finding

Operational verification is not being carried out. This is a major non-compliance with the international standards and good oilfield practice.

2.5.4 Verification Key Recommendations

Implement a verification scheme and all its associated processes which clearly define and maintain the expected performance of safety critical elements.

2.5.4.1 Suggested Solution

Step 1: Configure the maintenance and inspection processes, including CMMS and other related systems to link tagged and non-tagged equipment to the relevant safety critical elements and their performance requirements.

Step 2: Prepare operational performance standards which draw from the design hazard studies and good international practice to establish the necessary functionality, availability, reliability, survivability (of a major accident event) and interdependency to maintain a safe operating environment.

Step 3: Draft the supporting OMS documents and job plan procedures to carry out the assurance and verification tasks.

Step 4: NEML must ensure that the selected IVB is performing competently and can demonstrate that the system is working effectively with, *inter alia*, all necessary reporting and standards by February 28th, 2021.
Note: the audit team believe this work could be completed by this time, if a serious effort is made. We would expect verification in all its forms to be functional by then, assurance, verification, reporting and all the associated maintenance and inspection infrastructure within the CMMS, Smart etc.
3 INCIDENT INVESTIGATION

3.1 Purpose

The purpose of the incident investigation audit was fourfold:

1. To understand the underlying issues which have given concerns to MoE/RPS in terms of the quality of the investigations.
2. To ensure that NEML is working in accordance with the processes laid out in Element 11 of OMS/SEMS.
3. To establish if and how the actions being generated by these investigations are being tracked and closed out once completed.
4. To ensure that any knowledge or learnings were being utilised to reduce the potential for future incidents.

3.2 Incident Investigation – Requirements

The requirements for incident investigations are common across most regulatory environments. For NEML operation in Israel they are set by 30.CFR.250-1919 which is incorporated into the Leviathan Field Leases, and quoted below:

§ 250.1919 What criteria for investigation of incidents must be in my SEMS program?

To learn from incidents and help prevent similar incidents, your SEMS program must establish procedures for investigation of all incidents with serious safety or environmental consequences and require investigation of incidents that are determined by facility management or BSEE to have possessed the potential for serious safety or environmental consequences. Incident investigations must be initiated as promptly as possible, with due regard for the necessity of securing the incident scene and protecting people and the environment. Incident investigations must be conducted by personnel knowledgeable in the process involved, investigation techniques, and other specialties that are relevant or necessary.

(a) The investigation of an incident must address the following:

(1) The nature of the incident;

(2) The factors (human or other) that contributed to the initiation of the incident and its escalation/control; and

(3) Recommended changes identified as a result of the investigation.

(b) A corrective action program must be established based on the findings of the investigation in order to analyze incidents for common root causes. The corrective action program must:

(1) Retain the findings of investigations for use in the next hazard analysis update or audit;

(2) Determine and document the response to each finding to ensure that corrective actions are completed; and

(3) Implement a system whereby conclusions of investigations are distributed to similar facilities and appropriate personnel within their organization.

3.3 What Was Done During The Audit

The team interviewed a number of personnel on the installation using a proforma of initial questions which had been shared with the installation management team in advance. The audit team intended to ask the questions on the proforma to each person and type a brief summary of the answers given. This question set
is in Appendix C. All of the initial interviewees were asked the initial question set. The audit team asked the questions on the form to each person and typed a brief summary of the answers given. Occasionally, the team asked additional questions related to the answers provided by each interviewee to further clarify some of the answers given.

A more detailed question set had been prepared in advance of arrival at the platform, which was intended to guide much more in-depth questioning, but on consideration within the audit team, it was decided to address most of these questions to the NEML team who were monitoring the audit and who were considered to be appreciably better informed than the majority of the interviewees.

3.4 What Was Found

Overall, the platform personnel were aware of incident investigations, as required by CBT (Computer Based Training) for Element 11 of the OMS and that the technique used is the Five Why’s process. Only the Occupational Safety Lead mentioned that for more serious incidents, TapRoot methodology is used. This person was not subject to interview (although they were part of the platform audit monitoring team) and offered the information freely.

Several of those interviewed knew how an investigation should be structured, but these were more senior personnel. It was noted that personnel who were not in management positions appeared less likely to be familiar with the process.

Most of those interviewed had not been involved in an incident investigation although they had a basic awareness of the activities that would be involved, due to the computer-based training that they had undergone.

Although it is understood that incident refresher training should be undertaken annually, this does not appear to be widely complied with.

None of the interviewees knew where they were on the competency scale with respect to incident investigation. This suggests that there is a fairly flat structure when it comes to competence and experience, and in theory (although unlikely in practice), anyone who has undertaken the training could investigate anything.

The Five Why’s reports do not appear to reflect a rigorous effort to establish the root cause; they appear more to attempt to find five possible causes. The methodology of the Five Why’s is to keep asking why something occurred in an effort to identify a systemic failure which can then be addressed. The intention is not to fill the five rows or to stop at five rows. The starting point should generally be – the automation system of the gas release or whatever negative event occurred and then ask sufficient “whys” to obtain a root cause. In very few cases will a root cause not be a systemic problem, such as competency, a lack of rigour in procedures or sometimes violations.

The audit team has been furnished with the questions and answers from the computer-based incident investigation training. This system is intended to give everyone on-board LPP a baseline level of understanding. Personnel involved in writing and performing incident investigations receive additional training.

Additional training in being a witness in an investigation would likely offer a benefit in the form of more thorough witness statements, in turn aiding the incident investigators to identify the root causes.

3.4.1 2nd May Gas Release

As part of the exploration of the effectiveness of the incident investigation process per OMS Element 11, the Gas Leak on 2nd May was further examined. A team from the MoE visited LPP on the 5th May to follow-up on this incident and the general consensus from NEML personnel was that this was not an important issue, indeed it was referred to as an ‘event’ rather than an incident.

In the interim period NEML had re-examined the event and compiled an evaluation report and a review of this evaluation by Xodus. The NEML evaluation report established that the incident had the potential for a
large loss of life in the event that the release had ignited. We fully agree with this finding which was apparent to RPS on the initial report. It is a matter of great concern that it was not apparent to NEML personnel.

As of the time of writing this report there is still no detailed investigation report to cover this incident, whilst the evaluation report has informed NEML of the event's severity there is little in it to understand why this drain might have been operated, indeed the evaluation report states “The scope of this report covers the physical release of gas during the event. Issues such as the cause of the release and the sequence of events are discussed only at a high level as they are discussed in greater detail in other incident investigation documentation, such as the Five Why report”[1]. This direct quote from the evaluation report refers to the initial Five Why report.

Figure 1: Site of 2nd May Gas Release

Whilst the initial Five Why’s and the later evaluation report do give much more detail there is no overall investigation summary or findings. The last Why in the Five Why’s report is “Valve location and position leads to two separate and independent teams failing to locate and confirm valve position/plug”. OMS Element 11 states that for Level 3 incidents a root cause analysis must be performed.
We believe the Five Why’s reports fall considerably short of a root cause and so this is a minor non-compliance with Element 11.

The evaluation report quotes a Noble Energy document - Process Safety Event Standard. The NEML audit monitoring team showed the auditors a ranking table from this document which assesses this incident as Process Safety Event Tier 2 – based upon the amount of gas which was estimated to have been released. The use of corporate documents to override the NEML OMS is not considered good practice and categorising incidents upon the mass of substances released is inappropriate. If the potential of an incident is not being realised then any potential learning, or warning from an incident is likely to be ineffective.

**OMS Element 11 follows good oilfield practice and requires the potential consequences to be determined, the Process Safety Event Standard does not appear to be do so and so is an area for improvement, as is the inter-relationship between corporate and NEML procedures.**

### 3.4.1.1 What Was Found

The team was taken through some of the incident investigation training material. The training is computer-based and confirms knowledge has been absorbed by the trainee via the use of confirmatory questions. If the trainee does not answer the questions correctly, they must undergo that part of the training again.

The computer-based training appeared to be well thought out, although the team was not taken through the whole of the training materials due to time constraints.

It is understood that once the training is completed, a trainee may be considered competent to undertake incident investigations. For simple investigations, this may be true but for more complex investigations, it is unlikely to be so. Naturally, experience is a formidable educator, but it is considered that if the computer-based training were followed up by practical training, this would be beneficial. It is unknown if this occurs.

### 3.4.1.2 Reporting Requirements

Due to MoE requirements, incidents are not just limited to those which could have an adverse effect on safety, the environment or assets. Indeed, process upset events which lead to flaring (a critical safety operation) must also be reported within 24 hours. This could be said to hamper the thoroughness of an incident investigation by not allowing sufficient time to reach a well-considered conclusion.

### 3.4.1.3 Five Why’s Content

The Five Why’s reports reviewed were mostly short documents, suggesting that most incidents are minor. Whilst this level of incident is to be expected, the frequency of such occurrences should be monitored to ensure that there is not a systemic underlying cause which requires attention.

Upon review of the Five Why’s reports, it is apparent that the incident investigation is generally identifying the apparent causes and not the root cause; although there are one or two exceptions to this where a more diligent approach has been taken. This may be due to the time frame within which the investigation must be completed. It is recommended that each apparent cause is interrogated for a root cause until a point of diminishing returns is identified. It could be argued that incidents occur due to a systemic failure and not due to mechanical failure; i.e. something was not done, done incorrectly, or not done frequently enough; therefore a re-think of maintenance and operating practices as a result of the investigation may yield some benefits.

### 3.4.1.4 Investigation Follow-Up

Lessons learned from incident investigations are shared with the crew, and this is commendable. However, the learnings are not necessarily used for forward planning to identify whether the same incident could happen elsewhere on the platform and taken preventative action. (The audit monitoring team were asked about the guided wave radar initiated PSD, as to whether more of these transducers were fitted to the plant –
this was not known). Therefore, it is entirely conceivable that the same event could happen a number of times due to the same cause when in fact it could be remedied and avoided.

All of the incidents to date are held in a SharePoint site, administered by the Operations Compliance Manager. We found that this system appeared to be complete and to have the necessary action tracking and closeout to ensure a sufficient level of control. It also has a suitable level of reporting which allows the assessment of outstanding or overdue actions or issues.

### 3.4.1.5 Information Available To Assess Incidents

These findings led to the team exploring why the severity of the Gas Leak had not been understood.

The audit monitoring team was asked to show the auditors the hazard analysis (facility level) required under 30.CFR-250-1911 which form part of the Lease conditions. Searching the NEML document database resulted in a directory of some 80 documents – none of which were identified as applicable to this requirement. There was no indexing or explanation of the various hazard assessment studies which have been undertaken for the LPP and so the lack of understanding by platform staff is understandable.

The audit monitoring team were then asked to perform the same task – finding the hazard analysis (facility level) for Tamar. Again, they failed to be able to find any applicable document(s).

We find this is a direct contravention of the 30.CFR-250-1919 requirements and is judged to be a major non-conformance within OMS Element 3.

During this period of the audit the monitoring team volunteered that some process safety training has been undertaken with personnel. This background knowledge is not required within the Training and Competency Matrix.

We believe that a good understanding of process safety is essential for all personnel. For those in supervisory positions, the ability to find and understand the hazard assessments which have been carried out for LPP and which justify its design is essential.

It is apparent that this understanding is not present amongst a significant proportion of the supervisory personnel and we find this falls considerably short of good oilfield practice.

### 3.5 Summary

#### 3.5.1 Requirements

The LPP Production Lease requires compliance with 30.CFR. 250-1900 to 1933 (Clause 1919 requires the investigation of incidents) and Guidelines of the Petroleum Commissioner: Reporting Exceptional Events (latest 02 June 2020).

#### 3.5.2 Current Status

NEML are carrying out incident investigations in accordance with OMS Element 11 and 30 CFR 250 requirements.

#### 3.5.3 Incident Investigation Key Finding

There are concerns regarding the event reporting, as well as the content and quality of the incident reporting.

#### 3.5.4 Incident Investigation Key Recommendations

Undertake the actions necessary to improve the quality of the investigations and ensure that the lessons learned are effectively implemented.
3.5.4.1 Suggested Solutions:

Step 1: NEML should consider establishing a core team with the necessary competence to generate effective and professional investigations. The team should operate with clear procedures and guidelines to ensure a consistent and thorough approach. Investigation reports should be based around a timeline which extends as far as is necessary to include all initiating or root causes, and the recovery.

Step 2: MoE should consider revising the instructions given in Guidelines of the Petroleum Commissioner: Reporting Exceptional Events (latest 02 June 2020) to separate the reporting and investigation requirements such that initial reporting occurs as soon as practicable (e.g. within 24 hours), with appropriate weekly updates and sufficient time given for NEML to conduct an effective and professional investigation.

Step 3: NEML should implement a mechanism to promote consideration of the ramifications of incident investigation findings to help prevent future occurrences from similar causes.

Step 4: NEML should ensure that all studies which aim to satisfy compliance with the installation hazard analysis and the job safety assessments, as per 30.CFR.250-1911 are readily available to all operational personnel, and particularly those conducting investigations who need to consult them, and that studies are updated/amended as a result of the investigation.

Step 5: NEML should conduct process safety training to ensure that all management and incident investigation personnel can assess the necessary level of investigation that is required to be carried out should an incident occur. Process safety knowledge should be incorporated within NEML’s training and competency processes for all personnel but with emphasis on the competency of management personnel.

Step 6: NEML should continue competency training to ensure that all personnel are aware of the incident investigation process and responsibilities in an incident reporting structure. NEML should continue to train personnel to their expected level of responsibility in incident investigations and involve additional onshore or remote resources as needed to aid in incident investigations.
4 COMPLIANCE WITH IEC 61508/11

4.1 Purpose

The purpose of the functional safety audit was fourfold:

1. Establish the level of compliance with the International Electrotechnical Commission (IEC) functional safety standards IEC 61508 and IEC 61511,
2. Establish whether the emergency shutdown system was operating in line with the design assumptions,
3. Establish whether the platform was operating in line with the emergency shutdown design arrangements, and
4. Identify any potential instrumented protection system safety enhancements.

4.2 Functional Safety – A Brief Overview

Functional Safety is the use of electrical, electronic or programmable electronic equipment to provide a determined minimum quantum of protection. The purpose of functional safety is to maximise protection by minimising the likelihood that the safety function does not work when needed, by seeking to eliminate faults in specification, design, manufacture and operations as well as those introduced through change.

The protection is provided by one or more safety instrumented systems (SIS), which contain one or more safety instrumented functions (SIF). A SIF is commonly referred to throughout the process industries as a ‘trip’.

The overall standard to comply with is IEC 61508 and equipment which is intended for use in such a system must, in most cases, be certified by the manufacturer as compliant with this standard. There is a ‘daughter’ standard, IEC 61511, which is formulated specifically for the process industries (the LPP can be considered to fall within this category) and is aimed at the designers of safety instrumented systems (SIS). Compliance by designers to IEC 61511 ensures compliance with IEC 61508.

Standard IEC 61508 introduces the concept of a Safety Integrity Level (SIL), which has four discrete ranges, from 1 (lowest) to 4 (highest). The amount of rigour required to demonstrate compliance with the standard (and thus the minimisation of design faults) is significant and increases in line with the SIL.

Prior to commencing operations (when the SIF is required to provide protection), it must undergo stage 1, 2 and 3 functional safety assessments. Note that it is allowed by the standard and indeed commonplace on small projects for stage 1 and 2 functional safety assessments to be captured during the stage 3 functional safety assessment.

The LPP has SIS of SIL 1 and SIL 2. Per the requirements of the functional safety standards, the burden upon NEML is to prove that the SIS can achieve their required SIL. Functional Safety Assessments are the method by which proof is demonstrated. This was incorporated into the design Performance Standards for the project by NEML.

4.3 What Was Done During The Audit

The team intended to interview several personnel on the installation using a proforma of initial questions which had been shared with the installation management team in advance. The audit team intended to ask the questions on the proforma to each person and type a brief summary of the answers given. This question set is in Appendix C.

A detailed question set was prepared in advance of arrival at the platform, which was intended to guide an exploration of the emergency shutdown system settings and performance. The detailed question set was prepared using the following documentation:
IEC functional safety standards IEC 61508 and IEC 61511,
NEML Functional Safety Management Plan, and
NEML Safety Requirements Specification.

The detailed question set was issued to the platform management the day prior to a conference call with the platform designer, Wood, who are based in Texas.

4.4 What Was Found

Upon discussion of the base questions, the team were assured that the platform design had been prepared in compliance with the functional safety standards. However, the platform management team did not appear to be well informed of these standards and a conference call with the platform designer (Wood Group in Houston) was duly arranged. The platform management team stated that functional safety assessments stages 1 through 3 had not been carried out.

This is in direct contravention to Clause 5 of IEC 61511 which requires knowledge of the legal and regulatory functional safety requirements and can be classed as a minor non-conformance with the IEC standard.

During the conference call, Wood personnel confirmed that a hazard and risk assessment had been undertaken and that safety functions had been allocated to protection layers, but that Functional Safety Assessments had not been undertaken.

This is in direct contravention to the design performance standards in which NEML stated that they would comply with IEC 61508 and can be considered a major non-conformance with their own processes, a minor non-conformance in terms of good oilfield practice regarding verification.

Given that full compliance with IEC 61508 was not undertaken and that the platform management were not familiar with the standard or its requirements, it was agreed between the parties that interviewing the platform management team would yield little further benefit.

It is apparent that some aspects of the functional safety standards (and of industry good design practice) had been applied during the design phase; for example a Hazard and Operability Study (HAZOP) and Layer of Protection Analysis (LOPA) were undertaken and a Safety Requirements Specification (SRS) was produced to convey the basic requirements of each SIF.

The Wood personnel on the call were unable to confirm whether or not SIF validation testing had been undertaken for each SIF, and although it is acknowledged by all parties that commissioning tests have been undertaken, the extent and rigour of testing is not known and was not demonstrated by NEML. SIF validation testing is a key requirement of standard IEC 61511. The purpose of the testing is to prove that the SIF functions as designed, including in fault conditions.

The inability to demonstrate SIF validation testing has taken place is in contravention to the requirements of IEC 61511 and can be considered a non-conformance with the IEC standard.

4.4.1 System Implementation

A discussion with the ESD system programmer was arranged and questions asked based around the contents of the detailed question set. The main findings of this were as follows:

1) For SIFs with analogue inputs, the SRS requires any signal outside of the 4-20mA measurement range to be classed as a demand on the ESD system. The ESD system in fact treats signals between 3.5mA and 20.5mA as measurement signals.

This is in direct contravention to the SRS and the ICSS Design Specification and can be classed as a minor non-conformance with good oilfield practice.

However, the purpose of this arrangement is to distinguish between what is a correctly functioning signal and what is a fault signal from a smart sensor which is furnished with internal diagnostic capability, therefore it is
suggested that guidance such as NAMUR NE43 is implemented. This would enhance the ESD system functionality and maximises the use of diagnostic information for the benefit of the control room operator and maintenance personnel. This finding also suggests that any SIF validation testing undertaken was insufficiently rigorous.

Demands on the ESD system are investigated as part of the Five Whys process, however the trip frequencies are not being gathered and analysed. Standard IEC 61511 distinguishes between real demands and spurious demands; the latter being those demands which are due to a fault and not due to a potentially hazardous process condition.

One purpose of investigating a demand is that valuable information about the performance of the ESD system is made available to the platform management which may otherwise not be available, given that a demand on a SIF can be considered to be infrequent (theoretically less than once per year to comply with the IEC standard). Credit may be taken for a correctly functioning SIF in lieu of a planned periodic verification proof test.

A second purpose of investigating a demand is that the design demand assumptions can be validated. Standard IEC 61511 has three categories of demand: continuous, high (>1/year) and low (≤1/year). The platform has been designed on the low demand category. If a SIF is demanded more than once per year then it may require re-categorisation as a high demand SIF. The effect of such a re-categorisation can sometimes result in an increase in SIL.

Key settings which reduce the likelihood of a spurious demand, such as switch denounce settings and signal filters were not applied. Although these are specified in the SRS with a maximum set point and no minimum set point, they do have a purpose.

This finding can only be classified as an observation because the lack of application could be said to meet the requirements of the standard but not represent good oilfield practice.

A discussion with a control room operator was held during which the human-machine interface (HMI) was demonstrated. The operator demonstrated that he would be provided with sufficient information in the event of a demand on the ESD system to allow him to determine the cause. The operator also demonstrated how the ESD system health could be monitored from the HMI and how communications problems within the system would be brought to his attention. The operator confirmed that the number of alarms he sees on an hourly basis has vastly reduced since start-up; which is indicative that the platform processes are able to be adequately controlled.

A visual inspection of a remote input/output (RIO) panel was undertaken (see Figure 2: Internals of the Remote Input/Output Cabinet), facilitated by two platform instrumentation engineers. They described how the system worked from where signal cables enter the RIO, are communicated to an I/O card and how the I/O card is part of a fault tolerant communications ring which has redundant components.

4.4.2 Process Incidents

4.4.2.1 ESD on 11th February

There have been several communications problems which have occurred since platform operations began; some of which have been addressed and others not. In particular, the fault tolerant communications ring is known to have failed due to an Ethernet cable incident, which caused a demand on the ESD system. This led to the change out of Ethernet cables from Cat.5 to Cat.6, the latter having a greater data capacity. In addition, the termination of the cables has been strengthened and the bend radius increased; this appears to have had the effect of eliminating the problem. However, if rigorous SIF validation testing were to have been performed, then it is possible that unrevealed failures in the fault tolerant communications ring would have been revealed; as a single cable failure should not have caused a demand on the ESD system given that the systems are designed to be fault tolerant.
4.4.2.2 PSD on 18th May

A second incident involved a power cycle to guided wave radar instruments which were part of the process shutdown system. (LT-2184-1, 2 & 3 on the LSM Non-Process Open Drain sump – PSD on 18th May 2020).

Although the process shutdown (PSD) system is not part of the audit scope, the platform management team were unable to confirm whether or not similar instruments are part of the ESD and therefore it is considered relevant to the functional safety audit to discuss this event.

The investigation of this incident considers that an anomaly in the power supply is thought to have been the cause of the fault. Inspection of the RIO panel showed that it is common practice on the LPP for redundant I/O cards to be positioned adjacent to each other on the same rack. This is apparently a standard design feature from Allen Bradley.

Further, although the rack has two power supply connections, one at either end, they are understood to have come from the same power supply. Therefore, although there are redundancy arrangements, these redundancies are still susceptible to common cause failures, as demonstrated by this incident.
Although the common fibre-optic communications medium is mentioned in the ICSS design specification, it does not appear in the SIL verification calculations and is not fully described. There are a number of Ethernet to fibre-optic converters in the RIO cabinets and it is assumed that there are additional converters feeding into the safety shutdown system. This is effectively a subsystem and it is unclear whether such converters are trusted devices and thus meet standard IEC 61508. Standard IEC 61511 Clause 11 requires that:

- Devices selected for use as part of a SIS with a specified SIL shall be in accordance with IEC 61508-2:2010 and IEC 61508-3:2010 and/or 11.5.3 through 11.5.6, as appropriate, and
- Appropriate evidence shall be available that the devices are suitable for use in the SIS.

The audit team do not appear to be in possession of such evidence.

This finding can be classified as minor non-conformance with the IEC standard.

4.4.2.3 Further Information

Note: HART is an acronym for Hardware Addressable Remote Transducer protocol. Modern transducers can be programmed to respond with their identity, and have their characteristics altered via this protocol. This means the calibration, responses and nature of the measurements can be changed. Sometime this is implemented direct from the control room via a console, in the case of LPP this is done via a hand held unit which is physically connected to the transducer. The use of HART capability means that the configuration of the transducer could be changed from the design requirements leading to unpredictable outcomes if the process is not tightly controlled.
A further discussion was held with the two platform instrumentation engineers regarding HART capability and the use of a hand-held HART communicator with smart devices in the ESD system. The auditors’ concerns were that HART was being used to test the ESD sensors in lieu of physically simulating a demand. The auditors were assured that the HART capability is only used to check measurement spans, check diagnostic functions and for initial set-up.

However, the engineers confirmed that they do not usually set any HART write switches into the disable position. It is understood that operators cannot change ESD sensor settings, that such changes are controlled through the management of change process and that access to the hand held communicator is controlled and limited to key personnel.

This finding can only be classified as an observation because there is no evidence of non-compliance with the IEC standards.

4.4.2.4 Cyber Security

A discussion with the ESD system planner was held. Cyber security was discussed, amongst other topics such as analog input out of range signal treatment and HART functionality and usage. The programmer described some of the features which prevent the safety shutdown system from unauthorised changes, such as firewalls. However, there was no mention of a cyber-security risk assessment and although the subject is indirectly address in section 16 of the SRS and directly in the Automation basis of design, there is no evidence of a cyber-security risk assessment.

Indeed, the information provided in the Automation basis of design is ambiguous in that it claims compliance with National Cyber Security Alliance requirements, but does not reference any particular standard or document. Standard IEC 61511 clause 8 requires that a security risk assessment shall be carried out to identify the security vulnerabilities of the SIS.

The audit team do not appear to be in possession of evidence of a security risk assessment.

This finding can be classified as an opportunity for improvement.

4.5 Future Actions

It is understood that NEML has awarded a contract to a third party, DNV GL, to undertake a stage 3 functional safety assessment.

4.6 Summary

4.6.1 Requirements

The LPP design performance standards stated that the ESD system would be designed in accordance with IEC 61508. The associated process industry standard is IEC 61511 and it would be expected that LPP would comply with this element.

4.6.2 Current Status

The LPP design process incorporated Hazard and Operability (HAZOP) studies, Layer of Protection Analysis (LOPA) studies, Safety Integrity Level (SIL) Assignment and SIL Verification; as well as the creation of a Safety Requirements Specification (SRS).

It is not clear if BV verified compliance with IEC 61508 from the information currently available. Wood have stated that they did not undertake Functional Safety Assessments stages 1, 2 or 3, as required by the standard prior to operations commencing. A level of testing has been carried out during the commissioning process by an NEML contractor, but the level of compliance with IEC 61508 is not known.

NEML are understood to have contracted DNV GL to undertake a Stage 3 Functional Safety Assessment.
4.6.3 Functional Safety Key Findings

There is no evidence of direct compliance with IEC 61508, nor the associated process industry standard IEC 61511. This is a major conformance with NEML's design performance standards, overall it is classed as a minor non-conformance with good oilfield practice.

4.6.4 Functional Safety Key Recommendations

NEML should carry out a stage 3 functional safety assessment, which incorporates the necessary elements of stage 1 and stage 2 functional safety assessments, to ensure compliance with the design performance standard.

4.6.4.1 Suggested Solutions

Step 1: Ensure that the Functional Safety Management Plan incorporates all the requirements of the relevant functional safety standard.

Step 2: NEML should consider using suitable guidance (e.g. NAMUR 43) for settings on analog smart sensors such that fault conditions can be identified and conveyed to the control room operator.

Step 3: NEML should consider preparing a suitable Safety Instrumented Function (SIF) Validation Proof Test Procedure for each individual SIF which is under the control of the installation. The procedure should include all relevant requirements of the functional safety standard, including management of change and fault identification.

Step 4: Following successful completion of the stage 3 functional safety assessment, the future compliance methodology should be agreed upon between MoE and NEML.
5 OTHER MATTERS DURING THE AUDIT

The audit team was given several tours of the installation and inevitably a large number of topics were discussed with the audit monitoring team. This section captures these points, all should be treated as observations.

- **PSSR Procedure**
  - As an outcome conclusion from the IGV valve failure investigation, the interaction between the contractor and the operation team described within the handover procedure, should be reviewed and improved. Process control tuning parameters and key values should be reviewed and verified by both sides for the process integrated systems in an effective and thorough manner before the start up.

- **Process safety observations**
  - Process/venting/drainage manual ball valves from “Habonim” manufacturer should be checked both for stoppers mechanism availability and handle direction to reduce the risk of unwanted change of position (this should be completed within the period of 1 month).

- **Procedures were audited during the visit**
  - Isolation (LOTO) Produced for water pump PBA6095A was performed according to cold work permit and in compliance with *Tier 3 - Control Of Hazardous Energy Standard*. 
Appendix A
Outline Scope Of Audit

Leviathan Production Platform Audit – June 2020

Audit Intent: To assess the current Leviathan operations with respect to:

- Incident investigations
- Integration of Verification into operations
- Compliance with IEC61511.

These topics have been chosen due to levels of synergy between them and in response to ongoing LPP operational issues.

Audit Scope

Incident Investigations

This scope will include a review of the incident investigations carried out from start-up to present day. It is hoped to directly talk with a selection of persons who have been directly involved in the incident investigations on-board LPP, probably followed up by the onshore personnel involved in communication with the MoE.

The NEML procedures will be reviewed, the effectiveness of the investigations assessed and follow-up and closeout activities covered.

[Personnel to be interviewed to include: Management positions (PIC) and foremen; discipline specialists; also personnel who are on board who have been directly involved in any of the Five whys reporting. Shore based personnel as necessary.]

Integration of Verification into Operations

This scope will include a review of the current operational performance standards and their linkage to the design performance standards. The NEML procedures for undertaking verification activities, scheduling within the CMMS and demonstrating compliance with the performance standard will be assessed. Personnel knowledge of the verification process and requirements will be assessed – primarily for platform management positions. The ability of the CMMS to identify, schedule and report on performance standards and verification activities will be covered. This will likely require communication with CMMS co-ordinator/controllers, verification contract holders and platform management. The supporting NEML OMS documents will be included within the scope.

[Personnel to be interviewed to include: Management positions and foremen; CMMS co-ordinator/controllers verification (BV) contract holder i.e. person responsible for managing verification (BV) activities.]

Compliance with IEC61511

This scope covers the follow on activities from the PSSR activities which have been undertaken during commissioning. The NEML procedures for managing functional safety elements of their plant will be reviewed. This will include the level of integration of functional safety management into the CMMS and all maintenance and inspection planning. NEML procedures covering these aspects will be reviewed and the integration into performance standards and their reporting. As part of this scope there will be some review of functional safety issues to date and the progress / actions on resolving them.

[Personnel to be interviewed to include: Primarily instrument discipline technicians / supervisors; and CMMS coordinator / controller.]
Personnel

NEML Personnel

From the Audit Scope above it can be seen that LPP platform management positions will be interviewed. Discipline specialists such as LPP instrumentation technicians/supervisors will also be interviewed. Depending upon where the CMMS and verification activities are undertaken those personnel will also be interviewed (if necessary, by video). A selection of technical personnel on LPP will be interviewed to assess their understanding and knowledge of the incident investigation, verification and IEC61511 requirements.

MoE Personnel

The audit will be led by Pete Morris, supported by Nick Howard from RPS. They will respectively concentrate on the verification and IEC requirements. MoE personnel, Michael Belinsky and Avishai Karat will concentrate on the incident investigation aspects.

3rd June 2020
Appendix B
Audit Scope And Potential Interviewees

Leviathan Production Platform Audit – June 2020

Potential Interviewees

From the Audit Scope it can be seen that LPP platform management positions will be interviewed. Discipline specialists such as LPP instrumentation technicians/supervisors will also be interviewed.

Depending upon where the CMMS and verification activities are undertaken those personnel will also be interviewed (if necessary, by video).

A selection of technical personnel on LPP will be interviewed to assess their understanding and knowledge of the incident investigation, verification and IEC61511 requirements.

Below is a draft list of potential NEML and contractor personnel that could be interviewed. The final list will depend upon staff availability and whether the actual person in that post has had any experience of the topics covered by the audit.

Audit Scope

Incident Investigations

<table>
<thead>
<tr>
<th>Management positions (Person In Charge (PIC))</th>
</tr>
</thead>
<tbody>
<tr>
<td>Production Authority (Supervisor / Foreman?)</td>
</tr>
<tr>
<td>Foremen: Production Maintenance Control Electrical</td>
</tr>
<tr>
<td>Discipline specialists: Production Maintenance Control Electrical</td>
</tr>
<tr>
<td>Shore based personnel as necessary</td>
</tr>
<tr>
<td>Others as determined during audit</td>
</tr>
</tbody>
</table>

Details from Five Why's Investigations

<table>
<thead>
<tr>
<th>Technician (who filled out form)</th>
</tr>
</thead>
<tbody>
<tr>
<td>XXXX</td>
</tr>
</tbody>
</table>

Action Parties by Discipline

<table>
<thead>
<tr>
<th>CRO</th>
<th>LPP Chemist</th>
<th>Offshore Maintenance Team</th>
<th>Turbo Expander Commissioning Team</th>
</tr>
</thead>
<tbody>
<tr>
<td>I&amp;E</td>
<td>W-Ind Programmer</td>
<td>Production Foreman</td>
<td>Process Engineering Team</td>
</tr>
<tr>
<td>W-Ind</td>
<td>Offshore Operations</td>
<td>Operations</td>
<td>NEML Engineering Team</td>
</tr>
</tbody>
</table>

(Note: To be clarified: Disciplines are as listed on Five Why’s reports – could be different terms for same discipline (e.g. Offshore Operations & Operations; W-Ind & W-Ind Programmer).
Action Parties by Named Personnel/Companies

<table>
<thead>
<tr>
<th>Company/Person</th>
<th>Company/Person</th>
<th>Company/Person</th>
<th>Company/Person</th>
</tr>
</thead>
<tbody>
<tr>
<td>XXXX</td>
<td>XXXX</td>
<td>XXXX</td>
<td>XXXX</td>
</tr>
<tr>
<td>XXXX</td>
<td>XXXX</td>
<td>XXXX</td>
<td>XXXX</td>
</tr>
<tr>
<td>XXXX</td>
<td>XXXX</td>
<td>XXXX</td>
<td>XXXX</td>
</tr>
<tr>
<td>XXXX</td>
<td>XXXX</td>
<td>XXXX</td>
<td>XXXX</td>
</tr>
<tr>
<td>XXXX</td>
<td>XXXX</td>
<td>XXXX</td>
<td>XXXX</td>
</tr>
</tbody>
</table>

Supervisors

<table>
<thead>
<tr>
<th>Company/Person</th>
<th>Company/Person</th>
<th>Company/Person</th>
<th>Company/Person</th>
</tr>
</thead>
<tbody>
<tr>
<td>XXXX</td>
<td>XXXX</td>
<td>XXXX</td>
<td>XXXX</td>
</tr>
</tbody>
</table>

Integration of Verification into Operations

<table>
<thead>
<tr>
<th>Role</th>
<th>Production</th>
<th>Maintenance</th>
<th>Control</th>
<th>Electrical</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management positions (PIC)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Production Authority (Supervisor / Foreman?)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Foremen:</td>
<td>Production</td>
<td>Maintenance</td>
<td>Control</td>
<td>Electrical</td>
</tr>
<tr>
<td>Discipline specialists:</td>
<td>Production</td>
<td>Maintenance</td>
<td>Control</td>
<td>Electrical</td>
</tr>
<tr>
<td>CMMS co-ordinator/controllers</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Verification (BV) contract holder i.e. person responsible for managing verification (BV) activities</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Compliance with IEC61511

<table>
<thead>
<tr>
<th>Role</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Primarily instrument discipline supervisors;</td>
<td></td>
</tr>
<tr>
<td>Instrument discipline technicians</td>
<td></td>
</tr>
<tr>
<td>CMMS coordinator / controller</td>
<td></td>
</tr>
</tbody>
</table>

17th June 2020
**Appendix C**

**Initial Question Set For Interviewees**

<table>
<thead>
<tr>
<th>Table 1</th>
<th>Verification</th>
</tr>
</thead>
</table>
| **What is the Purpose of the Audit(s)** | To assess the current Leviathan operations with respect to:  
  - Incident investigations  
  - **Integration of Verification into operations**  
  - Compliance with IEC61511  
  
  These topics have been chosen due to levels of synergy between them and in response to ongoing LPP operational issues. |
| **What is the Scope of the Audit** | **Integration of Verification into Operations**  
  
  This scope will include a review of the current operational performance standards and their linkage to the design performance standards.  
  
  The NEML procedures for undertaking verification activities, scheduling within the CMMS and demonstrating compliance with the performance standard will be assessed.  
  
  Personnel knowledge of the verification process and requirements will be assessed – primarily for platform management positions. The ability of the CMMS to identify, schedule and report on performance standards and verification activities will be covered.  
  
  The supporting NEML OMS documents will be included within the scope. |
| **Standards Applicable to Audit** | DNV-OSS-202 Verification for Compliance  
  UK HSE Guidance on verification – (website information). |
| **What specific operations and procedures/processes will we focus on** | How NEML has structured their maintenance and inspection activities to align with the verification process.  
  How NEML will schedule assurance and verification tasks.  
  How NEML will monitor the status of their SCEs. |
| **Initial Information Required** | OMS, NEML Performance Standards, Safety in Design report for Leviathan, safety critical maintenance routines. |
| **Personnel we will require access to** | This will likely require communication with CMMS co-ordinator/controllers, verification contract holders, platform management and the relevant maintenance technicians. |
| **Pre-planned topics and questions** | Team Composition |
### Table 2  Incident Investigation

<table>
<thead>
<tr>
<th>What is the Purpose of the Audit(s)</th>
<th>To assess the current Leviathan operations with respect to:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Incident investigations</td>
</tr>
<tr>
<td></td>
<td>• Integration of Verification into operations</td>
</tr>
<tr>
<td></td>
<td>• Compliance with IEC61511</td>
</tr>
</tbody>
</table>

These topics have been chosen due to levels of synergy between them and in response to ongoing LPP operational issues.

<table>
<thead>
<tr>
<th>What is the Scope of the Audit</th>
<th>Incident Investigations</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>This scope will include a review of the incident investigations carried out from start-up to present day. It is hoped to directly talk with a selection of persons who have been directly involved in the incident investigations on-board LPP, probably followed up by the onshore personnel involved in communication with the MoE.</td>
</tr>
<tr>
<td></td>
<td>The NEML procedures will be reviewed, the effectiveness of the investigations assessed and follow-up and closeout activities covered.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Team Composition</th>
<th>Standards Applicable to Audit</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>NEML’s Incident investigation processes within OMS guidance on incident investigation.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>What specific operations and procedures/processes will we focus on</th>
<th>How NEML has adhered to the OMS procedures for the recent incidents.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>How NEML has assured themselves of the completeness and competence of the incident investigation reports.</td>
</tr>
<tr>
<td></td>
<td>How NEML will monitor the status of their recommendations and assess their effectiveness.</td>
</tr>
</tbody>
</table>

| Initial Information Required | OMS, Recent Five Why’s investigation reports. Supplementary investigation reports. Recommendation close out and MoC if found necessary. (What is NEML’s Process Safety Event Standard?) |

| Personnel we will require access to | Management positions (PIC) and foremen; discipline specialists; also personnel who are on board who have been directly involved in any of the Five whys reporting. Shore based personnel as necessary. |

<table>
<thead>
<tr>
<th>Pre-planned topics and questions</th>
<th>Have you had any formal training in incident investigation processes?</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Incident investigation – Can you describe to me how you would set up an incident investigation?</td>
</tr>
<tr>
<td></td>
<td>Are you aware of how the severity of incidents is assessed?</td>
</tr>
<tr>
<td></td>
<td>How can you tell if any particular incident is a major accident event (MAE)?</td>
</tr>
<tr>
<td></td>
<td>Are there any NEML documents which describe how investigation processes will be carried out?</td>
</tr>
</tbody>
</table>
What is your understanding of the reporting requirements in the event that an incident occurs?

What is the process for agreeing the report?

Have you been involved in an incident investigation?

Where are you on the competency assurance chart?

Have you been involved in the investigations?

Which incident(s)?

In your own words can you describe what happened from incident to report sign off?

What happens with actions from an incident report? How are learnings from incident investigations disseminated to the workforce?

Do any of these actions start off the MoC process?
### Functional Safety

#### What is the Purpose of the Audit(s)
To assess the current Leviathan operations with respect to:
- Incident investigations
- Integration of Verification into operations
- Compliance with IEC61511

These topics have been chosen due to levels of synergy between them and in response to ongoing LPP operational issues.

#### What is the Scope of the Audit
**Integration of IEC61511 into operations**

This scope will include a review of the current situation with safety instrumented functions and their compliance with the IEC standard 61511 and the related requirements of IEC 61508.

The NEML procedures and processes for undertaking functional verification activities (Functional safety management procedure), scheduling within the CMMS and demonstrating compliance with the standard will be assessed.

Personnel knowledge of the IEC process and requirements will be assessed – primarily for platform management positions. The ability of the CMMS to identify, schedule and report on performance will be covered as will overall compliance with the IEC 61511 lifecycle (Figure 7 of the standard).

The supporting NEML OMS documents will be included within the scope.

### Team Composition

<table>
<thead>
<tr>
<th>Standards Applicable to Audit</th>
<th>IEC 61511 and linkages to NEML’s verification processes. Industry guidance on IEC 61511 processes.</th>
</tr>
</thead>
<tbody>
<tr>
<td>What specific operations and procedures/processes will we focus on</td>
<td>How NEML has structured their maintenance and inspection activities to align with the IEC process (including MoC). How NEML will schedule inspection and testing tasks? How NEML will monitor the status of their SIFs and compliance with the IEC standards?</td>
</tr>
<tr>
<td>Initial Information Required</td>
<td>OMS, NEML Performance Standards, Safety in Design report for Leviathan, HAZOP and LOPA reports, LPP Safety Requirements Specification document. Verification proof test procedures, SIF dossier/inventory, inspection and testing records, as well as competency records in relation to functional safety.</td>
</tr>
<tr>
<td>Personnel we will require access to</td>
<td>This will likely require communication with CMMS co-ordinator/controllers, platform management and the relevant maintenance technicians.</td>
</tr>
<tr>
<td>Pre-planned topics and questions</td>
<td>IEC 61511 – could you describe your understanding of the functional safety lifecycle? Are you aware of how safety instrumented functions (SIF) were identified?</td>
</tr>
</tbody>
</table>
How can you tell if any particular tag is a SIF?
What do you know about performance standards?

Are there any NEML documents which describe how the verification processes will be carried out?

What is your understanding of the availability element of each SIF?

What do you think might happen if an SIF does not meet its required safety integrity?

How are demands on a SIF investigated? (because each demand should be)

What processes are in place to manage a SIF which fails its verification proof test or fails to meet its safety requirements?