COMAH Competent Authority Follow up Report

ESTABLISHMENT DETAILS			
Name of Operator:	Exxon Mobil Chemical Limited (EMCL)		
Establishment Address:	Mossmorran (MM) site: Beverkae House Mossmorran Cowdenbeath Fife KY4 8EP Braefoot Bay (BB) site: Po Box 14 Braefoot Bay Aberdour Burntisland Fife KY3 0XR	**COIN Site Ref:**	MM: 1036032 BB: 1036087
		Case No:	MM: 4121602 BB: 4171550
		Service order No:	MM: SVC4345694 BB: SVC4345753

Summary:

Review of eight outstanding actions from MM inspection of 2014 and BB inspection of 2016.

In general there had been significant progress to deal with the issues raised.

Functional safety management procedures had been implemented, although there were still some omissions to resolve.

Improvements had also been made to the SIL assessments. However, there were some issues remaining with respect to demonstrating the effectiveness and independence of some protection layers, in particular low integrity functions such as alarm functions.

The assessment of installed SIS with respect to reliability had been addressed but with respect to fault tolerance and independence further work was required, especially where non-failsafe actuators were in use.

Some of the actions raised during assessment were also not sufficient to demonstrate ALARP – in general only replacement of SIF components to full company standards was being considered, whereas simpler more cost effective improvements had not been considered.

The overall approach, and template for maintenance, inspection and test was improved. Some further documentation is required to demonstrate closure of the actions.

Relevant documentation seen:

D1. Email from EMCL dated 01 Feb 2017 – 'EC&I Action Closeout' including attachments:

D2. Jan17 HSE Functional Safety Actions and Responses
D3. Jan17 Functional Safety Management Manual
D4. Jan17 New Company OIMS Approval Request Form (FSM proposal)
D5. Jan17 EDOP 06-18 - RA in Support of AT Determination.doc
D6. Jan17 Extract from Procedure EDOP 06-17 Periodic Verification of Control Measures
D7. Jan17 Demethaniser Availability Target - Updated 6-12-2016
D8. Jan17 Ethane Tank Availability Target - Revised 7-12-2016
D9. Jan17 Furnace Low Fuel Gas Pressure Availability Target - Updated 8-12-2016
D10. Jan17 Furnace Flame-Out due to Low FP Pressure - Event Tree.xlsm
D11. Jan17 Exemplar SRS Demethaniser Brittle Failure Protection
D12. Jan17 Exemplar SRS Ethane Tank Overfill Protection
D13. Jan17 Exemplar SRS K-P-117-LCOA Low Fuel Gas Pressure
D14. Jan17 Installed SIS Assessment including FSA - Demeth
D15. Jan17 Installed SIS Assessment including FSA - K-P-117-LCOA Low Fuel Gas Pressure
D16. Jan17 Instrument Proof Testing - Guiding Principles
D17. Jan17 Instrument Proof Testing - Appendix 4 (Test Data Feedback Form)
D18. Jan17 CH052COS Demeth
D19. Jan17 SL_074_HCOA S-TK-01
D20. Jan17 KP_17LCOA Low Furnance Fuel Gas Pressure Initiator Test
D21. Jan17 KH_08_S Low Furnace Fuel Gas Pressure Final Element Test
D22. Jan17 Ethylene Tank Availability Target 8-12-2016
D23. Jan17 C5 Plus Storage Tank Liquid Overfill Risk Assessment - 12-12-2016
D24. Jan17 B-TK-15 Overfill - Event Tree.xlsm
D25. Jan17 Ethylene Ship Excessive Movement Availability Target - Revised 9-12-2016
D26. Jan17 Exemplar SRS Ethylene Tank Overfill Protection.doc
D27. Jan17 Exemplar SRS C5 Plus Tank Overfill Protection.doc
D28. Jan17 Exemplar SRS Ethylene Ship Movement Protection.doc
D29. Jan17 Installed SIS Assessment including FSA - B-L-021-HCOA B-TK-01 Overfill Protection
D30. Jan17 Installed SIS Assessment including FSA - B-L-804-HA B-TK-15 Overfill Protection
D31. Jan17 Installed SIS Assessment including FSA - B-X-904-COA Ethylene Ship Loading
D32. Jan17 BL_021_HCOA B-TK-01
D33. Jan17 BL_804_HA B-TK-15
D34. Jan17 cptc0110 - Loading Arm Checks - Initiator.doc
D35. Jan17 cpbb0440 - Ship Loading Ethylene - Partial FE Test
D36. Jan17 PERC Full Function Test
D37. Jan17 HSE E I follow up actions - BB4 - Ex Equip withdrawn from service

Operator Performance Rating:						
Topic	Rating					
	10	20	30	40	50	60
Functional Safety				X		
Explosive Atmospheres	Not assessed					
Electrical Power Systems	Not assessed					

Report author: [redacted]

CA Organisation, Unit & Team: HID CEMHD 2E

Date of report: 10/08/2017 (1st Draft)
17/10/2017 (Final)

Location: Newcastle

Copies to: [redacted]

Discussion and Conclusions:

Background

1. EMCL have two COMAH establishments in Fife – MM primarily cracks ethane to ethylene; BB is a jetty / storage area supporting MM.

2. A functional safety visit was conducted at MM in 2014 including verification of a number of MM MAH scenarios. A follow up was completed in 2016 to review progress on the 2014 actions and to conduct verification of BB MAH scenarios.

3. Eight actions were raised at the 2014 inspect, with a further four raised at the 2016 inspection. Feedback on the 2014 action responses was also provided to EMCL at the 2016 inspection.

MM Action 1 – SIS Management

Part a – Review RGP

4. EMCL had previous conducted a 'gap assessment' to review the requirements of BS EN 61511 and determine where these requirements were covered by existing management systems (for the purpose of developing the FSM systems below).

5. This part was therefore complete.

Part b – Implement FSM Procedure

6. EMCL submitted a functional safety management (FSM) document. It was noted that this was largely based around the Fawley document but modified to make relevant to the local site.

7. The document was split into lifecycle phases, with reference to relevant tools, documentation and responsibilities.

8. Also provided was an updated form used for requesting approval of external companies.

9. With respect to the specific requirements of the action:
   i. Signposting – the FSM document included signposting to existing relevant procedures.
   ii. Responsibilities and competence – the FSM document included responsibilities for each phase, including third party vendors (e.g. for the design stage). However, this was largely limited to the new projects – for example for existing installed SIS (covered under FSA4), the responsibilities, inputs and outputs were not defined. An approval for external companies was shown to have a instrument engineer approval step. However, there was nothing that showed what the competence criteria were for both internal and external roles or how these would be assessed.
   iii. Gaps – the FSM document now included the relevant activities. However, there was confusion in some cases – for example FSA stages 1-3 were listed as a verification activities (although other valid verification was identified), validation (FAT) was identified as verification.
   iv. Indirect changes to SIS – the response made reference to the small project development checklist (not provided). Reference was made in the FSM document to corporate OIMS and GMOC standards. There was nothing provided that showed how indirect changes to the SIS would be identified.
   v. MOC Impact assessment - the response made reference to the small project development checklist (not provided). There was nothing provided that showed how an impact assessment would be completed (both for small or larger changes).
   vi. Legacy SIS – Reference was made to a procedure yet to be developed – this was therefore not yet completed. However, some examples of stage 4 FSAs were provided – see below.

Summary

10. There was evidence of significant progress with FSM systems being developed, but these were not yet sufficient, in particular:
    a. The competence criteria and how they are assessed for both internal and external roles was not demonstrated.
    b. There was confusion between verification, validation and assessment. EMCL should ensure that verification activities are defined to ensure that the relevant lifecycle outputs meet the defined lifecycle activity requirements.
    c. The action requirements for management of change (identifying indirect changes and, impact assessment) were not shown to have been addressed.
    d. Responsibilities and requirements for legacy (installed) SIS were not defined.

11. Ultimately, it will be the responsibility of EMCL to ensure appropriate management systems are in place – this could only be judged by their application. Once procedures are developed, they can be used by EMCL to capture requirements.

12. However, at the moment there are clearly some omissions compared to the requirements of the action, although it was noted that some of these omissions may simply be due to relevant document not being provided in the response, rather than those requirements not being implemented.

13. Therefore, action not completed.

MM Action 2 – Determining SIS Requirements

Part a – Procedure and Practice

14. An updated procedure was provided (EDOP 06-18). It was noted that this was now a formal EMCL document and referenced in the FSM document.

15. With regard to the requirements of this part of the action, the 2016 inspection noted that these were addressed in the document, but identified issues on the exemplars provided at that time.

16. As stated in 2016, it remains the responsibility of EMCL to ensure that procedures remain fit-for-purpose and compliance would be judged through their application – see review of exemplars below.

Part b – Exemplars

17. Updated risk assessment documents were provided.

MM Demethaniser AT

18. No significant comments were made on this assessment at the 2016 inspection and so this AT was not reviewed again.

MM Ethane Tank AT

19. There had been significant change since the comments made at the 2016 inspection:
    a. The consequence was now stated as CS-1. This was said to be based upon a PHAST model – although this was not provided in the document, nor was a document reference / version number provided.
    b. The SIF being assessed was now referenced by tag.
    c. The W-factor had been selected as W1 (0.001 per year). This included consideration of

i. Initiating events – control failure (0.1 assumed) and equipment failures (0.15 assumed), as well as general plant upsets (1-2 per year).

ii. Response to alarms – It was stated that there were in some cases several alarm responses. It had been assumed that the response to these alarms would be PFD=0.01 (i.e. alarm function on SIL 1/2 border!). This was not consistent with EMCLs own rules on assumptions made for alarm response.

iii. Notwithstanding these comments, the overall frequency assumed for the above was 2x0.01 – it was not possible to determine how EMCL had determined this from the figures quoted. The overall value was reasonable given that there was a control layer and an alarm layer within the BPCS – however these were not shown to be independent.

iv. Conditional modifiers – weather disperses cloud (CM=0.22) and ignition probability (CM=0.24) – the applicability of these was outside the scope of an EC&I inspection and was therefore taken as read.

d. Credit was taken for the P-factor on the basis of response to alarms. There was not sufficient demonstration that this was sufficiently independent in terms of operator response and final elements from the response to alarms credited within the W-factor.

e. Credit was taken for the F-factor on the basis of infrequent attendance. This was taken as read.

f. The result was AT=92% (SIL1, PFD=0.08)

20. In summary, some of the issues identified in 2016 were now addressed. However, it was still the case that credit was being taken for several alarm functions within the assessment without adequate justification, i.e.:

a. The alarm sensor, required response and output element was not defined for each initiating event identified and therefore was not shown to be an effective layer of protection. I.e. there was not clear line of sight between an initiating event and the risk reduction measures and their component parts.

b. The sensor, alarm function, alarm response and output element were not shown to be independent from the initiating event.

c. Too much credit (PFD=0.01) had been assumed for alarm functions.

21. The way the AT was being used was problematic. In particular, the W-factor contained conditional modifiers and the P-factor contained reference to alarms that would reduce the demand on the SIS (i.e. should be covered in the W-factor?). In some respects, it did not matter where the conditional modifiers and alarm responses are considered. However, it did mean that the actual assumed demand rate on the SIS was not clearly stated (see part d below)

22. Using the data provided, the residual risk would probably be around $4x10^{-5}$ per year (0.1x0.1x0.22x0.24x0.08). This suggested that the risk was not unlikely to be ALARP – a lower PFD SIL1 function might be reasonably practicable.

MM Furnace AT

23. The assessment provided was not using the AT tool but was instead based upon consideration of operational experience of a low pressure situation and described within an attached event tree.

24. Note – only the low pressure trip exemplar was provided – it was assumed that there would be other assessments for other scenarios (e.g. liquid carry over) but this assessment would be representative of those assessments.

25. It was assumed that the initiating event would be due to control failure (0.1 per year) since there was a BPCS pressure control loop.

26. Reference was made to a number of alarm functions (back calculating suggests that a PFD=0.1 was selected for operator response to alarms). This was not demonstrated as a effective layer of protection since the alarm response (and output elements) were not defined – i.e. how does this alarm prevent this scenario? Also, the alarm (including response and output elements) were not shown to be independent.

27. It had been assumed that likelihood of ignition and significant furnace damage was 0.1 and that persons were only present 0.25 of the time.

28. As a result, the SIL1 (AT=96.6%) SIF reduced the residual risk to $8x10^{-6}$ per year, below the EMCL risk criteria for this type of consequence (CS1 low) which was $1x10^{-5}$ per year.

Part c – Time-bound Plan for AT Review

29. The response indicated that the 40 SIL2 SIFs would be reviewed by mid 2018 and the remaining 200 SIL1 SIFs would be reviewed as part of the HAZOP schedule by end 2023.

30. This was insufficient detail as required by the action (and stated in the 2016 report) – EMCL should provide a breakdown of SIF numbers by plant unit or by year so that progress can be reviewed over time.

31. This part of the action therefore not completed.

Part d – SIS Performance

32. Clarification had been provided on this issue in the 2016 report, i.e. that this requirement was associated with demand rate monitoring to ensure that the actual demand rate did not exceed that which was assumed within the SIL assessment (AT determination).

33. The EMCL response made reference to an updated FEP procedure (EDOP 06-17) – an extract was provided. This set out requirements to periodically review the demand rate against that assumed in the risk assessment.

34. Whilst the requirement was now captured, it was not clear how this would be done because the example AT setting documents provided did not identify the demand on the SIS and therefore what would this be compared to? (the W-factor contains conditional modifiers also and therefore does not represent the demand on the SIS).

35. It is recommended that verification be completed at future site visits to determine if the requirements can be completed in reality.

36. It was noted that this procedure was not referenced in the Functional Safety Manual.

37. However, the requirements of this part of the action had been completed.

Summary

38. The definition of the procedure had significantly improved the quality of the exemplar SIL determination assessments and should ensure that these improvements are rolled out across site.

39. It was noted that EMCL had also produced retrospective SRS documents. These were not reviewed as generation of these was not actioned. It would not be necessary to generate SRS documents if existing documents provided sufficient information for the purpose on ongoing management of the SIS. However, it is agreed that moving to a common standard could be advantageous, especially where information is missing or in multiple formats.

40. However, there remained some common issues to resolve:
    a. There was not clear line of sight between the initiating events and the protective functions, e.g. which alarm functions address which initiating events when considering the W-factor.
    b. There were still issues of demonstrating effectiveness and independence of some protection layers – alarms in particular – because the sensor, operator response and output element were not

defined.

c. In some cases there was over-reliance on alarm functions which was not justified.

41. EMCL should update their procedures (e.g. EDOP 06-18) to ensure consistent future resolution of these issues before continuing with AT reviews.

42. The time-bound plan provided was not of sufficient detail.

43. Therefore, action not completed.

MM Action 3 – Achieving SIS Requirements

44. At the 2016 inspection, EMCL had proposed:

a. Completion of SILSolver calculations on complex loops by end July 2016.

b. Completion of PFD evaluations on loops without end-end testing by end July 2016.

c. Completion of HFT issues by end June 2018.

d. Completion of procedural updates associated with independence by end 2016. However, EMCL should note the comments above to address these concerns also.

e. Completion of revised Braefoot bay sampled assessments by end 2016. EMCL should also update the Mossorron sampled systems by this date.

f. Completion of all SIL2 loops by June 2018 and SIL1 loops during the HAZOP process (end 2023).

Part a – PFD calculation

45. The EMCL response stated that all 'complex SIFs' had now been re-calculated by SILSover.

46. With respect to the end-to-end testing issue EMCL had responded that all SIF sub-systems were tested.

Part b – HFT

47. The EMCL response stated that HFT would be checked as part of FSA4. The adequacy of this was sampled by reviewing the exemplars below.

Part c – Independence

48. The EMCL response made reference to the RA procedure EDOP 06-18. As stated in the 2016 report (Para 45) this action was targeted at situations where, for example, a control valve was used by both the SIS and the BPCS as a final element (e.g. the demethaniser SIF).

49. I.e. this requirement is one of assessment of the SIS design, i.e. achieved independence. Based upon what EMCL had already submitted, it is recommended that this check is completed as part of FSA4 – i.e. at the same time as the HFT check above.

Guidance – this check should ensure that the SIF is, in design, independent to other protection layers (as specified in the risk assessment) and if it is not (e.g. use of BPCS control valve) assess if there are functional safety issues that therefore need to be resolved - e.g. can the lack of independence have a detrimental effect upon functional safety achieved.

Part d – Exemplars

PFD Calculations

50. SRS documents were provided (showing PFD calc assessment):

a. The demethaniser SIF PFD had been calculated using the TMEE062 lookup method to give an AT=99.5% with a 3-monthly proof test interval.
b. The ethane tank SIF PFD – had been calculated using the TMEE062 lookup method to give an AT=92% with a 24-monthly proof test interval(it was noted that no partial test option was now available).
c. The furnace SIF PFD had been calculated using the TMEE062 lookup method to give an AT=96.8% with a 6-monthly proof test interval.

HFT Assessment

51. FSA4 documents were provided (showing HFT assessment) for the demethaniser and furnace low pressure SIFs but not for the ethane tank.

52. The FSA4 for the demethaniser SIF was sampled (SIL2, PFD=0.005) with respect to HFT. Note – BS EN 61511 requires a HFT=1 for SIL2 as long as the dominant failure mode is to the safe state but this can be reduced to HFT=0 if a prior use demonstration is made.

53. The FSA4 stated that the equipment had been in service for 20 years and therefore prior use applied – however this was not sufficient to make a prior use claim – there should be some assessment of the quality of the manufacturer, the performance in similar operating environment and the volume of operating experience. There was no indication that the assessor had even reviewed the operating and maintenance history of this type of device.

54. Also, the assessor had not confirmed that for these devices the dominant failure mode was to the safe state.

55. The FSA4 for the furnace low pressure SIF was sampled (SIL1, PFD=0.032) with respect to HFT. Note – BS EN 61511 requires a HFT=0 for SIL1 as long as the dominant failure is to the safe state.

56. The FSA4 simply stated that this was SIL1 SIF with a HFT=0 – the assessor had not confirmed that for these devices the dominant failure mode was to the safe state.

57. It was accepted that checking HFT during FSA4 was appropriate. However, EMCL need to demonstrate that they have made the appropriate considerations during assessment, i.e.
a. To confirm that the dominant failure mode is to the safe state (otherwise increase HFT by 1)
b. To include some assessment of the manufacturer quality, device performance in the operating conditions and volume of operating experience when making a 'prior-use' claim. Simply stating that the equipment had been in use for many years does not in itself cover this requirement.

58. EMCL should therefore review their approach to FSA4 to capture these requirements and capture within appropriate procedures / management systems.

Independence Assessment

59. No documentation was provided showing how achieved independence had been assessment – e.g. for the demethaniser SIF (control system valve) and ethane tank (shares level instruments with the alarm system and valves).

Part e – Plan for SIF Reviews

60. As above, the plan should be further broken down by unit / year so that progress can be reviewed.

Summary

61. The approach to PFD calculation was acceptable.

62. The approach to HFT assessment (i.e. assess during FSA4) was generally acceptable, although further

information needed to be included associated with dominant failure modes and prior-use claims.

63. Achieved independence was not being suitably assessed despite additional guidance being provided in the 2016 report.

64. The FSA4 template may require additional placeholders or instruction and guidance to ensure that suitable assessment of HFT and independence is completed.

65. Therefore, action not completed.

MM Action 4 – Operator Response SIS

Part a – Identify SIAFs

66. This part previously completed apart from capturing requirements within their management systems.

67. Note – 12 SIL1 SIAFs had been identified.

68. Requirements were included within procedure EDOP 06-18 for SIAFs. In particular it was noted that SIAFs would not normally by specified but where they were additional requirements were identified including reference to GPs, design and testing requirements, response definition, training and auditing requirements etc.

Part b – Managing SIAFs

69. Although the requirements were now defined, there was no information from EMCL that indicated if the 12 SIAFs had been assessed to determine if they could be automated, reduce their integrity or show that they met the reliability requirements.

70. This part of the action was therefore not completed.

Summary

71. Part b still outstanding.

72. Therefore, action not completed.

MM Action 5 – Uncertified Logic Solvers

73. This action was previously closed.

74. However, EMCL reported that the final upgrade had slipped from end 2017 to Feb 2018. Considering the timescales originally quoted where 2020, this small delay was not of major concern.

MM Action 6 – SIS Overrides

Part a – Enable Window

75. This part previously closed.

Part b – Normal Operational Overrides

76. Note – as described in the 2016 report, EMCL should review the overrides that are present during

normal operation to see if they can instead be configured as operating modes within the software so as not to 'water-down' the override monitoring.

77. An operating mode configuration would typically not display as a 'override' but would instead take some action to ensure that the hazard couldn't be present (e.g. forcing a safety valve closed for a route not in use).

78. No further response received – this part of the action remains outstanding.

Part c – Integrity of Mitigation Measures

79. EMCL made reference to procedure EDOP 06-18 which required that as part of the control of defeat procedure, a risk assessment would be completed. It was stated that the SIF integrity, independence of the mitigation measures and duration of the override should be considered at that time.

80. Furthermore, the procedure required that as part of the hazard and risk assessment process, general guidance mitigation measures were to be developed during the assessment process to be used as a basis by the control of defeat assessment team.

81. Examples of general guidance mitigation measures were noted in the exemplar risk assessments provided. Note – it was not possible to determine if these were appropriate mitigation measures but it was demonstrated that mitigation measures had been defined.

82. Remaining SIFs will be dealt with as part of ongoing review programme.

83. This part therefore complete.

84. However, it is recommended that on-site verification is completed at a future site visit to review the effectiveness of this system and the proposed mitigation measures.

Summary

85. Part a previously completed; part c now completed.

86. Part b still outstanding.

87. Therefore, action not completed.

MM Action 7 – SIS Maintenance, Inspection and Proof Testing

Part a – Coverage of Tests

88. An updated 'guiding principles' document was provided – this had now been made site specific.

89. Appendices 1, 2 and 3 were not provided and therefore it was not possible to review these.

90. With regard to part i (testing at the defined PTI), the procedure required testing against the identified TMEE062 performance standards (equivalent to PFD calculation). However – it would be better if this procedure also made reference to SILSolver where appropriate.

91. With regard to part ii (identification of dangerous failure modes) the document did include some general requirements. However, further detail was missing (in appendix 1?) to fully demonstrate this.

92. Therefore, although significant progress, this part was not yet demonstrated as completed.

Part b – SIS Inspection

93. The EMCL response stated that inspection was covered in the guiding principles – this was not the case – it may be in appendix 1 (not provided)?

94. Note – the 2016 inspection specifically identified that inspection / maintenance of TRICONEX SIS panels was deficient as filters were found to be missing.

95. Therefore, this part was not yet demonstrated as completed.

Part c – Preventing Inadvertent Operation

96. The guiding principles document set out requirements to fit security / anti-tamper devices to ¼ turn valves etc. that could cause a dangerous failure of the SIS.

97. This was to be checked during proof test – but since appendix 1 was not provided, it could not be verified that labelling / fastening checks had been satisfactorily defined.

98. Therefore, this part was not yet demonstrated as completed.

Part d – Update Sampled Proof Tests

99. Updated procedures were provided. These were based on a new template.

100. Note safety critical task analysis had been completed associated with these procedures – this was outside the scope of an EC&I inspection and therefore these documents were not reviewed.

101. Note that it was not possible to check the content of these procedures from a table-top exercise alone, and so the procedure were only reviewed with respect to previous comments made:

Demethaniser SIF

102. With respect to original comments made (2014) the procedure now included:
    a. Inspection (although this was reference to appendix 1 of the guiding principles which was not provided)
    b. Operating all valves
    c. Simulating the thermocouples using mv sources at the trip points.

Ethane Tank SIF

103. With respect to original comments made (2014) the procedure now included:
    a. Inspection (although this was reference to appendix 1 of the guiding principles which was not provided)
    b. No option for partial test

Furnace Low Pressure SIF

104. With respect to original comments made (2014) the procedure now included:
    a. Two procedures – one for inputs, one for outputs
    b. Inspection (although this was reference to appendix 1 of the guiding principles which was not provided)

Summary

105. Although it was not possible to verify the content of the exemplar procedures it was noted that they had been significantly updated to address the issues identified at the original inspection and written to a consistent standard.

106. It was not possible to verify the content of the inspection – i.e. did it include checks on labels / fastenings etc. However, there was reference to the guiding principles appendix 1 – this issue will therefore be dealt with by part b above.

107. This part of the action completed.

Part e – Plan for Proof Test Procedure Updates

108. As above, a more detailed breakdown of planned review / update was required.

109. This part not completed.

Summary

110. There had been significant progress on proof tests.

111. Whilst proof test procedures are generally subject to continuous improvement, the guiding principles document was a good basis for this and should allow consistent and suitable procedures to be developed over time.

112. It was not possible to close the action, largely because not all documents were provided – EMCL should review the comments above and respond in due course.

113. Significant progress but action not completed.

MM Action 8 – Furnace Standards

Part a – Gap Assessment

114. Previously completed and to be used as basis for part b.

Part b – Improvements

115. The EMCL response stated that this was due for completion by end 2017.

116. EMCL are reminded to address the points made at the 2016 inspection, in particular the functional safety requirements to prevent liquid carry over, low temperature, other failure modes etc.

Summary

117. Due end 2017 – action not completed.

BB Action 1 – Non-Failsafe SIF Subsystems

118. This action was concerned with the identification (part a) and assessing the design adequacy / identify improvements (part b) of SIF subsystems that were not fail-safe.

119. The EMCL response stated that this would be addressed by the FSA4 review programme. This would be an adequate way to address this action.

120. The BB ethylene tank overfill SIF was reviewed with respect to the non-failsafe electrical MOV:
    a. The FSA identified that the SIF was not failsafe.
    b. Under GP 15-09-02, item 8.13 it was confirmed that power loss was detected.
    c. However, there was no check to confirm supplemental supply present or loss of circuit integrity (if the tripping circuit also not failsafe).
    d. It was also noted that the FSA did not identify that the HFT was not acceptable (on the basis of being non-failsafe)

121. The BB PERC SIF was reviewed with respect to the non-failsafe hydraulic MOV and release coupling:
    a. The FSA identified that the SIF was not failsafe.
    b. The FSA noted that loss of power / supply was not detected.
    c. There was no check to confirm supplemental supply present (e.g. hydraulic accumulator)
    d. It was also noted that the FSA did not identify that the HFT was not acceptable (on the basis of being non-failsafe).

122. In both cases, EMCL had identified actions to consider if replacement with 'GP compliant' components was reasonably practicable.

123. Whilst, replacement would be worth considering if reasonably practicable, this is not sufficient – if the failsafe components were to remain, it would be necessary to consider supplemental power, fault and power loss detection as indicated in the original action.

124. EMCL should also note that at present, the SIFs are likely to be limited to PFD≥0.1 without the supplemental power / fault detection – this should be the basis for any CBA.

125. The FSA process did not really pick up some of the key issues – there were no placeholders within the document to address issues of HFT, non-safe etc. and therefore it was not demonstrated that this would be addressed as part of future FSAs. It is recommended that EMCL update the FSA template to ensure that this specific issues are assessed and provide guidance on how they should be assessed.

Summary

126. Addressing these issues during FSA4 was appropriate. However, the FSA4 template was not sufficiently detailed to identify and assess the issues.

127. Furthermore, the actions raised in response to non-compliances were not adequate in that they only proposed replacement with compliant equipment and did not consider other more reasonably practicable options.

128. Action not completed

BB Action 2 – Low Integrity Instrumented Safety Functions

Part a – Identify

129. EMCL procedure EDOP 06-18 was provided – this set out requirements for identification of low integrity BPCS / alarm functions within the risk assessment.

130. As discussed above with respect to the exemplar risk assessments:
    a. There was not clear line-of-sight between the initiating events and the protection layers
    b. And it was not always demonstrated that the protection layers were sufficiently independent from each other and the initiating events.

131. This indicated that the requirements in the procedure were not sufficient. These should be improved to address these issues.

Part b – Manage

132. Where low integrity functions are claimed within a risk assessment, then they must by adequately managed – i.e. specified, tested, auditable etc.

133. Review of the exemplars showed the full safety function (sensor(s) through to final element(s)) was not specified.

134. Furthermore, there was no information within the risk assessment (or elsewhere) that indicated if the functions that were credited were appropriately specified, designed, maintained etc. (refer to OG46 for full requirements).

135. Again, this shows that the requirements in the procedure were not sufficient.

Part c – Plan for review

136. The response stated that this issue would be addressed during the SIF review process.

137. As above, the plan should be further broken down by unit / year so that progress can be reviewed.

Summary

138. EMCL had added some useful guidance in their procedure. However, this did not go far enough to ensure that suitable consideration was given during the risk assessment phase of the adequacy of these risk reduction measures (and that this was documented).

139. Action not completed

BB Action 3 – Braefoot Bay Sampled Systems

140. Updated documents associated with the three exemplars were provided. Note that it was only possible to review these against the issues identified at the 2016 inspection, i.e. without on-site knowledge of the scenarios and equipment a full review could not be conducted.

141. Each exemplar was reviewed against the requirements of the action:

Ethylene Storage Tank Overfill SIF

Part a.i. – SIL Determination

142. A revised SIL determination was provided.

143. The consequence was selected as CS-2 based upon PHAST modelling (not included and no document reference included in the assessment?). This was outside the scope of an EC&I inspection and therefore taken as read.

144. W factor was chosen as W1 on the basis of:
    a. An overall factor of 0.02 was selected on the basis of failure to operator to monitor tank level. The basis of this was EMCL human error probability tool.
    b. Conditional modifiers for weather / dispersion (0.22) and likelihood of ignition (0.24). The acceptability of these was outside the scope of an EC&I inspection and therefore taken as read.

c. This gave an overall frequency of 0.001, equivalent to W1.

145. The assessment did not clearly specify how the operator monitored the level, but it was likely that this was via the BPCS level instrument (this may be based of the SIF sensors? See discussion on independence below in part a.iii.) – failure of this would be limited to around 0.1 per year and therefore would be dominant of the operator failing probability selected above.

146. It was noted that the assessment no longer took credit for the un-maintained temperature sensors.

147. P factor was chosen as P1 on the basis of:
   a. Reference to high level alarms (B-L-013/14HA). However, the assessment stated that these were not independent and therefore this was not a valid protection layer to be considered within this type of assessment.
   b. Note there was also reference to a high pressure DCS alarm which was independent and could have been used to justify the P1 claim.
   c. The assessment stated that there were independent valves for shutoff in the event of an alarm but did not confirm that the defined response to the alarm was to close the relevant valves. Therefore the protection layer was not shown to be effective.

148. F factor was chosen as F1 on the basis of infrequent access to the tanks.

149. The result was AT=96.8% (SIL1, PFD=0.032)

150. If the initiating event was instead considered to be BPCS failure then residual risk would be (0.1x0.1x0.032x0.22x0.24) $1.7x10^{-5}$ per year. It therefore may be reasonably practicable to consider a lower PFD for the SIF.

151. Whilst there were some issues of demonstrating the effectiveness and independence in the assessment, in my opinion, these would be unlikely to change the outcome significantly.

152. However, these issue do indicate some fundamental issues with the EMCL assessment process that might be significant on other assessments.

Part a.ii. – PFD Calculations

153. A SRS and FSA4 document was provided. In the SRS section 2.2 the text on a logic drawing indicated that the PFD had been achieved by reference to the EMCL lookup process based upon the least reliable part, in this case the final element MOVs. This was acceptable.

Part a.iii. – HFT / Independence

154. In the SRS document it was noted that HFT=0 was achieved (limited by the 2oo2 valve arrangement).

155. The FSA4 documentation did not explicitly state that HFT was not met (because non fail safe), although it did identify that the output elements were not failsafe.

156. As discussed for BB action 1 above the FSA4 did not clearly consider if the requirements for supplemental power, line and power monitoring were included. And, as above, the resulting action only considered replacing the MOV, not providing these other functions.

157. With respect to achieved independence – there was a potential issue – i.e. that the level instrument used for normal level monitoring may also be one of the three used for the SIF. In reality, the fact that there are three sensors (2oo3 for the SIF and 1oo3 for indication) would be sufficient since it would be easy to imagine that even if one sensor was reconfigured to be for indication only, the remaining two (1oo2) would still be sufficient for the SIF.

158. However – it would have been expected that the lack of physical independence would have been picked up in the FSA4 and justified in a similar way to discussed above.

159. There is currently nothing in the FSA4 template / instruction that indicated that this should be considered at FSA4.

Part a.iv. – SIAF Assessment

160. Not applicable in this case.

Part a.v. – Maintenance, Inspection and Proof Test

161. An updated procedure was provided. With respect to the comments made at the original inspection:
   a. The procedure included inspection requirements.
   b. All three sensors were tested around their trip points.
   c. The MOVs were confirmed as closed by checking their position indicators and travel times were confirmed (the SRS stated that tight shutoff not required but leakage was to be checked at shutdown).

C5+ Tank Overfill SIF

Part a.i. – SIL Determination

162. A SIL determination was provided as a fault tree analysis based upon the following:
   a. Initiating event assumed to be a failure to monitor tank level (frequency of 0.025 per year assumed). Since the monitoring was based upon a level instrument this should have been limited to 0.1 per year.
   b. It was assumed that 90% of the time the overfill would not cause the tank to overfill but instead travel back through the vapour line. The basis for this was not justified and should have at least been considered as part of a sensitivity analysis.
   c. Response to bund gas detectors – PFD=0.1 assumed. The response was stated as to stop the transfer pump. There were clearly some potential common cause failures with the HLA here that were not addressed in the assessment (same operator?). The assessment noted that some parts of this function were currently not tested and raised actions to address this.
   d. Likelihood of ignition (0.04) – taken as read as outside the scope of an EC&I inspection.

163. The assessment concluded that the integrity requirements for the SIAF were AT=89% (non SIL, PFD>0.1) to reach a corporate risk target of $1x10^{-5}$ per year.

164. It was also understood at the inspection that the high level alarm was also a BPCS function and therefore not independent to the actual initiating event.

165. Note – if the initiating event was considered to be level instrument failure (BPCS) and the credit for the vapour balance line was removed, then the requirement would be AT=97.5% (SIL1 PFD=0.025).

Part a.ii. – PFD Calculations

166. An achieved PFD calculation was currently not necessary as the function was not SIL rated (the provided SRS and FSA4 was therefore not reviewed).

167. This would change if the function became SIL rated.

Part a.iii. – HFT / Independence

168. An achieved HFT / independence assessment was currently not necessary as the function was not SIL rated (the provided SRS and FSA4 was therefore not reviewed).

169. This would change if the function became SIL rated.

Part a.iv. – SIAF Assessment

170. This function was not SIL rated and therefore not a SIAF.

171. However, it was to become SIL rated, it would need to be assessed. The risk assessment did include a review of the alarm function. It did not consider if automation would be reasonably practicable (note that automation would also deal with the potential independence issue).

172. It might, for example, be relatively simple to cause the high level alarm to trip the transfer pump or close the inlet valve – this option should be considered if the requirements become SIL rated.

Part a.v. – Maintenance, Inspection and Proof Test

173. A function test procedure was provided. This was adequate for a non SIL system.

Ship Movement SIF

Part a.i. – SIL Determination

174. A revised assessment was provided which included a fault tree.

175. The contents of the assessment were outside the scope of an EC&I inspection but were sufficient to define the SIF integrity requirements for the PERC at AT=98.9% (SIL1 PFD=0.011)

Part a.ii. – PFD Calculations

176. The SRS included a PFD calculation which required input check monthly, a partial final element test every 3 days (as part of ship loading checks) and a full final element check every year.

Part a.iii. – HFT / Independence

177. In the SRS document it was noted that HFT=0 was achieved.

178. The FSA4 documentation did not explicitly state that HFT was not met (because non fail safe), although it did identify that the output elements were not failsafe.

179. As discussed for BB action 1 above the FSA4 did not clearly consider if the requirements for supplemental hydraulic power, line and power (pressure) monitoring were included. And, as above, the resulting action only considered replacing the PERC actuator, not providing these other functions.

180. Note – it is unlikely that a failsafe PERC would be available, but it might be possible to include a hydraulic accumulator (already exists?) and hydraulic failure monitoring so as to provide fault tolerance.

181. There was nothing in the FSA4 to indicate if independence issues had been considered (in this case there probably aren't any). There is currently nothing in the FSA4 template / instruction that indicated that this should be considered at FSA4.

Part a.iv. – SIAF Assessment

182. Not applicable.

Part a.v. – Maintenance, Inspection and Proof Test

183. Note, it was not possible to assess the adequacy of the procedures without detailed knowledge of the PERC and associated equipment.

184. However, compared to the comments made at the 2016 inspection:

a. A test of the initiators was provided.
b. A full disconnect test of the PERC was provided.
c. However, there was still no test of the hydraulic accumulator (if provided?)

Summary

185. The revised documents showed significant progress in all areas. However, there were some remaining issues (similar to as above for the MM scenarios).
   a. Initiating events associated with operator monitoring did not always consider the likelihood of the BPCS failure.
   b. The demonstration of effectiveness and independence of protection layers (particular alarm functions) during AT setting remained inadequate.
   c. The assessment of achieved HFT and achieved independence (during FSA4) was not sufficient.
   d. The actions raised during FSA4 were not sufficient to demonstrate ALARP with respect to non-failsafe components.
   e. Assessment of SIAFs did not first consider if automation was reasonably practicable.

186. In order to close this action, EMCL should review the remaining issues identified above for each exemplar.

187. EMCL should also update their management system procedures to ensure that these issues are addressed in future risk assessments, SIS reviews and documentation etc.

188. Action not completed

BB Action 4 – EX Equipment Withdrawn from Service

Part a – Procedures

189. The EMCL response stated that four procedures had either been updated or created to address the requirements of the actions. These procedures were said to be in review stage prior to being approved.

190. However, these four procedures were not provided (as required in the action), or any reference made to standards followed and therefore it could not be verified that suitable procedures were adopted (i.e. compared to BS EN 60079-17 clause 4.6.3).

191. This part of the action was therefore not completed.

Part b – Instruction and Training

192. The EMCL response stated that the procedures, once issued, would be shared via Supervisors via toolbox talks and field visits to instruct relevant personnel on the required site standards. EMCL noted that relevant Technicians are already COMPEX trained.

193. This would be an appropriate approach. Due to be completed in Feb 2017.

Part c – Survey

194. The EMCL response stated that a survey had been completed at each location and examples provided of non-compliances along with actions to complete.

195. Photos were also provided showing how the example identified during the inspection had been correctly terminated in a certified junction box.

196. This part of the action completed.

Summary

197. Proposals adequate but waiting for procedures to be issued to closed out the action.

198. Action not completed.