5.4.1 Verification activities for initial suitability of SCEs in design projects

The verification activities in the design phase for SCEs usually comprises one or more of the following generic activities to assess whether they are initially suitable:

- Design deliverables examination (e.g. MAH identification, correct SCE chosen that meets required risk criterion (e.g. ALARP), calculations, PS has appropriate FARSI criteria traceable to design deliverables, records, and changes to design).
- Review of QA/quality control (QC) plans.
- Visual physical examination of equipment procured vs. a procurement register, fabrications, construction.
- Witness and/or review of factory acceptance tests. There may be an efficiency opportunity to accept CE marking for specific European directives in lieu of some testing (e.g. for pressurised systems or ignition protected equipment) providing that the testing body and tests meet suitable criteria.
- Review records of construction (e.g. material certification, welding, non-destructive testing (NDT), pressure testing, etc).
- Examine and witness hook-up, installation and commissioning at site.
- Verification during start-up.

For offshore E&P facilities, some verification methods would be carried out onshore (e.g. at the location of fabrication), whereas other methods would be implemented offshore once the SCE is *in situ*.

Design documentation should be divided into logical packages per SCE, in consultation with the verifier and a schedule for submission/examination should be established. This should allow the progress of the verification scheme, with regard to the different SCEs, to be easily established.

The verifier should not repeat the work of the designer – the intent is to review a sample of design documentation to get confidence that the design will deliver suitable SCEs with appropriate PSs, that will meet the defined risk criterion (e.g. ALARP).

The verifier should be given the opportunity to review and comment on the design early enough to be able to influence any changes necessary to ensure SCE suitability. Subsequent verification should be carried out through construction to start-up. Conducting it in stages should avoid anomalies only being raised after installation, e.g. where there is a deviation in procurement that could have been identified and rectified before installation and commissioning. The verification activities should be integrated within the operating company's project planning system.

Start-up marks a transition from initial suitability of SCEs to ongoing suitability when bringing the new or modified facility into use. This transition may bring about a change of MAHs and risks, and some SCEs may require to be fully functional (and verified) sooner than others. In consultation with the verifier, the operating company should define the required verification for this transition in a documented process that covers each stage of the start-up process. In any case, before commencement of operations, the verifier should have confidence that each SCE meets its PS.

5.4.2 Verification activities for ongoing suitability of SCEs in operate phase

The verification methods for SCEs in the operate phase usually comprise one or more of the following generic activities to assess whether they are suitable:

- Review assurance records, so as to assess the robustness of assurance processes, including whether:
  - assurance activities are carried out on time and as documented in the PS;
  - the required SCE performance (e.g. reliability) is achieved;
  - defined assurance activities will reveal foreseeable failure modes, so that preventative action or repair may be carried out;
  - the frequency of assurance will reveal failures before items of equipment degrade leading to failure, having considered the historical failure rate for those items of equipment and the risk resulting from failure, having considered the level of redundancy.
- Witness and review critical function tests. There may be an efficiency opportunity to accept vessel classification society tests for mobile offshore E&P facilities (e.g. for firewater pumps on a floating production, storage and offloading (FPSO) installation), providing that the vessel classification society tests meet the required criteria.
- Visual physical 'as found' examination of SCE hardware condition vs. that stated in maintenance management system records.
- Review MoC outputs that identify the impact of change on existing SCEs for each modification and that identify any new SCEs resulting from the changes to MAHs.
- Review proposed major repairs (e.g. specification, materials, etc.) to reinstate the SCEs.
- Reassess SCE suitability after major repairs to SCEs.
- Review procedures used to defer assurance.
- Review and comment on the processes for managing impaired SCEs, including ORAs. This should consider:
  - The risks associated with failure of the impaired SCE.
  - Whether MAH safety risks continue to meet a defined risk criterion (e.g. ALARP), until the deficiencies with the impaired SCEs have been rectified, including use of temporary risk reduction measures proposed for implementation.

The scope of these verification activities includes normal operations as well as verification related to changes.

These verification activities may be carried out at different frequencies for different SCEs, and for different items of equipment or components that comprise an SCE system. Verification on each SCE does not necessarily need to be carried out annually or every time the operating company carries out an assurance activity on an SCE – the key is for the verifier to get confidence that the operating company has defined SCEs that are suitable initially and on an ongoing basis. 5.5 provides guidance on verification frequency and 5.6 refers to determining the verification sample size.

Verification of ongoing suitability should commence following start-up.

5.4.3 Verification activities for change

The extent of verifier engagement in the MoC process should depend on the complexity of the change regarding MAHs and SCEs. Verifiers should ensure that modifications are

correctly selected, developed and implemented, which requires their engagement in several stages. See 2.9.

5.5 VERIFICATION ACTIVITY FREQUENCY

The frequency of verification activities may vary for different methods of verification. Some verification activities for initial suitability may only be carried out once (e.g. a factory acceptance test), whereas those for ongoing suitability should be repeated periodically to determine ongoing suitability. Verification activities for initial suitability may need to be repeated if there is a change to the pertinent SCE (e.g. project work).

Where carried out more than once, the frequency of verification activities should depend on factors such as:

- The overall risks of the facility's operation (e.g. ranging from a relatively simple operation with a few well known MAHs, through to one with a complex and innovative design that has numerous MAHs with a high consequence of failure).
- The extent and frequency of the operating company's inspection and maintenance of different SCEs, which in turn should depend on:
  - requirements of good practice (e.g. technical publications such as codes, standards and industry good practice);
  - original equipment manufacturer recommendations.
- The relative risk associated with failure of each SCE on MAH risks.
- The findings of previous verification activities.
- The confidence in the operating company's assurance processes (e.g. whether there have been many failures/non-compliances).

For example, PSVs are usually tested at intervals depending on the requirements of specifications/standards (e.g. API 510 or API RP 576), past performance and risk associated with non-operation of the PSV. Typically, there are numerous PSVs meaning that sufficient verifier confidence can be gained that tests are being carried out correctly, and that inspection records reflect tests done, and by witnessing only some tests. The operational part of the verification scheme for PSVs could comprise a combination of activities, such as:

- witness the minimum of [value]% PSVs and [value]% of all PSV lift tests each year including, if there are any, some that failed their previous test;
- review PSV deferred maintenance assessment for minimum of [value]% PSVs and [value]% of total deferments, and
- [value] year review of the assessment of PSV reliability.

Note: [value] implies a pertinent number. These values are not necessarily equal.

5.6 VERIFICATION SAMPLE SIZES

The verification sample size should be determined by SCE criticality (see Annex H) and number of SCEs. The objective should be to assess confidence in the operating company's assurance process. Therefore, each SCE or item of equipment that forms part of an SCE system does not have to be verified annually, or every time an operating company carries out maintenance or repair on it.

For SCEs with several similar, or even identical, components in a system, e.g. gas detectors, PSVs and emergency lighting, the operating company's assurance processes should cover all these items on a regular basis, whereas verification need only be carried out on a sample of items at an appropriate frequency to give confidence that the PS criteria are being met, e.g. for emergency lighting and, with operating company assurance in mind, EI *Guidelines for managing inspection of Ex electrical equipment ignition risk in support of IEC 60079-17* provides a sampling method than enables statistical confidence to be gained regarding the Ex integrity of a defined lot of Ex rated equipment. A similar approach could be applied to verification of a defined lot of Ex rated equipment. If sampling is used, those items of equipment for verification should be selected randomly, so that there is no bias (e.g. only selecting low level luminaries that are convenient to access but omitting those at high elevations).

A similar sampling approach may be applied to an F&G detection system, which may have several hundred gas detectors. A target sample of critical function tests to be witnessed in verification may be defined as only some need to operate to meet a typical PS; but the key is to assess confidence in the operating company's assurance process. Verifier witnessing of critical function tests should be supported by review of relevant maintenance records for the complete system.

The allocation between witnessing and review of relevant maintenance records should vary for different SCEs and may be determined by whether they are systems with multiple items of equipment and redundancy (e.g. F&G detection system) or SCEs that comprise a single item of equipment (e.g. a blast wall).

A high integrity pressure protection system (HIPPS), preventing the over-pressurisation of a hydrocarbon containment system, may require 100 % witnessing by the verifier.

5.7 CRITICAL FUNCTION TESTS

As noted in 2.7, SCEs are either active or passive.

Where SCEs have an active requirement and are required to initiate an action on demand (e.g. activation of AFP system (e.g. deluge), detection of flammable gas, etc.), the verifier should witness a sample of the critical function tests. The purpose of verifying a critical function test is to confirm that the PS compliance is achieved, and that the critical function test has been carried out correctly to a defined test method and recorded in the maintenance management system (so that the verifier may gain confidence in operation of the maintenance management system). The verifier should ensure records accurately reflect the results of the critical function tests performed.

Examples of active SCE critical function tests that should be witnessed include (numerous other types are omitted):

- fire water pump starting (by all methods);
- fire water pump flow rate;
- ESDV closure time;
- ESDV leakage rate;
- gas detector response time, and
- gas detector alarm level.

Where SCEs have a passive role (e.g. where measured by dimensions, quantity, condition, etc.), the verifier should visually examine a sample, but the main competent of verification activities for these systems should be verifier review of the operating company's assessment of their integrity.

Passive SCEs usually visually examined include (numerous other types are omitted):

– vessels and piping;
– structural supports;
– escape routes;
– emergency exit doors;
– blast walls, and
– PFP.

5.8 VERIFICATION RECORDING AND REPORTING

Records should state explicitly whether the PS for each SCE is met, and whether for initial or ongoing suitability. Each verification report should include the following information:

– unique report number;
– SCE examined;
– PS reference;
– unique verification activity identifier and description;
– description of the verification activities completed;
– equipment/records examined;
– documents reviewed and other relevant references;
– percentage of activities completed against the requirements of the verification scheme;
– details of any outstanding activities, including reason for activities not being completed (statements like 'not examined due to operational reasons' should be avoided);
– findings from the verification activity (e.g. pass/fail vs. PS measurable compliance criteria);
– anomalies reported to the operating company;
– remedial actions to rectify anomalies and planned schedule for closure by operating company;
– verifier acceptance of anomaly closure;
– details of personnel attending close-out meeting with the operating company;
– name(s) of the verifier staff that performed the verification activity, and
– signature by the verifier report author and operating company's reviewer.

Relevant aspects of these records should be integrated with assurance records in the operating company's maintenance management system.

Findings might include identified shortcomings in the operating company's SCE assurance processes and supporting documentation or non-conformances in relation to any specific SCE condition or performance. These instances should be reported by the verifier and

acknowledged by the operating company in order to allow appropriate remedial action to be taken.

The verifier findings should include positive reporting of verification activities, not just where an anomaly is raised.

Verification findings should be categorised according to their impact, and a proportionate schedule should be defined to close out the findings. The verification findings are declared closed once the required remedial work has been performed and the SCE is demonstrated to be suitable for service, which the verifier should review.

To aid the operating company, the verifier should carry out a focused review where there are particular concerns with any of the findings raised. This review should seek out common and systemic failures by reviewing maintenance history and previous findings raised. The verifier should conduct checks to ascertain if failed equipment was appropriately maintained by reviewing the effectiveness of the maintenance and inspection routines, including their scope and frequency. See 6.4 regarding integrating learning from verification to avoid recurrent anomalies and so improve SCE integrity.

The operating company should regularly monitor progress against the findings of the verification activities to demonstrate that anomalies are closed-out. Regular review meetings should be held with the verifier. The verifier should also raise concerns when the verification scheme is not being completed in a timely manner.

6 MEASUREMENT OF SCE PERFORMANCE, REVIEW AND CONTINUAL IMPROVEMENT

6.1 MEASUREMENT OF SCE PERFORMANCE

Operating companies should use KPIs to monitor SCE status, performance trends, and implementation of improvements, and identify areas for audit and inspection.

SCE KPIs should be reported to leaders so that they know whether SCEs are capable of meeting their defined MAH role, and so whether there is a valid case for safe operation of the facility.

SCE KPIs should be reported on a regular basis. Operating companies should put in place robust systems for gathering and analysing the necessary data.

EI *Guidance on meeting expectations of EI Process safety management framework element 16: Management of safety critical devices* includes example KPIs (albeit called performance measures) aligned with specific points in its logical flow diagram process, and are called implementation, operational or outcome KPIs. The implementation and operational KPIs are predominantly leading indicators designed to enable the measurement of the outputs from the element and the level of compliance with the expectations (e.g. observed non-compliances with management of SCE arrangements), whereas the outcome KPI is lagging and relates to incident root causes that are failures of Element 16.

EI *Guidance on meeting expectations of EI Process safety management framework element 16: Management of safety critical devices* notes that accountability for performance against each performance measure should be clearly identified and that the accountable person understands the interventions that need to be made to correct deviations in performance against the KPI.

More generally, HSE HSG 254 provides a process for defining KPIs; SCE KPIs should be carefully defined to distinguish between leading and lagging SCE KPIs. The former provide active monitoring of SCEs to ensure their ongoing suitability.

Example of leading SCE KPIs include:

- number of anomalies raised during specified period;
- number of anomalies that were not closed-out by the planned due date at the end of the quarter;
- number of unplanned activations of an SCE (e.g. an ESDV);
- number of SCEs with incomplete assurance (e.g. maintenance) past a planned completion date (SCE backlog), as well as for routine (non-safety critical) maintenance;
- number of hours required to remedy an SCE maintenance backlog;
- number of SCE repairs;
- number of bypassed or inhibited SCEs;
- number of live operational risk assessments (ORAs);
- SCE cumulative risk, and
- number of SCEs not meeting their PS (e.g. unavailable).

Lagging SCE KPIs typically relate to incidents through to major accidents, where the SCE did not function as defined in its PS. Examples of lagging SCE KPIs include:

– occurrences of impaired structural integrity;
– failures or malfunctions of safety critical equipment and components (i.e. at tag level);
– uncontrolled releases of a dangerous substance (e.g. hydrocarbon gas, with sub-divisions according to quantity, e.g. using the KPIs set out in API RP 754 or IOGP 456);
– ignition of released hydrocarbon gas (leading to fire or explosion), and
– occurrences of loss of mooring, stability or buoyancy.

As well as technical SCE KPIs, there also should be human and organisational factors KPIs that indicate the status of wider SCE management issues, such as process safety culture. EI *Research report: Human factors performance indicators for the energy and related process industries* reports on a research project that investigated the viability of measuring human and organisational factors KPIs for the process industries. Human and organisational factors KPIs also should be applied to SCEs that have associated safety critical tasks, so as to ascertain whether defined human reliability is delivered in practice. The means to test human reliability in safety critical tasks (e.g. for functional safety, where a human action is required in a SIL 1 rated SIS loop) is not as mature as for equipment and components; however, field observations by supervisors, documentation, audits and incident reviews are options.

A further aspect of performance measurement and compliance checking is to establish regular management and supervisory compliance checks. Some of the suggested operational KPIs listed in EI *Guidance on meeting expectations of EI Process safety management framework element 16: Management of safety critical devices* are derived from the results of these field observations. It proceeds to provide a proforma, which seeks to ascertain the level of compliance on issues such as:

– Are the SCE inspection, maintenance and testing procedures available and in date?
– Are the procedures for making changes to, and the bypass and inhibit of, SCEs suitable and sufficient?

6.2 REVIEW OF SCE PERFORMANCE

SCE KPI data should be reviewed by senior technical personnel. This should include, but may not be limited to, reviewing whether:

– inspection, maintenance and testing of SCEs are ensuring that MAH risks are being managed;
– there are any collective issues regarding SCE integrity;
– trend analysis reveals potential degradation of SCE performance, both for physical and process failures;
– PSs are valid (e.g. do actual plant process data or well composition data align with that expected);
– there have been any unfavourable changes to SCEs or their performance (e.g. an unmanaged change to plant operating parameters that increased internal corrosion rates or creeping changes that challenge integrity), and
– wider SCE management issues are undermining SCE integrity (e.g. processes or human and organisational factors issues such as process safety culture).

Workforce representatives should participate in these reviews.

The results of the reviews should be communicated to leaders so that they understand the condition of SCEs (i.e. whether they meet their defined MAH role), the potential impact on MAH risk, and whether there is a valid case for safe operation of the facility.

The review also may be part of a wider review of PSM arrangements, such as for those operating companies that are aligned to the series of guidelines that support EI *High level framework for process safety management framework*.

The findings from such reviews may identify issues requiring resolution or identify opportunities to enhance arrangements, whether the SCEs themselves or the SCE management processes. These should feed into continual improvement processes. See 6.2.

Records, including KPIs, should be reviewed in order to assess:

– results – e.g. pass, fail, or failed and fixed;
– quality and completeness of data entry in maintenance management system;
– level of achievement of assurance tasks and KPIs vs. targets;
– trends in SCE condition (e.g. creeping degradation, forecasting of degradation, etc.);
– whether there are any 'bad actor' SCEs that have poor performance;
– equipment failure frequencies (e.g. to better define reliability using operating company data – see 3.2.3), and
– root causes of failures (e.g. whether there are common factors).

For example, analysis of ESDV assurance data trends may be used to forecast likely date for failure. An increase in closure times or leakage rates should trigger pre-emptive maintenance.

6.3. MANAGING SCE AGEING, OBSOLESCENCE AND LIFE EXTENSION

The impact of ageing, obsolescence and life extension on SCEs should be considered in an integrity management process. The principle is that SCEs should be suitable to perform their role throughout the operate phase through to decommissioning.

Measures for managing ageing, obsolescence and life extension include:

– Having in place robust structural and process integrity management systems.
– Performing appropriate fabric maintenance of structures and process containment equipment.
– Focusing integrity management not exclusively on current and near future threats, but also having long-term plans that address threats introduced by ageing and life extension.
– Defining expected lifetime in the PS, initially at design, and having in place a regular review (e.g. every five years) to re-evaluate design life, ageing and life extension.
– Considering issues arising from MoC reviews, e.g. creeping changes to specification of dangerous substances or processes.
– Performing audits to inform formulation of ageing, obsolescence and life extension processes.

Whilst design and construction standards are important for new facilities, as the facility ages more importance should be given to asset integrity management.

For further information on managing SCE ageing see EI *Research report: A framework for monitoring the management of ageing effects on safety critical elements.*

The decommissioning phase offers an opportunity to review the ongoing need for SCEs using MoC, and if retained, what should be their performance in this phase. See 2.9.

6.4 CONTINUAL IMPROVEMENT OF SCE MANAGEMENT

As noted in Figure 2, processes for managing SCEs (both assurance and verification) should be subject to continual improvement so as to improve the management of SCEs. As well as periodic review, examples of continual improvement opportunities for SCE management, from MAH analysis through to SCE verification (for design through to decommissioning) include:

- Understanding level of MAH risk, e.g.:
  - improvements in risk assessment techniques and assumptions;
  - trends from review of SCE performance (e.g. reliability lower than expected), and
  - knowledge of human and organisational factors.
- New or amended:
  - technology (e.g. availability of new SCEs);
  - knowledge (e.g. transferrable learnings from better arrangements on other facilities within the operating company or wider industry learnings), and
  - legislation, regulations or good practice technical publications (e.g. codes, standards and industry good practice).
- Learning from review of SCE performance, such as KPIs and trend analysis (see 6.2), ORAs and deferments to inform risk management, e.g.:
  - evidence for changing the inspection, maintenance and testing interval;
  - there are 'bad actor' SCEs that have poor performance and warrant a change to the inspection, maintenance and testing or a project to change the SCE.
- Understanding of ageing mechanisms and obsolescence (see 6.3).
- Learning from a review of MoCs applied to SCEs.
- Findings from inspection reports, including verification reports and competent authority reports.
- Learning from operation of the SCE management plan, including inspection, maintenance and testing.
- Learning from incidents (e.g. SCE failures) within and beyond the operating company, including:
  - commonality in root causes;
  - assessing whether actions recommended are comprehensive, appropriate and completed according to an agreed close-out date, and
  - lessons learned are not just communicated to staff, but staff are tested to assess whether deep learning has occurred.

Some of these changes may be driven by changes to, for example:

- the facility safety case (e.g. as required by national legislation or regulations that transpose EU OSD or EU Seveso III).

– Operations and conditions (e.g. conversion from staffed installation to an NPAI, which requires a different set of SCEs, or cessation of production and transition to decommissioning, which removes some MAHs but introduces construction-type hazards).
– The plant and the process (e.g. processing a different fluid, such as a sour rather than sweet fluid).
– Organisational arrangements (e.g. operation managed remotely, rather than with local TA/SME support).

The workforce should be engaged in reviews of continual improvement opportunities for SCE management so as to capture their experience, e.g. through interviews and observations of working practices. Moreover, they should be engaged in safety workshops to evaluate potential improvements to eliminate, prevent, detect, control, and mitigate MAHs.

The outcomes of such reviews may be revision of PSs for existing SCEs, selection of different SCEs and definition of new PSs, or revision to processes (e.g. MoC process or assurance process).

Where selection of different SCEs is identified, proposed improvement projects should be assessed to evaluate the justification, priority and feasibility.