

Offshore critical barrier identification; management of their continuing suitability and their verification

Richard Potter[1] and Justin Holroyd[2*]

[1] Health and Safety Executive, Norwich, Norfolk NR7 0HS

[2] Health and Safety Executive, Harpur Hill, Buxton SK17 9JN

*Corresponding author: Justin.Holroyd@hsl.gsi.gov.uk

Managing major hazard risks 'proactively' is a challenge, particularly at a time of a sustained low oil price. If mistakes are made, it could be catastrophic. This paper discusses a regulatory pilot which demonstrates that the industry's ability to proactively prevent major incidents can be enhanced by focusing on critical barrier identification, their continuing suitability (including integrity) management, and their verification. Verification is third party auditing carried out by an independent competent person (ICP) for the dutyholder. Within the UK Continental Shelf, verification is a legal requirement.

A 'line of sight coaching style inspection' forms the cornerstone of this regulatory approach. Inspections are designed, through targeted sampling, to assess the suitability of dutyholders' barrier management and verification schemes, including the ability of key dutyholder personnel to predict and prevent major incidents, especially in the early stages. The necessary 'line of sight' is between the dutyholder's case for safety and what is being done to both ensure and verify that the major hazard barriers are, and remain, suitable.

To start with, documents (e.g. the operator's safety case and the verification scheme) are scrutinised, ideally by a multi-disciplinary team, to identify key hazard initiators and relevant SECEs (Safety and Environmental Critical Elements) along with their essential characteristics, the testing of which will demonstrate the effectiveness of both the duty holder's major hazard management arrangements and their verification arrangements. This paper describes the methodology used, what has been found, lessons learnt and how HSE is using it to enhance its regulatory effectiveness. This approach is resilience engineering in action.

Keywords: verification, SECE, barrier, offshore safety case, resilience

Introduction

Following the fire and explosion at the Macondo well (Deep Water Horizon Study Group, 2011), Oil and Gas UK told Parliament that such an event was less likely to happen on the UK Continental Shelf because of verification (Oil and Gas UK, 2010). Verification, a legal requirement (HSE, 2015), is third party auditing carried out by an independent competent person (ICP) for the dutyholder (the owner or operator). Post Macondo, the EU issued a Directive (2013/30/EU) that requires verification of the major hazard hardware barriers for all installations operating in European waters. The Directive requires the dutyholder to ensure the verifiers are competent and are given sufficient authority to be able to do their job.

Managing major hazard risks 'proactively' is a challenge, particularly at a time of a sustained low oil price with increased pressure on resources. If mistakes are made it can be catastrophic. This paper will discuss a regulatory pilot which demonstrates that the industry's ability to proactively prevent major incidents can be enhanced by focusing on critical barrier identification, their continuing suitability (including integrity) management, and their verification. Verification has to be effective for HSE to retain regulatory compliance excellence. For it to be effective:

- verification has to address current and likely continuing suitability, and be installation as well as hazard specific, not generic in nature or solely compliance focused;
- verifiers have to be 'individually' competent; given sufficient authority to do their job; the significant issues identified by the verifiers have to be addressed in a timely fashion; and
- there has to be an industry wide understanding of what good practice looks like in key areas, including the part it plays in the governance statement within the safety case.

A 'line of sight coaching style inspection' forms the cornerstone of this regulatory approach. Inspections are designed, through targeted sampling, to assess the suitability of dutyholders' barrier management and verification schemes, including the capability of key dutyholder personnel to predict and prevent major incidents, especially in the early stages where the ability to identify and address weak signals can make a real difference. The necessary 'line of sight' is between the dutyholder's case for safety and what is being done to both ensure and verify the major hazard barriers are in place, and remain suitable. A 'coaching style' inspection is where the inspector asks open-ended questions in order to draw out an understanding of the barriers, Safety and Environmental Critical Elements (SECEs), the associated management and verification arrangements and to explore with the dutyholder and/or ICP any gaps from good practice.

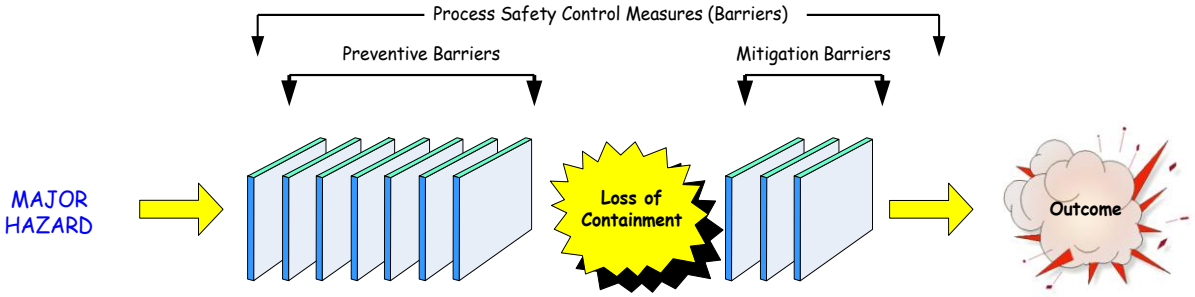
An ultimate aim is for dutyholders to proactively develop and use 'effectiveness' approaches to monitor, review and enhance their own barrier suitability arrangements and the associated operational understanding of them. Resilience engineering is the ability to spot and deal with potential barrier weaknesses proactively, building increased robustness in the process. The approach adopted is an example of resilience engineering in action.

SECE Management

The barrier approach to accident prevention

There are various versions of the barrier approach to accident prevention, including James Reason's Emmental Swiss Cheese Model (Reason, 1997), Layer of Protection Analysis (LOPA) (Chambers and Pearson, 2011) and the bow tie model of layers of protection (HSE, 2013). The general principle is that barriers are stacked up side by side (one behind the other), with any risk from the progression of a threat/hazard being prevented by, or mitigated by, the different types of barriers/layers. It is possible to depict the barriers (layers of protection) as a 'bow tie' (combined fault and event trees with, for example, loss of containment as the central node) to emphasise the way the barriers link in sequence in relation to each major hazard event (HSE, 2013), given the multiple initiation and consequence paths.

Figure 1: Trajectory of an incident through a barrier / bow tie Diagram (HSE's HID Regulatory Model)



However, there is always a need to be mindful of the potential for common mode failure, or unforeseen linkages and weaknesses.

Proactive Major Hazard Management

There exists a concern that dutyholders and employees can remain focussed on generic solutions to major hazard safety, while having a limited appreciation of the installation and operational specific major hazards that exist offshore as highlighted by a number of major incidents. Hopkins (Hopkins, 2012) when discussing Macondo said a focus on what might cause injury to individuals (e.g. slip hazards) does not necessarily equate to a focus on major hazard risk, similarly a focus on generic major hazard risk is not necessarily a focus on true major hazard risk. It is recognised that effective proactive major hazard management involves:

- Systematic learning, as captured, for example by codes and standards, and more generally by industry good practice, and by the identification and tackling of underlying causes designed to prevent the recurrence (including verifiers' findings);
- Barrier management: bow ties and reliability centred maintenance are typical frameworks employed;
- Resilience engineering.

Those in key dutyholder major hazard roles need to be able to draw systematically on all three approaches, harnessing the capabilities of those around them to do so, including the verifier.

The Cullen Inquiry (Cullen, 1990) into Piper Alpha led to the formal introduction of a systemised transparent barrier approach in the UK. Texas City (Goff et al, 2015) highlighted the need to be ever mindful of what could go wrong, for example through failure to recognise accumulated risk (creeping change), and the need organisationally to be capable of doing so. Macondo drove the message home and resulted in a barrier approach and its verification being adopted more widely (including throughout the EU).

Safety and Environmental Critical Elements (SECEs)

Key to the control of major hazards is the identification of appropriate risk control measures (SECE barriers), the performance required of them, and their effective management. SECEs as hardware barriers that are defined by Offshore Safety Case Regulations 2015 (HSE, 2015), as:

> "…parts of an installation and such of its plant (including computer programmes), or any part of those —
>
> (a) the failure of which could cause or contribute substantially to a major accident; or
>
> (b) a purpose of which is to prevent, or limit the effect of, a major accident."

The initial and continuing suitability of SECEs is required to be verified.

Any failures of the barriers requiring immediate action to be taken are notifiable to the regulator. The verifier's findings are leading indicators and reported voluntarily on an industry wide basis.

Verification

The Competent Authority (HSE and the Department for Business, Energy and Industrial Strategy (BEIS)) have a duty under the Offshore Safety Case Regulations 2015 to take action if the operator is not competent in discharging its duties. The verifiers' findings, and the way in which the dutyholders address those findings, has a bearing on such action, as does the quality of the work done to produce those findings; this is the focus of the line of sight inspection work.

Verification (third party independent verification of the continuing suitability of the SECEs) is a development of (pre Piper Alpha) Certification. Certification was introduced in 1971 following the loss of the Sea Gem (Adams, 1967) in the southern North Sea whilst prospecting for gas. It was modelled on Classification (of ships) and designed to enhance the long standing requirement for 'oil field good practice' within the industry, enshrined in law since the 1930's. Six Certifying Authorities were appointed by the then offshore regulator (the Department of Energy) to assess installations' initial and continuing fitness for purpose. They were paid for by the dutyholders and audited by the Department of Energy. The dutyholders could choose which one to employ and in theory could have proposed another if they could convince the regulator that they had the necessary skill set. There are four primary operational installation verifiers/ICPs today, all of which were Certifying Authorities under the old regime. Mergers and the market have reduced the number.

Following the introduction of Certification it soon became apparent that, in order for Certification to operate more effectively, guidance was needed. What later became known as the '4th Edition' (referenced in HSE (2012)) was introduced. The Certifying Authorities were required to consider it when assessing an installation's fitness for purpose.

The guidance initially tried to fill the gaps where good practice was lacking, for example in relation to the fatigue assessments of offshore installations. At this time there were too many fatigue failures in the North Sea due to poor design, as a Gulf of Mexico design approach was initially used without the necessary appreciation of the differences between the two environments. The loss of the Alexander Kielland in 1980, a semisubmersible that listed dramatically almost immediately following the loss of a critical member before turning over about 20 minutes later, is the worst example of a fatigue failure to date.

All guidance produced was done in consultation with the dutyholders, designers and the certifying authorities. It was in effect industry guidance, but badged as Department of Energy guidance. That guidance, like all guidance, requires the supporting evidence (applied research), this takes time to produce. The work was contracted out.

Even with the guidance and auditing of the Certifying Authority, significant problems were found and addressed. For example a semisubmersible was operating without leak detection designed to detect through thickness cracks in its critical members. This was due to a lack of understanding of its importance on the part of the dutyholder, despite advice from the designers, i.e. an organisational competent behaviour issue.

Following Piper Alpha and the enquiry led by Lord Cullen, the industry was required to produce a case for safety for each installation and submit it to the regulator. Following a transition period no installation could operate in controlled waters without an accepted safety case. Lord Cullen (Cullen, 1990) reviewed the future of the Certification Regime and recommended that it should run in parallel with the Safety Case Regime initially, and that the regulator should then consider its future.

The regulator concluded, after consultation, that an installation specific barrier model supported by good practice was the way forward. This was contained within the Post Piper Alpha goal setting safety case regime, with verifiers appointed by the dutyholders undertaking independent third party audits of both the barriers initial and continuing suitability. Thus verification was born, placing the responsibility for the competence of the independent third party auditor (verifier/ICP) on the dutyholder rather than the regulator.

HSE's goal is the avoidance of catastrophic incidents, which requires SECEs (barriers) to be correctly identified, adequate in performance and dependable when required. This is echoed in the EU's response to Macondo (2013/30/EU) requiring the European-wide introduction of verification. The EU has gone further than the introduction of verification. It has explicitly asked for what is in effect a governance statement within the safety case that needs to be accepted by the regulator. As outlined above, that governance statement asks the dutyholder to make a statement to the effect that its hardware barriers (SECEs) and maintenance scheme are suitable having considered the comments made by the verifier/ICP. Note that the safety case has to be resubmitted to the competent authority if there are significant changes to the case for safety. A letter of reservation issued by the verifier could be considered a significant change. A thorough review of the safety case has to be done every 5 years, and in future this should consider a review of the dutyholder's governance statement.

Line of sight

Texas City, a major onshore refinery incident that pre dates Macondo, highlighted the importance of embedding high reliability organisation principles (Lekka (2011); Mellor et al (2015)) and the need to engineer resilience into it, as not everything is predictable. This underlines the need to not only continue to review the suitability of the chosen barriers, the performance standards, assurance and verification activities, but also, in doing so, the ability of the dutyholder's personnel to spot and investigate potential weaknesses proactively.

A line of sight should exist between the potential hazard initiating events, the safety case, the hardware barriers (SECEs) and their performance standards, the dutyholder's assurance activities, and the verifier's activities. It is the acid test of the verification schemes effectiveness. 'Line of sight coaching style inspections' are designed through targeted sampling, to assess the dutyholders' understanding of (and the appropriateness of) the barriers in place to prevent major accidents; the suitability of their barrier management and verification schemes to ensure their continuing suitability; and the ability of key

personnel to detect weak signals and thus prevent potential major incidents, especially in their early stages before control is lost.

Without an obvious and clear line of sight there may well be significant gaps in the prevention and mitigation barriers, their assurance, and the knowledge and understanding necessary for effective operational major hazard management. For example the arrangements in place may be generic, inadequate and not take into account the installation's specific major hazard initiating events, as happened when the jack-up installation, Interocean 2, sank during a field move, at around the same time that Piper Alpha was lost. Its damage stability assessment was based on generic ship impact related damage criteria, not the shearing of deck vents to a very large central space by shifting cargo following the loss of the towline (and the resulting significant amounts of green water on deck).

Unless the ICP has this line of sight, it will not be possible for them to comment on the completeness/coverage of SECEs designed to address the specific major accident hazards (MAHs) of the installation.

The Inspection Pilot Project

A pilot project was organised to help develop the line of sight approach to inspecting the effectiveness of the duty holders' verification activities. It built on the preliminary work done by the 'project team' facilitator.

To undertake this work a well-motivated, multi-disciplinary team was formed with experience of assessing Safety Cases and providing incident support appropriate to the type of installations being assessed.

Having explained the purpose of verification and the required end result of the exercise, guidance was given to the team as to what to look for, namely high consequence/high risk events that looked from the evidence (the Safety Case, the verification scheme, and associated operational knowledge) to have the potential to have significant deficiencies in the way they are being managed. The team were looking ideally for 2 to 3 events that (if it were found through subsequent inspection were not being managed effectively) would by themselves dramatically demonstrate the untapped potential for improvement and the ability of the coaching style inspections to achieve improvements to the verification process. Examples of what had been found to date, coupled with a review of the material used as part of that process, helped show the team the potential impact they could have and gave them the confidence that they could do what was being asked. The use of an experienced multidisciplinary team enhanced the ability of the facilitator to identify key areas to inspect and improved the interdisciplinary understanding essential for growing the capability internally through repeated exposure to the process.

The team sought novel, installation specific high consequence / high risk events / areas, preferably where there appeared to be gaps or weaknesses in the hazard management logic (sometimes in cross discipline areas), or where changes (outside the norm) may have introduced risks.

Documentation (e.g. SECE performance standards, safety case, written scheme of verification and verification inspection reports) were studied. Issues were uncovered and shared in a regulator team forum to identify links between the different specialists' findings. Where necessary other specialists were co-opted onto the team depending on the potential issues. The specialist multi-disciplinary team forum/meetings were led by an experienced HSE inspector, who acted as the facilitator, and through in-depth discussion of all the issues uncovered would typically gather together 2-3 related/overarching issues to take forward to the offshore regulatory inspector. The role of the facilitator was important to the success of this project, as they were able to see and explore the links between the specialists' findings, proactively spotting barrier weaknesses and homing in on potentially crucial area/issues.

Typically two specialist multi-disciplinary team forum/meetings were held per case. Following the first meeting specialists would reflect on the issues raised at that forum/meeting. At the second they would confirm the 2-3 related/overarching issues after sharing any additional information they had found that would assist the inspection. They would then prepare their presentation to the offshore regulatory inspector. Having discussed and agreed the issues to take forward with the offshore regulatory inspector at the pre-onshore inspection meeting, specialists would, where appropriate, accompany the offshore regulatory inspector to the verifier and dutyholder onshore inspections. Both the onshore and offshore inspections are designed to scrutinise the robustness of the arrangements in place drawing on the competence of the duty holder's personnel by adopting a coaching style, where appropriate.

Conclusions

Currently, verifiers do not necessarily always have an up to date 'line of sight' between the major accident hazards (MAH) described within the dutyholders' case for safety; and the SECEs and their associated continuing suitability arrangements that provide protection against those MAHs. Unless the ICP has this line of sight, it will not be possible for them to comment on the completeness/coverage of SECEs designed to address the specific MAHs of the installation.

The line of sight approach has been designed to test the effectiveness of the dutyholders' major hazard arrangements, and represents resilience engineering in action. The approach can be used by dutyholders' and others to enhance the robustness of their arrangements. It has consistently been shown to pay real dividends in terms of improved understanding and risk reduction.

In a time of increasing pressure on resources, effective technical oversight arrangements supported by effective verification arrangements can, using the right methods, help maintain and enhance the robustness of the duty holders major hazard arrangements including the capability of their people to identify and address weak signals.

Acknowledgements and Disclaimer

The authors would like to thank Jill Wilday, John Hare, Nick Bailey, Mike Stewart, Jason Gill, Ed Corbett, Richard Goff Eoin Young and Helen Pitts for their useful contribution to the project.

This publication and the work it describes were funded by the Health and Safety Executive (HSE). Its contents, including any opinions and/or conclusions expressed, are those of the authors alone and do not necessarily reflect HSE policy.

References

Adams, J.R., 1967, Inquiry into the Causes of the Accident to the Drilling Rig Sea Gem. The Ministry of Power, HMSO CM3409, London

Chambers, C. and Pearson, J., 2011, A discussion of some common pitfuls in the application of layer of protection analysis (LOPA) to the overfill of storage tanks at Buncefield type sites, IChemE Hazards 22 Symposium, Paper 156

Cullen, The Hon. Lord W. D., 1990, The public inquiry into the Piper Alpha disaster, H.M. Stationery Office, London

Deep Water Horizon Study Group, 2011, Final Report on the Investigation of the Macondo Well Blowout, http://ccrm.berkeley.edu/pdfs_papers/bea_pdfs/dhsgfinalreport-march2011-tag.pdf (accessed 8/12/16)

Goff, R. J., Wilday. J. and Holroyd, J., 2015, Creeping Changes, IChemE Hazards 25 Symposium, Paper 26

HSE, 2015, Offshore Installations (Offshore Safety Directive) (Safety Case etc.) Regulations (S.I.2015/398), 2015, http://www.hse.gov.uk/offshore/assets/pdfs/safety-case-regs.pdf (accessed 8/12/16)

HSE, 2013, HID Regulatory Model, http://www.hse.gov.uk/hid/hid-regulatory-model.pdf (accessed 8/12/16)

HSE, 2012, Status of technical guidance and information on design, construction and operation of offshore installations Operations, Notice 27, http://www.hse.gov.uk/offshore/notices/on_27.htm (accessed 8/12/16)

Hopkins, A., 2012, Disastrous decisions. The Human and Organisational Causes of the Gulf of Mexico Blowout, CCH Australia

Lekka, C., 2011, High Reliabilty Organisations. A Review of the Literature, HSE RR899, http://www.hse.gov.uk/research/rrhtm/rr899.htm (accessed 8/12/16)

Mellor, N., Wilday, J., Lunt, J. and Holroyd, J., 2015, High Reliability Organisations and Mindful Leadership, IChemE Hazards 25 Symposium, Paper 26

Official Journal of the European Union, 2013, Directive 2013/30/EU of the European Parliament and of the Council on safety of offshore oil and gas operations and amending Directive 2004/35/EC http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32013L0030 (accessed 8/12/16)

Oil and Gas UK, 2010, UK Deepwater Drilling - Implications of the Gulf of Mexico Oil Spill - Energy and Climate Change http://www.publications.parliament.uk/pa/cm201011/cmselect/cmenergy/450/450we03.htm (accessed 8/12/16)

Reason, J., 1997. Managing the risks of organizational accidents. Aldershot: Ashgate.