Guidance on vulnerability review and assessment for safety and environmental critical equipment to control escalation risks on atmospheric storage tank sites

Ian L Herbert, Director, Vulcan Hazard Management Ltd, Colorado Close, Warrington, WA5 8WY

John Evans, Principal Consultant, Thornton Tomasetti, The Brew House, Wilderspool Park, Greenall's Avenue, Warrington, WA4 6HL

Mark Scanlon / Laszlo Komaromi, Energy Institute, 61 New Cavendish Street, London W1G 7AR

Abstract:

The Energy Institute is in the final stage of a project that will result in the generation of a new guidance document. This project was originally aimed at aiding bulk petroleum and fuel storage installation operators in addressing Recommendation 12, from the Buncefield Major Incident Investigation Board (BMIIB) Final report, which requires operators to assess the location and protection of emergency response facilities to ensure survivability. However, it was determined that survival was only one vulnerability and that emergency response facilities could also be impaired through failures in equipment function, availability, reliability, and integration [with other measures]. It was also noted that the requirements on these emergency response facilities will also vary during the course of AST (Atmospheric Storage Tank) incidents.

This paper summarizes the key components of the new guide, which is expected to be published in 2022.

The vulnerability assessment guide aims to work in conjunction with the update to EI 19 'Fire precautions for refineries and bulk storage installations' and is related to the vulnerabilities to emergency response equipment and associated human interactions for AST operations. The use of the guide will enable duty holders to ensure that their Safety and Environmental Critical equipment (SECe) and associated human interactions remain fit for purpose.

Key aspects, in the new guide, in assessing SECe vulnerabilities include:

1) That performance and survivability requirements on SECes and associated human interactions need to match different release and fire and explosion conditions at different stages in an AST incident, from single tank or bund incidents up to worst case multiple tank incidents. 2) The determination of different hazard ranges for escalation and survivability assessment of SECes and associated human interactions. 3) The acceptability of SECes and/or contingency measures against identified vulnerabilities and the need for additional measures. 4) The use of record tables in the vulnerability assessment supported by example assessment sheets and a list of typical safety and environmental critical equipment for AST incident escalation risk control.

The guidance document should result in readers being more familiar with performance and survivability vulnerabilities of emergency response safety and environmental critical equipment and to have available a method to help duty holders in assessing these vulnerabilities.

Keywords:

Vulnerability, Hazard Ranges, Safety and Environmental Critical equipment, NaTech, Open Flammable Cloud Explosion (OFCE), Emergency Plans, atmospheric storage tank (AST), Fire and Explosion Hazard Management (FEHM),Emergency response,

Introduction

A two-phase project was commissioned by the Energy Institute's (EI) Containment Systems Working Group (CSWG), which is a working group of EI's Process Safety Committee (PSC). This project had the aim to reduce a shortfall in industry guidance on options for protecting safety and/or environmental critical equipment and the people that operate them from credible fire (thermal radiation) and blast (open flammable cloud explosion (OFCE) – a Buncefield-type event), at existing bulk petroleum and fuel storage facilities.

This technical development project aimed to meet the requirements of Buncefield Major Incident Investigation Board (BMIIB)[1] Final report Recommendation 12, which states:

Recommendation 12 '*Following on from Recommendation 11, operators of Buncefield-type sites should evaluate the siting and/or suitable protection of emergency response facilities such as firefighting pumps, lagoons or manual emergency switches.*'

The HSE Process Safety Leadership Group (PSLG) Final report [2] Appendix 6 provides a methodology for undertaking that analysis; however, the HSE PSLG Final report and other industry technical publications lack detailed guidance on to how to take forward that analysis and transpose it into a generic assessment approach.

A starting point for the technical development project is the assumption that an analysis of the extent and severity of locations affected by credible fire and blast events has been carried out that meets the requirements of Recommendation 11 of the BMIIB, such as by the use of Fire and Explosion Hazard Management as detailed in EI 19 [4].

Phase 1 of the project developed a list of applicable Safety and Environmental Critical equipment (SECe). This was generated from a review of legislation, regulations, and industry technical publications. A questionnaire was also circulated amongst CSWG stakeholders to validate and add to the list of equipment identified. On its own the listing of SECe provides

a good resource to operators and duty holders in reviewing the survivability of their emergency response resources and provides potential options if deemed vulnerable or even missing from existing plans.

The second phase was to generate guidance for risk assessment and options on the survivability of the SECe and people that operate them from identified scenarios at existing bulk atmospheric storage tank (AST) sites. The aim was to provide a generic process linking the determination of credible fire and/or blast events to the identification of SECes, the survivability or otherwise of these SECes and risk reduction options if vulnerable.

The guide was developed to cover SECe at AST sites, such as found at new and existing bulk petroleum and fuel storage installations, but would also include biofuels, alcohols, blends etc. It was not developed to cover pressurised, cryogenic or heated storage, such as for gases, LPGs, LNGs, bitumen, etc or vessels/tanks as part of process operations. However, the basic approach could be adapted for use in these applications.

Safety and/or Environmental Critical equipment (SECe)

The scope of the project was to review the survivability of SECe against fire and blast exposure. Such equipment was determined to be critical because of its role in mitigating incident escalation e.g., for inventory isolation or fire-fighting response, and consequential impacts to people, the environment and plant assets. As such the equipment covered in the review does not cover that required to prevent an initial incident, such as preventing losses of containment e.g., overfill. It can be seen that the SECe, covered in the guide, therefore forms part of emergency response measures on an AST site. The guide has taken a loss of containment from ASTs as one of the starting points. This has the potential to lead to the formation of unignited material, which if ignited, could result in an incident and as such, equipment to prevent ignition for such events is included. Other starting points include atmospheric tank vapour space fires and explosions and rim seal fires on floating roof tanks.

Vulnerability of SECes

Although the project set out to review the survivability of SECe, during development of the guide it became increasingly difficult to separate this from other vulnerability factors such as poor design or operation. For those familiar with offshore safety these other vulnerability factors are part of the recommended model for developing Safety Critical Element Performance Standards, based on Functionality, Availability, Reliability, Survivability and Interaction (FARSI), see HSE's management guide [3]. Functionality refers to the required purpose to be performed to prevent, detect or mitigate a hazardous event. Availability refers to the proportion of the time that the item will be required to perform on demand. Reliability refers to how likely it is to perform on demand. Survivability refers to how it will perform after a major accident has occurred, i.e. how well it will survive a fire, explosion, dropped object, etc, and Interaction which refers to the way that the equipment in question is dependent upon other safety critical items to operate or otherwise interacts with other safety critical items.

These factors have been collectively referred in the guide as SECe 'Vulnerabilities' and have been further segregated into Performance vulnerabilities (Function, Availability, Reliability and Integration) and Survivability, with the larger focus of the guide being supporting details on the Survivability assessment.

In addition to physical equipment failures, the review of vulnerabilities to SECes in the guide also covers vulnerabilities associated with Human interactions required for the operation of SECes. Human vulnerability in operating SECe is often the major potential failure mechanism in correct SECe operation.

Different requirements at different stages in an AST incident

As for all good Fire and Explosion Hazard Management, as outlined in the likes of the EI 19 guide, the determination of measures required for risk management of AST fire and explosion hazards should be scenario based. The vulnerability guide uses existing assessments to define the risk management measures and hence the SECe required for fire and explosion risk management.

The vulnerability to SECe is dependent on the conditions present during individual incident scenarios. The HSE PSLG Final report [2] also states that scenario-based determination should be used in evaluating survivability of SECe. However, the PLSG guidance refers to the use of credible worst cases scenarios for the determination of critical equipment. One factor that can differentiate AST fire and explosion incidents from other process plant incidents is the duration of such incidents and that fires and explosions can go through different escalation stages. The guide highlights that it is as important to review vulnerabilities of SECes at all stages from initial incident through to potential worst case. Examples from large AST incidents such as the one that occurred at Deer Park, Texas (a manifold release into the bund escalated to a multi tank fire) and Singapore (the fire spread from an initial floating roof tank to adjacent tanks) highlights that there may be smaller fire stages which if not successfully managed can allow escalation to larger scale events.

Hence it is as important to review the vulnerabilities of SECe for these smaller fire stages as well as for worst case 'multi tank' events. This is both to prevent escalation from smaller incident stages but also because equipment required for response to earlier smaller fire stages is more likely to be required closer to hand either as installed equipment or held on site. SECe required for later and larger fire stages is likely to include that held by offsite emergency response resources, such as emergency services and mutual aid groups.

The guide and SECe review methodology breaks down AST incidents into a number of credible 'stable' incident stages. These should be developed from a review of any FEHM assessment already undertaken for the Specific AST location and operation. Stable incident stages are those where the AST fire remains basically the same size, before escalation to a larger

fire size. Examples include rim seal fire before escalation to full surface fire, single tank fire (full roof fire) before tank failure and escalation to tank and bund fire, fire escalation one tank to adjacent tanks (Singapore incident) and bund fire before escalation to engulfed tanks in the bund (Deer park incident). In order to assist in this identification of applicable fire stages, and escalation events between fire stages, the guide has generated two example logic flow charts for Fixed and Floating roof ASTs. The example for fixed roof tank scenarios is shown in Figure 1

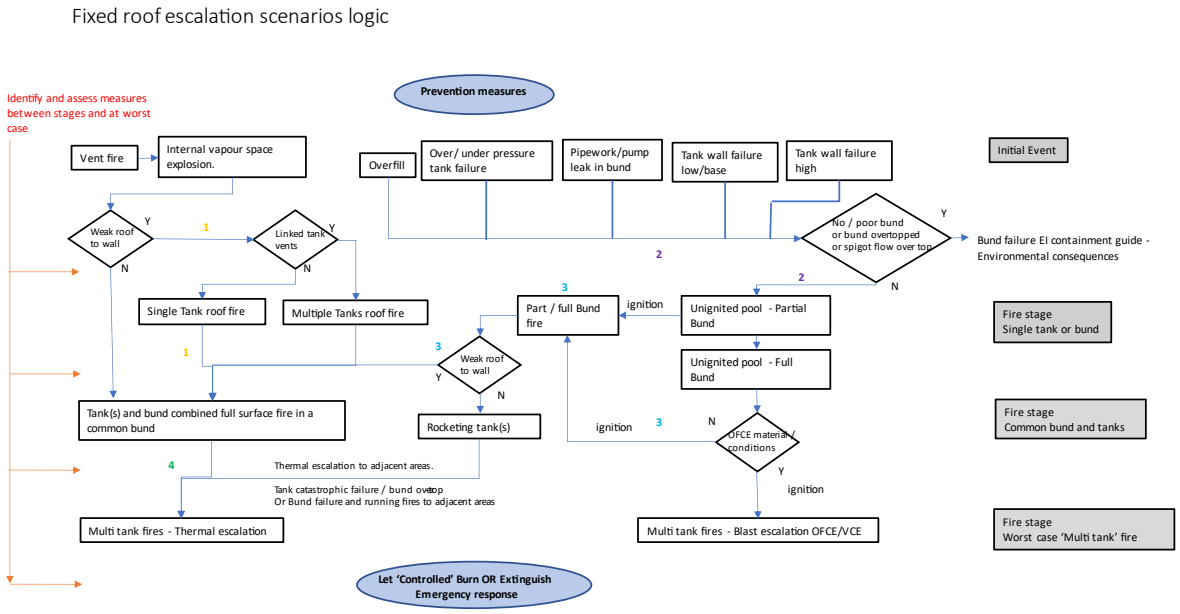

Figure 1, Fixed roof escalation scenarios logic tree – from guide

A similar logic flow chart has been prepared for floating roof ASTs. If existing FEHM assessments have not been undertaken or contain limited scenario information, these escalation event logic trees may also be used to assist in developing the site-specific scenarios. However, the intent is not to replace these assessments as the guide does not cover prevention [of initial incident event] measures, such as asset integrity, overfill protection, etc.

Escalation and Survivability Hazard Ranges

The survivability of SECe will be dependent on their location related to their exposure to adverse conditions present during the stages of the incident, from initial event e.g., unignited release or explosion, through to worst case multi tank fires. This adverse exposure is determined as particular hazard ranges which have the potential to result in escalation.

Hazard ranges are required to:

- understand and confirm potential escalation targets (whether separation is sufficient), and as such to confirm equipment operational requirements in escalation management (functional requirements), and
- determine survivability of SECe and human interactions from adverse exposure.

Four types of hazard range should be determined for their effects on SECes. These include:

a) Unignited liquid and vapour cloud releases

The spread of unignited material from credible accident conditions can be greater than 'normal' hazardous area classification distances.

b) Smoke and/or toxic vapours

This exposure can significantly affect related human interactions,

c) Overpressures and missile impacts

The effects of explosion from vessel failures if at pressure, deflagration (VCE), or from large Open Flammable Cloud Explosions (OFCE or Buncefield type events), and

d) Thermal levels

Pool fires and boil over events. As the scope is for ASTs, pressurised ignited jet releases are not covered in detail, but pump discharge type are mentioned.

The guide provides details on typical acceptable exposure levels in the review of these hazard ranges. However, the ultimate choice on acceptable hazard range criteria is down to the duty holder.

As detailed in the preceding section there will be different stages in the AST incident. The potential hazard ranges should be determined for each of the different fire stages.

Vulnerability

SECe is vulnerable if it will failure to function, as required, when and where required. This may be either because of performance failures, through incorrect function or low availability/reliability, and/or failure of interdependent equipment, or failure to survive the adverse conditions present at particular fire stages.

Performance failures comprise direct design and operational elements, but also include time as a vulnerability factor. For example, is there sufficient time and/or speed of response during a fire stage in which to set up and correctly operate the required SECe, such as emergency response setting up portable fire and foam monitors etc.

Survivability vulnerability, that is vulnerability due to failure to survive an event, covers physical equipment survivability and human interaction survivability where these are within hazard ranges. Survivability also includes resistance to severe environmental factors/events also known as NaTech events (Natural Hazard Triggering Technological Disasters). With climate change NaTech events will play an increasing role in exacerbating future AST incidents. For an example, a fire water lagoon used as a fire water source during the Buncefield event was reported to occasionally dry out or at least have low water levels during summer months. Questions should be asked, such as can events like site flooding, extreme wind, rain and storms affect AST incidents both to increase event likelihood but also lead to failure of emergency response? Other examples of NaTech survivability include delays in offsite resources arriving at the site (failure to meet required time in order to respond to smaller earlier stages in an AST incident), physical conditions on ERT members reducing their response ability, ability to control runoff to environmentally sensitive targets (larger runoff inventories or lack of capacity in drainage and containment systems), etc

Vulnerability Acceptance or Additional Measures

Risk assessment in the use of SECe, as part of emergency response, is not normally undertaken. This is due to difficulty in defining both the ability of such equipment to effectively mitigating the escalation (uncertainty in effectiveness), and in defining the failure probabilities for the equipment. The selection and operational requirement of SECe, as part of emergency response, is typically made against Recognised Good Practices and should, through good FEHM, be developed into emergency plans. The failure, through a realised vulnerability, can lead to the overall failure of emergency response. However, as part of emergency response there is the possibility to employ alternative plans and equipment, for example, even to the extent of moving to a controlled burn emergency response plan.

If vulnerabilities are identified, then the assessment treats this as a failure of that particular SECe. If the SECe cannot be modified or protected against the vulnerability, i.e., relocate the equipment, then the failure criticality should be determined for its acceptability. Acceptability of a SECe can be because the equipment is not critical in preventing escalation at the fire stage under review, or that other SECes are available as alternatives. The vulnerability review assesses the acceptability of the failure and if the failure is critical and there are no other acceptable alternatives, then additional measures should be determined.

The determination of additional measures applies the risk management hierarchy as an aid in the identification of such measures. This is: Inherent (elimination, separation, moderation), Passive (design and PFP), Active, through to Procedural. As mentioned previously significant vulnerabilities and a lack of feasible alternatives can lead to a planned ‘controlled burn’ emergency plan.

Any alternative SECes detailed from the vulnerability review should be included in the emergency plans for the AST site.

Assessment Methodology

An assessment methodology for SECe is detailed in appendix 6 of the PLSG report [2] on Buncefield. However, this does not cover requirements for SECes at different stages in an AST incident, it also does not fully cover the performance requirements with the focus on survivability. The new EI guide applies a tabular approach, similar to in style to those familiar with HAZID. This tabular review table is broken down to individual tables reflecting each of the different fire stages that are applicable to the site-specific AST. The assessment record tables can be used to record summary details on hazard ranges at the fire stage, potential escalation targets and for each SECe, columns for the review of performance, survivability, contingency measures (alternative SECes), acceptability /addition measure and comments.

The guide includes example assessment tables for a fixed roof AST escalation case. Part of each example table shows potential entries, with the majority of the table providing example questions to be asked when reviewing the vulnerability of particular SECes. The example tables are just that, examples, and not planned to be used as definitive cases. This is due to the fact that the site specific nature of incidents can significantly affect the selection and vulnerability of SECes.

The overall vulnerability review and assessment process is shown in a sequence flowchart within the guide and is repeated in Figure 2 for information.

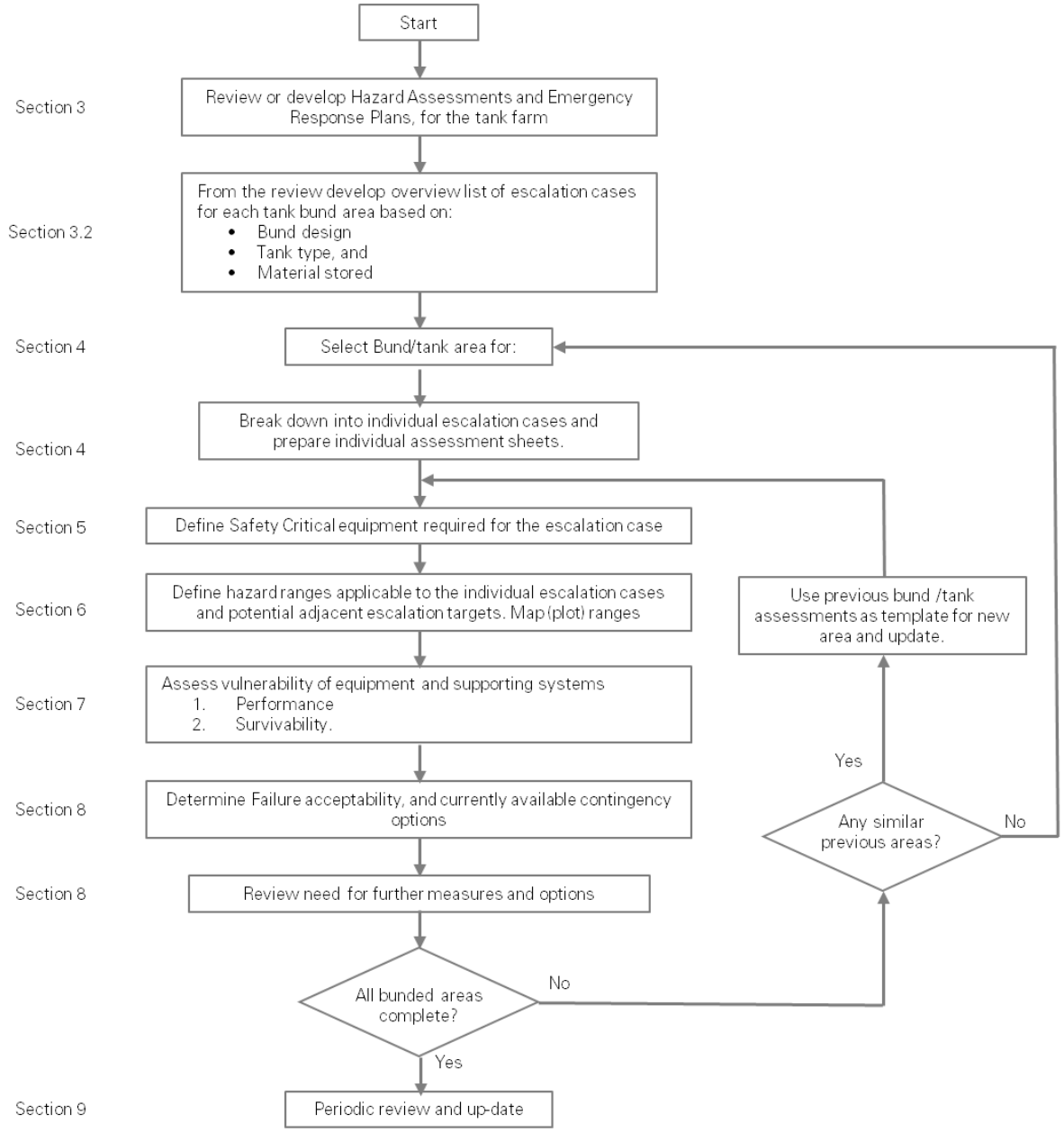

Figure 2: Vulnerability Assessment sequence (from the guide)

Summary

The vulnerability of SECe, as part of emergency response, is not just down to the ability to survive exposure to fire and explosion adverse effects. It is also the failure to ensure acceptable performance (Function, Availability and Interaction). Survivability may also be affected by environmental (NaTech) events. The requirements on and hence potential vulnerabilities of SECes is also dependent on the stage of a fire and/or explosion following an initial AST event. The focus on equipment requirements for worst case consequences could miss the importance of reviewing vulnerabilities on equipment required at earlier, smaller, fire stages such as individual tank and/or bund fires. Effective emergency response at these earlier stages can significantly reduce the likelihood for worst case events being realised.

The new EI Vulnerability guide, in additional to having a good listing of applicable Safety and Environmental Critical equipment, contains supporting information and a tabular assessment approach to enable duty holders of AST operations to review and assess the vulnerabilities to their SECes. This will enable them to comply with Recommendation 12 from the BMIIB [1] report, and will also strengthen their FEHM as outlined in EI 19 [4] particularly when reviewing and preparing site emergency response plans.

References

[1] HSE, Buncefield MIIB Recommendations on the design and operation of fuel storage sites

[2] HSE, Process Safety Leadership Group (PLSG) report ‘Safety and environmental standards for fuel storage sites. Final report’

[3] HSE, The Offshore SECE Management and Verification Inspection Guide, March 2020

[4] EI, Model code of safe practice Part 19: Fire precautions at petroleum refineries and bulk storage installations Energy Institute (a.k.a. EI 19)