How are you managing Process Safety Events? Who’s defining safety critical elements at your site?

Sylvia Layton, Yen Sham
6 October 2015
Contents

• Need for Safety Critical Elements Identification at Cenovus
• Approaches; key legislation

• Safety Critical Element Practice at Cenovus
  • Safety Critical Element (SCE) Definition
  • Current Practice
  • Application
Need for SCE Identification at Cenovus

Cenovus: Canadian integrated oil company, formed in 2009
Ongoing evolution of management systems
Focus on prioritization of resources; driven by corporate risk tolerance
Key emphasis upon Asset integrity assurance
Requirement for identification of SCE for prioritization of maintenance activities; which are safety critical?
The concept of Safety Critical Elements (SCE) originated from the Piper Alpha Disaster (UK 6 July 1988). Following his investigation, Lord Cullen’s report led to a change in the previously prescriptive legislation; introducing a risk based safety case regime including the requirement for operators to identify their own SCEs. A suite of new legislation has since been introduced from the 1990s, including Offshore Installations (Safety Case) Regulations 2005 (“SCR”) and Offshore Installations (Design & Construction) Regulations 1996 (“DCR”). DCR introduced the concept of safety critical elements; with legal definition as:

“Such parts of an installation and such parts of its plant (including computer programmes), or any part thereof – The failure of which could cause or contribute substantially to; or A purpose of which is to prevent, or limit the effect of, a major accident.”

SCR introduced the requirement for major hazard assessment as well as identification & documentation of mitigative measures to prevent and/or control major accident hazards (MAH). The identified MAHs would then form the basis for determining SCEs to be covered by the verification scheme. Performance criteria to maintain asset integrity were also introduced; Functionality, Availability, reliability, Survivability, Interaction, Dependency (FARSID).

The safety case based approach currently followed in UK, Europe and other regions.
regions comprises the steps of; safety assessment to identify the SCE; this typically includes a HAZOP (to identify risk scenarios and levels of control), followed by Bowtie analysis (helps provide structure to key elements of an MAH), Summary of Operation Boundaries (SOOB; validation of shut-down keys and actions of the SCE to prevent deviation from safe operating envelopes and thus prevent MAH), list of SCEs, performance standard and verification scheme including functional performance definition and testing, Independent and Competent Person (ICP) Verification, including witness tests, inspections, audits, review of records.

Recent UK Developments:
UK Health & Safety Executive (HSE) introduced in 2004-2007 Key Programme 3 (KP3) to oversee Asset Integrity inspections. Since that period, the data yielded through KP3 highlighted industry wide shortfalls in asset integrity management as well as key performance indicators to focus the necessary attention and resources to drive improvement.
In 2009, the following KPIs were agreed upon between HSE & the UK offshore industry and introduced: KP1 - # no of hydrocarbon releases KP2 - verification non-compliance KP3 - safety critical maintenance backlog.
Over 80% of UKCS offshore installations are participating in providing data to Oil & Gas UK who issue quarterly updates. Further information can be found here;
-Oil & Gas UK Knowledge Centre – Hydrocarbon Releases >> http://www.oilandgasuk.co.uk/Hydrocarbonreleases.cfm
OGUK are also measuring independent and competent person activity to provide update on planned verification activities: OKUK Assurance & Verification Senior Management Summary http://www.stepchangeinsafety.net/knowledgecentre/publications/publication.cfm/publicationid/88
Prescriptive Approach US Regulations

One of the primary legislation addressing SCEs is API RP 14C "Recommended Practice for Analysis, Design, Installation & Testing of Basic Surface Safety Systems for Offshore Production Platforms" (March 2007). This was incorporated as US law within 30 CFR 250.1628(c). API 14C is recognized as being very prescriptive with respect to the safety shutdowns and safety devices required for the equipment from wellhead to custody transfer to the pipeline companies. It also mandates rigorous testing of the safety devices to ensure required functionality. It does not address implementation of any safety system or framework.

Whilst the title indicates application for Offshore Facilities, API RP 14C is also being applied to onshore/upstream.

Excerpt from Petrowiki:
"The American Petroleum Institute (API) has developed RP 14, a safety-analysis approach based on a number of traditional hazards-analysis techniques such as failure-mode-effects analysis (FMEA) and hazard-and-operability studies (HAZOPS). The purpose of a safety analysis is to identify undesirable events (overpressure, leaks, liquid overflow, gas blowby, underpressure, excess temperature, direct ignition, and excess combustion vapours in firing chamber) that might pose a threat to safety and define reliable protection measures that will prevent such events or minimize their effects should they occur. Potential threats to safety are identified through proven hazards-analysis techniques that have been adapted to hydrocarbon-production processes. Recommended protective measures are common industry practices proved through many years of operating experience. The hazards analysis and protective measures have been combined into a “safety analysis” for onshore and offshore production facilities.

The RP 14C safety analysis is based on the following premises:
1. Process components function in the same manner regardless of specific facility design.
2. Each process component is analyzed for “worst case” input and output conditions.
3. If fully protected when analyzed standing alone, the analysis will be valid for that component in any configuration.
4. If every component is protected, the system will be protected.
5. When components are assembled into a system, some devices can be eliminated.

A safety analysis is required to determine:
- which undesirable event could be associated with each component
- which safety devices are required for the protection of the component
- what responses the safety devices must make to ensure adequate protection.

The safety analysis comprises of safety analysis tables (SATs), safety-analysis checklists (SACs) and safety-analysis function evaluation (SAFE) charts. SACs provide a guideline for eliminating redundant devices while maintaining the required level of protection. API RP 14C requires that two levels of protection is always in place.

Table B.1 lists Composite SATs/SACs for each component.
SAFE charts are used to evaluate the function of each safety device and to document precisely what each safety device does. For example, the SAFE chart not only shows that a flowline PSH shuts off inflow, it indicates how it shuts off inflow (e.g., through the closing of a particular well’s surface safety valve).
SAFE charts also indicate everything else that happens when a PSH trips. SAFE charts provide a mechanism for considering every component in the facility and then, for each component, to fully account for each required safety device. SAFE charts are used to ensure that the facility is as fully protected as it should be and also can be used as a troubleshooting tool.

The major benefits of this analysis are:
- Concise, easy-to-audit documentation
- Minimized subjective decisions
- Consistent results

Appendix C addresses Support Systems such as ESD, fire/gas/flame/smoke/heat detection, ventilation, containment systems & sumps, Sub-surface safety valve systems (SSSVs), and flare systems. These are described as ‘essential systems that provide a level of protection to the facility by initiating shut-in functions or reacting to minimize the consequences of released hydrocarbons’.
Appendix D specifies Testing and Reporting Procedures for each of the safety devices/systems identified.
Canada Regulations/Standards Addressing Safety Critical Elements:

There are no overarching regulations driving Safety Critical Elements within Canada, however, at provincial level, ABSA (Alberta’s pressure equipment safety authority) addresses pressure related SCEs within AB-525 ‘Overpressure Protection Requirements for Pressure Vessels and Pressure Piping’ ie Safety Critical Elements are equipment and process parameters that can have an impact on the Maximum Upset Pressure determined in the ORA (e.g. pump impellers, instrument maintenance requirements, instrument redundancy, liquid specific gravity).

For other, non-pressure related SCEs the primary guideline addressing identification and testing is Canadian Society for Chemical Engineers (CSChE) Process Safety Management Standard (PSM) which refers at a general level, to SCEs in Element 6 ‘Process & Equipment Integrity’:

‘Each facility shall:

a) Identify equipment that is critical for process safety; and

b) Establish predictive maintenance schedules for monitoring, inspection and performance testing of equipment critical to process safety to enable cost effective correction of problems before they develop to the critical stage’

Another source of guidance impacting the Canadian energy sector is The Association of Oil & Gas Producers (OGP) – of which the Canadian Association of Petroleum Producers is a member - which published ‘Asset Integrity – the key to managing major incident risks’ for new and existing upstream assets. It proposes use of the Swiss Cheese model using barriers which include functional groupings of safeguards; Prevention, Detection, Control and Mitigation. Following this grouping, the OGP guidance proposes additional evaluation to define barriers at a system level, and then define the performance requirements, standards and testing for each barrier.

None of the Canadian based guidelines or regulations mentioned above specify testing methods/frequencies (as required in US) nor do they refer to verification of competency of persons completing the SCE performance testing (as required in UK).

Informal feedback indicates that the practice of SCE identification/testing is in its infancy throughout Canada.

It should also be noted that the August 2014 CAPP report on ‘Process Safety Management: Regulatory Scan’ includes a recommendation, as part of its 5 year strategic plan, for goal oriented PSM regulations, including identification, inspection and maintenance of Safety Critical Components. This report also recommends the use of bow-tie analysis within risk assessments.
Options Available

**Prescriptive approach**
- Quick and easy to apply
- SCE list is somewhat conservative *(and by how much?)*

**Risk based approach**
- SCE list is more defined
- Less costly to maintain
- Higher upfront engineering costs
- Takes *TIME and EXPERTISE*

Our situation: We are moving to the risk based approach, however, in the meantime.....
Cenovus SCE Definition

Safety Critical Elements are any devices, equipment, system, engineering or other administrative control that are required to ensure process conditions are maintained within safe operating limits, or the purpose of which is to prevent, or limit, the effect(s) of a Process Safety Event (PSE).

- PSE = event such as: major release, fire/explosion resulting from uncontrolled operation of facility; leading to fatalities/serious personnel injury/significant property or environmental damage.
- We added the filter of PSE risk rating level = Extreme or High against the Cenovus corporate risk matrix.
- *Addresses current AB 525 requirements relating to overpressure related SCEs.

The latter part of this definition includes items such as Emergency power systems, horns/beacons, firewater suppression systems. Further, the above definition addresses Cenovus’ interpretation of current AB-525 requirements with regard to overpressure related SCEs. This will be reviewed upon any changes to the AB-525 definition.
Development of Cenovus’s Safety Critical Element Identification Practice

• Main objective: to improve prioritization/allocation of asset integrity assurance activities
  • Also provides formal definition for safety critical elements and a basis to modify as required
  • Prescriptive approach
    • SCEs tabulated and categorized based on function
  • Incorporated a validation step against past Process Hazard Analyses

After much research on the different methods and legislations from other jurisdictions, we decided the best approach for our company at this time is to use a PRESCRIPTIVE METHOD. We did our due diligence by validating our process against a risk based approach, as discussed later, using past HAZOPS.
The above table is an excerpt from our Safety Critical Elements Identification Practice prescriptive tables. The prescriptive tables are based on API RP 14C. We chose to categorize these SCEs a little differently than API RP 14C, basing them on their function rather than process components. There are the obvious categories such as Pressure Relief Devices which consists of PSVs, PVSVs, Pressure switches and transmitters for pipelines; all used for overpressure protection. The category for Emergency Evacuation was included as an example of a mitigative safeguard; which are ones that help with recovery after a loss of containment, recovery from fire & explosion, or used for emergency response, etc. API RP 14C also mentions of supporting systems that are essential systems that provide a level of protection by initiating shut-in functions. We went a little further by specifying the major pieces of equipment that could fail catastrophically and their associated shutdowns. Examples would be Fired Heaters, Flare Stacks, Compressors and Pumps. Notes were added to indicate any exclusions, for example only pumps that move flammable or hazardous fluids and notes referring to other tools that could be used, such as shutdown keys to find the associated shutdown devices.
As discussed earlier, one major step in the development of Cenovus’s Safety Critical Element Identification Practice was a validation test. We validated the prescriptive tables against a risked based approach but not to the extent that is required by the UK due to limited time and resources; we did not complete a bowtie analysis or validating shutdown keys for SCE actions, etc. We used previously completed HAZOPs and reviewed the scenarios with risk exposures before applying safeguards) that were EXTREME or HIGH according to our corporate risk matrix. In reviewing the list of safeguards identified during the HAZOP, we pinpointed the “last line of defense” device (as M&R was our major stakeholder, we wanted to identify devices that could be maintained and function tested; administrative controls such as critical procedures are managed under another management system) and this device(s) was considered the safety critical element(s) for that scenario.

A simple example would be to consider a tank containing hazardous/toxic commodity, with a pump installed on the discharge line. The scenario would be a blocked inlet to the pump with the consequence being a loss of containment. This would be a high risk exposure due to the toxicity of the fluid if it were to be released. The design will have some safeguards in place to protect equipment but can also be used as prevention for a PSE. Safeguards listed would include FALL, PALL/PAHH but by following the process back to the tank, our last line of defense would be the level device on the tank. The LAHH will be our SCE. Note that the FALL, PALL/PAHH, etc would be critical to safety as they are used to reduce the risk exposure but the LAHH would have a higher priority to ensure that it would function properly when
needed. To emphasize, maintenance plans will be in place for all assets/devices, however safety critical elements would have the highest priority.
Another part of our validation test included comparing the results from the different approaches and to what was listed as high priority in our asset management database. We reviewed one area of one of our operating facilities and compared the SCEs identified using the prescriptive tables (green circle) and reviewing the HAZOP notes (red circle). We compared the two lists with our current list of SCEs (blue circle) which was ranked by our asset integrity group without a very clear definition of what is safety critical. The results showed that we were providing higher standards of maintenance to assets that didn’t require it. 75% of our high priority assets were identified as SCEs using our prescriptive table but only 35% were identified as SCEs as per our HAZOP review. By comparing the prescriptive approach with the risked based approach, we were able to get an idea of how conservative we may be using a prescriptive method (prescriptive approach identified more devices as SCEs than the risked based approach). Another point of interest was the overlap of the risked based approach and the prescriptive approach. This indicated the common SCEs found using both the prescriptive tables as one would if one completed a risk assessment, therefore it gave us an opportunity to update our prescriptive tables to include the missing categories to ensure that we were not missing any devices that were identified as the last line of defense from a risked based approach.
By putting some numbers to our results, we are able to show the effects of having a clear definition of what safety critical elements are and having a tool to identifying them. The above graphs show an example of the effect at one of our operating facilities, before and after applying the prescriptive tool to identifying safety critical elements. At this particular facility, we have over 65,000 assets. By defining what is safety critical and providing our asset integrity group with the tool to identify them, they were able to re-prioritize and reduce the number of extreme (1) and high (2) ranked assets (where safety critical elements would be prioritized) down by 10%. These assets would have had PMs assigned to them and there would be measurements in place to ensure that they were completed on time and tested to a certain standard. The lower priority assets (shown in green and yellow) were assets that had PMs assigned but would not be to the same frequency or to the same testing standards.

In conclusion, by defining what is a safety critical element and providing a prescriptive tool to use to identify what is safety critical, our operators, our maintenance and reliability team, and our engineers have a robust understanding of what is safety critical and which devices are necessary to prevent or limit the effects of a process safety event. It allows us to provide consistency across the different operating facilities and to any new phases or designs and allows for us to set a baseline for future refinement as we continue to evolve to a risk based approach. Our practice, although it may represent a conservative approach, but through our validation and refinement, we are confident that we can maintain safe operations of our facilities and
sleep at night.
Questions for the Audience; Hand-out

1) Is your company using prescriptive/risk based/haven’t decided?

2) For either risk based or prescriptive; is this formalised?

3) What % of your sites have you evaluated for SCEs?

4) Where are you based? Canada or international?
10.0 References:
http://petrowiki.org/Recommended_methods_for_safety_analysis
Major Hazard (Asset Integrity) Key Performance Indicators in use in the UK Offshore Oil and Gas Industry; Bob Lauder – Health & Safety Policy Manager – Oil & Gas UK: CSB Meeting – Houston – 23 & 24 July 2012

ABSA AB-525 Overpressure Protection Requirements for Pressure Vessels and Pressure Piping.
Asset Integrity – the key to managing Major Incident Risk; International Association of Oil & Gas Producers, Report # 415, December 2008.
www.emersonprocessexperts.com; Jim Cahill’ The Prescriptive Approach to Process Safety for Oil & Gas Producers.
Canadian Association of Petroleum Producers “Process Safety Management: Regulatory Scan” August 2014