Process Safety Management Implementation at a Mature Asset: An unconventional approach to rapid and effective improvement

Peter Wilkinson
General Manager - Risk
Noetic Group
Equinox 3, 70 Kent Street, Canberra, ACT 2600, Australia

Abstract

This paper describes how process safety management (PSM) was improved at a mature asset following a significant process safety event. An unconventional approach was adopted to enable rapid improvements, drawing on the "Critical Control Approach" (CCA) documented in ENFORM's *A Barrier Focused Approach* (similar to the International Council of Mining and Metals (ICMM) publication, *Critical Control Management; Implementation Guide*) as well as high reliability organisational (HRO) principles.

The revised approach owes its intellectual origins to the concept of "safety critical elements" (SCEs) first enunciated by the United Kingdom (UK) Health and Safety Executive (HSE) following the Piper Alpha disaster, in 1988. The history of the CCA is briefly discussed and how the original SCE idea has been enhanced. In particular, the paper will describe how the critical controls (or barriers) have been made more "visible" to those charged with implementing and managing them.

The paper will describe the successes and difficulties of this approach including the shift in thinking required on the part of process safety experts as well as changes to organisational structure. The paper will also illustrate how the existing documentation of the critical controls was substantially reduced and rationalised to make the "PSM problem" (as perceived by senior managers) more manageable and sustainable.

Finally, the paper will consider the extent to which well-known international PSM frameworks contribute or inhibit the adoption of this approach.

Introduction

This paper describes how process safety management (PSM) was improved on a number of sites by applying the Critical Control Approach (CCA), also known as the "barrier focused approach" (ENFORM, 2016). It will describe how this has been applied in different industry sectors and the lessons learnt. The paper covers the essential elements of the CCA including those aspects which were regarded by some as unorthodox. The genesis, development and implementation of the critical control idea is also briefly covered.

The catalyst for the implementation of the CCA was a major process safety incident in a company that was implementing process safety improvements in a deliberate, highly structured manner. The objective of the CCA was to improve the implementation of those risk controls that really matter to major incident prevention and to make progress as rapidly as possible. This was achieved in four main ways. First, by identifying and then focusing on those controls which were crucial to preventing or mitigating the consequences of a major incident. Second, by ensuring the most important details of the critical controls was clear to all those in the workforce who interact with them. Third, by introducing a rigorous routine of checking to ensure these critical controls are working as intended. Finally, by reporting the results of this checking to all involved; especially senior managers. There were two aspects of the CCA approach which proved controversial to some observers. These involved reducing the number of controls presented on bowtie diagrams to allow a stronger focus on a smaller number of critical controls (in apparent contradiction of the defence in depth mantra) and summarising the essential aspects of each critical control on a single page. The following accounts brings together experience gleaned over the last 8 years from implementing this approach in a variety of "brown field" situations.

Background – the problem

Almost a decade ago, the Operations Manager of a listed Australian oil company asked how risk controls for major incidents could be more effectively implemented. Following the Piper Alpha disaster, significant improvements were made to formal safety assessments and in turn, to *identifying* the controls needed to prevent major incidents. However, his main concern was it was not clear that *implementation* of the risk controls had seen an equivalent improvement. Familiar types of incidents were repeated. What should have been well known controls for well-known

risks were apparently not well known and even where the controls were identified, they were not implemented effectively. Trevor Kletz memorably summarized this in the title of his 1993 book; “Lessons from Disaster: How Organisations Have No Memory and Accidents Recur” (Kletz, 1993).

The introduction of the safety case approach to managing operational risk was a game changer. It removed much of the prescription and permitted needed innovation; forced companies to think through their hazards, risks and controls; and developed more formal safety management systems. This was all beneficial. Similarly, Quantitative Risk Assessment (QRA) had limited but important benefits such as comparing the relative level of risk for different platform concepts at the design stage. But despite the improvements in designs and the quality of the formal safety assessments, one important problem persisted – namely the quality of risk control implementation at the operational level. Something different was needed.

Part of the problem was the volume of paperwork. Formal Safety Assessments, safety management systems, more and more procedures all added to the paperwork. But there was another subtler aspect to the problem. Part of the safety case system was the introduction of safety critical elements (SCEs). SCEs are defined by the United Kingdom (UK) Health and Safety Executive (HSE) as “… major hazard risk control measures … and the performance required of them” (UK HSE, n.d.). This was an important innovation. The concept of SCEs explicitly involves selecting those controls which impact on major hazards.

However somewhere along the line, ‘SCE’ had become safety critical *equipment*. The requirement for performance standards may have inadvertently encouraged this. This was because regulatory guidance expected performance standards (a fundamentally sound concept) to be couched in predominantly engineering terms such as “functionality, availability, reliability, survivability” etc. But when one came to look at the numbers, the performance standards claimed all of the equipment operated at 99.975% reliability and was available for 99.95% of the time. But there were other problems too. QRA always seemed to predict risks between 1x10-4 and 1x10-5. The bowties were growing in size – one operator showed 10 bowties each with over 75 controls.

None of this helped operationalize the controls once the bowtie was produced. Safety cases often stated that the engineering controls or safety critical equipment was managed predominantly by the maintenance management system. But non-engineering risk controls, which were not typically classed as SCEs, tended to be managed by ‘procedures’. Many are poorly written, overly long, start with the control history of the document and most importantly do not emphasise what really matters. The twenty-nine-page procedure for small bore tubing produced by a major company was a classic of its kind. Yes, we now had much more rigorous risk assessment and more information, especially on the equipment, but did this coincide with better risk control implementation?

Researching the Problem

Colleagues seemed to agree there was a problem and a variety of solutions were articulated. Nobody argued against the importance of robust hazard and risk assessment procedures as the starting point for identifying the controls. Some emphasised the explanatory power of bowties and their ability to illustrate where a particular control fitted into the broader prevention strategy. Some focused on the importance of identifying the accountabilities (usually by job title) for controls and making these accountabilities known to the workforce (at multiple levels). Using lead and lag indicators for measuring control systems was seen as the answer by others and the literature on the methods of doing this increased after the British Petroleum (BP) Texas City disaster.

There was no disagreement with any of these points. All are needed but we were not convinced they really did enough to solve the control implementation problem. From our perspective, hazard identification, risk assessment, identifying controls and putting them on a bowtie was the easy part! But control implementation was qualitatively different. For example, hazard and operability studies (HAZOPs) are typically carried out by a group of experienced personnel, under the leadership of an independent HAZOP chair. This process may take a few days, weeks or months. Sometimes it took even longer to catch up with a backlog. But even so, this was still easier than implementing the controls faithfully over two or three shifts each day over the remaining life of the facility (perhaps 20 years or more). Added to this are the almost inevitable organizational changes such as new owners, cost reduction initiatives and the turnover of staff. All of which make reliable implementation of controls over a long period difficult.

Something more radical was needed. In particular, something simpler, shorter, easier to manage but still sufficient to provide indication of how the controls themselves were working – not just the high-level systems such as the maintenance management system, the management of change system or the usual favourite, the permit to work system. We wanted to go to the heart of the matter – which are the most important controls, the critical controls.

Furthermore, how 'visible' are these to the workforce, amidst all the other documents, how well are they working and is this information reported on to the most senior managers?

The answer came from a number of sources. Perhaps the three most important were:

+ BHP Billiton's (BHP) focus on critical controls in their internal risk management system
+ The ideas espoused in the UK HSE's guidance on Developing Process Safety Indicators (UK HSE, 2006)
+ The Barrier Analysis Matrix (Corcoran, 2007)

BHP had given some thought to the critical control idea and were applying the concept to their most significant risks and produced a flow chart (ICMM, Critical Control Management: Implementation Guide, 2015). In other words, they had explicitly decided some controls were more important than others and suggested a method of identifying these. In 2006, the UK HSE produced guidance on developing process safety indicators. This suggested: "A small number of carefully chosen indicators can monitor the status of key systems and provide an early warning should controls deteriorate dangerously" (UK HSE, 2006). This was intriguing as it seemed consciously or unconsciously, to echo some of the quality theorists' writings of the 1980s and 1990s including the importance of the knowledge of "variation." In particular the idea that one does not need to measure everything to understand how a system worked (including in process safety) offered the possibility of reducing the paperwork burden. Finally, Corcoran's work is discussed in the context of the Pantex guide to avoiding the system accident by applying high reliability organization (HRO) concepts (B&W Pantex, 2009). This led to some ideas on how information could be organized in a simplified more practical and useable way.

It was at this point (at least from this author's perspective) that the International Council of Mining and Metals (ICMM) entered the scene and we found out lots of others were working on this problem too. Their safety committee had pondered similar questions and commissioned work from a respected academic and consultancy firm. This led to the publication of their Health and Safety Critical Control Good Practice Guide (ICMM, Health and safety Critical Control Guide, 2015), in which this author played a small part as the technical editor. This was followed by ICMM's Critical Control Implementation Guide (ICMM, Critical Control Management: Implementation Guide, 2015). It should be emphasized that this was our journey to coming up with a solution and we fully understand that others will naturally and quite legitimately feel ownership of the ideas and how they are described below. We all stand on each other's shoulders.

What is the Critical Control Approach (CCA)?

The focus for what follows is applying the CCA in a 'brown field' situation. Where examples are given, they are taken from a range of companies in the process industries including upstream petroleum and mining processing.

The CCA can be seen as a modified version of what is currently and typically done. However, it differs in a number of qualitative but important ways. For example, rigorous hazard identification and risk assessment using appropriate tools and techniques is still required. However, it accepts that risk control improvements can still take place even if the hazard identification and risk assessment have not taken place or are not complete. This is because there are numerous actions that can be taken whether or not formal hazard identification (HAZID) and risk assessment techniques have been completed based on experience, data and standards.

The CCA approach accepts that too many controls can make it difficult to manage controls effectively. The CCA method recognises that less can be more (Hoffman & Wilkinson, 2011) and applies a methodology to identify the *critical* controls. Once these are identified, the essential elements of the critical controls are summarised on one A4 page critical control data sheet. The essential elements include the technical aspects of the control, any maintenance requirements, human and organisational aspects, including accountabilities and how the critical control is to be checked and reported upon. In this way the technical (or engineering), human factors associated with individual skills and their application, and the organisational aspects of monitoring and reporting on the controls is documented and integrated in a succinct document. Finally, the CCA provides guidance on suitable senior management practices (sometimes referred to as 'behaviours') to support and drive the CCA. The next section discusses each of these points.

Is Hazard Identification and Risk Control the Starting Point?

Ideally yes, but we are rarely in an ideal world. At one site which had experienced a number of serious process safety events, PSM implementation was focused on hazard identification and risk assessment and less on making field improvements to controls. Part of the reason for this was an assumption that one follows the other. Hazard identification and risk assessment is of course very important. However, it does not mean that PSM improvements cannot be made in parallel to carrying out process hazard analyses (PHAs). For example, if a company uses methane at 110 bar, we do not need to carry out a risk assessment to know that it makes sense to have a program to

manage high pressure flanges. We can, and should, draw on published data, standards and experience to make improvements which can be done in parallel with doing hazard identification and risk assessment process.

Controls, Critical Controls and Bowties

The CCA approach explicitly advocates an approach which says that some controls are more important than others. Critical controls are:

"controls that are crucial to preventing or mitigating the consequences of… [a major incident]. The absence or failure of a critical control will significantly increase the risk of … [a major incident] … occurring, despite the existence of the other controls." (ICMM, Critical Control Management: Implementation Guide, 2015).

For example, a bowtie produced by an upstream oil and gas company had as the 'top event', a loss of containment (LOC) of process fluids including oil and gas under pressure. One of the controls, in relation to the make of joints in the process pipework, was the companywide job hazard analysis (JHA) tool that was intended to be applied to all tasks before starting work. It was based on the premise that by taking 5 steps back from the job and spending 5 minutes to think through the work, that this will improve hazard management. When interrogated further, it was found that there was nothing specific in this tool about making up joints. This was a companywide tool which did not need to be on the bowtie and was removed in favour of specific guidance (one page – discussed below) on joint make up.

There was an interesting discussion with the process safety team on this approach. Their initial reaction was one of concern when the JHA was removed from the bowtie because this reduced defence in depth. On reflection, however, it was accepted that the JHA control (which appeared multiple times on the bowtie) was not specific to the risk, made the bowties more complicated than need be and tended to overstate the quantity of controls in place. There were many other examples of generic controls appearing on bowties which did not materially contribute to hazard management.

Critical Control Data Sheets (CCDS)

At the heart of this approach and arguably the most important part of the CCA approach is the concept of the critical control data sheet (CCDS). In many companies, the transition from the bowtie to field operations is often made by reference to procedures and/or maintenance routines described in the maintenance management system. However, we have often found this is one of the weakest areas of the hazard management process due to the volume of information and the difficulty of discerning what really matters in procedures and hence using them in practice in the field. The CCDS is a one-page document which summarises the essential elements of the control and is explicitly intended to make the key parts of each critical control clear in a succinct document. It also provides the basis of reporting, which is discussed later.

The CCDS contains the following important information:

- the name of the major hazard the critical control relates to
- the "owner" for the hazard (or risk) at a senior level
- the name of the critical control (plus a unique identifying number)
- who is accountable for ensuring the critical control is effectively implemented
- the purpose of the critical control and performance criteria for the control or put another way, what it has to achieve to be effective
- how to check the critical control is working as intended
- who is responsible for carrying out this checking (normally one of the control owners team)
- the frequency of carrying out the checking and reporting on its status to the control owner

The one-page CCDS provides all the essential information to enable the control to be managed, including accountabilities, how it is to be implemented, checked and reported. An example of a CCDS is provided in Figure 1. This is in marked contrast to the previously discussed SCEs, which are predominantly engineering focused. However, as is acknowledged by the International Association of Oil and Gas Producers, (IOGP), "barriers" (a synonym for controls), "…typically includes a mix of plant (equipment), process (documented and 'custom and practice') and people (personal skills and their application)." (IOGP, 2008)

The CCDS provides this in a succinct way which is much easier to use, including on hand held devices in the field. Furthermore, by providing a copy of the simplified bowtie and a succinct account of an example of how this control has failed in the past (either from the company's records or from published sources), the document can provide additional context and rationale to the user as to why the control and its checking is important. Humans tend to do

things more reliably when not merely instructed to do something but are given the reasons and context for doing so. This is a practical application of human and organisational factors (HOF) applied to risk control management.

Process safety hazard	
Critical control	
Threat	
Control owner	
Control objective	

Activities to achieve control objective	**Performed by**	**Method of verification**	**Verified by**
Description of activity to achieve a healthy control	*Title of person who carries out the activity*	*Method to verify the activity has been performed correctly*	*Title of person who performs the verification*

Additional Information	
Performance criteria	

Figure 1: Critical control data sheet – example template

Developing the Critical Control Data Sheets

The process for developing the CCDS is a critical step. How was it possible to reduce a multi-page procedure to one page of A4? The key was to have people present in the room with relevant operational knowledge, supplemented by subject matter expertise in process safety. The right mix of skills and knowledge needed was remarkably similar to that needed for a HAZOP. Operations, maintenance, subject matter experts as well as front line supervisors and members of the workforce. As with HAZOPs an independent chair proved helpful and understanding of the CCA was essential.

An early criticism of the CCA from those with knowledge of HRO principles was that we would lose important details by using the one-page CCDS. The reverse happened in practice. Much of the content of the procedure was relevant but not essential to help manage the control. The procedures have not been removed so the information is not lost. However, using the CCDS template encouraged discussion on the key elements of the control. This included defining what the control had to do to achieve its objective as well as getting clarity around accountabilities for the control. For example, in one plant a fan was important to remove toxic and flammable gas from a closed drain. One of the checks was to check the fan was working as intended. When this aspect of the control was discussed, a question was raised as to why it was not possible to provide a range of quantitative values for the differential pressure across the fan. It was quickly found that values for the differential pressure range which indicated the fan was working effectively,

differential pressures requiring further investigation and ones requiring shutdown could be calculated and these were added to the elements of the critical control on the one-page CCDS. Important detail was not lost but added.

Checking the Critical Controls and Reporting

As described above, the CCA identifies the hazard (or risk) owner, the control owner and who is to do the checking of the critical control. All of these are line management roles. The assumption is that the line management is responsible for managing process safety, as with other aspects of health, safety and environment, and it is their responsibility to implement the critical controls effectively. An important aspect of this is checking (or monitoring) that the critical control is working as intended. Our experience with over a number of companies and industrial sectors is that the hazard (or risk) owner concept works best when this role is held at a senior level. Control owners are generally the direct reports of the hazard owner (typically superintendents). In turn, responsibility for the checking controls is typically allocated to the most appropriate member of the superintendent's team, depending on the nature of the control and the knowledge required. Reporting on the results of the checks provides a direct indication of the "health" or effectiveness of the critical controls. This is a key benefit of the CCA approach. Lead and lag indicators about the maintenance system or "challenges to barriers" (API, 2016) are described in various guides to process safety indicators. These are useful but should be supplemented by a more direct measure of the performance of the critical controls which this methodology provides.

Business 'rules' on how the reporting is done have proved essential. Reporting is best integrated into existing systems of reporting and most organisations choose to do this by some form of traffic light reporting. A typical approach is that if the control has not been checked as scheduled, it cannot be 'green' and must be 'amber' or 'red'. Green means the critical control was checked on schedule and all aspects of the critical control were working as intended. Rules to determine red and amber are also required. An important learning was that some space should be provided to allow some limited commentary on why it was green, amber or red. This proved very important. It enabled people to report problems but simultaneously explain what was being done about it. An unanticipated aspect of the requirement for a short explanation to supplement the colour was that there was sometimes an inconsistency between the colour and what was reported. The discussion that followed at the leadership team table usually provided useful insights to how the control was managed.

How leaders react to the reporting is, of course, a very important aspect of organisational culture and well-trod ground in the literature (Hopkins & Maslen, 2015) and is not covered again here. Suffice to say that we know that negative reactions to bad news is liable to deter reporting of such valuable information. The reporting of bad news must be welcomed and seen as an opportunity to improve. At one site, senior leaders have been encouraged on their 'field' visits to comment favourably on the ambers and reds but to pay particular attention to the greens. Why are they green, what has gone right and to check that they really deserve that status in the reporting?

Organisational Factors

At one site, the PSM team had been running the PSM project, with at best limited traction from line managers. This was changed and responsibility was given to a team of line managers supported by the PSM experts. This was not universally welcomed initially by the process safety specialists, but it transferred responsibility to the line while still leaving the PSM experts to advise. This is the conventional approach to safety and other business support functions such as human resources. Crucially, it provided an opportunity to integrate the PSM work into the broader asset management arrangements including 'Lean Manufacturing' techniques with PSM progress reported on lean boards around the plant.

This was more important than was first realised. To line managers, PSM experts can sometimes appear to be from a different world. In QRA we sometimes talk in a strange language talking about the risk to "hypothetical" or "statistical" people when conversing on individual risk in the context of QRA or use mathematical notations in an unusual way when talking about probability. Much of this is somewhat removed from many managers experience. However, the line managers in the PSM implementation team proved to be excellent translators of this PSM jargon and integrated the work to simplify bowties, getting frontline experience into the one-page summaries.

Lessons Learned

Our experience is that all those who have used the CCA have found it to be of great value. For the first time, all key information needed to manage a critical control has been provided in a single succinct document. There were two important factors which seemed to influence people's views on the CCA. Firstly, whether or not they had experienced a major process safety event. Those that had, listened intently and were happy to try and apply the critical control approach. Those who had not experienced a serious process safety event (even in the same company) were much less interested. This will be familiar to many readers and not discussed further. Secondly, there seemed to be a distinct difference between senior managers and safety professionals. Senior managers liked the apparent simplicity of the CCA approach and they also saw parallels with the work they already had underway on quality and existing business reporting systems. Measuring the variance of inputs compared with the intended inputs to a manufacturing

process was a core concept to many from their “lean manufacturing” experience. At its heart, the CCA requires performance criteria to be defined for the controls. This enables the variance between what is required and what is actually being achieved to be identified. This variance is a measure of how well the critical controls are being implemented. The variance can also be regarded as a ‘weak signal’ in high reliability organizational theory and practice (Sutcliffe & Weick, 2011).

Summary

In some ways there is nothing new in the CCA. All of the components described have long been in regular use except the one-page CCDS as the basis of managing the hazard. What is relatively new though is the documentation of the CCA and how it can be applied. Before the aforementioned ICMM and ENFORM documents, there was no documented description of the process. This is an important step from a number of perspectives. This makes the approach subject to peer review. Challenging the ideas is fundamental to progress. Finally, compared with other methods of developing safety indicators, this approach to reporting on process safety is not dependent on lagging measures such as losses of primary containment (API, 2016), “…challenges to barrier systems…” (API, 2016) or even the three types of so called lag and lead measures advocated in the UK HSE guidance on developing process safety indicators (UK HSE, 2006). Reporting on the ‘health’ of the critical controls provides a much more direct measure of risk control.

References

(API) American Petroleum Institute, 2016, ‘API Recommended Practice 754 – Process Safety Performance Indicators for the Refining and Petrochemical Industries’.

B&W Pantex, 2009, ‘High Reliability Operations: A Practical Guide to Avoid the System Accident’, United States Department of Energy.

Corcoran, W, R., 2007. ‘The Phoenix Handbook’, NRSC Corporation.

ENFORM, 2016, ‘A Barrier Focused Approach: How to Get Started with Process Safety, Vol.2’, viewed 26 March 2018, <http://www.enform.ca/files/A_Barrier_Focused_Approach-_How_to_get_started_V2_FINAL.pdf>

Hoffman, I., Wilkinson, P., 2011, ‘The barrier-based system for major accident prevention: a system dynamics analysis’, in Lyneis, J., *29th International Conference of the System Dynamics Society 2011*, Systems Dynamics Society, Red Hook, NY, pp. 1441-1459.

Hopkins, A., Maslen, S., 2015, ‘Risky Rewards: How Company Bonuses Affect Safety’, CRC Press.

(ICMM) International Council on Mining and Metals, 2015, ‘Critical Control Management: Implementation Guide’, International Council on Mining and Metals, London.

(ICMM) International Council on Mining and Metals, 2015, ‘Health and safety Critical Control Guide’, International Council on Mining and Metals, London.

(IOGP) International Association of Oil and Gas Producers, 2008. ‘Asset integrity – the key to managing major incident risks’, viewed 23 March 2018
<http://www.learnfromaccidents.com.gridhosted.co.uk/images/uploads/OGP_415_asset_integrity_the_key.pdf >

Kletz, T., 1993, ‘Lessons from Disaster: How Organisations Have No Memory and Accidents Recur’, The Institution of Chemical Engineers, Rugby.

Sutcliffe, K., Weick, K., 2011. ‘Managing the Unexpected: Resilient Performance in an Age of Uncertainty’, John Wiley & Sons. KENFORM

(UK HSE) UK Health and Safety Executive, n.d., ‘HID Inspection Guide Offshore: Inspection of Safety Critical Element Management and Verification’, viewed 21 March 2018, <http://www.hse.gov.uk/offshore/ed-sce-management-and-verification.pdf>

(UK HSE) UK Health and Safety Executive, 2006, ‘Developing process safety indicators: A step-by-step guide for chemical and major hazard industries’, HSE Books.