CHEMICAL ENGINEERING TRANSACTIONS
VOL. 77, 2019
A publication of AIDIC
The Italian Association of Chemical Engineering
Online at www.cetjournal.it
Guest Editors: Genserik Reniers, Bruno Fabiano

ISBN 978-88-95608-74-7; **ISSN** 2283-9216
DOI: 10.3303/CET1977074

Common Failures in Management of Change

Ian Clarke

Swiss Re Corporate Solutions, 30 St Mary Axe, London, EC3A 8EP
ian_clarke@swissre.com

As a Risk Engineer working in the insurance industry for nearly 25 years I have had the pleasure of visiting many operating onshore and offshore assets, as well as many others under construction, over the last few decades.
With the possible exception of permit to work systems, I doubt if I see a process safety management element abused more frequently than Management of Change (MoC). The control of changes, be it hardware, software, procedural or personnel, permanent or temporary, planned or emergency, seems to be a conundrum designed to trap not only the unwary but also the experienced plant operators.
There are as many different MoC systems as there are organisations, and there is no magic bullet or approved system. If there were, I assume everybody would be using it. Some are electronic, and some are paper-based. There is no right answer, but there are critical features that are essential in order to implement an effective MoC system.
In this presentation, I will cover these critical features of MoC systems and some of the common pitfalls. I will explain what we in the insurance world look for, and what we frequently find, both good and not so good. Finally, I will give an example from my own time in industry, which perfectly demonstrates the difficulties of implementing an effective MoC system.

1. Introduction

MoC is just one element of a process safety management system (PSMS) implemented by Operators to control risks. In many ways some of the other common PSMS elements could be considered to be a subset of MoC. As an example, the permit to work (PTW) and associated isolation controls such as lock-out tag-out (LOTO) are controls to manage the changes involved in the process of carrying out maintenance tasks on equipment.
For the purpose of this discussion we will restrict ourselves to the formal control arrangements around the MoC procedure and system itself, with one exception. Within the scope of this presentation is a limited discussion of the challenges around controlling bypasses of control systems, specifically how it relates to MoC. The reason for this is that there is significant overlap between the two control systems, and in fact for some Operators I have encountered they are part of the same management system. Other PSMS elements will not be considered as part of the scope. The various aspects of MoC that will be covered are policy, types of changes, safety reviews required, procedure and control, and finally key performance indicators (KPIs) around measurement of the efficacy of the MoC system.

2. MoC Policy

It is important that MoC is covered by an effective policy and procedure (see later section). Many organisations that have defined PSMS, particularly those that are regulated by the European Seveso (Safety Case) regime, define MoC within this framework.
The MoC policy should enshrine the most important elements of an MoC system, which are a definition of change, the requirement for a structured safety review, how the changes are managed, and finally how the system is audited and its efficacy measured.
We will now cover each of these areas in turn.

Paper Received: 21 December 2018; Revised: 15 April 2019; Accepted: 3 July 2019

Please cite this article as: Clarke I., 2019, Common Failures in Management of Change, Chemical Engineering Transactions, 77, 439-444 DOI:10.3303/CET1977074

3. Types of Changes

Hardware Changes

Hardware changes are the easiest ones to control and most sites I have visited have at least this part of the process (or components of it) in place. Changes are frequently defined as "any process or technological change that is not like-for-like", but this definition is quite simplistic.

A change in technology or process, or major change to equipment, is obviously a significant change. However, grey areas soon start to appear. Changing one valve for another, as an example, is a change I have seen made without an MoC. Similarly, in one extreme example, the change of one pump type for a different type was not deemed sufficiently worthy of an MoC. Finally, often we see upgrades to materials, particularly process piping to eliminate potential corrosion exposures, but these are still hardware changes that should be subject to MoC.

Many large losses over the years have been caused by the failure of MoC systems, most notably the incident at Flixborough in 1974. Often the reluctance of organisations to properly implement their MoC system correctly can be because of the system itself or the time required to initiate the process. I will return to this point later on.

Software Changes

Changes to systems, procedures and other management controls are deemed to be software changes for the purposes of this paper. The most obvious of these are changes to operating procedures, whether standard or emergency, or to process or equipment settings.

Most organisations review operating procedures at set intervals, or if there is a change in the process itself which necessitates a review. These intervals are (typically) every year for emergency operating procedures (EOPs) and every three years for standard operating procedures (SOPs). These reviews more typically seek to validate that the SOP or EOP is still valid, rather than proposing any changes. If changes are made these should be subject to an appropriate level of hazard analysis, although this is not frequently observed in my experience.

Changes to process and equipment settings can sometimes be easy to control and in other cases difficult. Most organisations will maintain controlled lists of alarm set points, often within the distributed control system (DCS) which can only be changed after appropriate review and analysis. Similarly for trip or emergency shut down (ESD) settings, which in many cases may be a hard wired system separate from the DCS. However, other management controls may not be as well protected. A good example is the setting of integrity operating windows (IOWs) which are developed in conjunction with inspection and/or process engineering. IOWs are intended to define the limits within which the process can be allowed to fluctuate for mechanical integrity, operational or product quality reasons. Control of the changing of these parameters at most facilities is, in my experience, nowhere near as stringent as process or equipment alarm settings, and these set points can frequently be changed within the DCS by the panel operator with only nominal referral. Unfortunately, extended operations outside of the optimum process conditions, even if "safe" from an immediate process upset perspective, can often have damaging effects on equipment longer term. A good example is reformer and/or furnace tubes, which suffer rapidly accelerated creep damage if exposed to temperatures even slightly above recommended operating levels, and this can drastically shorten tube life as a result.

Organisational changes are more difficult to control, and are frequently managed by a separate process outside of the MoC system. This is not a problem, so long as the change process is managed and appropriately risk assessed. There are a number of losses that had their origin in organisational change, the most notorious being the Exxon Longford explosion and fire. The investigative report following this incident was very critical of the Exxon decision to relocate engineering staff away from the plant to the Head Office some 200 km from the site, concluding that the absence of engineering oversight was a key contributor to the incident.

Deviations from the required number of barrier controls is a breakdown in control philosophy rather than a single change to a protective system. The barrier philosophy will require protective systems to function as intended but the decision to remove these barriers may include compromising procedural or hardware controls. The most obvious recent example was Deepwater Horizon, where layers of safety including blowout prevention, validation of cementing performance and well integrity procedures were all compromised. Failure of multiple barriers ultimately led to disaster.

Last but not least, changes to feedstock, particularly on refineries, can cause serious unintended corrosion problems. This is another example of a change that is frequently made without going through the MoC system. Approval for feedstock changes is often given by a distant marketing or procurement function, with no input from Operations or (most importantly) Inspection and Process Engineers to validate the suitability of the crude for the refinery.

Emergency Changes

Emergency changes should be included within the scope of the MoC procedure. However compliance can be made difficult if the MoC process is inflexible and does not allow for deferred approval processes while still providing adequate oversight. As an example, if the Plant Manager has to approve an MoC by signing a hard copy of an MoC form, operations personnel might avoid using the MoC system altogether when the Plant Manager is not present e.g. over a weekend or during night shift for fear of reprimand on his return.
It is therefore of critical importance to clearly define the controls, risk assessment processes and approval levels that are in place outside of normal working hours, what (if any) limits there are regarding what changes can be authorised on an emergency basis, and there should be a requirement to revert to the normal approval process within a defined (usually 24 hours) period.

Temporary Changes

Temporary changes are another type of intervention which frequently slip through the net. My own personal favourites are hoses, which are commonly found throughout process units to facilitate various draining or steaming activities (e.g. leaking flanges, seals and, in some cases, piping). Often, having been informed that the hose is only temporary, I discover that the hose has been in place for several months. This is not a temporary change. Other frequent offenders are temporary power installations, injection points and the use of cooling water from hoses (again) on heat exchangers during hot weather.
Temporary changes should have an associated finite time limit (in my experience, typically 30 days) and should be subject to the same approval process as a permanent change. Once this time limit is exceeded then it should be managed as a permanent change. Some organisations allow one or two extensions for a temporary MoC, with appropriate risk assessment and approval for each extension. This is acceptable in my experience provided the review is carried out rigorously and the period of the extension is reasonable. However, I would respectfully suggest that once a temporary change has been in place for three months it is no longer temporary and it is time to address it accordingly.

Overdue Inspections and Tests

The final category of software changes relate to overdue inspection and test activities. These include, but are not limited to, overdue inspections on pressure vessels and piping, ESD valve and PSV testing inspections, but should be applied to all safety critical elements (SCEs). Overdue inspections and tests typically occur because an Operator is unable (or unwilling) to release equipment, usually due to operational constraints.
It may well be perfectly acceptable to defer inspection or testing activities for a period of time, but this needs to be based on sound technical judgement that the plant will be safe to operate in such circumstances. Typically these validations and approvals are managed within existing maintenance or inspection databases and systems, or a separate procedure might exist. However, it is also appropriate to use the MoC system and in many ways this is the best place for it, as the MoC procedure will dictate that the risk is appropriately assessed by a multidisciplinary team, and the decision reached will be based on sound engineering judgement.

Bypass of Safety Systems and/or Controls

In most organisations managing the defeating of safety critical equipment and control systems is a separate procedure from the MoC, although some organisations use their MoC procedure for managing these changes. There is no right or wrong answer so long as the management system is fit for purpose.
All SCEs should be defined and the decision to bypass or isolate these needs to be subject to a change management procedure. This is similar to MoC in a sense that it needs to include a robust risk assessment and an appropriate approval process. However, for bypassing safety critical equipment and control systems it is important to understand their purpose and function, so that if the system is to be defeated, for whatever reason (start-up, calibration, maintenance or just an equipment fault), the risk assessment includes a section on mitigations that will be in place while the system is defeated. A simple example of a mitigation is to ensure that no hot work is authorised on a platform if one of the fire pumps is out of operation.
Bypass authorisations also need to have a start and end date, with approvals for this period only. The increasing importance of the system being defeated should require greater levels of oversight. If the bypass is to go beyond the original approval period, the original risk assessment needs to be reviewed and revisited for adequacy. Similarly for temporary changes, if the bypass extends beyond an authorised period of time then the change should be subject to a permanent MoC request.
The comments in a previous section relating to barrier control are particularly important here. The potential weakness in all bypass management systems is the very real possibility that inter-related SCEs will be isolated or bypassed, leading to a cumulative reduction in layers of protection. One client I have been to has

generated a complex bow tie analysis of all of their safety critical systems, which was a mammoth piece of work but very impressive. One of the many benefits this has given them is the ability to immediately identify what other safety critical systems are affected when a single element is isolated, thus in a single step providing not only the mitigating actions but also "red flagging" any further isolations or bypasses of related controls as being unacceptable. Thus the safety barriers are not eroded in a cumulative way by multiple bypasses on a one by one basis.

4. Safety Review

An appropriately detailed safety review is a critical step in the MoC process. It enables all the expertise within an organisation (and outside, if necessary) to be deployed to investigate a change, and what mitigating actions and/or improvements need to be made to carry out the change safely both at the time and in the future. There are many different types of safety and/or hazard review including Hazard and Operability (HAZOP) studies, Process Hazard Analysis (PHA), What-if analysis, Failure Mode and Effects Analysis (FMEA) to name but a few. This might sound basic but the type of analysis required will depend on the type and complexity of change being proposed. We have briefly touched on this topic already but I have seen clients hamstring themselves with massive MoC backlogs because of a well-intentioned but naïve procedural requirement to carry out HAZOPs on all changes. This is self-defeating and unnecessary, and usually leads to small changes that pass "under the radar" with no scrutiny at all, a very undesirable outcome. It also sounds simple, but it is imperative that the site has an adequate number of trained team leaders for each of the hazard review methodologies used.

Of particular importance, therefore, is the makeup of the team who decides what type of analysis is required. While there is often an attempt to specify what analysis is required for each type of change I have frequently found a "points" system (depending on the type of hazards involved) seems to work better.

The next most critical criteria is the makeup of the review team. There should be a requirement for personnel from various departments to participate, depending on the type of change, but typically operations, engineering, maintenance, inspection and HSE representation would be a minimum requirement. Various specific disciplines may be required in addition to these depending on the scope and/or complexity of the change.

Finally, there needs to be a responsible person delegated to ensure all recommendations are tracked to close-out. This will include the requirement for any further analysis which may have been identified during the safety review, and inclusion of any proposed changes as required into the scope and documentation of the project.

5. MoC Procedure and Control

Checklists

The procedural element of the MoC process requires a simple tracking sheet or page to indicate the appropriate steps have been carried out and signed off. This is the case whether the MoC consists of a set of paper files which passes through all members of the approval team, or whether the MoC system is electronic.

Software-based MoC systems are becoming increasingly common. For large organisations with large numbers of MoCs the major advantage of these systems is the ability of the system to hold a project at a "gate" until all aspects are signed off and reviewed. The other significant advantage is the ability of the system to generate KPIs which can quickly demonstrate the health of the MoC programme. However, the downside of the system, if too widely available, is that it can quickly become "clogged" with numerous small changes which can obstruct the true picture of the MoC process efficacy. I have seen clients with open MoCs numbering in the hundreds, if not thousands, with no intention of many of these ever being implemented.

Introduction and Approvals

The MoC process should not be too difficult or too easy to implement. This all sounds quite basic, but the consequences of the system not being efficient and effective for the people who use it are simple and obvious – they will find other ways of getting things done. If it is too easy for people to submit MoCs then in a flash you will have numerous housekeeping issues clogging up the system. If it is too hard people will find "workarounds" and before long there will be numerous undocumented small changes occurring on the plant. Neither of these outcomes are desirable.

Similarly, approval levels, like the safety review, need to be effective and commensurate with the change being made. It is not necessary for the Refinery Manager to sign off on every change, but it may be appropriate for him/her to sign off on some. It is up to the organisation to sensibly marry the approval levels to the type of safety review and the complexity of the change.

Validation, Pre Start-up Safety Review (PSSR), Closeout and Documentation

Following the change it is important to validate that what was supposed to have been done, based on procedures, documentation and technical drawings, has been implemented. Where differences emerge, then these need to be addressed and the "punch list" items tracked to ensure satisfactory completion.
Following hardware changes, the appropriate technical drawings, documentation and files such as P&IDs, logic drawings and asset registers need to be updated, as do the possibly potentially large numbers of associated procedures. As an example, consider the installation of an emergency block valve (EBV) in the suction line of a pump in light hydrocarbon service. Alongside the technical evaluations and safety reviews that will be required because of the potential process changes there will be changes to standard and emergency operating procedures, maintenance procedures, ESD testing procedures and requirements, the Safety Case documentation and even pre-fire planning for the area in which the valve was installed, and I'm sure I have probably neglected to mention several more.
Following the completion of the change and all associated documentation changes, it is then necessary to give training to staff on the change and all associated procedural changes that have resulted from it. It is important to ensure that this training is effective and documented. Of course, it is also important that the new changes are incorporated into the organisation's training manuals and any competency validation assessments for operators, maintenance staff and any other affected personnel. Once the change and all accompanying documentation has been completed, a pre start-up safety review (PSSR) should be completed to verify that what has been installed matches P&IDs. These should be validated by line "walk downs". In addition, the PSSR should independently verify the MoC procedure has been followed correctly, with appropriate safety reviews and approvals, and that procedures and documentation are up to date following the change.
Finally, any recommendations made following the safety review, the PSSR or generated during the course of the MoC process need to be completed. The MoC can then be formally closed out as completed.

6. Auditing and Measurement

Like all systems the MoC process needs to be audited to ensure it is being followed. This is a requirement of all good process safety management system elements. The audit should cover how the MoCs are being initiated, whether the MoC process is being followed and documentation completed, whether the risk assessment processes are effective and whether personnel involved are competent, including having the necessary training. To provide advice to management on the efficacy of the system, KPIs should be introduced. Good ones include the number of emergency changes, the number of temporary changes greater than due date, open MoCs at each stage, particularly those awaiting close-out or document upgrades, a measure of new versus approved MoCs, to measure "clogging" of the system and the number of open close out actions. There are others that can be used in addition to these.

7. An Interesting Incident

A serious incident occurred on a hydrogen reformer located within an experimental brown coal to oil conversion plant. The main process involved the hydrogenation of a coal/solvent slurry within a series of high pressure reactors (27 MPa). The hydrogen was supplied by the reformer in question. Following the incident the pilot plant was shut down for several months while the reformer and associated equipment was repaired.
The incident occurred when hydrogen escaped from a fracture in the outlet pipe. The hydrogen, at approximately 840 0C, immediately ignited and the subsequent jet fire caused major damage to an adjacent waste heat boiler. Fortunately the automatic shutdown systems activated due to low pressure alarms within the unit, and the reformer was flooded with nitrogen. The fire was extinguished within a few minutes. Fortunately nobody was injured, despite the fact that the reformer furnace box was located close to both a roadway and normal operator traffic (mainly because the incident occurred during the night shift).
The major factor in this incident was the management of change procedure. Although HAZOPs were carried out on key process changes, this incident was primarily caused by the decision to install insulation on the pipework several shutdowns earlier. The outer skin temperature of the pipe was designed to operate at about 135 0C, which then kept the temperature profile across the castable steel inner section below the annealing range. By installing the insulation on the pipework, the outer skin temperature was raised to an estimated 300 0C, and the internal castable steel section well into the annealing range. Over a series of start-ups and shut downs, because of the pilot plant operating profile, the materials were gradually work hardened until they were unable to withstand the 2 MPa pressure to which the pipe was subjected, and catastrophic failure resulted.

Other contributory factors were the unique operating and process ownership roles of the engineers at the plant, a lack of clear operating and maintenance procedures, and a lack of detailed information about process changes.
While the MoC system was found to be the major factor, it should be recognised that many organisations would not have performed a HAZOP on such a modification. In addition, even if a HAZOP had been performed, it is by no means certain that such a scenario would have been identified without a materials specialist present in the HAZOP team.

8. Conclusions

The MoC process is frequently ineffective at many of the facilities I visit. This is often due to basic deficiencies, some of which have been highlighted in the text of this paper, such as poor documentation control, ineffectual approval regimes, poor hazard analysis, a lack of control on temporary and emergency changes, poor auditing and a lack of effective KPIs with which to monitor the health of the system.
MoC, or rather a lack of it, has been implicated in many of the largest losses seen in the oil and petrochemicals sector over many years. Despite this, it still seems that the lessons are not being learnt. If this paper encourages management of high hazard facilities to take another look at their MoC system and to address some of the gaps, then I will be greatly encouraged.

References

Lees, F.P., 2003, Loss Prevention in the Process Industries Volume 3 Appendix 2, Butterworth Heineman, Oxford, UK.
Hopkins A., 2000, Lessons From Longford – The Esso Gas Plant Explosion, CCH Australia Limited, Canberra, Australia.
Hopkins, A., 2012, Disastrous Decisions – The Human and Organisational Causes of the Gulf of Mexico Blowout, CCH Australia Limited, Canberra, Australia.