1. Welcome and introduction to the series

The global mining industry has been communicating visions of Zero Harm for many years. As part of this vision, the industry has been committed to proactively managing operational risk.

To support this Operational Risk Management (ORM) initiative, a series of short articles will be offered providing a perspective on the related needs, opportunities and challenges. Obviously, this is one person's perspective, influenced by experience and bias, but the objective is simply to stimulate thinking.

These articles discuss the potential step change in ORM from current approaches that may have been developed in the 20th century to a newer overt focus on the systematic application of quality controls and, following that phase, a move to effective critical control implementation, verification and assessment of effectiveness.

No successful improvement in operational risk management (ORM) is rapid. Positive change requires recognition of the need for change, a clear understanding of the change, demonstration and appreciation of its value, and overt positive feedback once change occurs. This applies at individual, management, corporate and external stakeholder levels.

The challenge for risk management professionals is to chart a course for ORM evolution that provides not only attainable goals for effective change but also a strategy for influencing the

stakeholders, internal and external, individual and corporate, rapid-adopters and stragglers, over a period of years.

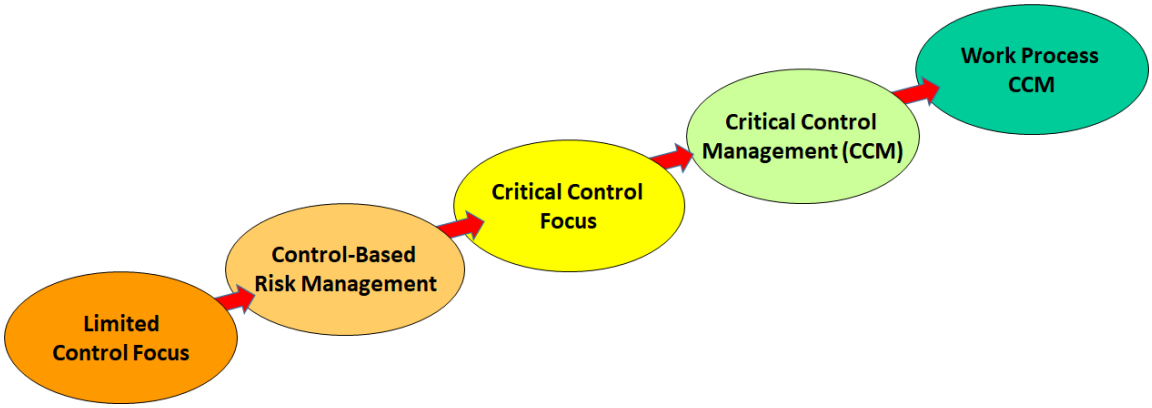
The articles will use the term **Control-Based Risk Management (CBRM)** to describe the evolution of ORM to an approach that focusses on the careful challenging, optimisation., installation and communication of controls for significant unwanted events.

Sites may believe that they are currently at, or even beyond, this phase of ORM evolution. These articles may challenge that belief, providing a means to review that control-focusing as part of the sites practices and culture.

Critical Control Management (CCM) is the next step in the evolution of ORM after successful CBRM. The objective of CCM is to focus the management system on ensuring the effectiveness of carefully selected critical controls. CCM moves away from a heavy reliance on risk assessment and analysis to a more effective control management approach. As such CCM is more about effective management than risk analysis. Organisational maturity will be discussed as a precursor for successful CCM.

The International Council of Mines and Metals (ICMM) published guidance on CCM in 2015 which is available on their website (http://www.icmm.com/en-gb/publications/health-and-safety/health-and-safety-critical-control-management-good-practice-guide and http://www.icmm.com/en-gb/publications/health-and-safety/critical-control-management-implementation-guide) . ICMM member companies were surveyed during the development of these resources. The survey identified that all respondents, despite a range of current emphasis on managing controls, saw CCM as the goal for managing their highest risks.

This series of articles is intended to stimulate strategic thinking as a company, business unit or site advances along the ORM journey, as illustrated.



The article topics are intended to align with this journey.

1. A short history of Australian mining ORM – one perspective
2. Key words and concepts in ORM - getting the conversations and thinking consistent
3. Making the argument - risk is all about controls and their effectiveness
4. Good practice ORM – four layers with risk assessment applications
5. Moving to CBRM – the need and the changes
6. Evolving ORM to CBRM at a site – the tools and the thinking
7. Introduction to CCM – the process and outputs
8. It's a Journey – the ORM/CBRM/CCM Journey Model
9. Influencing leadership mindsets – engage, involve, include, support
10. Changing individual mindsets - promote, require, reinforce, support
11. Finding the highest risk unwanted events (MUEs)
12. Ensuring the overall control strategy is adequate for an MUE
13. Identifying the most critical controls
14. Challenging required control performance – considering control erosion factors
15. Establishing verification methods and reporting processes
16. Embedding and managing controls – from accountability to real time ORM
17. Continuously improving controls – looking for action indicators

A short history of Operational Risk Management in Australian mining – one perspective

Revisiting the history of Operational Risk Management (ORM) not only helps us understand the technical evolution of ORM but also may help us recognise the mindsets of individuals who have been in the industry for many years. People at all levels of the mining industry have been exposed to a variety of ORM initiatives over the past three decades. They may have been early or late adopters or even, as the change management models suggest, laggards. As such, history can help us understand todays behaviours.

In the 1970s and 1980s, the Australian mining industry suffered many major disasters. The fatality rate was almost as high as it was in the early part of the 20th century.

Mining regulations in some Australian states started to change to reflect the 'duty of care' approach in the 1990s which often included a push, by regulation or strong recommendation, for mines to adopt risk assessment methods. At the time, some regulators had reviewed the approaches of other high hazard industries and felt there was an opportunity to reduce fatality and injury rates through ORM.

It's fair to say that the regulators push accelerated the adoption of ORM methods in Australia, as well as other jurisdictions. This benefited health and safety outcomes in mining but also often lead to ORM becoming part of the compliance mindset. In other words, ORM is done because of regulations require. The value is not appreciated.

Initial ORM methods included Job Safety Analysis and other tools that helped proactively review the work processes. Risk analysis methods, such as the Risk Matrix, were introduced across the industry. Much of the focus in the early to mid-1990s was on training the workforce about the basics of ORM and the use of these 'new' methods.

As with the virtually all major changes related to health and safety, disasters triggered evolution of ORM methods and requirements.

Several near or actual multiple fatality mining disasters occurred in the 1990s. On the east coast of Australia, the regulatory requirement for major or principal hazard management plans was defined. These plans included detailed analysis of selected hazards with highest potential consequences and the development of a plan to manage the hazard through a site-defined set of approaches such as procedures, training, accountability, etc. The plans also included the use of 'TARPs' or Trigger Action Response Plans. TARPs are documented action requirements for defined escalating levels of a hazard or an event. As such they dictate action even at early phases of a potential disaster. TARPs have been credited by some as a major contributor to the reduction in multiple fatality events in the Australian mining industry. Around this time many mining companies also recognised the need for corporate ORM procedures and guidelines.

Part of the ORM evolution in the late 1990s included the development of site risk registers. The register was intended to be a site resource, developed after risk assessments to find the highest priority risks, define required actions and set accountability for those actions. As such, it could be an up-to-date resource, offering the site management team a clear focus and risk improvement mechanism. Many would say that goal was not commonly achieved.

As we entered the 21st century the multiple fatality events virtually stopped and the focus moved to the prevention of single fatality events. Many companies augmented site ORM with Golden Rules or 'Fatal Risk' requirements that mainly, at least initially, defined required behaviours related to priority hazards.

Various state regulators also moved toward a common approach to ORM requirements during the first decade of this century. However, most mining companies had, by this time, defined ORM approaches that exceeded regulatory requirements.

Debate accelerated about ORM methods as mining companies acquired ORM expertise from other industries. The Risk Matrix was often the topic of debate amongst industry professional, including the real or perceived requirement to 'get it in the green'. In other words, ensure that there was no risk that was recognised as unacceptable. This mindset could lead to inadequate consideration of the adequacy of controls for the unwanted event. It may still be prevalent in some mining operations.

As the industry entered the 2nd decade of the 21st century the health and safety performance appeared to be greatly improved from earlier decades, sometimes diminishing the urgency of H&S priorities. Of course, the reduced commodity prices also affected the appetite for major changes to ORM. However, many H&S risk professionals recognised that valuable improvements could still be made in ORM. For some, the 2010 Pike River disaster indicated that we could undertake many ORM activities but if the method quality was poor or incomplete, a catastrophic event could still occur. Was this possible in Australia?

Several companies began to work toward a more aggressive control-based ORM approach. The Bowtie Analysis (BTA) method, developed by Shell many decades before, started to become a standard method for the control-based approach. However, like any tool, the quality of its application had an impact on the value of its outcomes. BTA teams often struggled with identification of clear, monitorable pre-event and post-event controls.

In 2014, an Australian Coal Association research project included workshops of representatives from most coal mining companies in discussions about the selection and optimisation of controls (ACARP Report C23007 – available to purchase at https://www.acarp.com.au/reports.aspx). Future articles will discuss the resultant new definition of a control, a significant change in ORM.

The Health and Safety Committee of the International Council of Mines and Metals (ICMM) had a major initiative running parallel to the ACARP work. This committee involved senior

health and safety risk personnel from many of the world's top mining companies; many of whom are leading experts in ORM. These individual and their organisations recognised the need to define a control-based ORM approach that included understanding the control set for highest priority unwanted events and the management of critical controls from that set through greatly enhanced methods of challenging the control, defining performance requirements and verification/reporting methods. Critical Control Management publications from ICMM (see www.icmm.com/en-gb/publications) circulated across the global mining industry. Many companies expressed their commitment to move toward CCM.

This next phase of ORM offers great benefits but the change in both methods and mindsets may be greater than first thought. Future articles will develop this further.

Key words and concepts in ORM - getting the thinking and conversations consistent

This article is the third in a series intended to stimulate discussion about advances in mining Operational Risk Management (ORM). The first article outlined the ORM advances and provided a list of 17 articles. The second article provided a perspective on the development of mining ORM in Australia since the late 1980s.

This third article will start to build a foundation for these recent advances; Control-Based Risk management (CBRM) and Critical Control Management (CCM).

Good ORM involves not only a set of methods or tools but also aligned 'mindsets' amongst all those involved. Mindset is defined by the Cambridge English Dictionary as a person's way of thinking and their opinions. We use terminology to help construct our thoughts and express our opinions, providing a basis for decisions. For example, a person driving a car may recognise a threat to safety because another car is speeding. The person knows what the terms speed and speeding mean. Speed is a measure of travel (distance over time) and speeding means exceeding a defined speed limit. The person can easily describe the issue to another person because his or her terminology for the situation is well known and commonly used.

In ORM there may be confused or inconsistent terminology, making thinking and communication of opinion or information less effective. For example, the terms 'hazard' and 'risk' are historically colloquial terms with broad meanings. If we want to have effective

ORM communication both terms, as well as others, require clear definitions. Four definitions are offered below. The terms 'unwanted event' and 'control' have been added to provide the basic terminology for a good ORM foundation. Consistent use of these terms as defined will affect both mindsets and methods.

- **Hazard** – something with the potential for harm. When considering physical harm to humans, assets or the environment, a hazard is any energy source that, if released in an unplanned way, can cause damage. Electricity is a hazard. It has the potential for harm but not necessarily an unacceptable risk.
- **Unwanted Event** – a description of a situation where the hazard has or could possibly be released in an unplanned way, including a description of the consequences. For example, failure to correctly isolate the electricity supply leads to the maintenance person being electrocuted.
- **Risk** – a proactive measure of the chance of something happening that will have an impact upon objectives such as safety. It is commonly measured in terms of unwanted event likelihood and consequences. As such, risk is a measure of the degree to which an unwanted event is a concern. Using the example above, the risk can be estimated by considering the likelihood an isolation failure will occur, combined with the fatal consequences. The determination of event likelihood should be based on an effective review of the existing controls.
- **Control -** an act, object (engineered) or technological system (combination of act and object) intended to arrest or mitigate an unwanted event. A control must be specifiable, measurable and auditable. For the example, an important control is probably the act of isolating as required. In some cases, other controls may contribute to the risk such as ground fault protection, PPE, etc.

This definition of a control may be different from current site practices. Often procedures, training and supervision are considered controls. However, this definition suggests more careful selection. This change may require greater explanation.

To expand, one type of control is a defined human 'act', which of itself, arrests or mitigates an unwanted event. The defined human act may be derived from a procedure (ex. The step in the procedure when effective isolation is done), training content (ex. The maintainer's

training has effectively included training and assessment on correctly isolating) or experience in applying specific practices in the given situation (ex. The maintainer has adequate experience in the specific isolation requirements). As such, a procedure is not a control but rather a specific act defined in a procedure.

The second type of control is a tangible / physical, 'engineered' or designed 'object', which of itself, would arrest or mitigate an unwanted event related to that hazard. It can be described as follows.

- Automatically actuated or operated, not relying upon a human act to actuate or operate,
- Passive (e.g. a windrow) or active (e.g. on-machine gas monitoring), and possibly
- Operated based on software.
- Ex. ground fault protection on the circuit, automatic fire suppression system, transformer bunding, pressure relief valves, etc.

The final type of control is a combination of an act and an object; an object control that requires human acts to actuate, operate or respond. This might be called a 'technological system' control. It can be described as follows.

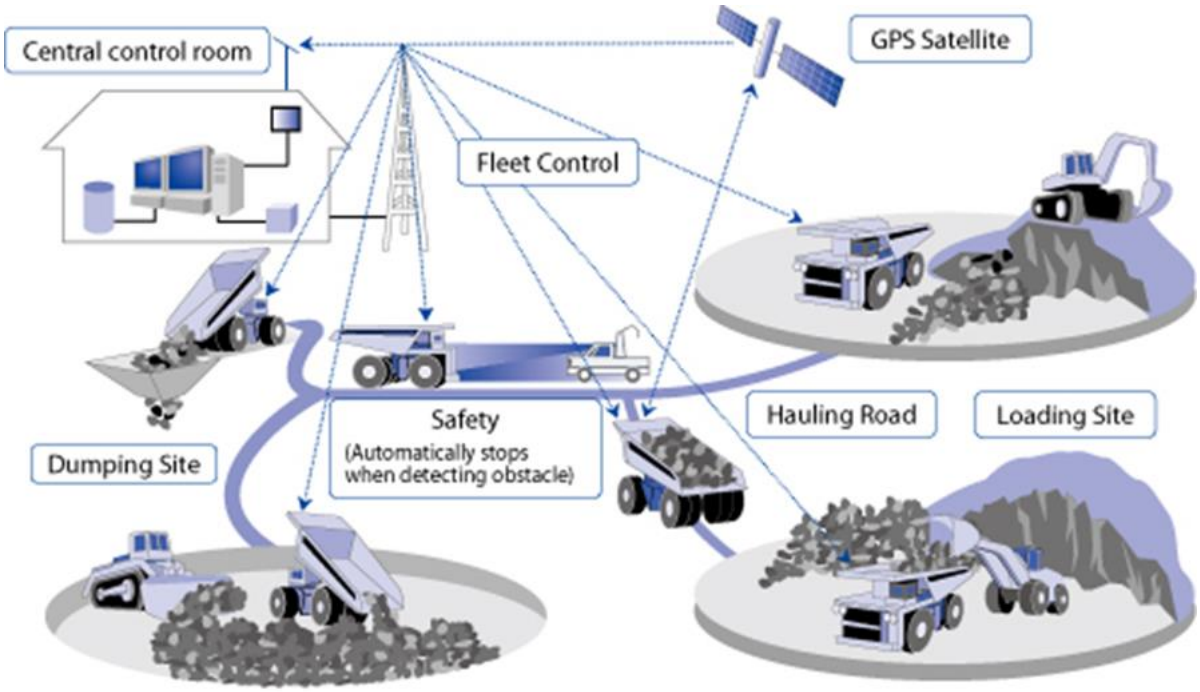
- Technology reliant upon a human act to actuate or operate when required such as a response to an alarm, and
- Passive (e.g. barriers installed near an ore pass) or active (e.g. ventilation system gas monitoring from a control room).
- Ex. smoke detection system that requires operator action such as actuating an alarm or message to evacuate, tell-tale system which requires physical inspection, proximity alarms that warn the operator to act, etc.

Also, a control must be specifiable, measurable and auditable. As the adage goes, 'if you can't measure it, you can't manage it'.

A 'human act' control for collisions at mine intersections is the driver operating the vehicle as defined at the intersection, the requirements being set by the related road rules

or procedures. For example, the vehicle coming to a T intersection will give way to all vehicles approaching from the right. As such **the control is specifiable.**

The illustration below shows an equipment suppliers summary of GPS-based equipment monitoring as part of fleet control. If vehicle position is tracked frequently, say once per 5 seconds, then vehicle operations can be measured against expectations. Specific to intersections, the GPS information can capture the vehicle's operation through the intersection and compare it to the defined rules or procedures. Thereby **the control is measurable** and, if the data is analysed, the technology offers an approach to **auditing the control** across individual vehicles, site intersections, over a time period, considering the entire fleet, etc.



The consistent use of the terms hazard, unwanted event, risk and, especially, control is critical to successful CBRM and CCM. For more information on controls and their effectiveness see ACARP Report C23007 (available to purchase at https://www.acarp.com.au/reports.aspx).

The next article will discuss ways to influence site personnel about being 'control-focused', based on a change management approach.

Making the argument - risk is all about controls and their effectiveness

Achieving control-focused mindsets and methods may be a step change. This article will discuss the mindset shift that forms part of the move toward site control-based risk management and critical control management. Subsequent articles will discuss the changes to risk management methods in more detail.

In the past, and perhaps even today, we have been 'risk-focused', primarily concerning ourselves with establishing that a risk rank, score or calculation has achieved an acceptable level. As such, our mindset (as a person's way of thinking and their opinions), whether an operator, supervisor or manager, may involve justifying that a number or colour (such as green in the basic risk matrix). This mindset may lead to inadequate consideration of the primary factor that affects the likelihood and consequences of an unwanted event; the existence and quality of relevant controls.

The argument for being control-focused may seem easy, or even obvious. If the things that prevent or mitigate an unwanted event are not present, the event will occur. However, sometimes common sense is not so common, possibly the result of Operational Risk Management (ORM) history (see the 2nd article in the series).

Often a general example will help introduce good understanding of controls.

I hope we would all agree that if there are no brakes on the car it will eventually crash. But how well do the brakes need to be designed and maintained to make the risk of operating the car acceptable? Braking systems are not 100% reliable, especially considering all driving conditions. Brakes are a technological system control (see the previous article for the control definition). As such the braking system is a combination of a human act that operates the brakes when needed in the correct manner, and the equipment that responds to the act by applying mechanisms to slow or stop the car. (Note that some new cars apply brakes based on distance sensors, without human action, in some situations)

The likelihood of an unwanted vehicle incident where a braking system is an important control is affected by both the braking act of the operator and the status of the braking mechanisms. The later component of the control is usually easier to gauge for effectiveness.

For example, if a son or daughter is trying to purchase a used car, Australian parents may be relieved to know that a safety inspection is required for a car to be legally sold. A potentially effective way to address braking mechanism effectiveness. Vehicle inspections cover a list of technological system controls, including brakes, steering, lights, etc. Adequate status of the listed controls is essential for a 'pass'. It's very likely that this overall approach resulted from investigating major car accidents, learning the hard way that inadequate controls increase the risk.

Mindsets may contribute to the success of this approach. Note that, according to Wikipedia, in 2010 approximately 30 US states did not require vehicle inspection for resale. For some reason, despite the 'common sense' that this approach will reduce accidents, it is not seen as necessary. What would parents think about their child's potential purchase if the family lived in a state that didn't require vehicle inspection?

In summary, to judge the risk of a car accident due to a problem with the vehicles roadworthiness by 'gut feel' rather than a systematic review of the vehicles important controls and systems would be foolhardy. As such, **risk is all about the controls**.

Many variables affect people's mindsets about controls, their importance and the degree to which they need to be challenged and monitored. Some sites may have healthy control-

focused mindsets while other sites may not. How can we establish the site status and, if required, moved forward?

Basic change management questions can aid the transition to control-focused mindsets and methods, as well as provide a clear demonstration of the need to evolve site ORM. The following set of questions and example answers illustrates the approach.

1. **What is the purpose of the intended change to a control-focused site?**

   All site personnel should recognise and appreciate that 'risk is all about the controls'. Proactive decisions should base the level or amount of risk on the existence and quality of effective controls.

2. **What are the expected outcomes from the change?**

   Ideal outcomes involve thorough control consideration across many areas such as:

   - Communication content – meeting agendas/formats, presentations, facilitated discussions and general conversations that include consideration of hazards, unwanted events, controls and thereby the risk.
   - Training content – risk, safety, health, environment, induction and skills courses that include learning about controls and their optimization.
   - Risk assessment forms design and application – that include good control consideration in broad brush, change management, WRAC, JSA, SLAM, project risk, and other methods.
   - Risk management procedures – having content about requiring control identification and reviews of control effectiveness
   - Promotion materials – pamphlets, posters, banners, messages and signage that are consistent with a control-based approach to managing risk.
   - Incident investigation methods – identifying the controls that failed or were absent, as well as the reason.

3. **What is the current situation?** How are things currently done at the site compared to the defined ideal above?

   For example:

   - Communication content – the conversation in meetings and informally tends to focus on ensuring the risk is 'acceptable' as measured by a risk matrix. Controls are

not discussed in detail. There is some reluctance to suggest that a risk is high so challenging of existing controls is not common.

- Training content – current training content does not define controls as acts, objects and technological systems (see previous article). The importance of identifying and challenging control status is not emphasized.
- Risk assessment forms design and application – forms include the requirement to note controls but the information is not acts, objects and technological systems so listed information is broad, vague and difficult to discuss to establish status and quality.
- Risk management procedures – the current procedure requires control identification and some consideration of control effectiveness but, again, the definition of controls as acts, objects and technological systems is not included.
- Promotion materials – current health and safety risk posters and signage does not include an emphasis on 'risk is all about controls'.
- Incident investigation methods – current investigations of significant near hit or loss related incidents identify the failures that contributed but not specifically defined as acts, objects or technological systems. Thereby the rational for failure is limited.

4. **How could the differences between the intended ideal and the current situation be addressed?** What actions could be taken for each difference between the current situation and the ideal to move toward the ideal?

   For example:

   - Communication content – reintroduce personnel to ORM by defining the risk conversations to include clearly definitions of hazard, unwanted events, risk and controls (see previous article for definitions). Suggest that all discussions about health and safety include the correct use of the terms. Reinforce the adage that 'risk is all about controls'. Monitor conversations and remind personnel if they use terms incorrectly.
   - Training content – review current training content and identify areas where new definitions of hazard, unwanted event, risk and controls including a strong focus on defining controls as acts, objects and technological systems. The importance of

identifying and challenging control status to ensure the risk is acceptable should also be emphasized.

- Risk assessment forms design and application – review the objective of current risk assessment methods to ensure that they emphasize adequate control for the unwanted event. Note that a later article will address the various methods in more detail.
- Risk management procedures – review the current procedure to include the definition of controls as acts, objects and technological systems, as well as the importance of effective control identification and review of control effectiveness.
- Promotion materials – review the objective of any health and safety risk promotion materials and ensure it aligns with the new definitions and the message; 'risk is all about controls'.
- Incident investigation methods – modify current investigation methods so that event related controls (acts, objects or technological systems) are identified with their status at the time of the event investigated, including reasons for any failures.

5. **What methods will be used to monitor the results of the change?**

   For example:

   A review of the status related to the topics above and their progress will occur in 6 months.

Clearly, the new definition of controls and the increased emphasis on their quality could potentially lead to major changes at the site. These changes should move the site along the Control Based Risk Management journey.

The next article will briefly overview a model of site good practice ORM based on four layers with risk assessment applications. This general approach is common on Australian sites, but the implications of the new control definition will be added.

Article 5 - Good practice Operational Risk Management (ORM)– 4 layers with control-focused risk assessment methods

Welcome to article 5 of 17. Thanks to those who have provided feedback.

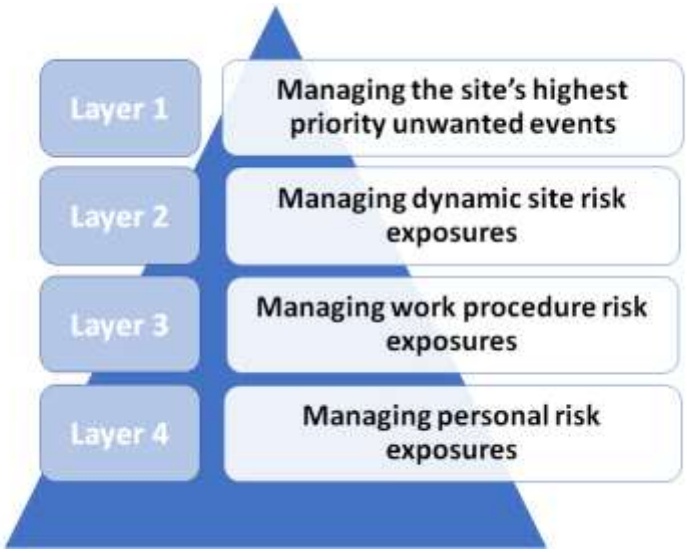
Article 3 and 4 of the series briefly presented a 'back to basics' discussion about terminology and the focus on controls, also called barriers. Potential changes were reviewed to help develop a good control focus considering conversations and mindsets, and to a lesser degree, methods.

Building on this foundation, we can start operationalising the previous content by using an overall site ORM framework. Much of the following approach is not new. In fact, many mine sites around the world have had all or most of the suggested activities in place. However, this list would have included the Pike River coal mine when it exploded in 2010, killing 29 men.

Clearly the quality of the ORM framework is crucial. It may be valuable to revisit the overall ORM framework to review objectives, methods and outcomes. For many this will also be another 'back to basics' exercise but with an added content related to the increased focus on controls, defined as acts, objects and technological systems. Those additions will be highlighted ***in italics***. They may generate new site discussions.

The following content is a modified version of information published in a 2007 ACARP report titled 'Coal Mine Safety Regime: A New Safety Case Process and its Implications to Australian Coal Mining'. This work was further developed and used as content for education and training programmes delivered in Anglo American and by the University of Queensland for the last 10 years.

Commonly, there are four layers of ORM activities at a mine site.



The above illustration shows the four layers and includes a triangle symbolising the risk assessment frequency from once-per-year (or less frequent) for the top layer, to several hundred times per day across the site for the bottom layer.

Layer 1 and 2 offer an opportunity to design-down the risk on the site by carefully considering controls, identifying factors that erode their effectiveness and noting opportunities to optimise or add controls. Layer 3 and 4 offer some opportunity to improve controls, especially in the development of task standards, but their main function is to ensure the required controls are understood, in place and effective.

Each layer involves a different process. The following information is intended to suggest some of the process features *with added focus on controls*. It is not a complete list but rather a set of important points.

Layer 1 – Managing the site's highest priority unwanted events - including principal hazard, site baseline or full site risk assessment methods

Objective: To develop and apply a site-wide effective management plan to manage the risks of potential major unwanted events (MUEs) to an acceptable level.

Processes that:

- systematically break down the entire site and its operations into appropriate detail to identify the most significant hazards.
- apply hazard identification that includes acquiring a clear understanding of the location, magnitude, mechanisms of failure and the uncertainties of the hazards.
- considering each significant hazard, establish the list of priority MUEs that need further analysis based on the potential consequences to health and safety (multiple fatalities and selected single fatalities events, including short term and longer-term H&S impacts).
- *review and analyse the MUEs with Bowtie Analysis (BTA) to an adequate depth so that it can be established that the overall control strategy is adequate (i.e. the risk is acceptable).*
- develop a site management plan and system to record and retain the output of the analysis. The plan should document the MUEs *and their overall control strategy from the BTA* with systems implications such as required improvements, accountability, monitoring, reporting, etc.
- *note that the 'plan and system' may meet the requirements of Principal Hazard Management or Control-Based ORM. With further development the information could form the basis of Critical Control Management planning or Safety Case development.* Later articles will offer more detail on Control-Based ORM and Critical Control Management.
- include a continuous improvement aspect so the plan is up to date
- link the plan and system to the next two layers (2. and 3.) *and integrate the defined control strategy information into other related plans, procedures, training and site activities.*

Layer 2 – Managing dynamic site risk exposures - including risk assessment methods for projects, changes or learnings from incidents

Objective: To develop and apply effective management plans to manage the risks of potential unwanted events in significant site projects and changes, as well as identify improvements after incident investigations. Thereby addressing dynamic site risk exposures that may not have been considered in Layer 1.

Processes that:

- are driven by site procedures for project management, change management and incident management that include the 'triggers' that initiate risk assessment and management based on some level of potential negative outcomes, as well as a set of risk assessment methods to suit the issues (e.g. hardware – Failure Modes and Effects Analysis (FMEA), process – Hazard and Operability Study (HAZOP), work methods – Workplace Risk assessment and Control (WRAC), single event concern - BTA, etc.)
- when the defined trigger is met or exceeded, apply the appropriate risk assessment method to the new project, change or incident learning.
- *ensure that the risk assessment method includes a careful review of existing and potential new controls for any significant unwanted event using the new definition of a control (act, object or technological system), considering control effectiveness and potential improvements.*
- *develop the required content for the project management, change management or incident management plans to record and retain the output of the analysis. The plan should document the controls with systems implications such as required improvements, accountability, monitoring, reporting, etc.*
- feed the results of risk assessments back into the plan and system established in layer 1.

Layer 3 – Managing work procedure risk exposures - including routine and non-routine task planning risk assessment methods

Objective: To develop and apply effective safe work expectations (guidelines, standard work procedures, task plans, etc.) to manage risk exposures in tasks as well as plan tasks where a procedure is not available or adequate.

Processes that:

- are driven by site requirements for standard work procedures, including the need to plan for tasks that are not common, utilising risk assessment methods such as Job Safety Analysis (JSA) or Workplace Risk assessment and Control (WRAC).
- *ensure that the risk assessment method includes a careful review of existing controls for any significant unwanted event in the task using the new definition of a control (act, object or technological system).*
- *do not re-rank risk but rather conclude that the task can be done safely if the reviewed controls are adequate.*
- set a process of documenting and integrating the information derived by the relevant risk assessment.
- define documentation criteria for the standard work procedures (SWPs), work guidelines, work plans for employees and contractors. *Include highlighting of important controls for the most significant potential unwanted events.*
- integrate the resultant document into training, monitoring and auditing requirements where relevant *with an emphasis on important controls for the task.*
- where relevant to an MUE, link the risk assessment and relevant resultant document back to the Layer 1 plan

Layer 4 – Managing personal risk exposure - including individual, informal, "face" risk assessment methods

Objective: To have all personnel execute a personal systematic process to 'stop, think and proceed only if safe' before a task or during a task should a hazard or condition change.

Processes that:

- *define a method of considering hazards (energy sources), unwanted events (what could go wrong?) and the important acts, objects or technological systems (controls) for ensuring the unwanted event does not occur.*
- provide the individual with clear criteria for determining when it is 'safe' to proceed, as well as action to be taken if 'unsafe'.
- train the individual, including contractors, in the method and 'safe' criteria, or ensure the contractor's method meets the same objective.
- reinforce the application of the layer 4 method through supervisor and management monitoring and engagement in pre task meetings and 'face' discussions *with an emphasis on discussing important controls*.
- link to work order systems should the process identify a need improvement of controls.

This article provides a set of information that can be used to review current ORM practices against generally accepted objectives and process requirements, as well as *added suggestions for increasing the focus on controls*. The review may indicate that site risk management efforts in the four layers do not achieve the intended objectives, suggesting changes or even elimination of some methods.

However, the main purpose of this article is to suggest that examination of the degree to which controls are effectively identified, challenged and managed in each of the four layers may lead to significant improvements.

As discussed in Article 1, this series of articles is intended to stimulate strategic thinking as a company, business unit or site advances along the ORM journey, as illustrated.

Articles to date have covered 'back to basics', considering a new definition of controls. As such, the articles have addressed the first step in the journey, moving from a 'Limited Control Focus' to 'Control-Based Risk Management (CBRM)'. Future articles will further develop CBRM and then cover the next steps.

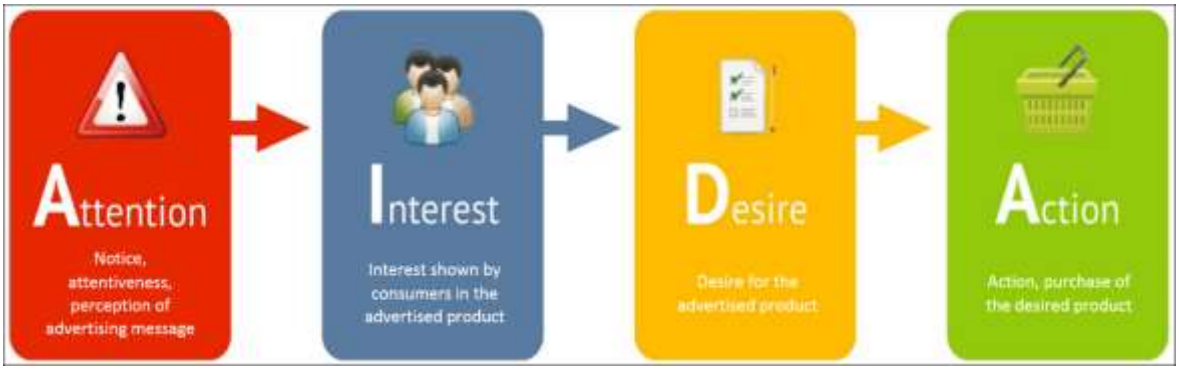
Article 6 - It's a Journey – using journey models to analyse and plan ORM improvements

Welcome to the 6th article in a series intended to generate discussion amongst H&S risk professionals and managers about improvements to the site Operational Risk Management (ORM) thinking and methods. The content should also help ORM personnel 'influence' line management at all levels.

The term, 'influence', has been deliberately selected to highlight the need for line management commitment and involvement in the change to Control Based Risk Management (CBRM) and, possibly, Critical Control Management (CCM). Ownership for the changes to more advanced mining ORM must overtly involve line management, as opposed to being seen as an initiative from the H&S department.

This article will discuss the use of Journey Models to plan for change and to influence line management understanding, and to gain overt line involvement in the changes.

Journey models are common across many disciplines for illustrating the steps in a change as well as to assist in planning. The illustration below shows the basic journey for a retail customer sourced from Zenith Media (http://zenithmedia.ch/en/news/?id=81). The customer proceeds through the 4 steps, unlikely to take "Action' without successful completion of the previous 3 steps.

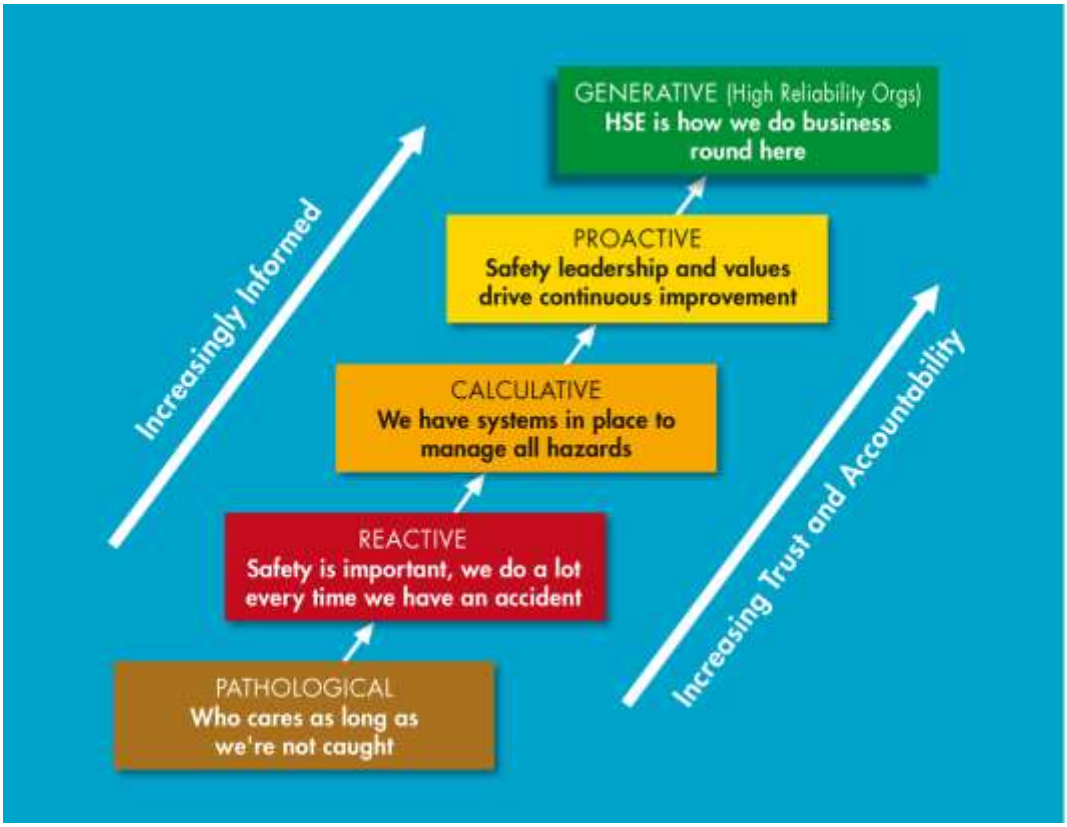


The above illustration could also apply to influencing line management about the CBRM or CCM 'product'. As ORM experts suggesting change, we can influence line management by influencing the first 3 steps; **attention, interest and desire**.

Once we have the **attention** of line managers, unfortunately often following a significant unwanted event, there may be **interest** in understanding potential improvements such as CBRM or CCM. The step from **interest** to **desire** for the CBRM or CCM 'product', or the motivation for commitment of line management, is a watershed or tipping point of this journey.

It is likely that line management **desire** for a significant change will require recognition that there is a need for change, as well as an image of what the change involves. Major changes like CBRM or CCM require moderate to long term planning and, as such, need a very effective argument to get line **desire** for and commitment to the change. A different, ORM specific, journey model may help the process.

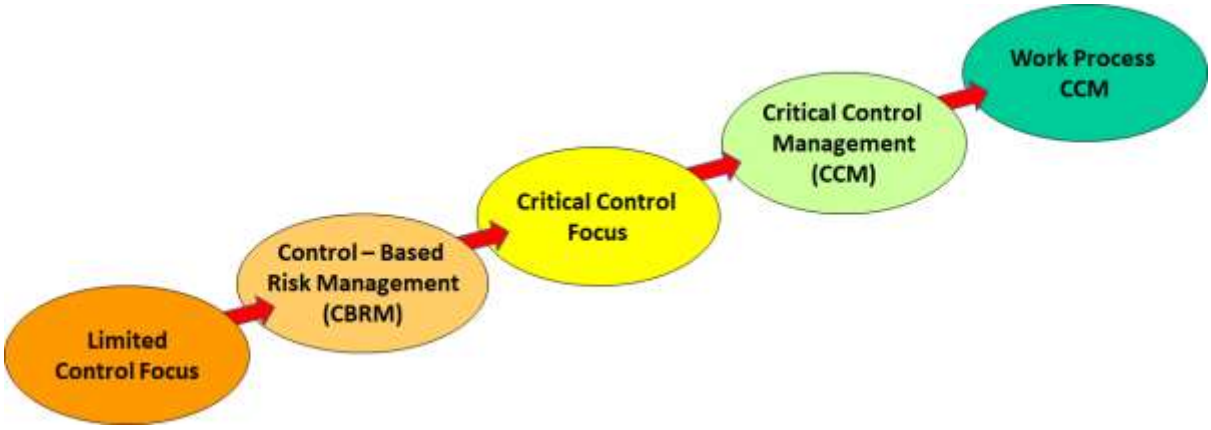
Many of us are familiar with the journey model below that is part of the Hearts and Minds programme developed by Shell with the assistance of Professor Patrick Hudson (http://publishing.energyinst.org/heartsandminds) . This journey model illustrates the levels of overall H&S maturity from Pathological to Generative. It can help line management understand the steps and some of their implications.



If descriptors for each of the journey steps are added, the model can become a planning tool. That tool can be used to identify the site's current status and the next step in H&S maturity. Some companies suggest that a journey model provides a map; where am I, where do I want to be, how do I get there.

The value of this approach to gain line management **desire** for the change, and thereby overt commitment to **action,** becomes even more significant when considering that movement up the maturity steps will take years of effort. The model provides the rationale for a multi-year plan that can capture the background for new line managers that were not involved in the original planning. Thereby, minimising the risk of deviating from a well-developed plan.

A specific ORM journey illustration was provided in earlier series articles suggesting 5 steps from a Limited Control Focus to integrated Work Process CCM.



This model can also be used as a map to help line management identify the current site ORM location, the next step on the journey and actions required to move forward. Detailed descriptors for several sub-elements of each step can be found in two sources, suitable for a mapping exercise. There is a one-page outline of related mindset and ORM method elements in the Appendix of the 2015 ICMM publication, '*Health and safety critical control management: good practice guidance'*, as well as a more detailed set of descriptors for the same elements in a 2015 ACARP report, C24006 '*Effective and efficient implementation of Critical Control Management in the Australian coal mining industry by 2020*'.

The need to consider mindsets of leaders and the workforce, as well as risk management methods, when moving to CBRM and CCM, has been suggested in previous series articles. The tools suggested in the references cover both mindsets and methods.

Undertaking a detailed ORM journey mapping exercise with line management may help the transition from **interest** to **desire** for CBRM or CCM improvements. However, the exercise and related discussions may also generate some classic failure modes. Following are a few examples.

Comfort with the status quo

The motivation to consider a major change in ORM methods is often driven by poor H&S performance; whether it be a single major unwanted event or cumulative outcomes. Interest in CBRM or CCM can also be driven by company interactions with peers. When

surveyed, the majority of ICMM and ACARP members stated their interest in moving to CCM, possibly because it was defined by the mining industry itself and not externally by suppliers or stakeholders.

As such, 'comfort with the status quo' is not a common issue at the mining executive level but rather more frequently encountered at middle management levels and sometimes with H&S personnel. Of course, perceptions related to added workload may generate resistance to change but sometimes resistance results from an inaccurate image of the effectiveness of current ORM messages and methods.

This failure mode suggests that site level personnel should recognise CBRM or CCM as a replacement rather than addition to current messages and methods. For example, as discussed in an earlier series article, initial actions should include reviewing current ORM messages and methods for their value and control focus. As a result, ORM related workload can be reduced and remaining methods improved.

Desire to move straight to Critical Control Management

As mentioned, CCM is commonly seen as the ORM improvement goal in the mining industry. While that goal may be desirable the magnitude of change to achieve successful CCM should be recognised.

Different mining companies and mine sites, even within companies, have varying quality of current ORM mindsets and methods. A short-term change to successful CCM may be unachievable in some cases. Sites that adopt CCM and define the 'critical few' controls without good quality overall control strategies risk over-simplifying their ORM, possibly leading to disaster.

CCM might sound very attractive to busy executives and line managers when seen as an opportunity to reduce seemingly complex and burdensome ORM efforts by focusing on the 'critical few'. Future articles will expand on executive, manager and workforce mindsets in the ORM journey. Future articles will also discuss the purpose of the 'critical few'.

The above ORM journey model was developed to help plan and manage for the pace of change so that important required steps in mindset and method enhancement are achieved through a planned transition. The next series article will discuss the need to have effective CBRM before moving to CCM. This appears to an important consideration for those who may be moving too quickly to CCM.

Failure to appreciate the magnitude of change and potential cost

Executives and line management can underestimate the amount of work required to move forward on the ORM journey.

For example, Bowtie Analysis (BTA) exercises are commonly undertaken on the highest priority unwanted events as part of CBRM. BTA-based identification of controls is intended to define an effective overall control strategy for a priority unwanted event. Control effectiveness should be challenged as part of the analysis, possibly by examining factors that can erode or compromise the control to address effectiveness issues. Improving effectiveness of existing controls or adding new controls to achieve a more effective overall control strategy is a potentially costly outcome of a quality BTA.

Discussion about important controls that are human acts, sometimes known as 'soft controls', may lead to recommendations about adding more effective object controls (hard controls) or technological systems (a combination of soft and hard). (Note that previous articles discussed the definition of controls as acts, objects and technological systems.) Of course, risk benefit consideration may be needed but often identified new 'hard controls' are cost effective. Also, verification requirements may lead to investment in time and technology for gathering useful control status information. Line management should be aware that these possible control improvement outcomes and be prepared for workload and cost implications.

A future series article will discuss establishing the risk acceptability based on control effectiveness. This approach may also generate business case information for the suggested control improvements.

Failure to understand the time frame and its implications

Changes in leader and workforce mindsets must run parallel to changes in ORM methods. It is often easier and faster to develop and introduce new ORM messages and methods than to change mindsets.

Achieving the desired workforce, supervisor and management mindsets about controls, CBRM or CCM will take time. A mindset is “a person's way of thinking and their opinions” according to the Cambridge online dictionary. Mindsets are part of the initial journey model in this article that basically covers customer purchase of a new product, or, as suggested, line management buy-in to changes. There are many aspects to CBRM and CCM that will require **attention, interest, desire,** and **action**. Social marketing experts might suggest that following **action** there must be **positive feedback** and **perception of gain or value** to convince the person that the change is good and worth continuing.

Support for development of CBRM and CCM may require ongoing reinforcement and communication of success such as, for example, communication about near-hit events where losses were minimised due to control effectiveness.

Lack of overt line commitment and involvement

Line management commitment and involvement is critical to the success of CBRM and CCM. Successful action, feedback and continued support are all necessary to acquire and sustain overt line management commitment to CBRM and CCM. These statements could probably be made for any major initiative in a company or site.

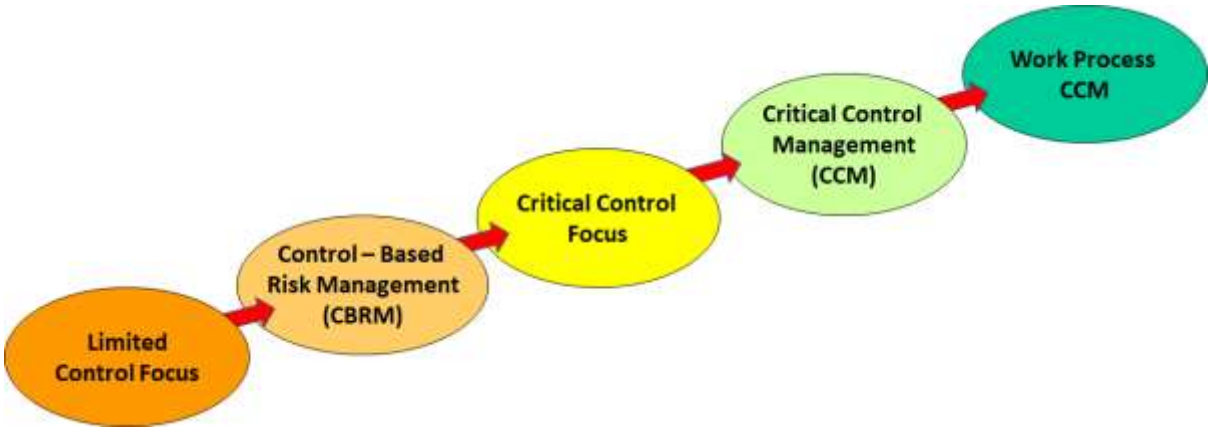
However, with CBRM and especially CCM, line management must be actively involved in designing the verification system for important or critical controls. The verification system must provide reasonably accurate information to management on the status of the control versus it intended function and performance. The control verification information is a measure of risk; lower control quality means higher risk. The greatest change in CCM is the much greater emphasis on gathering verification, reporting and reacting to control status verification information. This is the ‘check’ and ‘act’ part of the management process; plan - do – check - act.

Less mature line management teams may delegate the design of verification and reporting systems to H&S personnel. When this occurs, the verification system is not owned by line management. Mature line managers should know how to design a 'check and act' system that works for them. Control verification and reporting will be discussed in future articles.

The use of the ORM journey models to define and plan for major changes involved in CBRM and CCM has been successfully adopted in many mining organisations. This series of articles will continue to provide information on the theory of CBRM and CCM, as well as the learnings from related practical experience from applications.

Article 7 – Overview of Critical Control Management and a few of its challenges

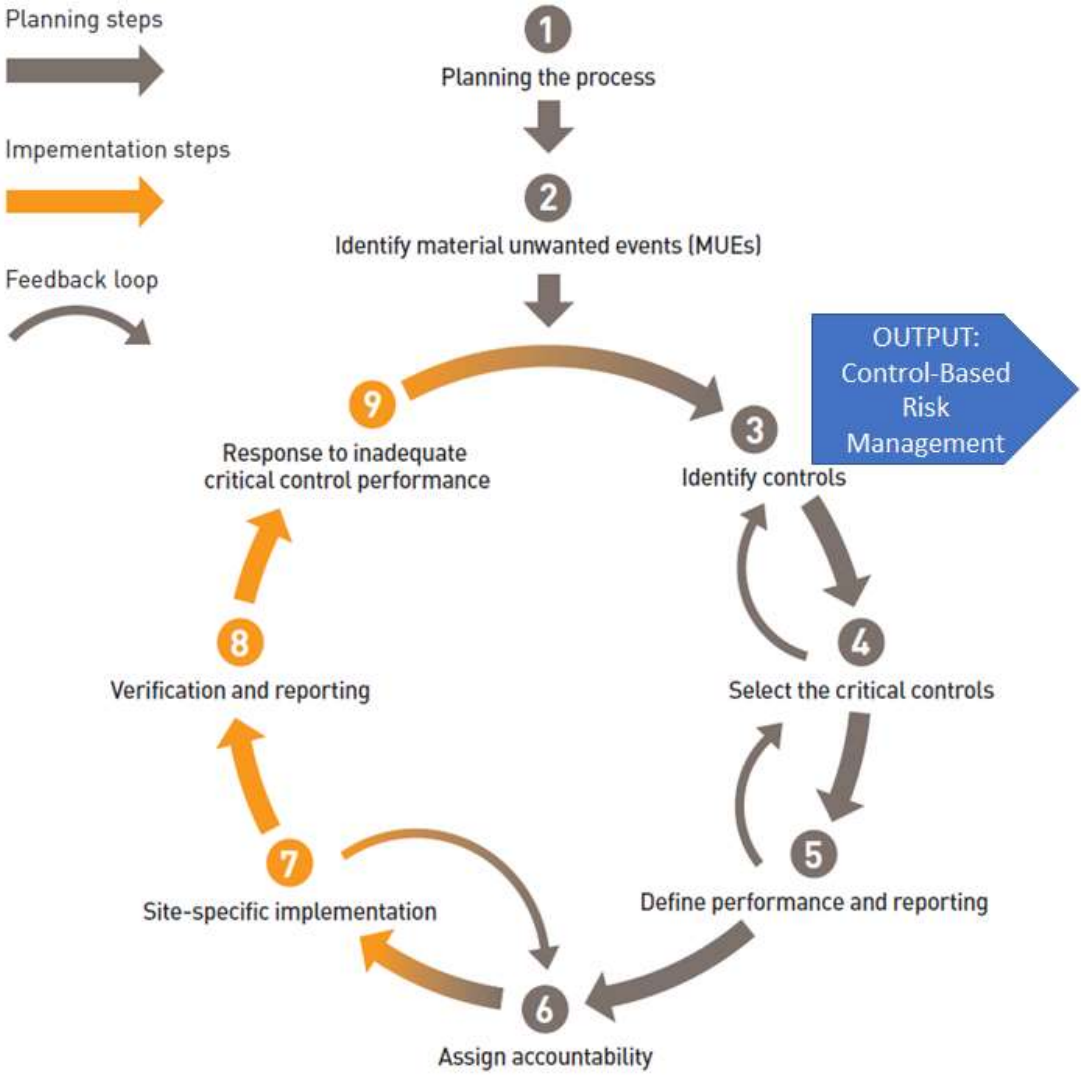
Welcome to the 7th article in the series covering Operational Risk Management (ORM) in the mining industry. Earlier articles attempted to set a foundation of terms and concepts to help understand the ORM journey, as well as to help a site identify its current position on the journey.



This article will start to discuss Critical Control Management (CCM), outlined in two ICMM publications available on their website (http://www.icmm.com/en-gb/library). ICMM initiated requests for services to write these publications in 2013 and 2014. The initial guide was written based on detailed survey and interview information from most ICMM companies, several of whom had advanced toward CCM. As such, CCM is an industry defined approach to managing H&S risks.

CCM involves a greatly improved alignment of risk management methods with effective management practice. Currently ORM can be undertaken with limited connection to the 'check and act' parts of the PDCA management process. Companies involved in CCM describe an example issue with Risk Registers that often include long lists of potential events and some controls but provide limited management value.

The illustration below shows the CCM process. There are nine steps, six of which are required to plan the CCM programme before implementation in the last three steps. The steps are presented in a PDCA style loop, recognising the need to learn from the process and the results to continually improve CCM.



The CCM process (reproduced from ICMM, 2015)

with output of step 3 added; Control-Based Risk Management (CBRM)

The CCM process outlined in the ICMM Resources provides detailed step-by-step guidance. This guidance will not be repeated in this series of articles. Detailed understanding of the above process should be acquired by reading the ICMM documents.

After two or more years of application some of the challenges of this approach have been identified. This and following articles will discuss a few of the challenges.

Challenge 1 - Incomplete step 3 before proceeding to step 4

This challenge is the most significant observation from the past two years. Some companies and sites have moved rapidly toward CCM without establishing that their overall control strategy is in place and functioning well for the priority unwanted events (PUEs). Note that the ICMM document uses the term 'material unwanted event' which this article considers to be synonymous with PUE.

Experienced mining people in the many workshops that introduced the ICMM CCM guide often expressed concerns. Individuals asked how only a few controls can be selected to manage a PUE. What about the other controls? Are they no longer important? I admit that at the time the provided answers weren't adequate. More emphasis should have been put on the importance of successful, FULL completion of step 3, including a better image of a specific target outcome. The term, Control-Based Risk Management, has been derived in this series of articles to describe this fully completed outcome for step 3.

The published ICMM Guide states the Key Actions for step 3 as :

1. *Identify the controls*
2. *Prepare a bowtie diagram*
3. *Assess the adequacy of the bowtie and the controls*

Experience seems to indicate that these steps are often completed in a single Bowtie Analysis (BTA) exercise for a selected PUE, possibly identifying new or improved controls. However, the results of the BTA have little impact on the effectivenss of the overall control strategy because they are not integrated into an effective control management approach. Sometimes the same exercise also includes selection of the critical controls. As such, the

team creates an image of the controls for an event and only briefy, if at all, discusses their current effectiveness, finally deciding which controls in the BTA are critical based on selection criteria.

Considering this observation, the questions in the various ICMM workshops may be well justified. Experienced site personnel may recognise that the overall control strategy for a PUE is not effectively in place so selecting a few controls to verify acceptable risk may be ill advised, possibly increasing the risk.

Suggested New Key Actions for Step 3

1. **Carefully define the PUE**, including the initiating event that will be the basis (or knot) of the BTA.
2. **Apply a BTA method** to identify and examine the current control strategy (Remember that a control must be an act, object or technological system – see article 3 for definitions)
3. **Critically examine the adequacy of the controls** by discussing their effectiveness (How reliable is the control? Will it be present and working as intended when needed?), erosion factors (What factors currently erode the control's effectiveness?) and supporting activities (What activities currently support the control so it is present and working as intended?). Note that the answers to these questions will also be important in the next two articles on selecting critical controls and determining verification processes.
4. **Identify ways to improve control effectiveness** by reducing the erosion factors, optimising supporting activities and other methods. Overall control effectivenss can also be improved by adding new controls. Remember that objects and technological systems are inherently more effective than acts.
5. **Define the planned overall control strategy** from the finalised BTA by drafting the Action Plan for improvements and additions, and ensuirng that the controls are integrated into relevant supporting activities such as work methods, training, engineering requirements, communication mechanisms, monitoring / auditing systems, etc.

Successful achievement of these 5 actions in step 3 of the CCM process should define a CBRM approach for the sites PUEs.

Challenge 2 – Inadequate planning for the CCM process (Step 1)

As mentioned in previous articles, the journey toward good CBRM and CCM may take many years. Planning for the entire CCM process, including the CBRM output of step 3, may be unrealistic for sites who recognise that their general focus on controls needs improvement.

Successful completion of step 3, including the establishment of effective CBRM, is a watershed for improving the control management focus of site ORM. Therefore, if the site needs to improve both methods and mindsets about controls (*managing risk is all about controls*) then planning should only consider the development of CBRM. In other words, planning that covers only step 2 and 3 of the CCM process. Once in place and effective, planning to move toward CCM from steps 4 through 9 will be much easier and the magnitude of the required work will be clearer.

The next article will address another CCM challenge, the selection of critical controls from the defined CBRM control strategies.

Article 8 – Identifying critical controls to meet objectives and selection criteria that considers cruciality, measurability and indicativeness

The 9 step Critical Control Management (CCM) process was shown in the last article with discussion about the need to establish quality Control-Based Risk Management (CBRM) for priority unwanted events (step 3) before moving to CCM. This article will continue with the CCM process, presenting a variety of approaches to selecting potential critical controls (step 4).

The 2015 ICMM guide defines CCM and critical control as follows.

> ***Critical Control Management (CCM) –*** *a process of managing the risk of material* (or priority) *unwanted events that involves a systematic management approach to ensure that critical controls are in place and effective.*
>
> ***Critical Control –*** *a control that is crucial to preventing the event or mitigating the consequences of the event. The absence or failure of a critical control would significantly increase the risk despite the existence of the other controls. In addition, a control that prevents more than one unwanted event or mitigates more than one consequence is normally classified as critical.*

CCM suggests that the risk of priority unwanted events (PUEs) can be better managed by focusing on the 'critical few' controls. CCM does not suggest that it replaces CBRM but rather supplements to achieve better risk reduction outcomes.

The above definitions can be operationalised in several ways. The guide mentions that CCM planning (in step 1) should include the identification of the Objective. Experience indicates that Objectives, defined and otherwise, for a CCM initiative vary greatly, leading to very different CCM outcomes.

EXAMPLE 1. A company or site may decide to use the CCM process to select the critical workforce acts for avoiding site PUEs. Thereby, using the process to define 'golden rules'. The Bowtie Analysis may become an illustration of controls that highlights critical acts for the workforce.

One mining company identified that 80% of its critical controls are acts. This should not be a surprise for an industry that continues, in most areas, to be people intensive.

The example illustrates a potential CCM Objective, applying the CCM process to achieve an improvement in workforce behaviour to reduce risk. However, this approach is not the intended purpose of CCM.

EXAMPLE 2. The company or site decides to select the controls for PUEs that a cross section of site personnel and experts identify as the most crucial. The Objective is to manage these selected controls with a CCM approach, so the risk is reduced. The critical controls could be acts, objects or technological systems.

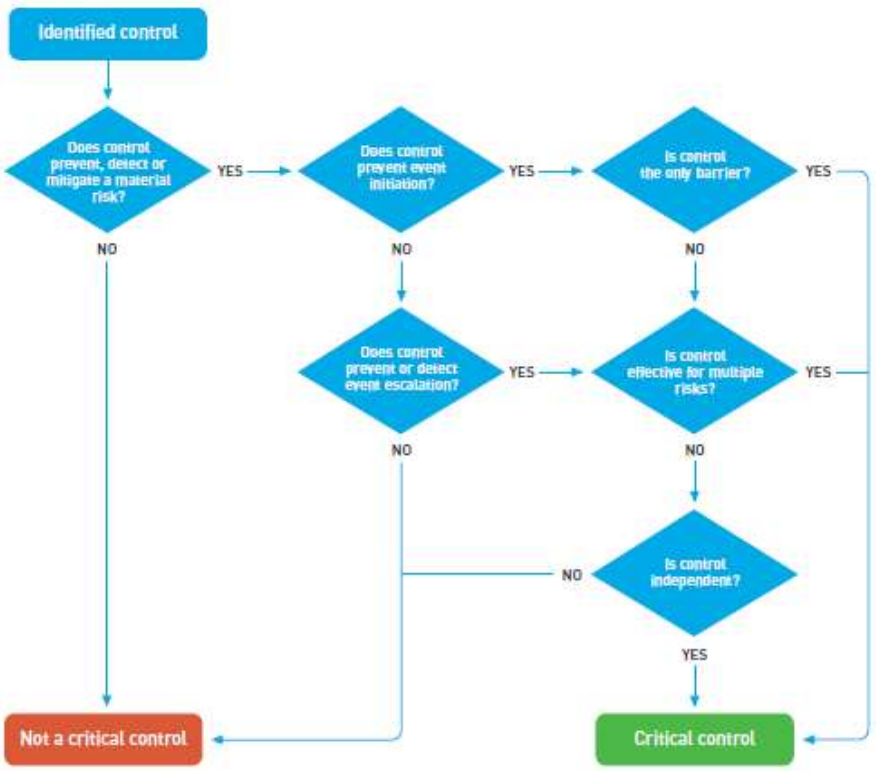
Surveys of companies involved in CCM provided insights on critical controls that align with this example.

- "A control is critical if its failure or ineffectiveness will lead to a risk scenario being greatly elevated."
- "A critical control is a control that is heavily relied upon to manage a major hazard through preventing an accident or mitigating the severity of its consequences. It needs to have a high amount of demonstrated adequacy."

- "A critical control is a non-negotiable control. If it doesn't exist, the business cannot operate."

From above, **the critical control must be 'crucial'**. What makes a control crucial? The illustration below was supplied to ICMM for the 2015 guide by BHP to illustrate their control cruciality criteria.

Figure 4. BHP Billiton critical control decision tree



Source: Adapted from BHP Billiton.

The illustration supplies a series of questions that determine the cruciality of a control so it might be classified as critical. These questions can be applied to any control whether it is an act, object or technological system.

There is another aspect of critical controls that is important to successful CBRM and CCM. **The control must be measurable**. In other words, there must be some method to identify the effectiveness of the control. If the control's status cannot be effectively measured against defined performance specifications, using some form of observation, checking,

tracking, monitoring, auditing, etc, it cannot be a control, and especially not a critical control.

Experience indicates that cruciality and measurability must be requirements of a critical control. Another may be **the degree to which the control is indicative of the overall control strategy risk.** I hope this is food for thought and discussion.

EXAMPLE 3. The company or site gathers a team cross section of site personnel and experts to review a completed Bowtie Analysis that includes the erosion factors that compromise controls and positive supporting activities for the controls. The team must decide which controls, erosion factors or supporting activities would, when measured, be the most indicative of overall PUE risk.

The Objective for example 3 is to manage the PUE risk by tracking status and changes in the expected performance of the critical indicators.

The first question is – 'would the CCM outputs in example 2 (selecting critical controls) be different for example 3 (selecting critical indicators), considering the same PUE?'

Consider a specific object that is seen to be crucial using the approach in example 2. The pressure relief valve (PRV) on a chemical process is identified as a critical control for a vessel overpressure explosion PUE. The erosion factors are corrosion (the site is close to the ocean) and poor maintenance. The supporting activities are regular testing and recording of results. The team discusses how to reduce corrosion issues and ensure maintenance is done as required. Actions are generated to address the two erosion factors. The PRV performance and verification requirements are developed to advance the CCM process.

If the same overpressure explosion is considered with the focus on critical indicators of inadequate or changing PUE risk (as per example 3), the team might identify the anti-corrosion programme acts or the maintenance planning and execution acts, as measurable indicators of the PRV status. These two potential erosion factors may also be relevant to other objects that are controls for risk in the chemical process. As such, the performance and verification requirements for the anti-corrosion and maintenance programmes would

be developed with potential implications to other threats related to the vessel explosion PUE.

If we also look at a specific act that is seen to be crucial, the difference between cruciality and indicativeness may be even more important.

An underground fall of ground may be selected as a site PUE. Review of the Bowtie for the event may identify the supervisor's inspection of the telltales on the roof as a critical control, crucial to managing ground fall risk. The inspection is an act.

The 'cruciality" team (example 2) might then begin discussions about performance requirements for the act, as well as verification mechanisms. Verification of acts using observation data usually presents challenges. (Note: more on this part of the CCM process in future articles)

The 'indicativeness' team (example 3) may identify erosion factors for the inspection of telltales such as supervisor workload causing time pressure or an inadequate reporting method for telltale data. Thereby choosing workload management and the application of a new reporting method as critical indicators.

Can a control be crucial but not indicative? Can a control be indicative but not crucial? Can something other than a control, such as an erosion factor or supporting activity, indicate the risk?

The answer is probably that the PUE risk is a combination of effectiveness measures that may be controls, erosion factors or supporting activities.

The three questions that should be asked as part of the critical control selection process should be, in addition to questions included in the BHP example above:

Is the control, erosion factor resolution or supporting activity

- Crucial? (*The absence or failure of which would significantly increase the risk despite the existence of the other controls)*
- Measurable in a manner that that indicates effectiveness?

- Indicative of the overall PUE risk?

Identifying measurable erosion factors or supporting activities for a crucial control, or individual critical control indicativeness, may be relatively easy.

Overall PUE Critical Indicativeness would require a broader look at the PUE control strategy. Once potential individual critical indicators are identified, the completed Bowtie could be considered by firstly examining the control set for each threat and considering the impact or dependence of the control indicators on the sets. High interdependence may suggest high indicativeness. High reliance on a single control for a threat would also indicate high indicativeness. This process would then be repeated for each significant threat and consequence set of the PUE Bowtie.

This approach may also help identify common critical indicators, therefore making that indicator even more powerful as a PUE risk measure.

From ICMM, *the absence or failure of a critical control would significantly increase the risk despite the existence of the other controls.* Therefore, if critical controls and/or their critical indicators can be effectively measured, and they are indicative of the overall control strategy for a PUE, they may be a relatively accurate measure of risk for the PUE.

Ideally this approach goes well beyond simply asking the question; 'If these few critical controls were the only measures of acceptable PUE risk, would I, as site manager, be comfortable?'

The next article will build on the CCM process by discussing critical control performance requirements and verification methods with an expanded focus on acts as critical controls.

Article 9 – Considering 'acts' as critical controls and the challenge of their measurability

Welcome to the 9th article in the series. Article 8 overviewed the selection of critical controls, hopefully generating some thoughts about setting company or site objectives for moving to CCM, as well as considering the concept of 'indicativeness' as a potential critical control requirement.

This article will continue with the critical control selection topic by expanding on the measurability and indicativeness of control **acts** that might be potential critical controls. As mentioned previously, acts are one type of control along with objects and technological systems (see article 3 for definitions).

Feedback on article 8 suggested that climbing onto a large vehicle or structure using 3 points of contact is an act, and possibly a critical control, if the company or site defines their priority unwanted events as single fatality consequences or higher.

Many mining equipment manufacturers have done major work to reduce precarious climbing onto or off equipment, but the need remains for people to climb at heights with 3 points of contact.

So, can this act of climbing potentially be a critical control. Is it crucial, measurable and indicative?

A generic company or site Bowtie Analysis for a fall from some defined height (possibly 1.5 m or more) would likely result in '*climbing using 3 points of contact'* as a control act for many of the related threats and possibly the sole control for some. Thus, the act could be seen as crucial.

Initial consideration of the acts 'indicativeness' may also suggest its' value as a critical control. A crucial act that is common across many threats should be indicative. However, the other part of the critical control discussion is measurability.

To be indicative of the overall fatal fall risk the act must be measurable. How do we measure this crucial, indicative act to gauge the effectiveness of controls and thereby the acceptability of the company or site fall risk?

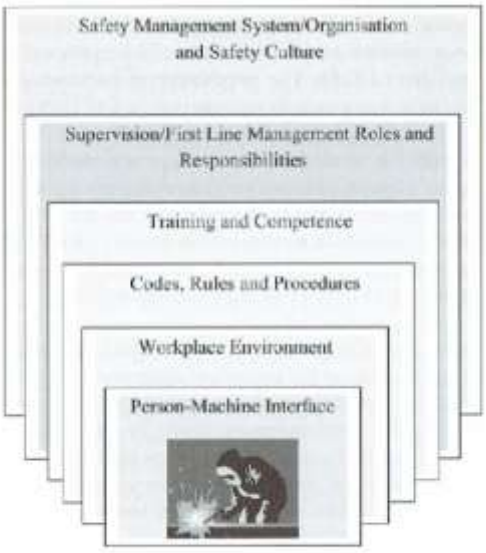
In article 8, the limitation of direct act observation was mentioned. In mining, it is often difficult to gather observation data on climbing. However, there may be related erosion factors and supporting activities that are possible measures of the likelihood that a person will use 3 points of contact when climbing.

An act has a life cycle like an object. The act must be defined, documented, transferred to the persons that are expected to act, and assessed to ensure the act is understood. Acts are also reinforced and modified to ensure they are up-to-date. Effectiveness of the steps in the act life cycle will affect the likelihood that the act will occur when required. This is how procedures, training and communication contribute to acts' effectiveness. As such, these aspects become part of an overall multifactorial 'algorithm' for the effectiveness of an act that can also include any available direct observation data.

In addition, and also mentioned in article 8, data related to the initiatives intended to reduce identified major erosion factors or to reinforce important supporting activities might also be part of an act algorithm.

The effectiveness of an act that is believed to be critical, like the *3 points of contact* example, can be established with adequate accuracy but the data used to verify the level of effectiveness will be sourced from multiple sources. Direct observation data about the act may only be part of the measure.

Another approach to considering act effectiveness contributors can be found in human error causation such as the work of Geoff Simpson and Tim Horberry as provided in the illustration below from their book “Understanding Human Error in Mine Safety” (2009).



Human error likelihood influence framework

Human error causation models such as the above provide possible prompts to help define potential erosion factors (negative influences) or supporting activities (positive influences) for a critical act. Any specific positive or negative influences on the desired act can be captured and discussed to determine the magnitude of their affect, and to identify any actions to reduce negative or reinforce positive influences.

For example, considering the Workplace Environment (assuming physical environment) related to an act such as ‘*3 points of contact climbing’*, erosion factors may be slippery climbing surfaces from equipment operation in muddy areas on site. Actions to provide methods to protect from mud or add grip to potentially slippery steps or holds could result from discussions. The success of these actions, such as the provision and maintenance of modifications, could be part of the measure for the *3 points of contact* act. In other words, act effectiveness is increased by successful reduction of erosion factors.

Related supporting activities may be initiatives to have clearly designated foot and handholds for climbing, where better engineering solutions are not feasible. This might be an existing improvement programme at the site. Measuring its degree of application across all potential climbing locations may be an indicator of act effectiveness. In other words, it is more likely the *3 points of contact climbing* will occur if the climbing location has clear and optimal hand and foot holds.

These two potential measures of act effectiveness form part of the overall effectiveness measure. Remember, we are only measuring a few controls for a high priority event so the workload to define and operate, with the assistance of computer technology, our 'algorithms' should not be excessive.

Safety Management System / Organisation and Safety Culture consideration may also help identify erosion factors for acts such as production bonus systems that reward short cuts or an absence of feedback when a person is seen climbing incorrectly. Supporting activities may include engagement of personnel in positive learning from falling incidents. Measures can also be developed for both these examples.

If a potential critical act can be measured by direct observation data, life cycle contributors, erosion factors reduction initiatives, and/or supporting activities initiatives so that line managers feel comfortable that the final measure indicates the reliability of the act, as well as being indicative of the PUE (in this case a fatal fall), then the act can be a critical control.

Another comment on Article 8 suggested that acts are also involved in the effectiveness of objects ,and the object component of technological systems, in areas such as design and maintenance. A control that applies with or without human intervention must be designed, installed, maintained and modified by human acts.

The previous discussion about measuring critical act effectiveness could also apply to object life cycle acts that contribute to the object's effectiveness. Of course, doing a maintenance act to keep a hydraulic ladder functioning well, for example, may involve a different type of act to the *3 points of contact climbing* example.

The object related act might be '*ladder maintenance done as required*', noting that the fitters experience and knowledge, as well as the conditions that he or she encounters determines the specific maintenance acts. The act is not as clearly specifiable as *3 points of contact climbing* which has implications to our measurement of effectiveness.

To explore types of acts, let's look at the various types of human performance (or acts) using Jens Rasmussen's theory. (see https://www.sintef.no/globalassets/project/hfc/documents/8-legacy-of-jens-rasmussen---andersen.pdf for a good summary).

- Skill based performance: – sensory-motor performance; – without conscious control, automated.
- Rule based performance: – stored procedures, induced by experience; – Taught problem solving/planning.
- Knowledge based performance: – in unfamiliar situations, explicit thinking; – develop plan, try it and see if it works.

The act of using *3 points of contact while climbing* is likely rule based since it has more conscious control than walking or climbing stairs which are skill based. The act of '*ladder maintenance done as required*' is knowledge based.

Measuring rule based acts has been discussed earlier in this article. Measuring knowledge based acts may require greater emphasis on measurement of factors such as knowledge and experience. It is probably a much more difficult to use direct observation of the maintenance act as an indicator that the critical control object is well maintained. Overall object effectiveness measures may be more aligned with maintenance plans and reports.

However, there may be also be valuable insights into measurable contributors resulting from discussing erosion factors and supporting activities for object design, maintenance and modification acts.

In summary, knowledge based acts may be potential critical controls or important contributors to a critical control such as an object. In both cases their measurability is more

significantly based on factors that contribute to the act occurring rather than direct measurement of the act itself which is often easier for rules based acts. This will likely increase the complexity of measurement, but both the related discussion and final measurement, and thereby verification process, definition should be a major contribution to the effectiveness of a knowledge based critical act.

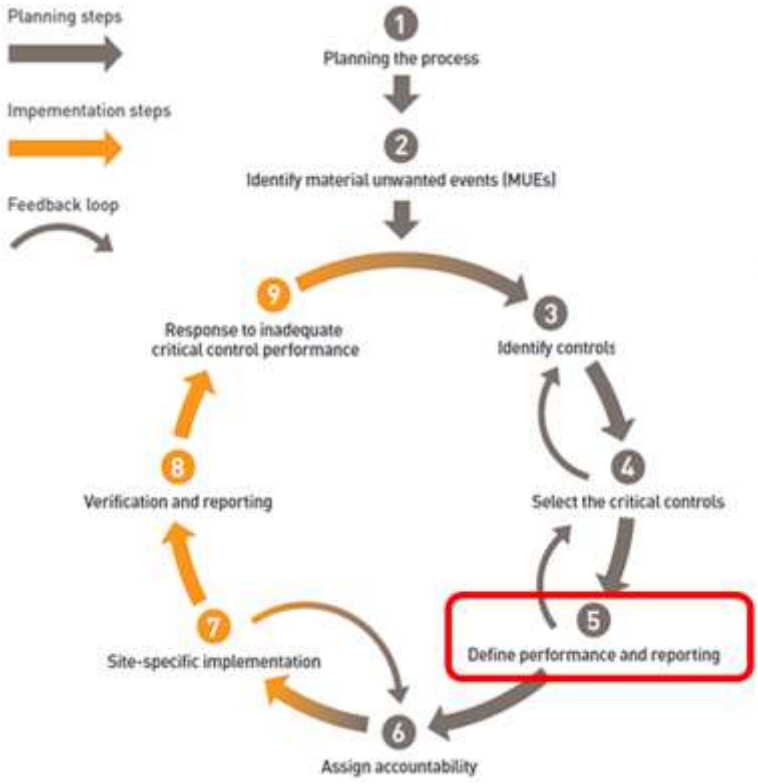
Finally, the challenge is to define a good act 'algorithm' (set of measures and their weighting in the final total effectiveness measure) that establishes control effectiveness and is an indicator of overall event risk.

The next article, early in 2018, will discuss defining performance requirements for a selected critical control, followed by more discussion about measurement 'algorithms' in critical control verification and reporting.

Merry Christmas and have a safe, healthy and happy 2018.

Article 10 – Challenging critical control performance requirements

Welcome to article 10. This article continues to discuss the Critical Control Management (CCM) process using the structure outlined in the ICMM CCM guide (2015) with additions based on experience related to CCM initiatives in major mining companies.



Article 9 dealt with critical control (CC) selection (step 4) and measurability issues with control acts. This article will discuss part of step 5 in the CCM process; the development of CC performance requirements. Verification, reporting and accountability will be covered in future articles.

When the ICMM guide was written, this step in the CCM process was seen as important by senior risk expertise in leading ICMM companies. The guide suggests that the selected critical control should be challenged with a series of questions to ensure its performance is appropriate for its purpose. Note that some information generated in this step may be like previous discussions about erosion factors and supporting activities for a control.

Discussing and documenting the performance requirements of a CC may be seen as extraneous work in an already significantly complex health and safety project. However, especially with objects and technological systems, discussing performance requirements may lead to important insights. Let's look at this step differently based on the type of control.

Let's firstly examine **CC objects** (controls that function without human intervention) and the **object/equipment component of the technological systems** (that require acts to apply). A pressure release valve (PRV) in a minerals processing or mining situation will be used as a simple example. The PRV must release over-pressure without human action. Therefore, it is an object control.

The potential CC object should be examined by answering a set of questions about its objective, performance requirements and current performance-affecting activities in the management system.

1. What is a clear description of the CC object and its specific objectives related to the relevant priority unwanted event (PUE)? The specific CC objectives describe the intent of the control related to preventing the threat or mitigating the consequence. Note that there may be several objectives for complex threats or where the same CC applies to multiple threats. *EXAMPLE: The control is a PRV located in the ____ process at _____ location. Its objective is to safely release excessive pressure from*

the process. This is its only objective in the process when all threats to process pressure explosion are considered.

2. What are the CC object performance requirements to meet the objectives? Consider aspects such as:
    a. What is the object required to do to achieve the objectives? *EXAMPLE: The PRV must open and safely direct the released _____ energy under pressure.*
    b. When is it required to function? What is the input or signal to the object that initiates application? *EXAMPLE: The PRV should automatically open when internal process pressure exceeds _____.*
    c. Where is the CC object to be located to function as required? Consider both input and output locations if relevant. *EXAMPLE: The PRV must be located where the energy release is directed _____, away from the following possible work areas based on the nature of the energy; _____.*
    d. Does it have any dependency on other controls or systems to effectively function? If so, this may compromise the CC which may require a design change. *EXAMPLE: No. The PRV is an independent control. Pressure sensing and release control are part of the PRV design.*
    e. What aspect ensures its survival during the PUE and ability to function if required? *EXAMPLE: An external fire and/or rapid over pressurisation event should not compromise the PRV function.*

3. What is the target CC performance? Try to define a metric that might be used to measure the CC status and is suitable for defining a target level (e.g. % applied, % function, etc.). *EXAMPLE: The PRV is a CC so its target performance is 99.95% of demand.* Note that design reliability of a CC object should be a purchasing criterion.

4. What level of CC performance would initiate immediate reactive action such as shutdown, CC review or investigation? *EXAMPLE: Any PRV failure on demand or observation that the PRV cannot function will initiate process shutdown and*

investigation.

By considering the above set of questions for a specific potential CC, weaknesses or issues with a potential CC may be identified. This will require improvement of the CC or replacement of the CC. In the latter case, the CC selection, step 4 in the process, will need to be repeated.

Now let's examine CC acts and the performance requirement step. The *3 points of contact when climbing* act will be used as the example.

Again, each potential CC act should be examined by answering a set of questions about its objective, performance requirements and current performance-affecting activities in the management system. Some of the questions are different from the CC object.

1. What is the clear description of the CC act and its specific objectives related to the relevant priority unwanted event (PUE)? The specific CC objectives describe the intent of the control act related to preventing the threat or mitigating the consequence. Note that there may be several objectives, for example, for complex threats or where the same CC applies to multiple threats. *EXAMPLE: the control is the act of using 3 points of contact when climbing. The act is intended to provide the climber with safe holds on surfaces being climbed whether it be equipment or structures.*

2. What are the CC act performance requirements to meet the objectives? Consider aspects such as:
    a. What is the act required to accomplish to achieve the objectives? *EXAMPLE: The act must involve gripping the equipment or structure with 3 of the 4 available hands and feet at any point in the climb*
    b. When is it required to occur? What is the input or signal to the person(s) that initiates the act? *EXAMPLE: The act is initiated by recognition that equipment or structure must be climbed to heights greater than ___ metres.*
    c. What is needed to support the act? E.g. procedures/instructions, equipment, knowledge/skill, signals, etc. *EXAMPLE: The equipment or structure to be*

climbed must be designed with clearly indicated, slip resistant hand and foot holds that are ergonomically located to optimise reach, or access should involve the use of suitable equipment such as scaffolding. Also, there must be no requirement for the climber to manually carry load when climbing.

d. Does the act have any dependency on other controls or systems to effectively occur? If so, this may compromise the CC which may require a design change. *EXAMPLE: 3 points of contact climbing is dependent on equipment and structure design for safe hand and foot holds, the availability of alternative access equipment such as scaffolds and the availability of equipment to lift loads to height so manual carrying is not required.*

Logically, the target CC act performance is 100%, or the act occurring whenever required. However, note that the measure of effectiveness will be further discussed as part of the verification 'algorithm' definition in the next article.

The level of CC act performance should be defined that would initiate immediate reactive action such as a work stoppage, CC review or investigation. For example, the site may decide that 20% deviation (or only 80% control effectiveness) from an expected act like *climbing with 3 points of contact* would warrant immediate addressing. As discussed earlier, the effectiveness 'score' may be an 'algorithm' of contributing factors that yields a percentage.

The performance requirements for the CCs should be documented for future review that should be required if a related potential or actual incident occurs, or simply for a timely CC review process as operations change.

The next article will discuss the derivation of CC verification activities, based on the definition of a CC specific 'algorithm' of factors that contribute to CC effectiveness. According to recent ICMM member feedback, this step has been challenging.

Article 11 – Establishing verification process – possibly the most challenging part of CCM

Article 11 in this series about Control Based Risk Management and Critical Control Management (CCM) will discuss a vital part of effective CCM, verification.

This article has been the most difficult to write. There is little agreement across mining companies about verification methods, generally aligned with their varying objectives for adopting some form of CCM.

A quality CCM process analytical steps should provide the following outcomes:

1. A list of priority or material unwanted events (PUE)
2. An image of the overall control strategy (all important controls) for managing the PUE risk, considering erosion factors and supporting activities
3. A carefully selected and challenged list of specific PUE critical controls that are crucial, measurable and, ideally, indicative of PUE risk
4. A verification process that captures timely data concerning critical control effectiveness and, ideally, provides an indication of any changes in PUE risk

The verification output of CCM is the most significant enhancement of previous good practice risk management. As suggested by one mining company, verification greatly improves the management in risk management.

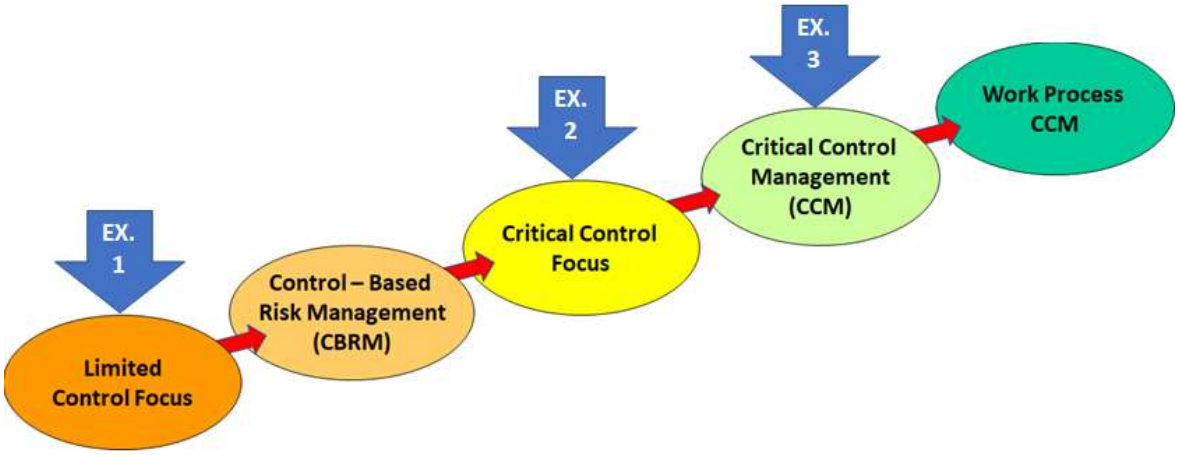
Verification is defined in the ICMM guide as "the process of checking the extent to which the performance requirements set for a critical control are being met in practice." This means that the verification process should align with the defined critical control (CC) performance requirements (see article 10 re performance requirements).

Verification should be a unique CCM term. To identify the degree to which a critical control is meeting its performance requirements (i.e. its' effectiveness), it is necessary to define a process that gathers data from multiple and possibly diverse sources ranging from direct observation to systems review, and other sources. It should not be confused with monitoring or auditing.

It's important to highlight the potential value of CCM verification as a timely indicator of changing risk. In an adequately mature company or site, CCM verification can more effectively 'keep tabs' on the risk of high consequence events, going well beyond just focusing the workforces' attention on a 'few critical controls'.

The sources of verification data, the frequency of data gathering, and the quantification of data to establish effectiveness are the most common areas where differences exist between industry opinions and practices. To discuss these differences, it may be helpful to continue using examples of companies or sites at various points in the CCM maturity journey.

In article 8 the variation in company or site CCM objectives was discussed. "*Experience indicates that objectives, defined and otherwise, for a CCM initiative vary greatly, leading to very different CCM outcomes*." Three examples were given. These examples can also be used to illustrate levels of risk management maturity (as illustrated below) that can be reflected in their verification process design.



EXAMPLE 1. *A company or site may decide to use the CCM process to select the critical workforce acts to prevent site PUEs. Thereby, using the process to define 'golden rules'.*

Example 1 illustrates a focus on human error to reduce PUEs that are usually single fatality issues. Verification might involve gathering of data from Task Based Observation (TBO) or similar initiatives that have been focussed on the new 'golden rules'. As such, though data observation quality is usually limited, the company or site may feel that a regular review of TBO results is adequate to understand whether the PUE risk is acceptable.

This approach adopts some ideas to improved control focus but is not a quality CCM approach.

EXAMPLE 2. *The company or site decides to select the critical controls for PUEs that are identified as the most crucial by a cross section of site personnel and experts. The Objective is to manage these selected controls with a CCM approach, so the risk is reduced.*

The focus in example 2 is more mature that example 1. The company or site is looking beyond human error to find controls that are crucial and measurable. Their verification process might include several data sources that cover a range of factors contributing to critical control (CC) effectiveness. The data may be combined using a checklist or stoplight approach to identify weak areas for action. However, there is no attempt to generate a single overall effectiveness measure for a CC or the impact on PUE risk.

Some Example 2 companies and sites use two major sources of CC verification data, supervisor **direct observation** data and systems review of **supporting activities** information

such as procedures, usually done by superintendents or managers. However, the data from the two sources is not combined to establish CC effectiveness.

This example utilises the complete CCM process but misses the opportunity outlined in example3.

EXAMPLE 3. *The company or site gathers a team cross section of site personnel and experts to review a completed Bowtie Analysis that includes the erosion factors that compromise controls and positive supporting activities for the controls. The Objective for example 3 is to manage the PUE risk by tracking status and changes in the expected performance of the critical indicators.*

Example 3 is the most mature. Leaders want CCM to provide an indication of PUE risk. CCs are challenged to identify measurable, performance requirement related factors that impact on their effectiveness. Those measures and other factors generate a quality result for that specific CC. However, the company or site is not satisfied with a single CC focus (example 2). The aim is to have a timely indication of the effectiveness of all PUE CCs; a measure of the overall PUE risk.

Consider a CC Object in a processing plant such as the pressure relief valve (PRV). The PRV manufacturer may supply PRV reliability or effectiveness figures which might be considered the baseline. The challenge is to appropriately consider local factors that affect the reliability to modify the baseline figure to reflect the local situation. The local data sources might include reports covering maintenance and repair work relative to performance requirements, as well as local operating conditions. Other sources might include design /modification / installation checks, records of past release events, etc. Using various methods, this approach has been used in petrochemical industry risk analysis for several decades to generate predicted reliability and compare that figure to safety requirements.

The challenge in CCM is to define dynamic measures of that reliability (or effectiveness) that will indicate any change in CC status. Timely data must be gathered on factors that may impact on the predicted PRV reliability, possibly reducing it. Very often in a processing plant this data, as well as unacceptable variation criteria, are part of process control.

However, when the CCs for a PUE are Acts, or Technological Systems where Acts and Objects must function together, then estimating ongoing effectiveness is usually a greater challenge. Difficult measurability as well as inherent human reliability issues should drive us try to evolve our CCs towards Objects or at least well designed Technological Systems. However, the magnitude of that change is great for traditional industries such as mining, as indicated by the mining company that suggested 80% ot its CCs for 20 PUEs were Acts.

There are baseline human reliability figures (called human error probabilities - HEPs) available through Human Error Analysis techniques in industries such as nuclear power generation. The methods also include Performance Shaping Factors (PSFs) that are used to modify the HEPs for local conditions. As such, roughly aligning with the previous approach example on the CC PRV.

However, it is unlikely that these probabilistic human error methods will be adopted by more traditional industries such as mining soon. As companies and sites rapidly move toward CCM another approach to measuring CC Act effectiveness and possibly overall PUE risk, is required.

The baseline for a specific human CC Act should be some form of observation. For example, supervisors' observations might yield figures such as 78 times out of 100 observations the act of *climbing equipment with 3 points of contact* occurred as expected. However, many confounders potentially affect the quality of CC Act direct observations, often making the related data questionable.

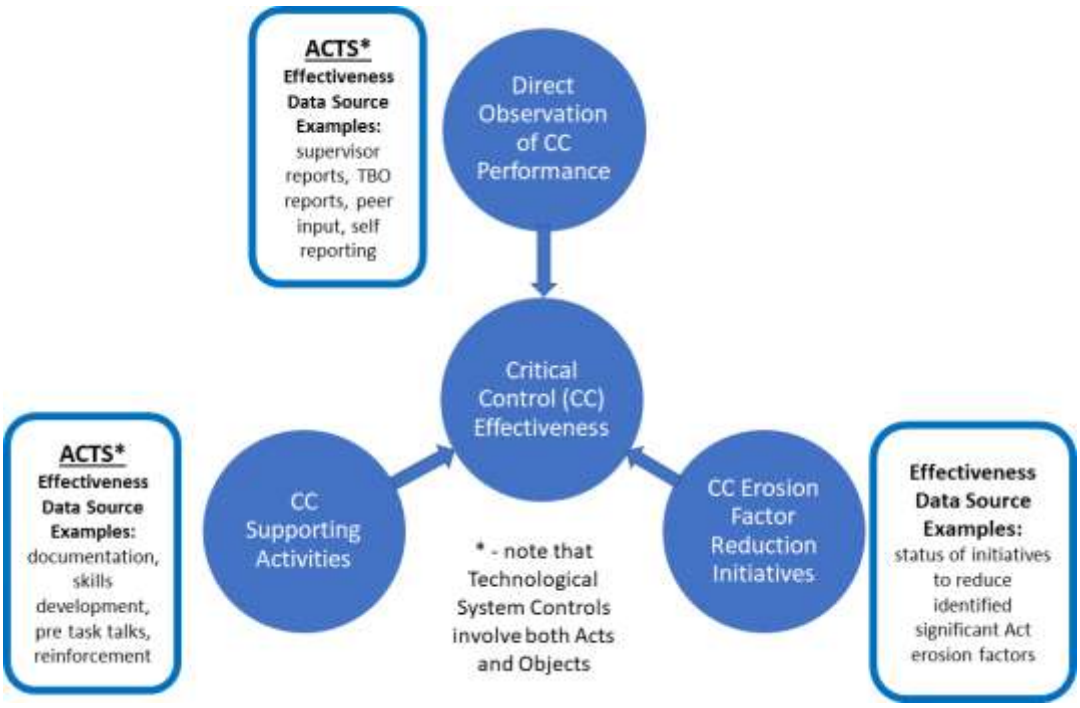
For a CC Act to have quality observation data it should

- Be observable for a significant percent of expected occurrence (ex 10-30% of the expected equipment climbing situations per defined time period to establish 3 points of contacts acts),
- Involve an Act that occurs with some regularity, such as a prevention control, and not an Act that only occurs during an unwanted event (i.e. a very rare act)

- Involve an act that can be observed without the person doing the act being consciously aware of the observation, especially if the observation data is to be significantly extrapolated across a large percentage of unobserved acts, and
- A data gathering method that records the act observation so that it can be easily gathered and used to generate the effectiveness.

In many cases, meeting these suggested criteria may be difficult. Solutions might involve developing an observation technology such as the example provided in article 3 on GPS-based vehicle operation monitoring in a surface mine. More commonly, however, limited direct observation ability will need to be supplemented by other data sources to gauge effectiveness.

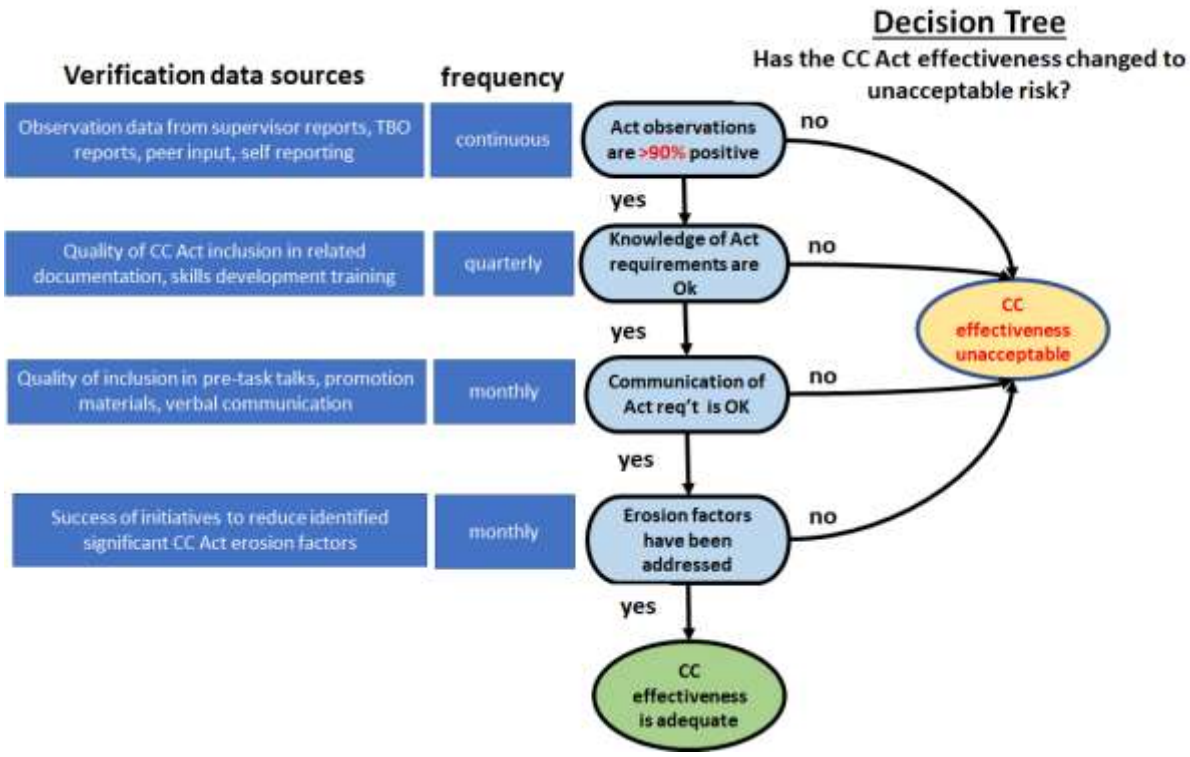
For some CC Acts this might involve some observations as well as review of related supporting activities to examine the degree to which the CC Act is adequately included. Past articles discussed erosion factors for a control. Regular systems review may also involve gathering data on the status of important erosion factor reduction initiatives.



The illustration above suggests three sources of data that could indicate CC Act effectiveness. If quality data is available from direct observation which is sufficient to quantify a measure such as percent effective, then data from other sources may not be as important. However, as discussed, this may be difficult.

In earlier articles the term 'algorithm' was used to provide an image of verification measurement. An 'algorithm' is a process or set of rules to be followed in calculations or other problem-solving operations. The term is used in these articles to refer to a process of combining data on CC effectiveness from multiple sources to generate a single CC effectiveness measure that can be combined or compared to other CC measures. Algorithms can be arithmetic or logic-based such as a decision tree.

If we build on this approach, based on the assumption that the company or site fits our example 3, that is the company wants to monitor for changes in PUE risk, the 'algorithm' decision tree approach to measuring effectiveness can be discussed.



This EXAMPLE illustration shows a specific set of decision nodes that could be used to answer the question 'has the CC Act effectiveness changed to an unacceptable risk?". The

decision nodes are based on the data sources listed in the earlier illustration. Example frequencies of data gathering are also shown.

Constructing a decision tree specific to the CC Act and the company or site performance requirements provides an opportunity to combine observation data and addition decision nodes to define a consistent ‘algorithm’ for the company or business to dynamically consider CC Act effectiveness.

Although this method does not generate a quantified measure of effectiveness like the PRV example, it can generate an indication of individual CC effectiveness when combined with other CC information for a PUE, providing an image of overall PUE risk.

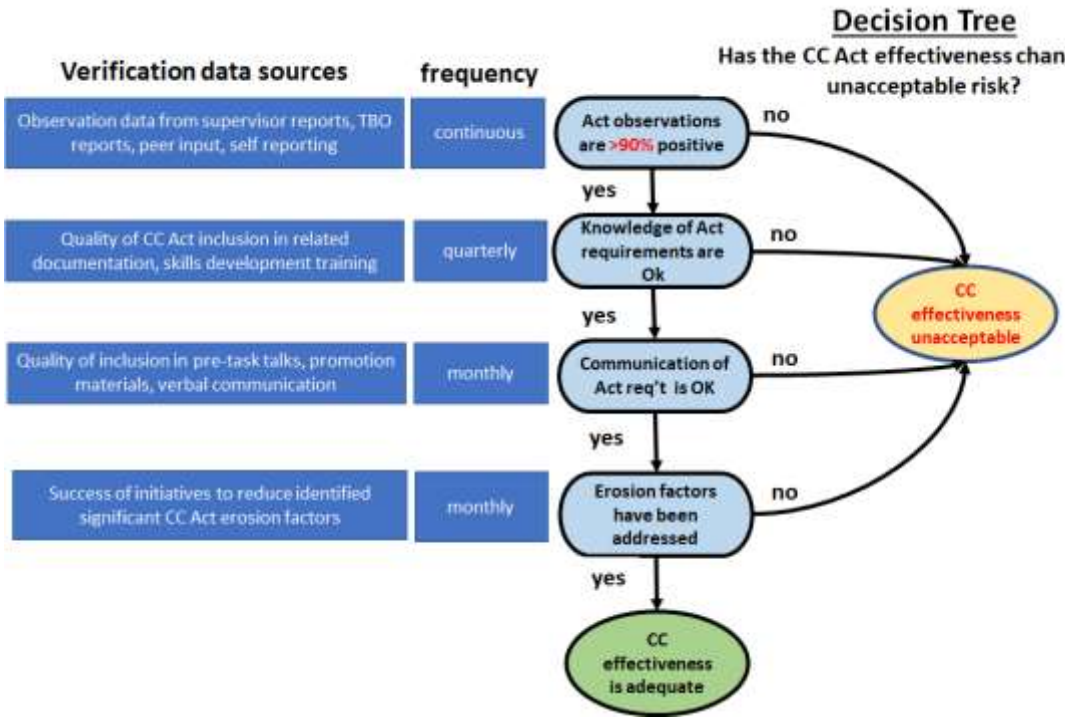
Future articles will complete the CCM process by discussing reporting, site integration and learning steps.

Article 12 – Linking the Critical Control Performance Requirements to the design of the Verification Process

Welcome to the 12th article in the series. intended to generate discussion amongst H&S risk professionals and managers about improvements to the site Operational Risk Management (ORM) thinking and methods.

The content of this article has been developed in conjunction with another retired risk management professional, Andrew Morrell. Andrew and I had several discussions before the last article was published, helping to demonstrate the importance of linking the verification process with Critical Control (CC) performance requirements. This is especially important if the company or site selects an Act as a CC.

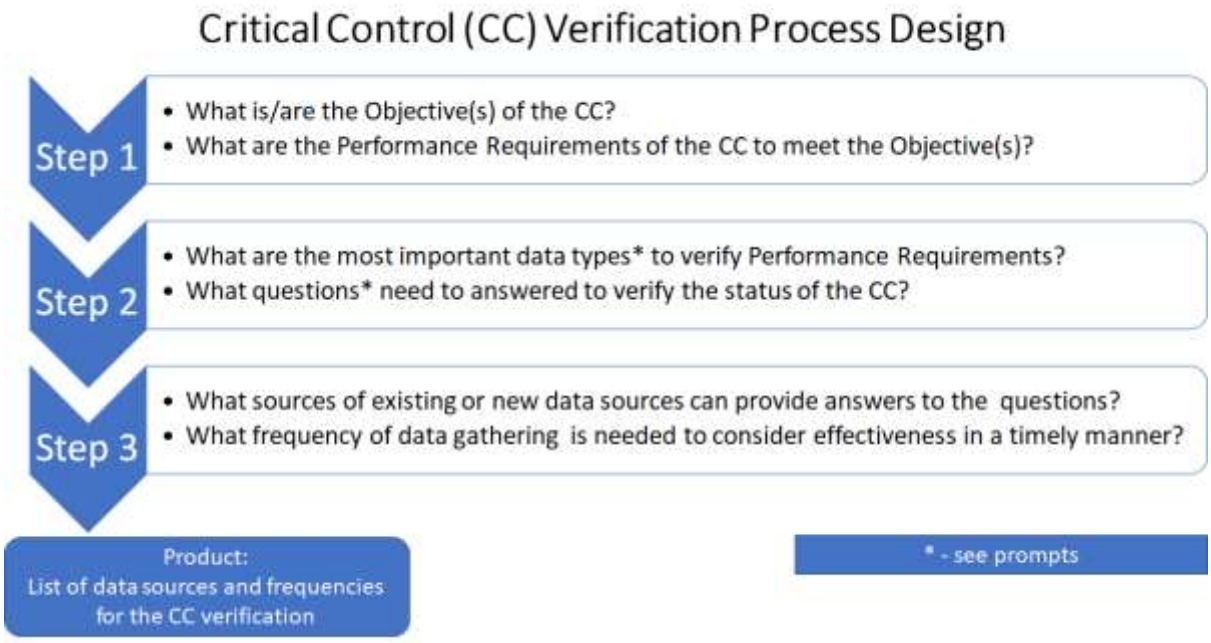
Several examples of companies or sites at different stages of the CCM journey were suggested in the previous article on defining the verification process. This article will continue with the discussion of verification for companies or sites that are advanced in their control-focused maturity.



In the last article the illustration above was used to illustrate a basic verification algorithm to examine the effectiveness of a CC Act. Four binary questions are used to create a decision tree that could establish if a CC Act is acceptably effective. Boxes on the left list potential sources of data to answer the suggested questions, as well as an example frequency -for gathering the required data.

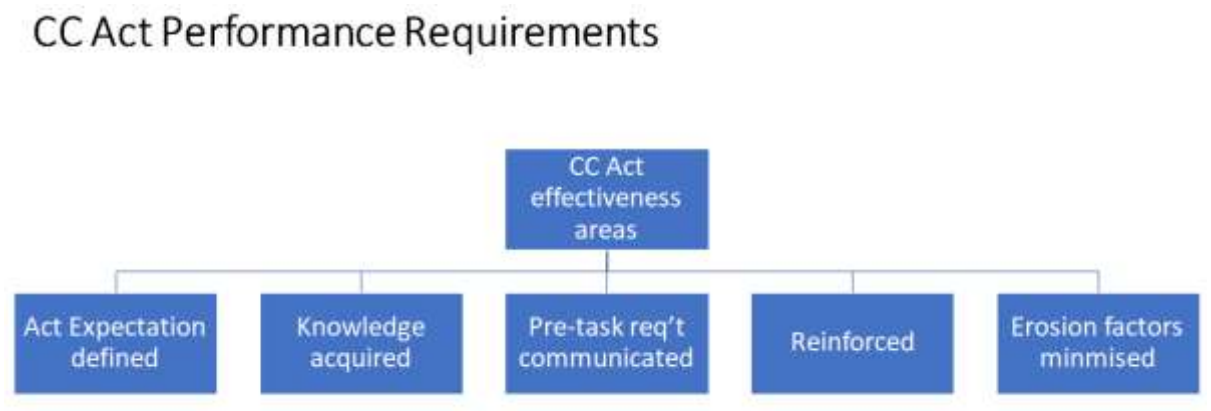
The previous article also mentioned the relationship between verification to determine CC effectiveness and the performance requirements. (Verification is defined in the ICMM guide as “the process of checking the extent to which the performance requirements set for a critical control are being met in practice.”)

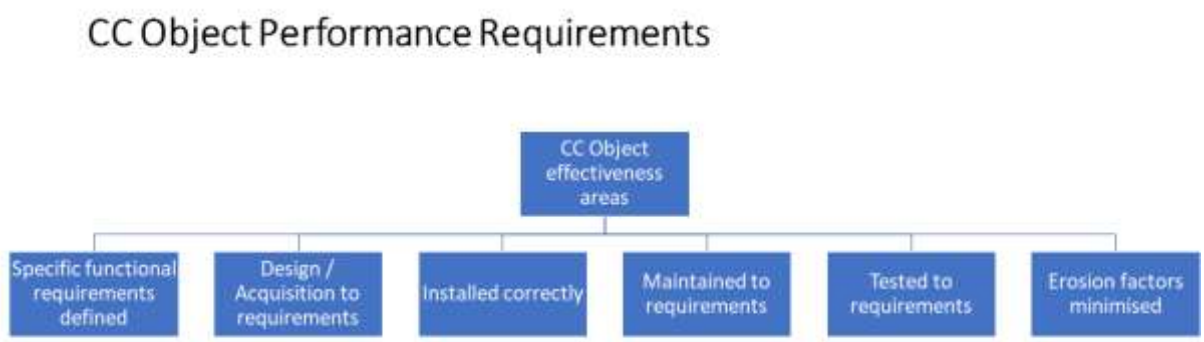
However, it may be important to take a more systematic approach to this relationship. The illustration below suggests a three-step process from CC selection to verification process design. Note that the illustrated process is linear but if the questions cannot be answered, the process would be iterative.



Step 1 was outlined in Article 10 of the series. The first illustration in this article, also found in article 11, is a basic illustration of Step 3. However, Step 2 has not been significantly discussed in earlier articles. Step 2 provides a systematic link between Performance Requirements and Verification design and, iteratively, may influence the nature of the Performance Requirements.

Following are two basic examples of prompts for 'data types' as suggested in Step 2. Note that these topics go beyond direct observation of acts or objects that gathers data on effectiveness. They generally describe an Act or Object lifecycle from left to right.



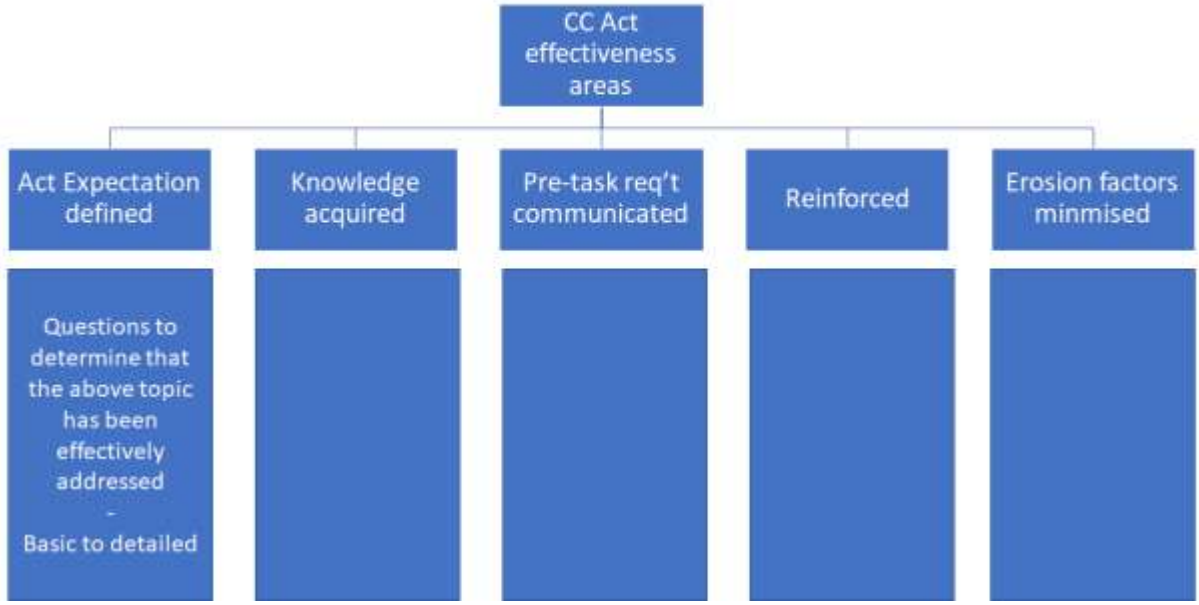


The above illustrations suggest a basic set of 'data types' that might be considered for topics to help define CC Performance requirements, other than direct observation data. Depending on the specific CC, some 'data type's may be more important Performance Requirements than others. For example, complex CC Acts may be more dependent on acquired knowledge. This should be reflected in the specific Performance Requirement description.

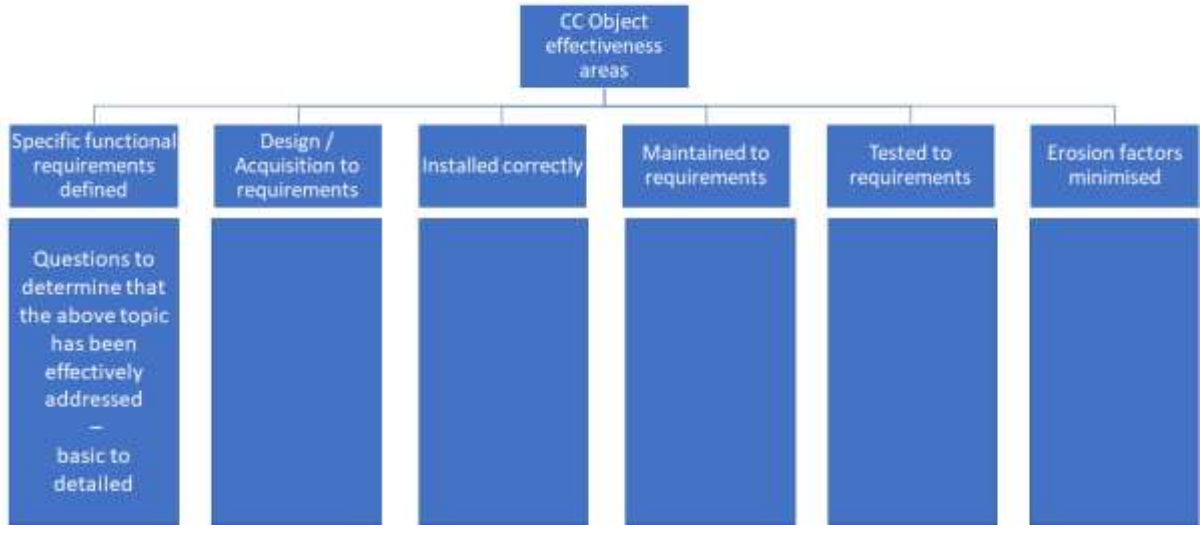
Once the Performance requirements, aligned with the data types, are defined, questions to determine whether the data type issue is adequately addressed need to be developed.

Questions could range from general to very specific depending on the Performance Requirements, as per the illustrations below.

CC Act Verification Questions



CC Object Verification Questions



Examples should help so consider two different CC Acts. In past articles we have considered the act related to ***climbing using 3 points of contact***. This Act is intended to prevent a fall.

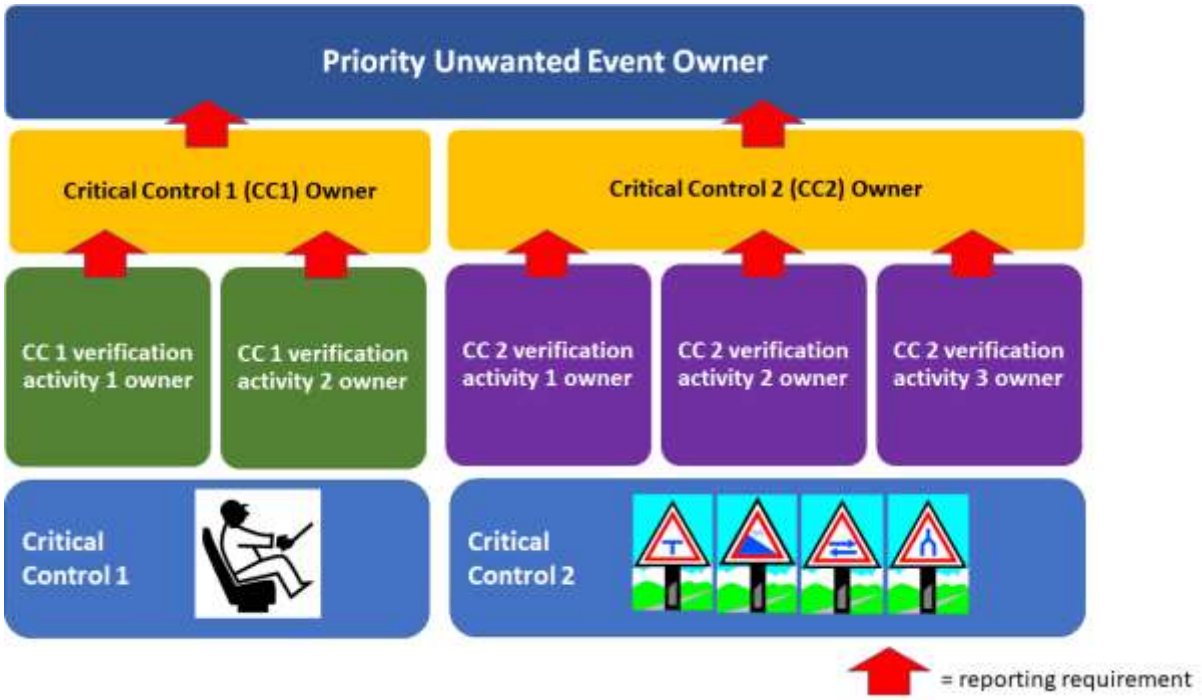
Our second example isa an act intended to mitigate an unwanted event; ***call for additional support for poor roof conditions.***

Article 13 – Defining accountabilities and the reporting process

Welcome to the 13th article in a series. This article will discuss establishing accountabilities and a reporting system so that the critical controls are effectively managed. As mentioned in previous articles, the Critical Control Management (CCM) process includes good practice risk assessment and analysis methods, plus an important greatly improved ingredient; more systematic management.

The last article addressed the careful definition of the verification mechanisms that gather data in a timely and effective manner. This is the 'check' in the Plan-Do-Check-Act model of management. Now we need effective reporting to connect the 'check' (verification) with the 'act' or action to improve by setting the accountabilities and defining the verification data-related information that should be reported to the accountable individuals.

The illustration below suggests an ownership model to set accountabilities for critical control verification and reporting. A site or company identifies several priority unwanted events (PUEs) that are included in their CCM initiative. Each of the PUEs is assigned to an owner. The owner is usually a line manager with responsibilities that include the activities where the PUE could occur. For example, at a site level the production manager could be the owner of a PUE related to vehicle collisions. If the CCM initiative is managed at the corporate level the vehicle collision PUE might be owned by a production executive.



The above illustration suggests three levels of ownership. The example PUE is related to vehicle collisions. Two example critical controls involving specific driving acts and road signage are provided.

In the example, two verification activities have been identified for critical control 1 (CC1) and three for critical control 2 (CC2). An owner is assigned for each of the verification activities. They are accountable for gathering the verification data with the defined frequency and forwarding that data to the critical control owner. Note that some assembly or interpretation of the data may be required before it is forwarded to the control owner. Acceptable levels of critical control effectiveness should have been defined as part of the performance requirements (see article 10). Formats such as stoplight reports, considering defined performance levels, might be helpful to concisely communicate verification data.

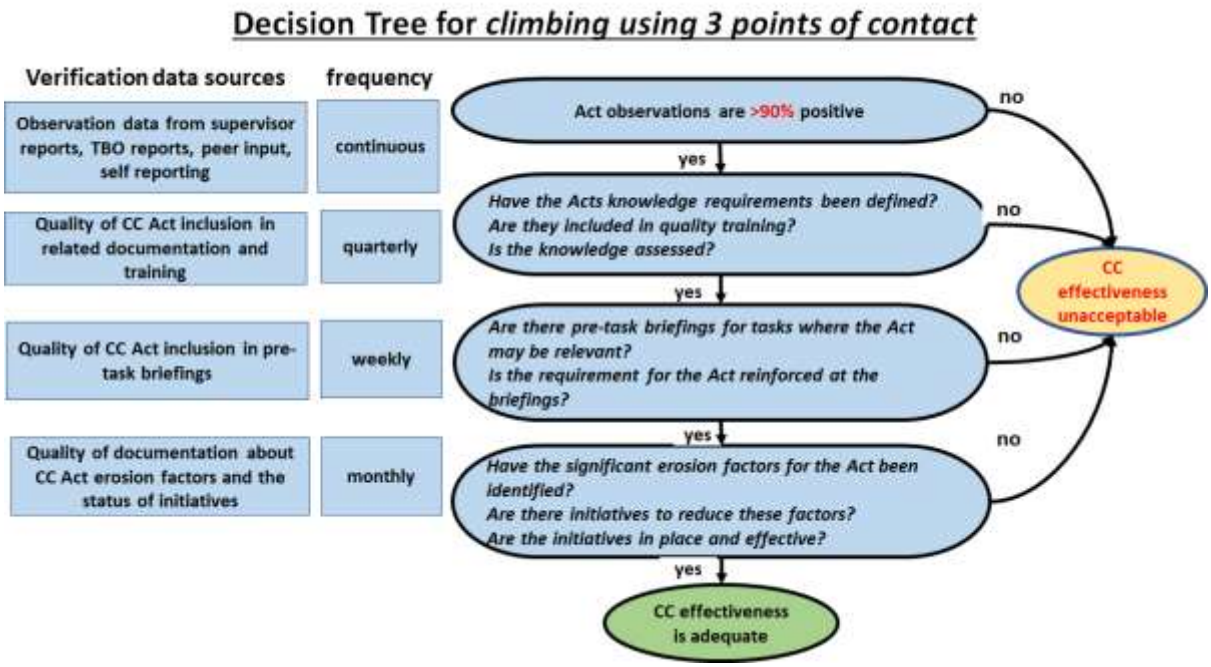
The illustration shows two critical control owners. Note that there may be more critical controls for a single PUE. The critical control owners assemble the data information from the verification activity owners to provide a single indicator of control effectiveness to the PUE owner.

As a result of this process, the PUE owner should get regular reports on the effectiveness of all critical controls related to his/her PUE with low and unacceptable effectiveness results

highlighted. Action should be taken to address unacceptable effectiveness as soon as possible, including the decision to stop the activities where the risk exists.

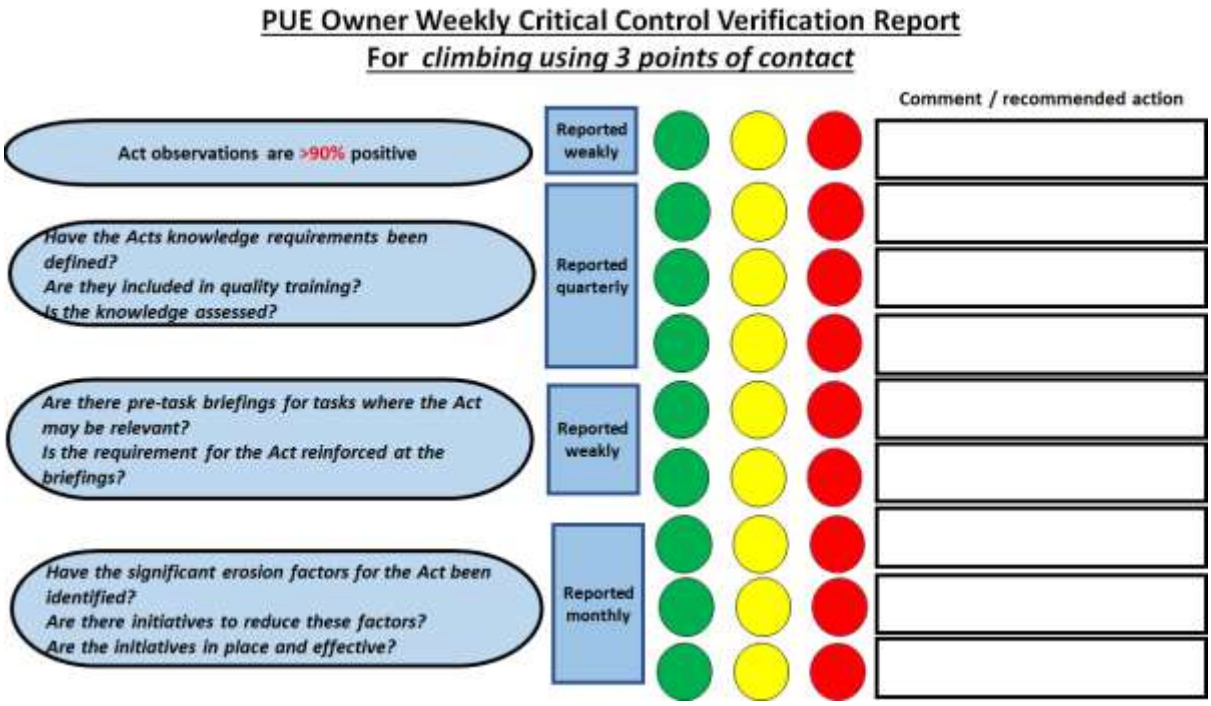
Managing the data and generating concise reporting can be a big challenge in this step of CCM. The above illustration shows only a small example segment of the process. If a site has 10 PUEs with 6 critical controls for each, there may be 5 verification activities for each control. That results in 300 sources of data and a team of 370 owners at various levels. Clearly a 'hard copy' paper-based approach to this size will be very punishing for a site or organisation. Data management technology should be considered.

The example verification process outline from article 12 can be used to discuss electronic gathering of data and computer-assisted assembly and analysis.



In the above example there are four verification data sources (left boxes) that need to be gathered, assembled and reported to the appropriate owners. Each of the four sources has a different defined frequency for data gathering ranging from continuous to quarterly. Part of reporting system design should include the required reporting frequency. The site or company will decide on whether each of the four data sources is reported to the relevant owner separately or as one report. The latter is recommended.

If one report format is used for communicating verification information from several sources, such as the four areas illustrated above, then the report should be sent to the PUE owner at least weekly with information on the continuous and weekly verification activities. The monthly and quarterly verification data would be updated on the report when data was available. A rough illustration is provided below as an example.

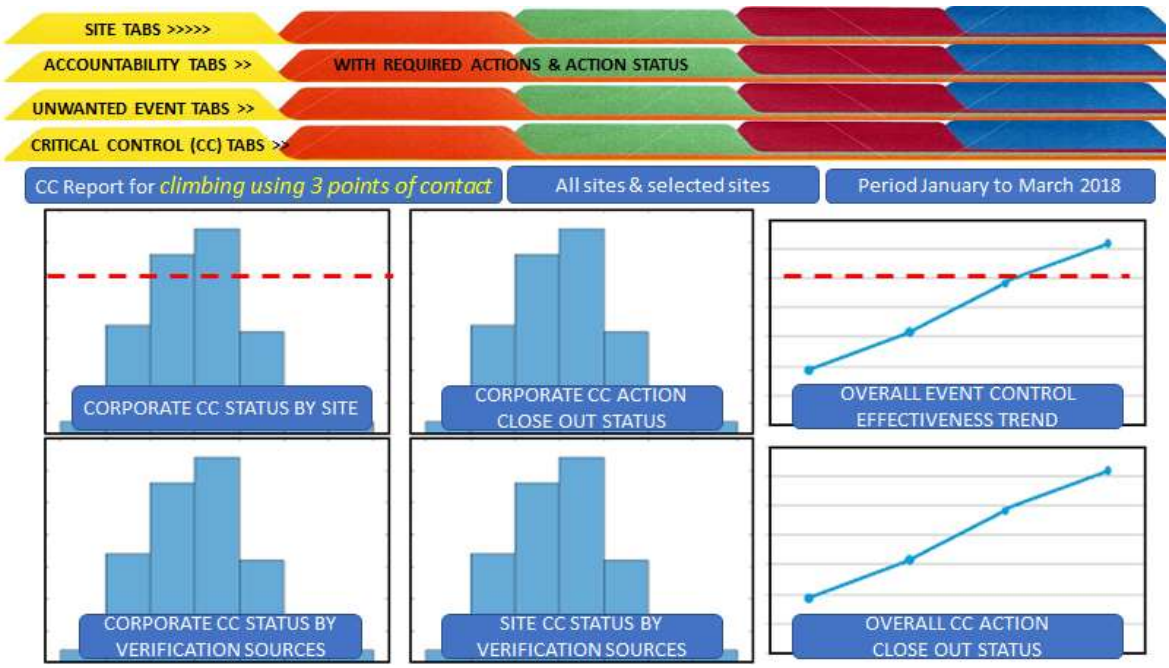


The previously established verification areas and frequencies have been included in a basic stoplight report that critical control owners would create, including their comments on any results including potential recommendations for addressing a yellow or red light. Trigger levels for verification data should be defined to establish green, yellow or red reports. For example, for "Act observations are 90% positive, at 90% or greater the result would be green. Red would be observation results below a figure usually identified in the verification design, for example 75%. Yellow would be an observation data levels between the 75 and 90% level. Other verification questions may require a more subjective guideline.

Computer systems offer an opportunity for streamlining input to this and other reports by gathering and aggregating data electronically, rather than using paper-based reports. As mentioned earlier, the data gathering magnitude for a site may be quite large, so it is

recommended that electronic data input and analysis be part of the design of the verification and reporting system from initial setup.

Executive committees or company boards may also require summary reports that include critical control status for all priority unwanted events at relevant sites. Of course, a good data management approach should facilitate the provision of effective 'dashboards' for the organisation. A basic example is provided below.



The above example suggests that a dashboard that includes all data about priority unwanted events, critical controls, verification activities, ownership and required actions for all sites or locations where the events may occur. Reports generated from this dashboard should be designed by engaging the recipients for input. Executive committees and boards will want CCM summary reports that answer the questions that are important to the organisation. If the data is well managed and analysable as the above example suggests, this dashboard can be used to provide a report or answer any questions from the executive committee or board.

Clearly verification and reporting are major components of an effective CCM initiative. The time and establishment costs should be considered in the design of the CCM initiative.

The next article will address the learning opportunities from CCM that can not only improve the process but also optimise critical controls. Huge opportunities exist in sharing critical control learnings between sites and companies that offer more rapid and more effective improvements for major mining risks.

Article 14 –Continuous improvement and learning opportunities with Critical Control Management (CCM)

Welcome to the final article in the series. If you have read the last few articles and you are not already involved in a CCM initiative, then you have been given some image of the work required to set it up. One of the reasons for writing this series was to provide an image of the journey and major work required to move toward CCM. Short cuts could lead to increased risk and disaster. However, once the critical control verification and reporting system is established, ideally with the help of technology, it should operate with relative ease.

An effective CCM initiative should provide a greatly improved indication of risk. The resultant optimisation, verification and reporting on critical controls for the site's priority unwanted events should highlight unacceptable changes in risk, based on weakening of the most important controls. This timely information greatly improves current risk analysis methods to the point where it possible to imagine a future situation where real time risk measurement will be possible, possibly even to the level suggested by the following illustration.

Having 'real-time' risk management is only possible by careful, timely verification of critical controls indicating changes in control status that, when compared to defined effectiveness expectations, alerts the accountable person(s) to take action. If the control effectiveness drops below a defined threshold, the risk is now unacceptable. Communication devices, like the above iPhone, allow for easy, literally automated alerts and action initiation. Could this be the future?

Learning from investigations

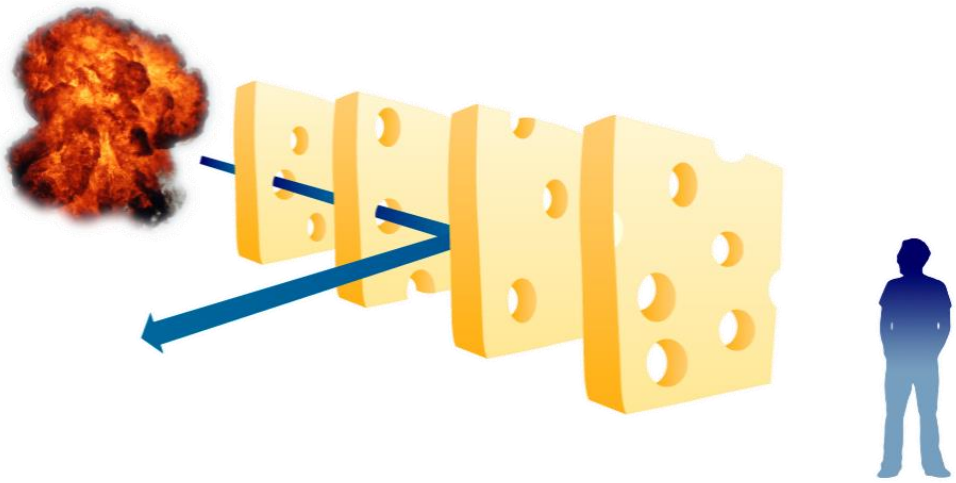
Another major opportunity with CCM, or any control-based approach to managing risk, is the valuable learnings that can be gathered and shared should an important or critical control partially or totally fail.

Most sites would investigate at least the top two of the three learning opportunities listed below.

1. Incidents with losses
2. Incidents without losses (near hits)
3. Failed critical control(s) without losses

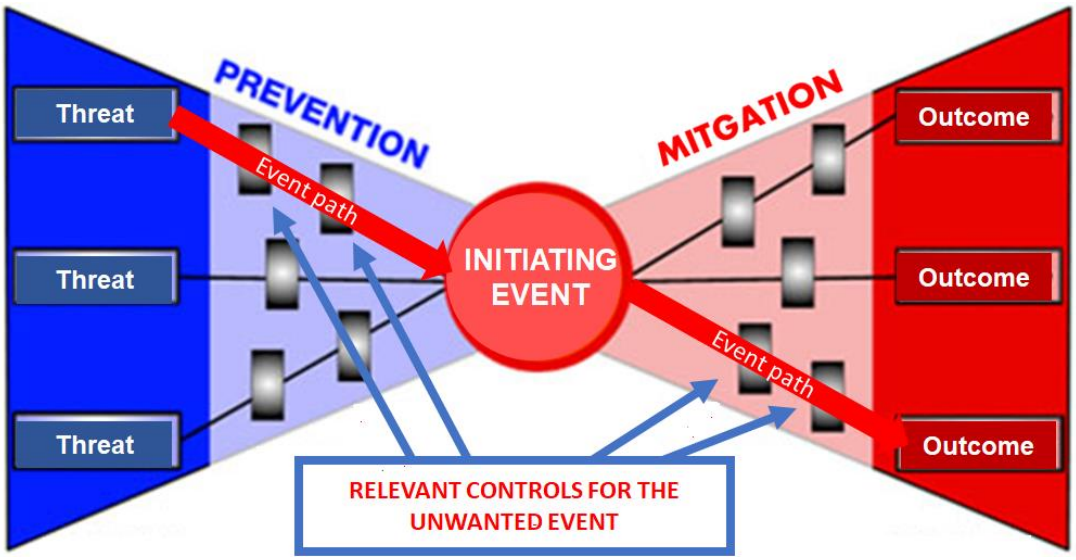
Most of us are familiar with the swiss-cheese concept attributed to James Reason. If we adopt this concept and have a good understanding of the important or critical controls

(remember Acts, Objects and Technological Systems) then its only logical that we should understand what happened to the controls we thought were in place and effective when an incident occurs.



Do our current incident investigation methods identify the expected controls and their status? If not, there is opportunity (and need) to align investigation with any control-based risk management initiative. In addition, situations where important or critical control effectiveness drops below the prescribed level of expected performance, by observation rather than incident, should be investigated like a near-hit event. That is point 3 above.

Should an incident in any of the 3 above categories occur that is related to one of the sites priority unwanted events (PUEs), then a significant investigation should be undertaken. In many cases, the event should have been predicted in the Bowtie Analysis (BTA) that was previously developed for the PUE. Defining the event path linking the threat(s) that manifested, leading to the unwanted event, as well as the consequences should provide the list of prevention and mitigation controls that are relevant to the investigation. Thereby past Bowtie Analyses become part of the investigators tool kit.



Once the incident pathway has been identified, the investigation turns to identifying the status of those controls at the time of the event. Controls must fail partially or fully for an incident to occur (Categories 1 and 2 above) but failed controls may also be identified through audits or verification (Category 3 above). If those controls are important or critical an investigation should be initiated.

Learnings about failed (and successful) important or critical controls usually affect multiple potential risks. As such, addressing those failures and their erosion factors can have a greater impact on improving priority risks then some current investigation outcomes.

For example, let's consider a haul truck / light vehicle near hit. If a BTA has been done for that type of incident there should be defined Acts, Objects and Technological Systems for preventing a set of related Threats. Operations related Threats might include 'operating to site requirements (practices, rules and procedures)'. The investigation may find that the light vehicle operator did not contact the haul truck operator before approaching to less than 50 meters (the site 'rule'). The Act of getting clearance is a control on the BTA Threat line.

The truck may also be designed so the ground access is located on the driver side to increase the likelihood that the operator will see an approaching person or vehicle. In our example, this failed to warn the haul truck driver. This truck design feature is an Object control, also in the BTA. Finally, the vehicles proximity detection system warned the operator that the light vehicle was too close, which caused him to stop the truck and

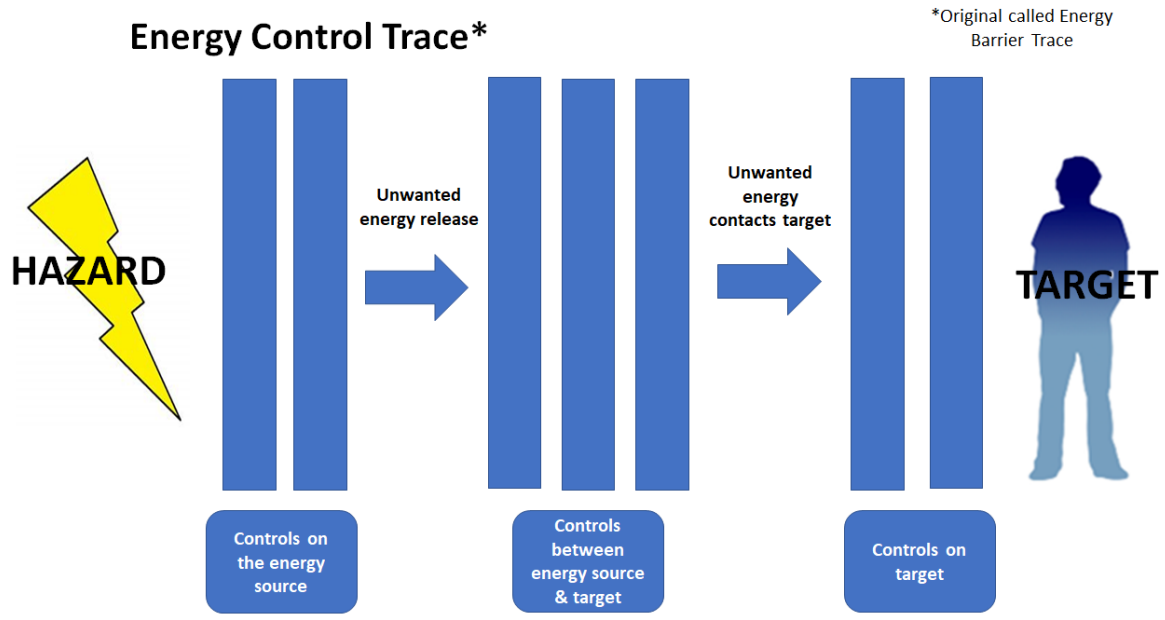
investigate, finally seeing the light vehicle. In this case the proximity detection system worked; a Technological System control from the BTA.

The investigation can then examine each of the 3 controls to identify why they failed or succeeded (successes are worth communicating too!).

Methods that identify 'upstream contributors' are fairly common in current investigation methods. Erosion factors for failed important and critical controls are upstream contributors to control failure. The identified contributors suggest improvements that should enhance the control's effectiveness in future.

Again, upstream erosion factors that may contribute to failures such as important or critical Acts may be relevant to many other potential incidents. As such, they are very important learnings.

Should the incident not have an existing Bowtie or not have a clear event path, then other investigation methods may be more appropriate. An Energy Control Trace is illustrated below. Note that the hazard is the energy source that has done or could do damage in an incident. This method is simply a more analytical version of the swiss cheese concept above.

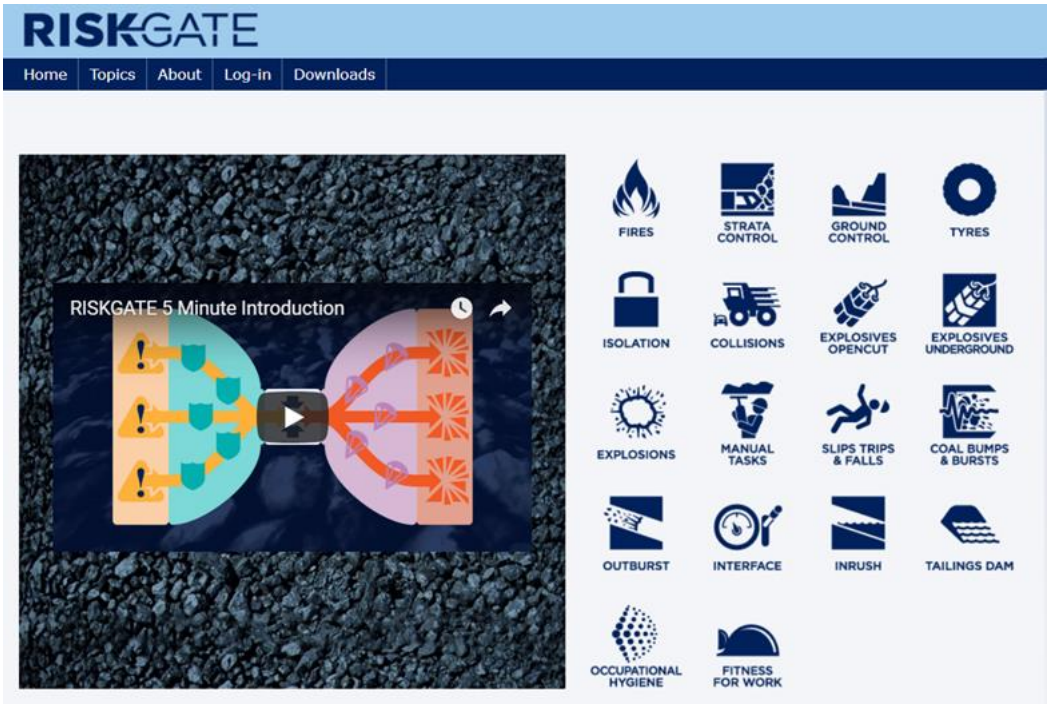


Sharing control effectiveness info learnings

Most of mining PUEs are generally consistent across the industry, considering underground and surface operations. So, it is logical that sharing information about incidents is helpful to reducing mining risks. However, we know that legal limitations have often restricted sharing, so the industry has seen many incidents that are total repeats of past events.

Investigating controls and sharing control effectiveness limitations and opportunities for improvement may offer a chance to greatly increase learning with minimal 'legal exposure'. Since the industries PUEs are very similar, industry PUE generic BTAs could define a set of controls that closely align with site controls. Sites could input information on learnings from failures or successes into an industry database that was accessible to all when considering new controls or ways to improve controls. This optimises learning efforts by reducing redundancy and paperwork.

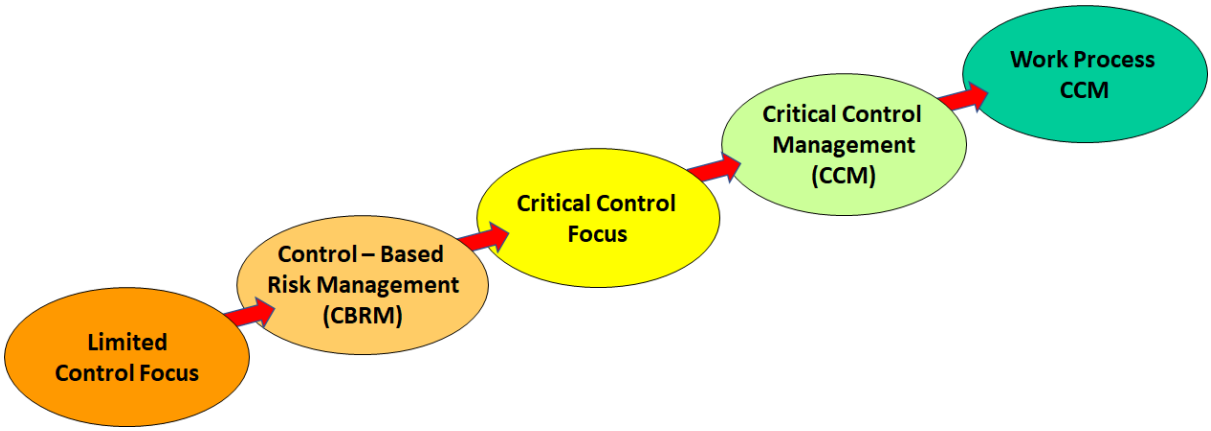
The Australian coal industry currently has a system that, with some modifications, could accomplish this outcome for both coal and metal mining. Check out RISKgate.org for more images of a potential future.



In conclusion

Thank you for your interest in this series of articles. If I can leave you with a final thought…. Proactive management of risk is a journey and always will be. We will improve our methods

and our results as we strive toward our goals. The task is to identify where on the journey your site or company is located and plan the next step.



There will always be risks in mining. It remains to effectively set the boundaries between risk aversion and risk avarice. I had to search for an opposite term for risk aversion. I would like to coin a new term - risk avarice; *too great a desire to have wealth through the assumption of unacceptable risk.*

Thank you for your interest in this series of articles. I hope they have been useful to your efforts for a safer and healthier mining industry. Stay safe.

Sincerely - Jim Joy