



Evolving Operational Risk Management in the Mining Industry

By Jim Joy

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

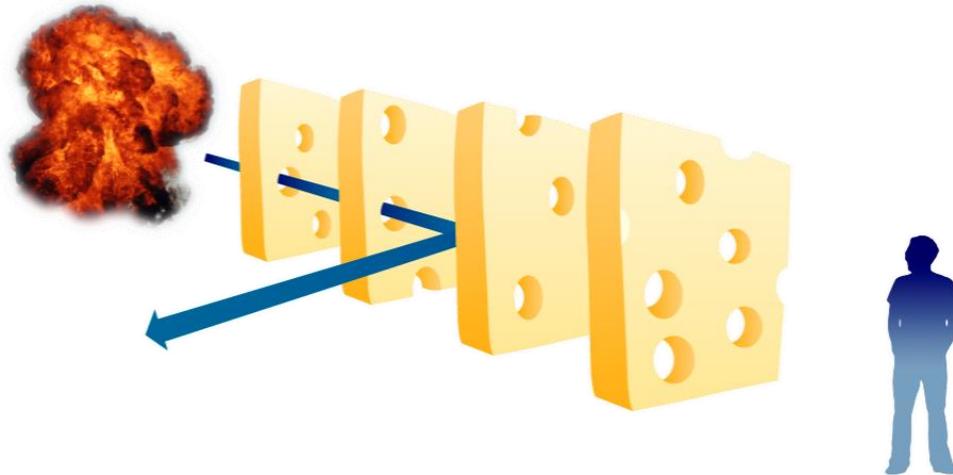
Another major opportunity with CCM, or any control-based approach to managing risk, is the valuable learnings that can be gathered and shared should an important or critical control partially or totally fail.

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

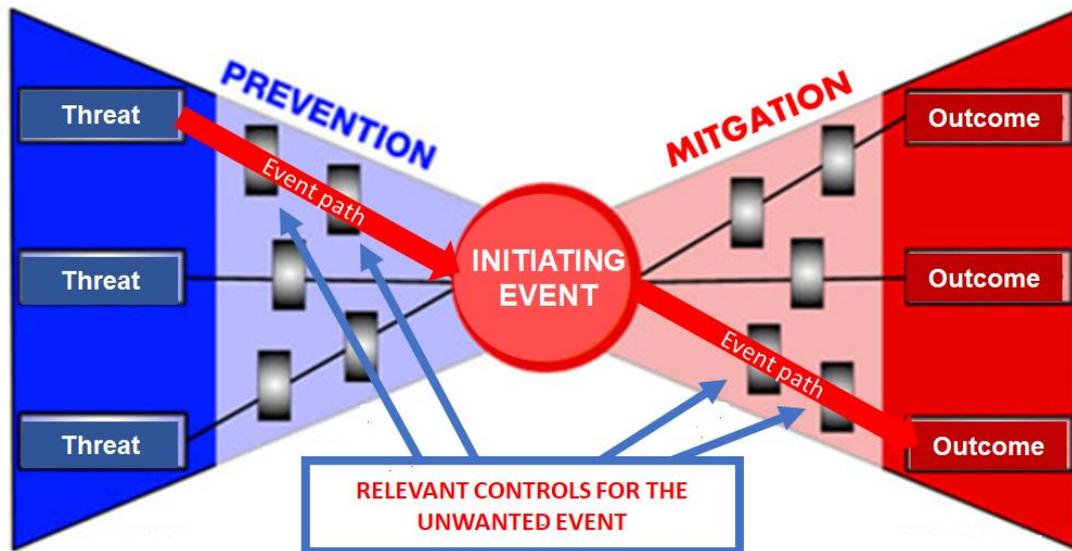
Most of us are familiar with the swiss-cheese concept attributed to James Reason. If we adopt this concept and have a good understanding of the important or critical controls

(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 than 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

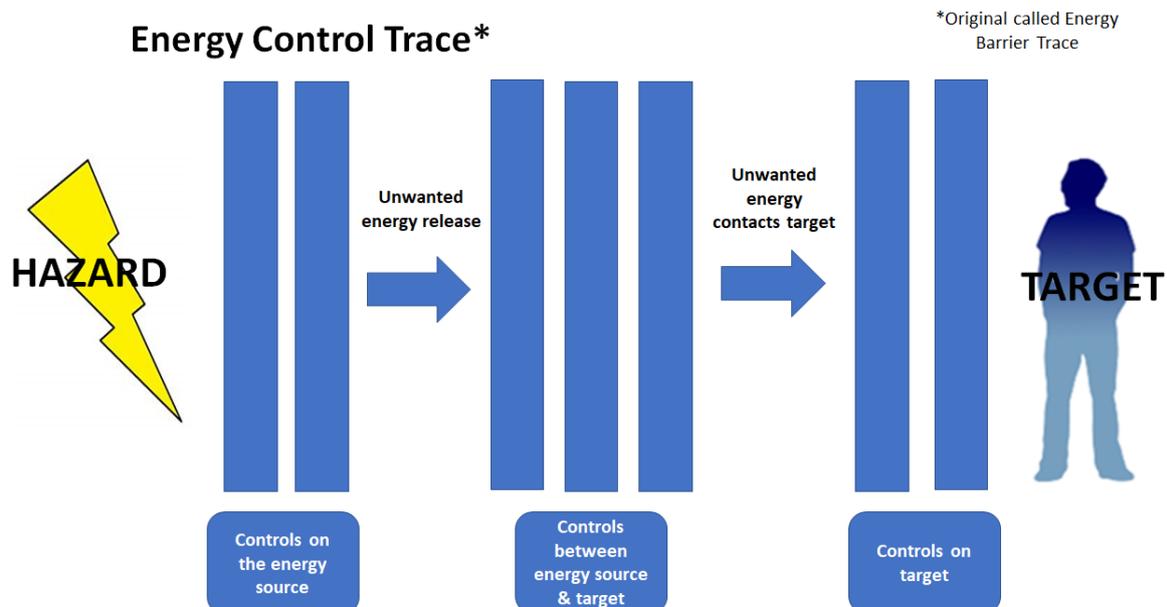
investigate, finally seeing the light vehicle. In this case the proximity detection system worked; a Technological System control from the BTA.

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.

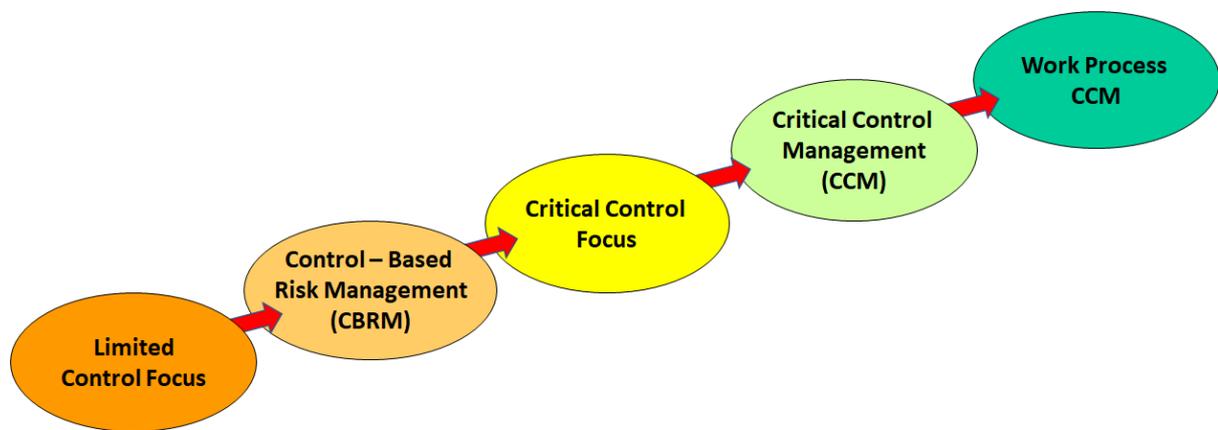
The Australian coal industry currently has a system that, with some modifications, could accomplish this outcome for both coal and metal mining. Check out RISKgate.org for more images of a potential future.



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