CHAPTER ?

Risk control through the use of procedures – A method for evaluating the change in risk

Gregory Praino
United Space Alliance, LLC
Cape Canaveral, FL 32920, USA

Joseph Sharit
Department of Industrial Engineering
University of Miami
Coral Gables, FL 33124, USA

ABSTRACT

Organizations use procedures to influence or control the behavior of their workers, but often have no basis for determining whether an additional rule, or procedural control will be beneficial. This paper outlines a proposed method for determining if the addition or removal of procedural controls will impact the occurrences of critical consequences.

The proposed method focuses on two aspects: how valuable the procedural control is, based on the inevitability of the consequence and the opportunity to intervene; and how likely the control is to fail, based on five procedural design elements that address how well the rule or control has been Defined, Assigned, Trained, Organized and Monitored—referred to as the DATOM elements.

Keywords: Procedural control, critical consequences, control failure likelihood, control value

INTRODUCTION

Organizations frequently find themselves mired by rules that have questionable value. Often these rules are the result of a knee-jerk reaction to failures, near misses or even successes, with the organization layering on additional rules to address circumstances that are perceived as significant. Unfortunately, these organizations rarely reconsider these rules later, at best allowing unnecessary rules to clutter the policies and procedures that govern workers, or in the worst case, leaving rules that confuse workers and lead to undesired behavior.

After the Space Shuttle *Columbia* accident, NASA had reason to believe such clutter existed in the policies governing space shuttle ground processing work instructions. In response, a method was sought to systematically evaluate the rules in place—both to determine if some rules could be consolidated or eliminated, and also to ensure that there was no false sense of security where the abundance of rules masked uncontrolled risks.

The resulting method was structured to examine any critical process; in the case of the Space Shuttle Program, it was directed at activities where loss of life or of a space shuttle vehicle was possible. The general case addressed physical controls (i.e., barriers) as well as rules, or procedural controls. However, the scope of the current work is limited to the applications on procedural controls because the transactional nature of shuttle ground processing depends overwhelmingly on people performing the right task in the right way at the right time.

The Control Assessment method explicitly considers the risk associated with each rule in the process individually to determine if that particular rule reduces risk, increases it, or has no significant impact. The risk assessment is based on two main factors: how valuable the rule is at preventing a critical consequence and how likely the rule is to fail under the real-world conditions that exist when it is called on to function.

Control Value describes how necessary the function of that control is. Necessity is determined based on how inevitable the consequence is in the absence of any control, and if the control leaves sufficient opportunity to intervene once an initiating event has occurred.

Failure Likelihood depends on how well the control has been designed, which is based on how well it is defined, assigned, trained, organized and monitored. Each of these five elements, which can be remembered with the acronym *DATOM*, are necessary for the sustained performance of the control, with deficiencies in any area contributing to the likelihood that the control will fail.

BACKGROUND

During the investigation of the Space Shuttle *Columbia* accident, NASA began three distinct efforts. The debris recovery in west Texas and the reconstruction of the recovered hardware were the higher profile tasks because the proximate,

physical causes would have been evident from an analysis of the debris. The National Transportation and Safety Board was consulted because the NTSB performs similar reconstructions of conventional aircraft mishaps to analyze the causes, and their methods and experience were expected to help speed the investigation.

The less visible task involved a complete review of the work instructions written during the prior two processing flows of *Columbia*, for the STS-109 and STS-107 missions. The review was intended to find any technical errors made by ground processing personnel that could have contributed to the accident. In its report, the Columbia Accident Investigation Board noted that in the roughly 16,500 work documents reviewed, there were no findings or observations that contributed to the accident. However, the board did note an accuracy rate of 99.75%, leaving a small number of work documents with "Technical Observations (technical concerns or process issues), and Documentation Observations (minor errors)" that revealed procedural issues (CAIB, 2003).

Interviews with the engineers who wrote the work documents revealed that many of the observations identified in the review were associated with rule interpretations. In some cases, rules still technically in-place could no longer be followed as-written or no longer provided the benefit intended because of process changes made since the rules were created. Other observations involved situations where a process improvement clearly implemented a better way of performing the function and the old rule was just never removed from the policy.

In light of the "Can-Do" culture in place at the Kennedy Space Center (Vaughan, 1996), it really comes as no surprise that technicians and inspectors on the floor would continue working when faced with some of these situations. It would be wasteful to stop working because a document that clearly described the task didn't comply with a formatting rule that no longer applied. There would be no value added by 'correcting' to comply with a rule intended for manually-typed instructions that had been phased out by the use of a computer-based authoring process several years before.

The real surprise is that errors like these weren't more common. Directions for engineers writing work instructions were distributed between 37 policy documents, so while one could argue the overwhelming compliance with obscure, redundant and ambiguous rules is somewhat wasteful, it is a testament to the thoroughness of those engineers that the accuracy was so high.

RISK DEFINITION

Typically, risk is defined in terms of failure likelihood and consequence severity of an outcome (Kumamoto and Henley, 1996), which in principle enables the expected loss or risk to be computed. Kaplan and Garrick's (1981) approach to understanding risk is based on obtaining answers to a triplet of questions: "What can go wrong?" "What are the consequences?" "What is the likelihood?" represents a more generalized approach to risk assessment that quantifies any hazard on an

absolute scale. In the proposed approach to defining risk, which is in terms of control value and failure likelihood, the key points that differentiate it from the general case are that the analysis is limited to only consequences that the organization considers critical and that it provides an indication of relative risk between possible options. Thus this approach helps to effectively target the relevant factors when the scope of the assessment is limited.

By choosing 'critical' consequences as those which, if they occur, would threaten the existence of the organization, then any practical need for quantification is eliminated. In essence, if any critical hazard is realized, it could mean the end of the organization. In the case of the Space Shuttle Program, loss of another vehicle would almost definitely result in the immediate and permanent termination of operations (Block, 2008). While loss of a life would probably not result in the premature end of the program, it would impact the career of the decision maker who allowed the circumstances to exist. A parallel example from another industry would be a death resulting from surgical malpractice—the hospital may not choose to select this as a critical consequence because a single fatality would present a minimal threat to its existence, but if the Control Assessment was being performed by the surgeon it would almost definitely be critical.

Another important assumption regarding risk that must be addressed before proceeding is that the assessment does not attempt to provide an aggregate measure of risk, but instead addresses the differences between alternatives, asking the questions: "what is the benefit derived from the presence of this rule?", or "is rule *A* better than rule *B*?" Techniques like Probabilistic Risk Assessment attempt to account for all risks faced by the organization (Kumamoto and Henley, 1996), but the intent of the Control Assessment is to only consider those items that can be controlled. Consider the hazardous release of chemicals due to a railway accident. There is a small but real risk to a factory adjacent to the rail-line, but the manager of the factory wouldn't be expected to try controlling that risk. Such a risk could be controlled at the corporate level though, so a Control Assessment there might look at the task of selecting new facility locations.

CONTROL VALUE

The way Control Assessment considers the value of the control being examined is to evaluate the inevitability of the critical consequence in the absence of the control and the opportunity to intervene should something go wrong. A control to prevent a consequence that would only happen occasionally is less valuable than a control to avoid an inevitable consequence. Likewise, a control that leaves ample opportunity for an active response would be less valuable than one where the consequence would be immediate.

To illustrate the impact of inevitability on value, consider two circumstances for a control the Department of Transportation could put in place on Interstate Highways. The design standard could be changed to require runaway truck ramps on all interstates to address the hazard of failed brakes on trucks. Obviously, a ramp

on steep section of road winding down through the mountains in Colorado would be far more valuable than on a straight and level section of road in the middle of Kansas farmland. On the steep road, a serious accident would be near inevitable because the lack of brakes would result in an increase in the speed of the truck, and impact with other vehicles that were under control. On the level road, the truck's speed would not increase and the vehicle could conceivably be allowed to come to a stop after running out of fuel, with no intervention necessary.

Opportunity to intervene can easily be seen in an example from space shuttle operations. Hypergolic rocket propellants are reactive enough that they will combust on contact, so no ignition system is required, allowing simpler and lighter thrusters to be used on the orbiter. On the other hand, the highly reactive chemicals pose a serious health risk to personnel; therefore one control in place at Kennedy Space Center restricts access to facilities when hypergols are being actively handled. A worker who entered the launch pad perimeter would have to cross an open field before getting close enough to operations to enter a dangerous concentration of propellant vapors. In the Orbiter Processing Facility, the hanger where maintenance and refurbishment of the orbiters is performed, a worker could be exposed to a hazardous concentration immediately upon entering.

In both cases, the control is necessary because a critical consequence would be inevitable during times that a hazardous concentration existed. However, the control value is much lower at the pad because there would be more opportunity to act once the worker enters the facility.

Whereas the Control Value can be used to explain where circumstances beyond the control of the organization are responsible for infrequent occurrences of critical consequences, the likelihood portion of the risk can be used to address the likelihood of the control failing. Rather than seeking an expected-value to describe risk, the procedural risk model focuses on whether the controls accomplish their intended function.

FAILURE LIKELIHOOD

Determining how often controls fail involves looking at the failure mechanisms of the controls. The most obvious case of a control that will not affect a worker's behavior is when the worker has a negative intent. Damage resulting from someone who intends to do harm by sabotage is outside the scope of control assessment because it is not the result of a control failure. Malicious compliance, on the other hand, is when an employee with a negative intent complies with a procedure they believe to be ineffective or counter-productive to the goals of the organization. This malicious compliance presents a procedural risk because the flawed procedure contains ineffective or failed controls—a worker who is aware that the procedure is not correct but who nonetheless follows the procedure would not be executing the actions desired by the organization but would be safe from reprisal.

Malicious compliance is a special case of the first way controls can fail: by not

clearly agreeing with the organization's expectations. A control that is ambiguous or conflicts with expectations will leave a worker unaware of the correct action to perform, or in the case of a malicious worker, provide a plausible excuse for acting against the best interests of the organization.

The second way controls can fail is to instruct the worker to perform an action they are unable to, either by providing insufficient details or identifying actions that cannot be performed under the time or resource constraints. The classic example of this second control failure is the production vs. quality conflict. Turning out high volumes of a product increase profit, but the need for oversight or inspection to ensure delivery of satisfactory products often slows production.

The final way controls can fail is by calling for actions that are harmful to the worker. A worker who is aware of what harm may come will not proceed with the action. Usually, such a situation will also be in conflict with the goals of the organization because the costs associated with the organization's liability in such a case could harm the organization as well.

In each of these situations, the worker performs a different action than expected or refrains from performing any action. An unaware worker may happen to perform the correct action, but that is treated here as an incorrect action—it is not a desired mode of operating to count on happenstance to ensure that workers act correctly.

Although these three failure scenarios describe how a process fails, they are not practical for facilitating an analysis of procedural risk because the level of specification is too general; that is, failures are specified to be the result of badly selected or incompletely described controls. Further specification is necessary to describe the process in useful terms. To accomplish this objective, it is proposed that Control Assessment consider a set of characteristics to describe a process based on five of six basic questions: what? why? when? how? where? and who? 'Why' is excluded because it does not describe the process, but provides rationale for its existence. Providing this rationale can be helpful in motivating the workers who will be performing the task, but is not strictly necessary for successful task completion.

DATOM and Failure Likelihood

DATOM, the model that uses the five elements—define, assign, train, organize and monitor—to fully describe a process was based on the "5 Ws." The original intent behind use of the model was as a tool for process design, but it also had value as a means of spotting where incomplete processes could fail.

Whether designing a new process or examining an existing one, the first step in describing the process is to define the actions that are expected to take place. 'What' must be firmly established for the action to be part of a process. Without an overarching scheme, a worker will not reliably perform an action or sequence of actions to provide the needed output. Defining the 'what' involves deciding on the extent of the actions involved with the task, along with choosing or identifying the parameters that control the task actions.

The unique skills and limitations of the workers influence the 'how' 'when' and 'where' so 'who' must be addressed before progressing to the other remaining questions. Without clearly identifying 'who' will be assigned to the task, some level of confusion is inevitable because of the assumptions that must be made by the participants. However, problems persist even when there is an explicit assignment. An action may be consistently performed by the same worker under normal circumstances, but a substitution creates opportunities for misunderstanding. A substitute worker who is capable of performing the task may be unaware that a particular action needs to be performed, or may assume that the action is performed by another worker.

Once the task has been defined and a worker has been assigned to perform that task, 'how' the worker will perform the task becomes relevant. For the task to be effectively performed, the worker needs training in the process knowledge specific to the task and in the skills required to perform the expected actions.

'Where' and 'when' the task will be performed are linked together because both are limited by the defined process sequence. Some aspects of 'how' are similarly constrained, particularly in the context of tools, equipment, and other supporting resources. These three items together describe how the process is organized and determine the efficiency, quality, and safety of the process if a trained worker is assigned to the task.

The links between the 'when,' 'where' and 'how' demonstrate the shortcomings with simply using the five questions as the criteria for evaluating a process. In contrast, Control Assessment does not attempt to split the operational details of task performance, leaving the answers to those three questions together under the concept of how well the task is organized.

This restructuring of the five questions resulted in the rough approximation of what became DATOM. The answer to 'what' is equivalent to the Define element and 'who' provides the Assign information. 'How' is split between Train and Organize, with the remainder of Organize coming from 'when' and 'where'.

Failures within these four elements can cause failures of the process, but they do not provide feedback on whether the process actually produces the desired results. Without some form of check, the process will be vulnerable to changes in the inputs, the environment, or interpretations of the wording of the documented rules. Based on this need, Monitor is the necessary final element in the process evaluation criteria, even though it cannot itself cause a failure in a fully defined process.

The concept of monitoring includes activities that report on the 'health' of the process but are independent of the process itself. Inspection activities are similar but differ in a subtle and significant way from monitoring. Where inspections address quality during a specific instance of procedure execution, monitoring does not rely on acceptance criteria to determine if corrective action must be taken.

A nonconformance resulting from known and accepted process variation would need remedial action for that specific case, but no corrective action would be necessary as a process 'fix.' For example, consider a drilling operation where it's possible for the first hole to be drilled under-sized before the bit heats up from use. An undersized hole would be cause to reject the part, but it would not necessarily

happen frequently enough to be worth the costs of changing the process. Monitoring, on the other hand, may catch a deficient process that is still producing conforming output. No short-term action would be needed but the process failure would eventually need to be corrected to prevent nonconformances. An example of this could be a machinist who makes a progressively larger, undocumented adjustment to a setting to compensate for a bad indicator on the machine—the output will conform, but the process is not sustainable.

SIGNIFICANCE

Since procedures are an organization's "mechanisms, techniques and processes that have been consciously and purposefully designed in order to try to control the organizational behavior" (Johnson and Gill, 1993), they are also the primary means for an organization to prevent the consequences that result from undesired action. The proposed method of considering procedures represents an attempt to understand not just if procedures are communicated effectively, but to see the procedure in context as an attempt at controlling workers' actions.

By using Control Value to understand if the organization's efforts have the potential to prevent or mitigate consequences and Failure Likelihood to determine if that potential is being realized, it should be possible for any organization to see if the actions taken by its workers to reduce a risk are succeeding. The technique won't provide the absolute measure of risk that a Probabilistic Risk Assessment would return, but it will allow the organization to see the relative impact on risk associated with the presence or absence of each control in its critical procedures.

The ultimate goal of utilizing the proposed technique is the development of a reliable tool that can be used to understand the relative risks when comparing alternative procedural controls. Using this tool, an organization could determine which rule among possible alternatives most effectively reduces risk. Similarly, the tool could be used when adding or removing a control to provide context to the change, particularly if the control under review is compared against existing controls intended to protect against the same hazard.

A series of validation exercises are under way within the workforce responsible for space shuttle ground processing and the initial results indicate that personnel with experience in a process can score a procedural control's elements—inevitability, opportunity for intervention, definition, assignment, training, organization and monitoring—consistently with the opinions of control value and failure likelihood provided by experts in risk assessment. The final configuration of the resulting tool is yet to be determined, but it appears that an assessment of procedural controls could be performed by a small group with expert knowledge of the process being assessed, facilitated by one who is familiar with the assessment technique, similar to the performance of a HAZOP analysis (AIChE, 1992).

REFERENCES

AIChE (American Institute of Chemical Engineers), (1992). *Guidelines for Hazard Evaluation Procedures: Second Edition with Worked Examples*. New York, NY: Center for Chemical Process Safety.

Block, R. (2008). NASA Chief: Odds grow for shuttle catastrophe. *Orlando Sentinel*. September 5, 2008

CAIB (Columbia Accident Investigation Board). (2003). *Columbia Accident Investigation Board Report*. Washington, DC: United States Government Printing Office

Johnson P. and Gill J. (1993). *Management Control and Organisational Behavior*. London: Paul Chapman Publishing Ltd.

Kaplan, S. and Garrick, B. J. (1981). On the Quantitative Definition of Risk. *Risk Analysis*, 1(1), 11-27.

Kumamoto, H. and Henley, E. J. (1996). *Probabilistic Risk Assessment and Management for Engineers and Scientists*. Piscattaway, NJ: IEEE Press

Vaughan, D. (1996). *The Challenger Launch Decision - Risky Technology, Culture and Deviance at NASA*. Chicago, IL: University of Chicago Press